SOCIEDAD DIGITAL Y DERECHO

Directores

Tomás de la Quadra-Salcedo

José Luis Piñar Mañas

Coordinadores

Moisés Barrio Andrés

José Torregrosa Vázquez

BOLETÍN OFICIAL DEL ESTADO

MINISTERIO DE LA PRESIDENCIA
RELACIONES CON LAS CORTES E IGUALDAD

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA

red.es

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO

SOCIEDAD DIGITAL Y DERECHO

Directores
Tomás de la Quadra Salcedo
y José Luis Piñar Mañas

Coordinadores
Moisés Barrio Andrés
y José Torregrosa Vázquez

Boletín Oficial del Estado
Ministerio de Industria, Comercio y Turismo y RED.ES

SOCIEDAD DIGITAL Y DERECHO

SOCIEDAD DIGITAL Y DERECHO

Directores

Tomás de la Quadra-Salcedo Fernández del Castillo

y

José Luis Piñar Mañas

Coordinadores

Moisés Barrio Andrés

y

José Torregrosa Vázquez

MINISTERIO DE INDUSTRIA, COMERCIO Y TURISMO

RED.ES

BOLETÍN OFICIAL DEL ESTADO

Madrid, 2018

Primera edición: noviembre de 2018

http://publicacionesoficiales.boe.es

NIPO BOE: 786-18-069-0
NIPO Ministerio de Industria, Comercio y Turismo: 084-18-021-5
ISBN: 978-84-340-2483-0
Depósito legal: M-21019-2018

Imprenta Nacional del Boletín Oficial del Estado
Avenida de Manoteras, 54. 28050 Madrid

A la memoria del Profesor Stefano Rodotà

ÍNDICE

Páginas

III
PRIVACIDAD EN UN MUNDO DIGITAL

Páginas

IV
CONDICIONES BÁSICAS PARA GARANTIZAR LA IGUALDAD EN UN MUNDO DIGITAL

V
CONFIANZA DIGITAL Y RESPONSABILIDAD EN LA RED

VI
SEGURIDAD Y CIBERDEFENSA

Páginas

Páginas

X
JUSTICIA Y TUTELA DE LOS DERECHOS EN UN MUNDO DIGITAL: EL PAPEL DE LA TECNOLOGÍA EN LA REGULACIÓN, LA SUPERVISIÓN, Y LA RESOLUCIÓN DE CONFLICTOS

XI
SALUD Y MUNDO DIGITAL

XII
RELACIONES INTERNACIONALES Y MUNDO DIGITAL

XIII
SOSTENIBILIDAD Y REVOLUCIÓN DIGITAL

Páginas

PRESENTACIÓN

Son ya muchas las iniciativas y declaraciones sobre derechos digitales o sobre la conveniencia y oportunidad de elaborar una Constitución digital. Tales iniciativas ponen de manifiesto la inquietud y el desasosiego que en muchos produce que la entrada en una sociedad digital y global pueda suponer, junto a sus increíbles ventajas y avances para todas las personas en cualquier parte del mundo, algunos riesgos para sus derechos fundamentales y libertades públicas.

El doble uso de cualquier invento es algo muy conocido desde siempre. El cuchillo nos sirve para cortar los alimentos, pero puede servir para matar a otros. No es a los avances e inventos en cualquier campo a lo que debemos temer, sino al uso que algunas personas puedan hacer de ellos.

El presente libro quiere abordar con profundidad las consecuencias de todo tipo que la digitalización de los datos personales –también los producidos por las cosas que utilizamos– pueden tener para los derechos individuales y para el funcionamiento mismo de la sociedad. Podemos ya hablar de la edad digital o, mejor, de la sociedad digital si quisiéramos enfatizar que no se trata sólo de instrumentos que permanecen fuera de nosotros y nos son de enorme utilidad, sino destacar que los incorporamos a nuestra vida diaria –incluso los llevamos encima como sucede con los wearables *o tecnocomplementos– y pueden llegar a influir en nuestro comportamiento y hábitos, crear nuevas necesidades y condicionarnos, incluso pueden condicionar nuestra propia identidad.*

En todo caso dejan de nosotros un reguero de datos sobre nuestra ubicación, nuestros gastos, nuestros gustos, nuestras inclinaciones, nuestras relaciones, nuestras opiniones, nuestra personalidad, etc. que puede ser muy útiles para que determinadas empresas –muy al tanto de las posibilidades del mundo digital–

nos hagan propaganda personalizada de la que no siempre somos conscientes o hagan muchos otros usos insospechados.
Los derechos a la protección de datos personales, a nuestra intimidad, a nuestra libertad de expresión (que conlleva la de no expresarnos) o de información pueden quedar alterados y eventualmente manipulados.
El desasosiego se incrementa cuando al inmenso océano de datos existentes se le aplican técnicas de inteligencia artificial para transformar los datos en información a partir de la cual se potencia infinitamente, pero ya en el plano de las personas humanas, el conocimiento. Y todo ello puede ser muy bueno según para que se emplee y siempre que no de ventajas ilegales a unos sobre otros.
La cuestión de nuevo es para qué se utiliza esa información por algunos, si eso afecta a nuestra intimidad o viola nuestro derecho a la reserva de nuestras opiniones sobre política, religión, orientación sexual, preferencias artísticas, literarias, culinarias, deportivas, etc.
A mucha gente puede darle igual, pero otras no.
En todo caso la inquietud surge al conocer que ello puede servir para elaborar perfiles que pueden determinar si las personas son contratadas, despedidas, ascendidas, aseguradas, etc. Incluso sobre la base de perfiles elaborados a partir de datos masivos a los que se aplican algoritmos de inteligencia artificial.
Las primeras inquietudes surgen en relación con los derechos fundamentales que pueden verse afectados. Pero las mismas se extienden, en realidad, al funcionamiento mismo de la democracia: si sobre la base de los datos que alguien ha obtenido, legítima o ilegítimamente de 85 millones de personas –como ha sido el caso de Cambridge Analytics en las elecciones presidenciales en Estados Unidos–, una elección ha podido quedar alterada, entonces los nubarrones alcanzan al propio funcionamiento y esencia del sistema democrático.
Sobre la base de los datos sobre inclinaciones, preferencias o preocupaciones de millones de personas se les dirigen falsos mensajes personalizados produciendo el error de confirmación: la creencia de que las inquietudes de uno mismo son compartidas por un inmenso número de personas que, además, tendrían todas la misma solución o identificarían al mismo culpable a quien no votar; confirmación que se logra sobre la base de la difusión de falsos mensajes provenientes de robots que pretende suscitar esa creencia en el destinatario, algo predispuesto tal vez, pero que una información plural y abierta no conduciría a determinar inevitablemente el sentido de su voto en modo alguno.
La propaganda subliminal, prohibida en nuestra legislación y en normas de la Unión europea, es un juego de niños comparado con los problemas de polarización y división que pueden producirse en la sociedad digital de nuestros días, por estas técnicas de manipulación de la opinión.

Son ya varios los documentos de la UE que han constatado el fenómeno de que determinadas buscadores o redes sociales confirman a la gente en lo que algún algoritmo considera que son sus gustos o inclinaciones de todo tipo y, progresivamente, van radicalizando los mensajes que reciben en línea de agudizar su tendencia.

De la inquietud por los derechos individuales, se pasa así a la inquietud y el desasosiego por la democracia. También al desasosiego por el mercado que puede resultar distorsionado y alterado si sólo algunos cuentan con los datos masivos para determinar las tendencias colectivas e incluso individuales. O si tales datos se utilizan por poderes públicos no democráticos que pretenden controlar a la ciudadanía. De modo que incluso, de forma desapercibida para las personas, puede condicionarse el libre desarrollo de la personalidad e incluso manipularse su identidad o el funcionamiento democrático de las instituciones.

En definitiva, la sociedad digital que permite acumular datos y tratarlos puede ser, y en realidad es, enormemente prometedora. Solo es necesario que la información tratada por las máquinas se transforme en conocimiento empleado para profundizar las libertades, la democracia y el mercado. Y que el acceso a ese conocimiento sea equitativo. Que las razones por las que a una empresa tiene acceso a determinados datos, le sirva en relación con el objetivo de esa misma empresa es algo que puede ser legítimo, pero habría que decidir si lo es que los utilice para otro mercado o con otra finalidad. Se trata de plantearse el problema de la concentración de la información en unos pocos gigantes mundiales.

Eso exige empezar primero por estudiar y analizar los diversos instrumentos, dispositivos y posibilidades de la sociedad digital, para después lograr una visión más profunda de conjunto que nos permita saber en qué dirección debe moverse la necesaria regulación –en sus diversas formas y modalidades, entre ellas la autorregulación, regulada o no– antes de que sea demasiado tarde. Todo ello, además, en el marco de un necesario diálogo, o mejor trílogo, entre derecho, tecnología y ética. El Derecho ya se ha enfrentado en otras ocasiones a situaciones disruptivas y ahora ha de hacerlo frente a tecnologías también disruptivas cuya evolución futura resulta simplemente impredecible. Sólo desde una perspectiva interdisciplinar podrán abordarse los retos que la innovación presenta en el marco de la sociedad digital.

A tal fin se ofrece este libro, Sociedad digital y derecho, elaborado por un grupo interdisciplinar de académicos y profesionales que tiene por objeto asumir colectivamente la responsabilidad de pensar para qué, por qué y cómo queremos abordar la transformación tecnológica desde el punto de vista del Derecho y de otras ciencias. Para ello, la obra analiza el estatuto de la persona en el mundo digital (primera parte), la ciudadanía digital (segunda parte), la privacidad en el mundo digital (tercera parte), las condiciones básicas para

garantizar la igualdad en un mundo digital (cuarta parte), la confianza digital y responsabilidad en la Red (quinta parte), las cuestiones de ciberseguridad y ciberdefensa (sexta parte), el trabajo y mercado laboral en un mundo digital (séptima parte), el mercado digital y competencia (octava parte), la creatividad, acceso a la cultura y deporte en un mundo digital (novena parte), la justicia y tutela de los derechos en el mundo digital (décima parte), salud y mundo digital (undécima parte), las relaciones internacionales y mundo digital (duodécima parte), y por último la sostenibilidad y revolución digital (decimotercera parte).

No puede perderse de vista, por otra parte, que la sociedad digital nace en un momento de nuestra civilización en que se producen sinergias entre ellas y los avances en la nanotecnología, la biotecnología y las ciencias cognitivas; sinergia que nos sitúa en un nuevo escenario, desconocido hasta ahora.

A sentar las bases del futuro abordaje de la regulación de la sociedad digital en ese nuevo escenario pretende contribuir el presente libro en que, en diversos capítulos, se ha tratado de ordenar y estudiar los diversos sectores y parcelas concernidos.

En fin, no podemos concluir esta breve presentación sin agradecer a todos y cada uno de los autores por el esfuerzo que han llevado a cabo al objeto de que este libro, creemos que único en el marco del derecho comparado, haya visto la luz en el plazo previsto. Agradecer asimismo a Moisés Barrio Andrés y José Torregrosa Vázquez por su rigurosa labor de coordinación.

El libro se ha realizado en el marco del proyecto de investigación UXXI:2017/00551/001 financiado por Red.es

Madrid, 23 de abril de 2018

Tomás de la Quadra-Salcedo Fernández del Castillo
José Luis Piñar Mañas
Catedráticos de Derecho Administrativo

I

LA PERSONA EN EL MUNDO DIGITAL

CAPÍTULO 1

RETOS, RIESGOS Y OPORTUNIDADES DE LA SOCIEDAD DIGITAL

TOMÁS DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO
Catedrático Emérito de Derecho Administrativo
Universidad Carlos III

1. INTRODUCCIÓN

Sociedad digital y mundo digital parecen expresar lo mismo, pero es preferible emplear el término sociedad, porque el concepto de «mundo» nos remite a algo exterior que sugiere que nos ha sido dado; algo así como la naturaleza. Pero la sociedad digital se ha construido sobre la base de descubrimientos, técnicas, dispositivos y aparatos creados por el ser humano (1). Por otra parte no se trata de aparatos que se integran sin más en un mundo exterior a nosotros facilitándonos los desplazamientos o la comunicación sobre la misma naturaleza en la que desarrollamos nuestras vidas, sino que tales descubrimientos y técnicas han acabando casi creando un mundo propio vinculado a nuestra vida, que da la sensación de autosuficiente y en el que a veces lo natural o convencional –que nos traigan a casa una compra hecha por internet por ejemplo– acaba siendo accesorio o instrumental. Lo relevante se ha consumado en la red.

Sociedad digital, pues, íntegramente hecha por el ser humano, que nos ofrece retos, oportunidades y también riesgos. Sobre todo ello se trata de hacer una reflexión aquí, pero al hacerla se debe empezar por destacar

(1) *Vid.* Arias Maldonado, Manuel, *El antropoceno*, Ed. Taurus, 2018.

que en la actualidad las oportunidades y riesgos de esta sociedad se producen en un momento crítico.

Las posibilidades que la sociedad digital abre a la humanidad representan una gran esperanza de mejora y seguridad, pero como siempre ocurre con los nuevos medios y descubrimientos el empleo que de todo ello hagamos puede ser positivo o negativo para esa misma humanidad. Desde luego los avances que experimenta esa sociedad digital nos hacen percibir que junto a las ventajas también se incrementan los riesgos; riesgos para los derechos y libertades fundamentales sobre los que es preciso pensar. Pero lo nuevo de este momento es que junto a los riesgos para los derechos y libertades de las personas, empiezan a aparecer riesgos serios para la misma democracia y para la economía de mercado que en la construcción europea está muy vinculada con la democracia misma.

Eso dota a la reflexión de una profundidad y una perspectiva nuevas. Y todavía es mayor si pensamos en la convergencia que la sociedad digital presenta hoy día con una corriente muy poderosa de opinión que sobre la base de los avances y descubrimientos en el campo del genoma, la genética y lo que podríamos denominar las biotecnologías está reclamando la aplicación de todos esos avances no sólo para curar las enfermedades y mejorar las condiciones de vida, sino para mejorar o aumentar la capacidad, la inteligencia o las habilidades de quienes no padecen ningún achaque, lesión o necesidad.

Para esa demanda se pretende contar no sólo con la genética y las ciencias biotecnológicas, sino también con los instrumentos de la sociedad digital. De ahí la conexión o convergencia de ésta con dichos movimientos.

Como en seguida veremos, a través de sensores en el cerebro –que harían de interfaces entre el cerebro y las computadoras– se conseguirían personas superdotadas conectadas a computadores con inteligencia artificial y Big Data en una especie de hibridación. Naturalmente eso suscita graves problemas en relación con la igualdad que es un valor fundamental en nuestras sociedades recogido en nuestra Constitución.

Estamos hablando, como no se escapará, de las propuestas que se denominan «transhumanistas» y «posthumanistas», sin considerar aquí las posiciones antihumanistas. Tales movimientos se han desarrollado inicialmente en el ámbito de las ciencias basadas en la biotecnología en relación con la mejora de la especie humana para mejorar las condiciones físicas o mentales de vida. Una vez que se avanzó en el conocimiento del genoma se vislumbró la posibilidad de intervenir en ciertos elementos genéticos del embrión para prevenir enfermedades. Pero naturalmente no se limita al embrión, cuyas características se quieren programar, sino que continúan con la intervención en el cuerpo o en el cerebro, pero no para curar,

sino para perfeccionar o potenciar (2). Se trataría también –para los partidarios del movimiento– de alargar la vida y si es posible evitar la muerte. Algunos incluso vislumbran o proponen la superación del hombre por las máquinas autónomas (3).

Sin entrar ahora en determinar si algunas de esas cosas nos parecen fantasías o historias de ciencia ficción, lo cierto es que buena parte de ellas se podrían conseguir o ya se están haciendo, especialmente en el ámbito de la curación de enfermedades o en la prevención de enfermedades transmisibles hereditariamente, que se quieren evitar seleccionando el material genético o interviniendo en el embrión.

De hecho son muchas las Asociaciones de transhumanistas o posthumanistas, con figuras muy reconocidas que tratan de empujar en esa dirección, especialmente en Estados Unidos donde, por ejemplo la Asociación Humanity+ (Humanity Plus) ha hecho un manifiesto sobre lo que consideran que debe hacerse para conseguir «el hombre potenciado» admitiendo que eso plantea problemas de todo tipo, pero sin renunciar a esta potenciación o mejora del ser humano (4).

Todas esas propuestas no se ciñen solo a la biotecnología, sino que también los medios y aparatos de la sociedad digital son llamados a esa potenciación del ser humano. La inteligencia artificial, vinculada a interfaces cerebro-computador pretenden que desempeñen un papel.

Como es lógico tales propuestas tienen sus contradictores, algunos muy poderosos en el campo de las empresas y de la academia (5) y están dando lugar a una enorme polémica por las cuestiones morales y de concepción de nuestra sociedad y de la humanidad que implican.

Las personas conectadas mediante interfaces a potentes computadoras dotadas de inteligencia artificial, suscitan problemas que afectan a la idea misma de humanidad; lo mismo sucede con las propuestas sobre perfeccionamiento biológico. Todo eso plantea, además, otro tipo de cuestiones como las relativas a la igualdad y la convivencia. Hasta ahora esas diferencias de capacidad intelectual eran producto del azar y en cuanto tales aceptadas generalmente. A partir de ahora habrá quien pretenda tener derecho a ese perfeccionamiento y eso plantea infinitos problemas. ¿Se podría presentar a un examen para una oposición una persona potenciada

---

(2) *Vid.* Hong, Ma; Martí-Gutiérrez, Nuria, *et al.* en «Correction of a pathogenic gene mutation in human embryos», en *Nature*, volume 5458, pp. 413-419 (24 August 2017). Se trata de conductas que en la mayor parte de los casos no encajan en la Declaración Universal sobre el genoma humano y los derechos del hombre (UNESCO), de 11 de noviembre de 1997, ni en el Convenio de 4 de abril de 1997, ratificado por Instrumento de 23 de julio de 1999 para la protección de los derechos humanos y la dignidad del ser humano con respecto de las aplicaciones de la biología y la medicina.

(3) *Vid.* Kurzwei, Ray *La singularidad está cerca. Cuando los humanos transcendamos la Biología*, Lola Books, 2012.

(4) El manifiesto puede consultarse en https://humanityplus.org/philosophy/transhumanist-declaration/

(5) Tales como Bill Gates, Elon Musk, Stephen Hawking (†)y Michel Sandel.

de alguna de esas formas? ¿Se crearían artificialmente dos tipos de personas: unas potenciadas o super-hombres y otras no? ¿Acabarían las primeras dominando a las segundas?

La cosa parece de ciencia ficción pero es bien seria. En el ámbito europeo Habermas plantea sus reservas a ese respecto y en los Estados Unidos lo mismo hacen Mandel y Fukuyama (6). Pero frente a ellos hay también científicos y filósofos que sostienen posiciones bien distintas. La mayor parte de todos son conscientes de lo que todo eso significa, lo que no quita que por ahora no se haya encontrado un terreno de encuentro. Tal vez el problema no sea para hoy, aunque ya hay realizaciones que se pueden hacer, pero sí para mañana o para un futuro no muy lejano. Otras no tienen visos de ser viables en plazos ni medios ni largos.

Al abordar ahora la cuestión de la Sociedad digital se hacía necesario plantear crudamente la cuestión más grave de todas que se vincula con el transhumanismo en relación con la sociedad digital. Más grave pero no la única como enseguida veremos. Más grave porque ha colocado al mundo en una encrucijada aquí y ahora, puesto que aunque la concreción de todo ello no sea inmediata, es preciso ser conscientes de que hay que empezar a tomar posiciones en un debate ya iniciado (7).

De hecho la Unión Europea ha empezado a encargar informes al respecto, sin que como tal haya adoptado una decisión todavía. El primero es de 2004 y en él se hace una primera pero profunda aproximación sobre la base de lo que llama las tecnologías convergentes en las que incluye la Nanotecnología, la Biotecnología, las tecnologías de la información y las ciencias cognitivas concluyendo con 16 recomendaciones.

El segundo es de mayo de 2009 y se emite por otro grupo de expertos a instancias del Parlamento europeo con el título de «Human Enhancement» y aborda todas las cuestiones que se han ido señalando en párrafos anteriores.

Pero junto a estos retos hay otros que dotan de particular importancia la reflexión sobre la sociedad digital. El enorme poder y valor que proporcionan los datos afecta de muchas formas a los derechos de las personas. El inmenso número de usuarios de las redes sociales y el tratamiento del Big Data –para los que los usuarios no siempre dan permiso y cuando lo hacen no son conscientes en muchos casos de la trascendencia que eso tiene– obliga a un análisis de la situación (8).

---

(6) *Vid.* Habermas, Jürgen: *El futuro de la naturaleza humana, ¿hacia una eugenesia liberal?*, Ed. Básica, 6.ª imp., 2016; Sandel, Michel: *Contra la perfección. La ética en la era de la ingeniería genética*, Ed. Marbot, Barcelona, 2007; Fukuyama, Francis: *El fin del hombre: consecuencias de la revolución biotécnológica*, Barcelona, Ed. B, 2002.

(7) *Vid.* Hottois, Gilbert: «Le transhumanisme est-il un humanisme?», Academie Royal de Bélgica, 2014, con un acercamiento muy interesante a la cuestión sentando las bases del debate.

(8) El primer informe oficial europeo lleva por título «Converging Technologies-Shaping the Future of European Societies», por Nordmann, Alfred, *rapporteur* del High Level Expert Group

Por otra parte empiezan a visualizarse riesgos para la democracia misma que está en la base de la garantía de los derechos fundamentales (9). Riesgos también para el mercado en la medida en que se está produciendo una concentración de información y datos que a la postre es concentración de poder de la que tenemos que ser conscientes.

Tal es el contexto sobre el que, desde el principio, es necesario alertar, para que seamos conscientes de la relevancia de las cuestiones que se van a tratar.

2. OPORTUNIDADES, RETOS Y DESAFÍOS DEL MUNDO DIGITAL

2.1 **El mundo digital, el yo y los otros: condicionamientos de la conducta, la responsabilidad y la igualdad**

Los enormes progresos en el desarrollo de la investigación sobre el cerebro impulsado desde el año 2013 especialmente en Estados Unidos [singularmente desde 2013 con la llamada Brain Iniciative (10)] dirigidos a conocer su funcionamiento y a realizar un mapeo de la actividad cerebral dirigido en última instancia a solucionar graves enfermedades (alzheimer, parkinson, esquizofrenia, depresión, etc.) están permitiendo avanzar, entre otras muchas cosas, en la creación de un interfaz cerebro-computador (11) que empieza a abrir ya grandes esperanzas en muchos campos médicos, aunque aún hará falta esperar para que estas técnicas se generalicen y desarrollen toda su potencialidad.

En todo caso ya se empieza a conseguir en el plano experimental que personas paralizadas por haber sufrido lesiones en la médula espinal puedan con solo su pensamiento realizar algunas operaciones, desde las más o

---

«Foresighting the New Technology Wave», 2004. European Commission. Luxembourg: Office for Official Publications of the European Communities. El segundo informe oficial de varios autores se titula «Human Enhancement Study Policy», Bruselas, 2009, encargado por Department A: Economic and Scientific Policy, DG Internal Policies. European Parliament. Accesible en http://www.europarl.europa.eu/stoa/default_en.htm. Aparte de ellos en el ámbito de la Unión Europea son muchos los informes que se han ido produciendo, así el de Rossi, Francesca «Artificial Intelligence: Potential Benefits and Ethical Considerations» Policy Department C: Citizens' Rights and Constitutional Affairs, European Parliament, 2016.

(9) *Vid.* Virilio, Paul, *El cibermundo, la política de lo peor*, Ed. Teorema 1997, pp. 88 a 90 y 93 a 94.

(10) *Vid.* https://www.braininitiative.nih.gov/index.htm

(11) *Vid.* Nijboer, Femke, *et al.*, «A P300–based brain-computer interface for people with amyotrophic lateral sclerosis», Clinical Neurophysiology 119(8):1909-16 · September 2008. El Brain computer interface (BCI) es uno de los instrumentos utilizados en el programa Brain Research through Advancing Innovative Neurotechnologies (BRAIN) también conocida como Brain Activity Map Project (proyecto de mapeo de la actividad cerebral) que se impulsó por la Administracion Obama en abril de 2013 y prevé inversiones de más de 3.000 millones de dólares durante los diez años del proyecto. El mismo prevé investigar en el cerebro humano, su forma de funcionamiento y ayudar a prevenir y curar algunas de las enfermedades que en él se localizan (alzheimer, parkinson entre otras).

menos elementales (beber por sí solos un vaso de agua con la ayuda de una prótesis o un exoesqueleto) hasta otras más complejas como podría ser encender un aparato de televisión, la luz o traer un objeto desde otra habitación de la casa con la ayuda de un robot al que dan órdenes, solo con el pensamiento y a través de un ordenador (12) que recoge los impulsos que con determinados sensores en el cerebro detectan esas órdenes pensadas.

Las posibilidades de mejorar la calidad de vida son inmensas y se basan en sistemas que permiten descodificar por medio de sensores e interfaces cerebro-ordenador los procesos mentales de la persona, de forma que pueden desde comunicarse con otras a través del pensamiento (13) hasta dar órdenes a través de un ordenador a una máquina que ejecuta la orden recibida. Innecesario decir que sin técnicas digitales tal cosa no sería posible, aunque, naturalmente, las técnicas digitales no son el único elemento indispensable para estos grandes avances, aunque sí lo sean para sus aplicaciones prácticas.

Junto a los importantes aspectos positivos derivados de la aplicación de estos sensores e interfaces cerebro-ordenador, son posibles otros que hay que considerar por sus efectos negativos en el plano de la personalidad o en el plano social. Debe tenerse en cuenta que dichos avances no sólo se podrían emplear para curar y mejorar la vida de quienes sufren determinadas enfermedades, sino también para potenciar la capacidad y las posibilidades de éxito de personas normales que sobrepasarían y superarían a los demás mediante el empleo de tales interfaces vinculados a ordenadores y datos en la nube tratados mediante inteligencia artificial.

He aquí, pues, enormes ventajas y oportunidades, pero también riesgos que han motivado que, recientemente un grupo de investigadores del proyecto BRAIN, liderados por un español, se hayan visto obligados a difundir en la revista científica *Nature* (14) su preocupación por las consecuencias del empleo de esta técnica para otros fines, que pueden acabar afectando a la identidad personal, a la igualdad y ofrecer a las empresas, hackers o gobiernos oportunidades para explotar o manipular a la gente y

(12) *Vid.* «People can control a robotic arm with only their minds», en *Science News* de 14 de diciembre de 2016 que cita como fuente el Colegio de Ciencia e Ingeniería de la Universidad de Minnesota; también «The Paralysed Man Who Can Control a Robotic Arm With His Thoughts», en *The Guardian*, 29 de marzo 2017 y también en *Motherboard-vice* de 12 de junio de 2015.

(13) *Vid.* Stocco, Andrea, *et al.*, «Playing 20 Questions with the Mind: Collaborative Problem Solving by Humans Using a Brain-to-Brain Interface», que puede consultarse en la siguiente página web de la organización editorial Plos One: http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0137303. También Nijboer, Femke, *et al.* «A P300–based brain-computer interface for people with amyotrophic lateral sclerosis» Clinical Neurophysiology 119(8):1909-16 September 2008.,

(14) *Vid.* Yuste, Rafael, *et al.*, «Four ethical priorities for neurotechnologies and AI», *Nature*, 8 noviembre 2017. https://www.nature.com/news/four-ethical-priorities-for-neurotechnologies-and-ai-1.22960. Rafael Yuste es el director del proyecto.

alterar algunas características del ser humano. El objeto de tal artículo no era otro, en última instancia, que el de reclamar del legislador una urgente regulación desde el punto de vista ético sobre las consecuencias de los avances y aplicaciones de todas esas investigaciones y descubrimientos que dejan a los investigadores en un terreno incómodo sin reglas ni normas ante los riesgos que perciben

Los sensores e interfaces cerebro-computador podrían acabar empleándose, en efecto, en una persona sin ninguna discapacidad, sino simplemente para obtener ventajas de una mayor capacidad que los demás en la vida diaria (realizar exámenes, oposiciones, acceder a un puesto de trabajo, etc.) como persona potenciada o aumentada (15), lo que plantea cuestiones sobre la igualdad en un mundo en que unos accedan a esas posibilidades y otros no. Pero al margen de los problemas de igualdad, que se señalan en el artículo citado, caben los riesgos de manipulación o interferencia en la vida y en las decisiones de las personas por la difusión de sesgos o prejuicios presentes en los algoritmos de la IA con los que se conecten a las personas. O por la interferencia de terceros sean ***hackers*** o gobiernos. Pero incluso, superados esos problemas, hay otros riesgos que afrontar; pues la experiencia demostraría que personas sometidas a estimulación cerebral mediante electrodos para tratar problemas de depresión acaban confesando haber perdido conciencia de su propio yo o de su identidad (16) como se recoge en el artículo de *Nature*; lo mismo podría

(15) De «hombre aumentado» se viene hablando desde hace tiempo por parte de muchos autores entre otros los que podríamos situar en la órbita del post-humanismo o transhumanismo. *Vid.* sobre el transhumanismo el Manifiesto del Transhumanismo de la Asocicación Humanity+ en la dirección https://humanityplus.org y el manifiesto en https://humanityplus.org) / Philosophy (https://humanityplus.org/philosophy/) / Transhumanist Declaration; *Vid.* tambien la posicion de Peter Sloterdijk con su polémico libro primero sobre «Normas sobre el parque humano: una respuesta a la Carta sobre el Humanismo de Heidegger» Ed. Siruela, 4.ª Ed. 2006 (criticado por Habermas en «El futuro de la naturaleza humana. ¿Hacia una eugenesia liberal?» de 2001) y con el siguiente «En el mismo barco: Ensayo sobre la hiperpolítica»Siruela, 2006, se ha erigido en el referente del posthumanismo y de la crítica a una idea de humanismo entendido por él como domesticación que vaciando de sentido la idea de humanismo (o criticando su sentido y función) abre un vacío que pueden rellenar las tecnologías; es un discurso de crítica al humanismo y a su supuesto fracaso –entendido como crianza, domesticación y sometimiento– frente a un mundo en que los medios actuales de uso y acceso masivo a la información (redes sociales, diarios digitales, buscadores, YouTube, etc.) dejan a la persona capacidad para, supuestamente, pensar por sí mismo y prescindir de los intermediarios y también para crear un ejercito de solitarios. Si en un primer momento el discurso posthumanista se centra en la biotecnologías, acaba promoviendo, después una, nueva relación con las máquinas o «seres sin alma» que acaban ocupando posiciones predominantes. En el ámbito del transhumanismo –término acuñado por Julian Huxley, profesor de zoología– muy relacionado con el posthumanismo la preocupación es la mejora de la condición humana mediante un uso intenso de todas las tecnologías.

(16) *Vid.* un trabajo anterior en que participaban dos de los firmantes de *Nature* –Goering, Sara, y Yuste, Rafael–, «On the Necessity of Ethical Guidelines for Novel Neurotechnologies» en *Cell*, Volume 167, Issue 4, pp. 882-885, 3 November 2016, donde afirman: «*Una de las más importantes cuestiones éticas y filosóficas a afrontar es la posibilidad de cambios sustanciales en el concepto del "yo". Mientras en la actualidad tendemos a identificarnos a nosotros mismos como relativamente separados y entidades privadas limitadas por nuestros propios cuerpos el uso de las novedades de las neurotecnologías puede dirigirnos hacia una parcial disolución de las ideas tradicionales sobre el yo*. Situándonos en el mundo digital y de internet, Carr Nicholas, en

ocurrir, plantean los autores del artículo, con la habituación a los interfaces cerebro-computadora.

La misma preocupación muestran los autores del trabajo citado por el empleo de la tecnología neuronal para fines militares o de dicha tecnología para potenciar las capacidades de determinados combatientes (aumenting neurotechnologies).

El artículo es, así, un llamamiento urgente desde su propio título (*«Four ethical priorities for neurotechnologies and AI»*) sobre la necesidad de una reflexión ética en cuanto a los límites de las aplicaciones derivadas de sus investigaciones. Reclaman en él la debida atención a varias prioridades éticas y el establecimiento de normas y guías de conducta en el empleo y aplicación de las neuro-tecnologías en su relación con la Inteligencia artificial: 1) el consentimiento y la privacidad; 2) la identidad y la dependencia; 3) la potenciación o aumento de la persona y sus límites, y 4) finalmente, los prejuicios que pueden difundirse a partir de algoritmos o experiencias que en lugar de ser rectificadas son confirmadas por la IA.

Todas estas tecnologías –especialmente el empleo de interfaces cerebro-ordenador– pertenecen a ese mundo digital convergente con otros avances y tecnologías. Mundo lleno de esperanzas y promesas que hay que aprovechar, pero conjurando los riesgos que puedan presentar, lo que exige para empezar detectar en qué pueden consistir tales riesgos y cuál es el grado de acuerdo sobre lo que es riesgo o no, lo que, sin duda, exige una previa determinación sobre lo que es el ser humano (17) y si se trata sólo de curar o también de mejorar. Éste es el gran debate sobre el transhumanismo y el posthumanismo en el que no sólo los técnicos están empeñados sino, también los filósofos con muchas y contrarias posiciones y también con muchos matices tanto entre los opuestos como entre los partidarios (18).

Los riesgos aquí apuntados afectan a la identidad de la persona, a la identificación del yo en un plano muy profundo en cuanto se producen en función de una conexión directa del cerebro humano con las tecnologías digitales. Pero los hay también que afectan a ese plano de la conducta personal y a la responsabilidad sin operar en ese plano de tan íntima conexión. Sería el caso de la inteligencia artificial aplicada a la medicina o al Derecho. En el caso de la medicina tenemos el caso del robot Watson de IBM (tenga o no forma de robot lo decisivo es la inteligencia artificial –los

---

«Superficiales. ¿Qué está haciendo internet con nuestras mentes?» Ed. Taurus 4. ed. 2016, sostiene que al confiar en los ordenadores para comprender el mundo nuestra inteligencia se aplana y convierte en inteligencia artificial; pp. 269 y 270.

(17) La cuestión, presente desde siempre en la filosofía, se plantea con sentido crítico desde Kant en su Lógica y está presente en el debate –a propósito de la relación del hombre con las nuevas tecnologías y la biomedicina– entre Sloterdijk (con su crítica a Heidegger) y Habermas a que antes se ha hecho referencia en nota anterior.

(18) Con posiciones contrarias al posthumanismo y muy críticas con ciertas formas de transhumanismo tenemos a Mandel y Fukuyama.

algoritmos– que emplea sea para analizar el genoma humano, sea para analizar síntomas y diagnosticar en enfermedades y proponer remedios) que acabará aportando mucha seguridad en el diagnóstico y tratamiento de enfermedades. Pero también plantea algunas cuestiones como determinar en qué medida los médicos seguirán sus opiniones o prescindirán de ellas. Mientras no las sigan no habrá problema, siempre que nada ocurra; pero si un día un mal diagnóstico del propio médico tiene consecuencias graves o fatales para el paciente, puede desencadenarse una acción de responsabilidad civil. En esa hipótesis, haberse apartado o despreciado el diagnóstico o el tratamiento propuesto por Watson, puede acabar siendo considerado imprudente y puede propiciar la tendencia a conformarse con la opinión de Watson.

Ya tenemos ahí un riesgo antes impensable: renunciar al propio criterio para acogerse al de una máquina con ánimo de eludir las consecuencias de la responsabilidad derivada de un error. Las primeras veces que eso pase, tal vez no tenga mucha trascendencia, pero si esa conducta se generaliza, se hace evidente cómo el mundo digital transforma y altera las pautas de conducta que hasta ese momento existían. Habrá quien proponga aceptar directamente el criterio de la máquina y quien proponga seguir el propio criterio tras haber tenido en cuenta los datos de la máquina. Pero para estos últimos podría acabar recayendo la carga de la prueba de por qué su criterio era mejor si se acabó produciendo un desenlace fatal. Claro que la cuestión puede plantearse al revés en la medida que seguir la propuesta de Watson tenga consecuencias fatales lo cual acabe por dejar las cosas como estaban o hacer que todo se resuelva en una explicación formal motivada de por qué se ha optado por ignorar a Watson.

Una cosa es que todos esos medios digitales puedan ser un elemento fundamental a la hora de tomar decisiones sobre diagnóstico y tratamiento y otra muy distinta que el profesional renuncie a tener su propio juicio y a limitarse a ratificar lo que los algoritmos dicen que hay que hacer. De lo que no cabe duda es de que la sociedad digital obligará a un cambio de prácticas y actitudes. El Derecho deberá dar también una respuesta.

Idénticos problemas se plantean en el plano de la igualdad. Esa persona aumentada o potenciada por la aplicación, en un futuro no muy lejano, a su propio cuerpo (cerebro) de determinados dispositivos que operan como interfaces cerebro-computador plantea graves cuestiones en relación con la igualdad y el futuro de la sociedad. Se tratará de saber si para preservar tal igualdad todos deberán de tener acceso a esos interfaces o no, simplemente porque no es posible económicamente. De saber también si la sociedad puede dividirse en unas cuantas personas con la capacidad aumentada y el resto. Una especie de superhombres y los demás, sometidos, tal vez, a los primeros.

Esos son los términos en que se plantean los debates entre humanistas, transhumanistas y posthumanistas.

Fuera de esos interfaces ya hoy se dan esas situaciones de desigualdad en relación con las pocas empresas (Google, Amazon, Facebook, Apple) que tienen acceso a datos masivos y a su tratamiento lo que determina una ruptura de la idea tradicional de competencia efectiva en el mercado por más que puedan estar cediéndolos mediante precio a otras empresas.

En definitiva el mundo digital, al margen de los beneficios que aporta, implica alteraciones muy notables en la personalidad, actividad y responsabilidad de las personas. Afecta también al tipo de sociedad que conocemos y a la idea de igualdad de sus integrantes. Les expone también a riesgos que hay que valorar y que demandan una nueva regulación. Regulación que abre un lapso temporal para que los ciudadanos vayan percatándose de los riesgos y oportunidades, completamente nuevos, a que nos enfrentamos como humanidad.

2.2 **Sociedad digital y democracia**

El mundo digital ofrece enormes posibilidades de profundizar la calidad de la democracia. No es solo una cuestión de una mejor Administración o un mejor acceso a los servicios, sino que es una cuestión de Gobierno y transparencia. La denominación de Gobierno electrónico se ha generalizado en muchos instrumentos nacionales e internacionales para referirse a la aplicación de las tecnologías de la información y la comunicación (19). Más allá de las ventajas que pueden obtenerse directamente por los ciudadanos en la prestación de servicios, el mundo digital afecta al concepto de democracia y gobierno en la medida en que permite nuevas formas de participación y control por parte de los ciudadanos. Tales formas se concretan desde la participación a través de medios electrónicos (consultas populares), hasta el acceso a sesiones de los órganos de representación de los ciudadanos a todos los niveles (local, regional o estatal) o incluso la realización de elecciones.

La participación directa a través de consultas populares ofrece grandes oportunidades cuando se trata de temas elementales, pero también riesgos cuando las cosas son más complejas, pues puede tender a transformar al ciudadano (que debe tener en cuenta todas las perspectivas y establecer prioridades con una visión total) en consumidor (que se inclina por las cosas que percibe más beneficiosas en el plano individual –bajar impuestos– sin tener en cuenta el impacto en otras áreas –deterioro de servicios–).

(19) *Vid.* Carta Iberoamericana de gobierno electrónico, en http://old.clad.org/documentos/declaraciones/cartagobelec.pdf.

Pero hay otras posibilidades de participación que tienen que ver con la transparencia en la gestión de la cosa pública en la que queda mucho por hacer. Las informaciones que se recogen en los portales de las distintas Administraciones, en aplicación de la Ley 19/2013 de Transparencia, se van llenando de contenidos, pero hay muchísimo que mejorar en ese aspecto, pues ni la información es completa, ni está organizada de forma tal que sirva al ciudadano para poder comparar lo que sus representantes hacen con lo que se ha hecho en años anteriores o con lo que hacen otras Instituciones similares en España o en cualquier país europeo. Cuando, además de datos, faltan términos de comparación es difícil extraer conclusiones y, en esas condiciones, la información –incluso un exceso de información desorganizada– es equivalente a falta total de información útil y, por tanto, de transparencia. La inteligencia artificial aplicada a los datos del gobierno y de todas las Administraciones públicas podría permitir a los ciudadanos interrogar a aplicaciones y programas –públicos y obligatorios– sobre cualquier aspecto de la gestión pública de una concreta Administración, o de varias, referenciada con comparaciones con gestiones anteriores en el tiempo de la misma Administración o con las de otras Administraciones del país o de cualquier otro país.

El control político no solo corresponde a la oposición, sino que los ciudadanos tendrían a su disposición instrumentos para verificar con facilidad y entender las cuestiones que les afectan como tales ciudadanos. Para los gobiernos constituiría un estímulo objetivo –aunque subjetivamente lo teman– para cumplir con sus obligaciones y para explicarlas a sabiendas de que los ciudadanos pueden comprenderlas y verificarlas.

Otras experiencias comparadas permiten percatarse de la importancia que el mundo digital ofrece para la participación y por tanto para la democracia. Sería posible, por ejemplo, que cuando un número importante de ciudadanos, previamente determinado, tuviera interés en una concreta cuestión pudieran formular preguntas a través de medios electrónicos a los miembros del Gobierno, que estarían obligados a contestar del mismo modo como lo hacen a las preguntas que les formulan los diputados, este número no sería difícil de alcanzar habida cuenta de las posibilidades de las redes sociales. Durante la Administración Obama se incentivaron iniciativas de este tipo en una página de la Casa Blanca –«we the people»– en la que la gente podía hacer sus preguntas y si en unos plazos predeterminados se adherían a la petición el número requerido de firmantes, las mismas debían ser respondidas (20).

(20) *Vid.* https://petitions.whitehouse.gov/ donde la página se encabeza con el *we the people* (your voice in the White House) de las primeras palabras de la Constitución estadounidense.

No son, desde luego, las únicas iniciativas que favorecen la participación y el control, ni mucho menos, pero muestran las enormes posibilidades que abre la sociedad digital para mejorar la participación en la vida política y la democracia.

Ello no obstante, la irrupción del mundo digital ha supuesto una disrupción de muchas cosas que exigen una reflexión sobre problemas nuevos que se plantean en la vida de las democracias. Se trata de dos cuestiones al menos que afectan al modo tradicional de funcionar la democracia. Por una parte la repercusión que ha tenido sobre el cuarto poder, es decir los medios de comunicación; por otra de los nuevos términos de una antigua tensión entre la democracia representativa y la democracia directa.

2.2.1 Medios de comunicación tradicionales y redes sociales

Los medios de comunicación tradicionales han sufrido el impacto del enorme desarrollo de las redes sociales y de la generalización del uso de internet, especialmente por las nuevas generaciones que pueden acceder a los mismos periódicos que sus padres y abuelos leían en soporte papel. Ello se ha traducido en una disminución de los ejemplares vendidos y, en consecuencia, en los ingresos recibidos por publicidad. También se ha traducido en una menor fidelidad al medio escrito puesto que se pueden consultar gratuitamente diversos medios.

El impacto ha afectado también a la televisión puesto que la forma de verla es mucho más selectiva tanto en cuanto a qué se ve, como a cuándo se ve y a través de qué medios se ve. También por la presencia de otros medios de ver el audiovisual como YouTube y otras plataformas.

La aparición de periódicos digitales, que siguen respondiendo en cierto modo al formato tradicional pero con menos personal y menos gastos, afecta al peso y función de la prensa en soporte papel.

Este impacto en el cuarto poder no ha dejado de tener consecuencias. Si hablamos de redes sociales, la primera es la capacidad de que cada una de las noticias que se producen diariamente pueden tener un reportero espontáneo y aficionado que a través de una fotografía que cuelga en la red da cuenta de cada cosa que sucede; muchas de ellas sin interés alguno, pero otras con mucho interés. La función del reportero de calle que buscaba la noticia –o se desplazaba a informar de ella de acuerdo con referencias recibidas de la policía, los bomberos o los juzgados– ha quedado complementada, a veces ventajosamente, por el ciudadano espontáneo que provisto de su teléfono cuelga en la red la noticia.

Pero junto al reportaje gráfico está también la opinión o la información que, en formato corto, da cuenta de algo o comenta, critica, alaba o apoya algo y lo difunde por una red social.

Ese tipo de información y opinión espontánea, en principio y la mayoría de las veces, tiene sus puntos positivos, pero también negativos. Se trata de una información que es la expresión máxima de la libertad del que la emite, siendo su espontaneidad su máximo valor; pero a la vez acaba dando igual peso a la información y opinión de quien habla con conocimiento de causa y la de quien solo expresa un prejuicio o una directa intención de faltar a la verdad. La red social tiende a igualar a todos. Por otra parte la noticia y la opinión, cuanto más extraña, exagerada y radical parezca, más atención suscitará. Desde luego siempre se había dicho que en periodismo la noticia no era que un perro hubiera mordido a un niño, sino que un niño hubiera mordido a un perro. En la red esa idea se agudiza al máximo: solo lo extravagante, radical y verbalmente violento parece que acaba suscitando la atención.

Si hablamos de información, la veracidad, en cuanto diligencia para comprobar la verdad, no es frecuente en las redes sociales; la noticia se reenvía a otras personas o redes sin ponerse a pensar en su veracidad: lo interesante es que sea noticiable y curiosa, sin importar demasiado su veracidad. Parece que la veracidad se la da el llegar a constituirse en *trending topic*.

Estamos en un terreno abonado para las noticias falsas y, lógicamente también, en el de los derechos de las personas que se sienten lesionados por esas noticias falsas. Si a eso se le une la existencia de difusión engañosa de noticias desde cuentas ficticias o automáticas (*robots* o *bots*) capaces de realizar campañas de desinformación sistemáticas, el problema tiene dimensiones preocupantes, especialmente si tales campañas se realizan desde una potencia extranjera que de algún modo pretende influir en el resultado de las elecciones como ha ocurrido en EEUU con ocasión de la elección del Presidente Trump y ha podido ocurrir en Francia, Italia o Cataluña.

Es evidente que el papel de la prensa escrita y en general de los medios de comunicación ha cambiado. Los medios de comunicación han sido siempre los mediadores entre la realidad y la creación de una conciencia sobre tal realidad. De esa tarea forma parte la selección de la noticia decidiendo lo que es importante y lo que no; la forma de contar tales noticias para reflejar lo más objetivamente posible lo ocurrido; también la selección de las opiniones y su contraste entre las varias existentes. Todo eso ha dejado de ser una tarea exclusiva de los medios por lo que han perdido el control de la creación de una opinión responsable y en competencia con otros medios. En buena medida la propia prensa escrita tiene una parte importante de responsabilidad por esa

pérdida de liderazgo de la opinión y de credibilidad, ya que las nuevas generaciones han podido percibir que no siempre ha actuado ni al servicio de la veracidad ni al de la objetividad en el cumplimiento de su función. En tales condiciones han preferido recibir las noticias espontáneas de las redes o de periódicos digitales y seleccionar por sí mismos lo que les parece más fiable.

La opinión se crea ahora en competencia con la que difunde directamente la gente a través de las redes sociales. La opinión es más espontánea y libre, pero también más sesgada, subjetiva y sectaria. Hay más fuentes de información, pero en el fondo con menos capacidad de contraste y contención, porque muy pocos asumen el riesgo de haber puesto en pie una organización que se responsabiliza, con su propia existencia y con el capital invertido, de ser una fuente fiable.

El reto es cómo aprovechar lo positivo de esa espontaneidad, pero poner límites a la mentira, la denigración, el acoso o el discurso del odio.

La función del cuarto poder como instrumento para encauzar la opinión pública y la información ha quedado tocada. Los medios tradicionales tendrán que recomponer su papel desde la base de su responsabilidad y seriedad en la búsqueda de la noticia. Ello no impedirá –ni debe intentarse– disminuir esa espontaneidad de los participantes en redes sociales que evitarán siempre que la prensa caiga en la complacencia con los poderosos políticos o económicos, pues siempre habrá algún ciudadano dispuesto a denunciarla. Las redes sociales y los nuevos instrumentos de comunicación se han constituido, así, en una especie de «checks and balances» del cuarto poder, al que no pueden sustituir.

Otra perspectiva ha de tomarse también en consideración. Se trata de la cuestión de en qué medida las redes sociales y la sociedad digital en general tienden a abrir una brecha en el diálogo entre los integrantes de una comunidad en cuanto les confirman en sus propias convicciones y no les ofrecen toda la información sobre un mismo tema, sino sólo aquellas que el algoritmo de los motores de búsqueda dice que se corresponde con sus preferencias (21). De esta manera se rompe una de las bases de una democracia deliberativa como es la del diálogo que no se reduce al ámbito institucional en que se parlamenta, sino que debe extenderse a toda la sociedad. En la sociedad electrónica los motores de búsqueda y las redes sociales tienen determinados mecanismos que pueden permitir dirigir y dar preferencia a lo que tales algoritmos creen que los usuarios quieren ver.

(21) *Vid.* Nickerson, Raymond S. «Confirmation Bias: A Ubiquitous Phenomenon in Many Guises», Review of General Psychology, The Educational Publishing Foundation, 1998, Vol. 2, núm. 2, pp. 175-220; también Pariser, Eli, «The Filter Bubble: What The Internet Is Hiding From You», The New York Times Bestsellers, 2012. *Vid.* también Schwab, Klaus en «La cuarta revolución industrial», Ed. Debate, 2016, donde hace un análisis de ventajas e inconvenientes de lo que llama cuarta revolución industrial; así en el apéndice, pp. 149 y ss.

2.2.2 Democracia representativa y democracia directa

La sociedad digital ha vuelto a poner de actualidad el viejo debate sobre democracia directa y democracia representativa, que se decantaba siempre a favor de ésta, aunque sólo fuera por la gran dificultad de reunir en un momento determinado a cientos de miles de ciudadanos en un territorio extenso que no es ya el de la ciudad ateniense.

Lo ha puesto de actualidad al romper esa primera barrera del tiempo, del espacio y del número de ciudadanos. En algún sentido los medios digitales parecería que han creado las condiciones de reconstrucción del mítico «ágora» ateniense; modelo de esa democracia directa, donde el debate y la comunicación entre todos es posible con independencia del número que quiera participar en él que ya no queda condicionado, por el espacio físico en que se desarrolla tal debate.

La potencia que esa ágora tiene se puso de manifiesto con motivo de los acontecimientos de lo que se denominó «la primavera árabe». Es significativo que esa potencia movilizadora tuviera tanta importancia en países sometidos a regímenes que habían tratado de ahogar las opiniones e informaciones a través de los medios convencionales. El resultado final más bien negativo, al menos a medio plazo, de esos movimientos en todos esos países (desencadenados a través de los medios e instrumentos de la sociedad digital) no impide reconocer la capacidad movilizadora y de oposición a un estado de cosas insatisfactorio, cruel o despreciativo de los derechos de la persona que la sociedad digital y sus medios tuvo, pero también las dificultades para construir alternativas positivas y compartidas a los problemas que se denuncian.

Sea como fuere, en el mundo digital ha surgido una especie de ágora. Un ágora virtual –pero bien potente y eficaz– en la que todo el mundo puede lanzar su mensaje, aunque no siempre sea escuchado por los demás o ni siquiera debatido en términos de suficiente racionalidad.

Es un ágora muy apta para difundir las noticias y las opiniones; muy especialmente las que por ser críticas con las cosas que no funcionan bien, suscitan la conformidad de muchos, aunque ni siquiera sean afectados directamente por todos y cada uno de los aspectos negativos de funcionamiento del sistema que se denuncia. No es, sin embargo, tan apto para la búsqueda de soluciones a los problemas complejos; para debatir los pros y los contras de las soluciones –eligiendo la mejor o la menos mala entre todos los partícipes del ágora que tienen intereses tan distintos entre sí– y alcanzar una posición común (22); aunque la alcanzan fácilmente en lo que se refiere a opo-

(22) En la teoría marxista el proletariado, como clase, permitía hacer descansar la revolución sobre una comunidad de intereses, contrapuestos radicalmente con los intereses de la clase dominante. Podía así no solo mantener un discurso de negación de lo existente, sino exhibir su capacidad de construir una alternativa compartida por todo el proletariado y dirigida por su

nerse al estado de cosas existentes en cuanto todos están afectados, si bien casi siempre por razones muy diferentes.

El ágora virtual no es así un ámbito adecuado para el compromiso en la búsqueda de soluciones a los problemas, en cuanto tal compromiso suponga renunciar a la perfección absoluta consistente en que todos obtengan las mismas o semejantes ventajas con los cambios a hacer. Tal cosa no es posible casi nunca; por eso tal ágora no es el foro ideal para la política concebida como arte de lo posible; arte que puede comportar, a veces, lograr mejoras, pero con sacrificios parciales o aplazamientos; o mejoras distintas según los colectivos; o mejoras para unos y pérdidas para otros.

El ágora virtual podría, a veces, ser presentada como una brecha entre una supuesta democracia directa (que se presentaría como cristalizando en las propuestas triunfantes en los debates de esa ágora virtual) y la democracia representativa que exige a sus participantes el compromiso entre todos ellos (en cuanto representantes de todos y cada uno los grupos sociales y políticos de una comunidad). Una brecha también entre el logro de todas las pretensiones y el compromiso con lo que es posible; con lo que permiten las circunstancias económicas y políticas del país.

Estamos así en una situación en que algunos podrían pretender –apoyándose en el ágora virtual– que los representantes políticos convencionales salidos de las elecciones quedasen eventualmente deslegitimados por los discursos en esa ágora virtual de los portavoces más radicales partidarios del logro de lo mejor y de la forma más inmediata. Eventualmente deslegitimados porque no siempre ocurre que los ciudadanos den por bueno que el único programa al que se adhieren sea el logro total, inmediato y a cualquier precio de sus deseos, al comprender que tal logro puede acabar comportando sacrificios para otros colectivos o sacrificios en el largo plazo y graves divisiones en el corto plazo.

En definitiva la recreación del ágora merced al desarrollo de la sociedad digital constituye un avance, una mejora y una nueva dimensión de los «*checks and balances*» que constituyen la esencia misma de una democracia. Es una nueva dimensión que integra y enriquece la democracia en cuanto da voz directa, siquiera sea de forma espontánea y desorganizada, a los ciudadanos. Ello habrá de ser una referencia permanente para el sistema de democracia representativa tradicional y un nuevo sistema de control por la ciudadanía de la democracia representativa. Pero no puede sustituirla, sino completarla.

Los beneficios de la sociedad digital para la democracia, pueden ser grandes. En cuanto a los riesgos, éstos vendrán de la eventual tendencia al populismo que, en determinadas circunstancias, pueda pretender en-

---

vanguardia. Pero esa división social ya no existe del mismo modo en el siglo XXI. De ahí la enorme dificultad para construir alternativas a lo existente.

frentar la democracia representativa con esa ágora pretendidamente expresión directa del pueblo; pretendidamente en la medida en que no es todo el pueblo. Algunos de los medios de la sociedad digital pueden favorecer un discurso populista, al ofrecer a cualquiera, y a todos, un medio para hacer muy visible la crítica al poder, más eficaz, probablemente, que el derecho de manifestación y que se presentaría como la voz del pueblo. De un pueblo que algunos querrían construirlo desde la identificación de un «nosotros» que se haría sujeto único precisamente por su crítica al Gobierno, o al sistema político, por muchos y diversos que sean los intereses y soluciones de tal «pueblo» (23).

Favorecen así algunos medios de la sociedad digital la idea de pueblo como aquella parte de la sociedad que se opone al poder o al gobierno; esa oposición es lo que definiría al pueblo (24) de lo que se sigue que quien no se oponga al poder no es pueblo. Ello conduce a una aporía cuando los gobiernos se eligen democráticamente. En efecto habría que entender o bien que todos los que han participado en el proceso electoral que condujo a la elección del gobierno no son pueblo (lo que pone en cuestión la idea de democracia misma que pretende ser el poder del pueblo) o bien que una parte de los que han participado en dicho proceso y han perdido –por no haber podido elegir «su gobierno»– han quedado fuera del poder (nunca del todo pues la oposición es una forma de poder: el de control al menos), pero han expulsado a los ganadores –y a los que les han votado–, del concepto de pueblo (lo que tampoco deja en buen lugar su condición de demócratas).

En cualquier caso, el mundo digital ha abierto un espacio público nuevo –el ágora con sus debates, sus informaciones, sus *trending topics*, etc.– que ha de jugar un papel muy positivo en la democracia representativa, articulándose con ella, pero sin que pueda ni deba pretender sustituirla ni ser una fuente de deslegitimación de la misma; aunque lo sea de crítica y de obligada atención.

2.2.3 La democracia en la era del Big Data

La irrupción del Big Data (datos masivos o macrodatos) en anglicismo que se ha impuesto en el uso corriente solo se entiende cuando esa inmensa cantidad de datos se vincula con mecanismos capaces de tratarlos. Inmensidad de datos que no sólo provienen de las fuentes conscientes, sino que ya hoy y en el futuro provienen de los que cada hora producimos

(23) *Vid.* Lasalle, Jose María: *Contra el populismo: Cartografía de un totalitarismo postmoderno*, ed. Debate.

(24) Ernesto Laclau en una entrevista al diario *La Nación* de Buenos Aires del 10 de julio de 2005 afirmaba: «Frente a la concepción tecnocrática del poder está la noción de la política como antagonismo, es decir, la emergencia de demandas sociales que se plantean a un cierto sistema. Esas demandas sociales constituyen un pueblo y *el pueblo se constituye siempre en su oposición al poder*»

los usuarios –muchas veces sin saberlo– de la multitud de dispositivos digitales que utilizamos al día; desde las pulseras, los teléfonos móviles, los ordenadores, las redes sociales, las tarjetas de crédito o débito, las compras por internet, las aplicaciones para el trafico, el pago del estacionamiento, el GPS, el internet de las cosas, etc. Dispositivos todos ellos que, sabiéndolo nosotros o no, producen millones de datos que, aun anonimizados, son uno de los bienes más preciados en el momento actual y en el futuro. Buena prueba de ello es la gratuidad de las redes sociales que en realidad se cobran con la propaganda, incluso personalizada que reciben los usuarios, y con la venta de sus datos a terceros.

Su importancia conecta con el valor comercial que tienen para las empresas y lo son también desde el punto de vista político, al que aquí nos referimos, en cuanto pueden revelar, de forma personalizada o no, una información trascendental. Información con la cual se pueden diseñar políticas o estrategias o influir en las elecciones como se acaba de poner de manifiesto con la denuncia de la filtración de datos de 50 millones de usuarios de Facebook que ha servido para que la empresa Cambridge Analytica LLC influyera en las Presidenciales americanas y en el Brexit.

Pero, incluso más allá de eso y de su gravedad, hay quien piensa –los que Harari ha llamado «dataístas» (25)– que en el futuro la política debería ser sustituida por la aplicación de la Inteligencia Artificial (IA) a millones de datos recolectados y referidos no solo a las preferencias o ideas de la gente, sino también los datos económicos, sociales, culturales, etc., del país y compararlos con los de otros países, semejantes o no, y con las experiencias de esos países en los más diversos temas: cómo salir de la crisis, cómo mejorar la productividad, cómo mejorar la agricultura, el comercio internacional, el cambio climático, etcétera.

En definitiva, la inteligencia artificial aplicada al tratamiento de datos masivos (Big Data) permitiría según los dataístas prescindir de la política. La propuesta no consiste como podría pensarse en emplear los análisis o propuestas del Big Data para tomarlos muy en cuenta en el debate político para mejorar la calidad de tal debate (manifiestamente mejorable en buena parte de los casos), sino pura y simplemente en dejar a las máquinas dirigir nuestras vidas en el futuro porque las estructuras democráticas actuales no pueden tratar los datos con la misma eficacia (26).

---

(25) Denominación que Yuval Noah Harari ha popularizado en su libro *Homo Deus. Breve historia del mañana*, Ed. Debate, 2017 p. 200, donde habla del «dataísmo» en el capítulo que titula «La religión de los datos» y en el que expone con gran complacencia la pesadilla del fin del humanismo y el sometimiento a los algoritmos (p. 429) y a los superhumanos (pp. 378 y 379). No es relevante para él saber quién elabora los algoritmos, pues son equipos enormes y, además, las propias máquinas y las redes neurales son capaces de aprender de sus errores y corregirlos.

(26) *Homo Sapiens*, *op. cit.* p. 408:«*Nuestras estructuras democráticas actuales no pueden recopilar y procesar los datos relevantes con la suficiente rapidez […] de ahí que la política democrática tradicional pierda el control de los acontecimientos*».

Tales propuestas de los dataístas parten, por otro lado, en algunos de ellos de una idea de la persona que ni tiene, ni habría tenido libertad (27), pues sus decisiones serían fruto de reacciones bioquímicas producidas en el cerebro (28). Las máquinas nos conocerían mejor que nosotros mismos. En todo caso se formulan dichas propuestas desde una entrega total a un mundo feliz que siempre será mejor que el actual, porque se basa en la exactitud de las previsiones de los algoritmos y de una idea del ser humano que no es sino el instrumento de los algoritmos (29) y cuyas ideas sobre su identidad, su conciencia y su libertad son falsas y fruto de sus reacciones bioquímicas cerebrales.

Ese paraíso o tierra prometida de algunos dataístas que desean que se presente cuanto antes, podrá ser visto por el resto como un desvarío o una pesadilla. Pero el hecho de que se haya formulado por gente con gran audiencia y en los términos en que se ha formulado la propuesta pone de relieve los retos y riesgos a que nos enfrentamos no en un futuro inmediato, pero sí, probablemente, como un debate recurrente sobre el sometimiento a la Inteligencia Artificial, el ***machine learning*** y los algoritmos. Debate que obligará a una reflexión teórica para situar en su justo lugar el papel de la IA en nuestras democracias.

No se trata de un tema menor para nuestra democracia, pues se ve que hay quien espera entregar todo el poder y toda su persona y conciencia (aunque para ellos se trata de procesos bioquímicos cerebrales) a las máquinas, a la espera de llegar al «nirvana» al haber conseguido al fin saberse reducido a puro instrumento de recolección de datos a la mayor gloria de las máquinas que se supone que harán cálculos cada vez más perfectos.

Esa idea, que se presenta a sí misma como basada en juicio científicos que se pretenden indiscutibles, viola en todo caso la idea de la persona humana y de su dignidad que está presente en el Título I de nuestra Constitución. Viola también los valores superiores de libertad, igualdad y plu-

(27) *Vid. Homo Deus*, *op. cit.*, p. 213, donde mantiene que «La palabra libertad es un término vacuo. El libre albedrío existe únicamente en los relatos imaginarios». Mas adelante en p. 360 «los algoritmos que conforman un humano no son libres. Están modelados por los genes y las presiones ambientales, y toman decisiones de manera determinista, ya sea al azar, pero no libremente». Vid. también la crítica de Foer, Franklin, «Un mundo sin ideas. La amenaza de las grandes empresas tecnológicas a nuestra intimidad», Ed. Paidós, 2017, a lo que llama en un capítulo «La guerra de Mark Zuckerberg contra el libre albedrío», pp. 63 y ss.

(28) *Vid. Homo Deus*, *op. cit.* p. 312, «Los científicos […] fueron descubriendo que no había alma, ni libre albedrío, ni «yo», sino solo genes, hormonas y neuronas que obedecen las mismas leyes físicas y químicas que rigen el resto de la realidad […] Los procesos electroquímicos cerebrales que culminan en un asesinato son deterministas o aleatorios o una combinación de ambos, pero nunca son libres». Y en p. 361 sostiene: «las personas ya no se verán como seres autónomos […] sino como una colección mecanismos bioquímicos que está constantemente supervisada y guiada por una red de algoritmos electrónicos».

(29) *Vid. Homo Deus*, *op. cit.*, p. 414, «los humanos son simplemente herramientas para crear el Internet de Todas las Cosas que podría acabar extendiéndose fuera del Planeta Tierra para cubrir toda la Galaxia e incluso todo el Universo».

ralismo político. En trance de plantearse nuestro futuro en la sociedad digital no pueden sino verse como una amenaza las ideas de los llamados dataístas que consideran las elecciones o los parlamentos sobrepasados por la inteligencia artificial de las máquinas (30).

Tales son las amenazas, hoy todavía sobre el papel, que se derivan del programa que algunos parecen tener en relación con los avances tecnológicos que configuran la sociedad digital; programa que consiste en hacer de buena gana al ser humano un instrumento de las máquinas y en acelerar la llegada de esa tierra prometida incrementando cada día más la remisión de cuantos más datos mejor en relación con todas sus actividades para que así las máquinas y la IA vayan perfeccionando sus técnicas y corrigiendo sus propios errores. Tal es el mandamiento más importante de los dataístas a sus miembros (31).

En su lugar un programa democrático a la altura de los valores que proclama nuestra Constitución debe dirigirse, desde luego, a obtener el máximo provecho de las novedades, descubrimientos y avances de la Sociedad digital, pero en beneficio y al servicio de la persona humana, de su dignidad y de los valores sobre los que hemos construido nuestro Estado y nuestra sociedad. Tal es la tarea que tenemos por delante (32).

Si en los párrafos anteriores se ha insistido en lo que podíamos llamar «credo» de lo que se ha venido en llamar dataísmo, es porque pone de

---

(30) *Homo Deus*, *op. cit.*, p. 314, donde desvaloriza el sentido de participar en una elección porque el voto es expresión de un proceso bioquímico: *«¿por qué prefiero votar por conservadores o laboristas? No elijo ninguno de estos deseos sino porque ésta es la sensación que los procesos bioquímicos crean en mi cerebro».*

Y en p. 426 *«¿Qué utilidad tiene celebrar elecciones democráticas cuando los algoritmos saben las razones neurológicas exactas por las que una persona vota a los demócratas mientras que otra vota a los republicanos».*

(31) *Homo Deus*, *op. cit.*, p. 415, *«el primero y principal [mandamiento]: un dataísta debe maximizar el flujo de datos conectándose cada vez a más medios y produciendo y consumiendo más información. Como otras religiones el dataísmo también es misionero. Su segundo mandamiento es conectarlo todo al sistema, incluidos los herejes que no quieren ser conectados. Y todo significa más que sólo los humanos. Significa todas las cosas. Mi cuerpo por descontado, pero también los coches […] El mayor pecado es bloquear el flujo de datos. ¿Qué es la muerte sino una situación en la que la información no fluye? De ahí que el dataísmo sostenga que la libertad de información es el mayor de todos los bienes».*

Y en p. 426: *«Permite que Google y Facebook lean tus correos electrónicos, supervisen todas tus charlas y mensajes y conserven todos tus "me gusta" y todos tus clics. Si haces todo esto los grandes algoritmos del Internet te dirán con quién casarte, qué carrera seguir y la conveniencia de iniciar o no una guerra».*

(32) Los retos reales y concretos que plantea la sociedad digital a la persona humana resucitan con renovada fuerza y alcance práctico, una reflexión teórica siempre presente en la filosofía con la pregunta sobre «qué es el hombre» formulada así claramente desde Kant en su «Lógica», pero heredera de la filosofía griega (Sócrates o Platón), reiterada, entre otros en la modernidad, con Descartes («Discurso sobre el método»), y continuada después especialmente en Heidegger («El ser y el tiempo», «Carta sobre el humanismo» y «Kant y el problema de la metafísica»), Nietzsche («Así hablo Zaratustra» o «Genealogía de la moral»), Sartre («El ser y la nada» o «El existencialismo es un humanismo») o Foucault («Las palabras y las cosas» y «Una arqueología de las ciencias humanas»). En directa relación con el mundo de las nuevas técnologías están las posiciones antes reseñadas de Peter Sloterdijk («Normas sobre el parque humano: una respuesta a la Carta sobre el Humanismo de Heidegger» o «Has de cambiar tu vida» Madrid; Pre-Textos; 2012).

manifiesto cuáles son los riesgos, no desprovistos de fundamento, que en la forma descarnada con que se han podido ver a lo largo de las citas y notas a pie, pueden parecer excéntricos, pero no son sino la consecuencia de una visión de las cosas que parecen poner su esperanza en construir una sociedad sin instituciones democráticas y al servicio de la inteligencia artificial y de las máquinas. Tal visión extrema no resulta verosímil, aunque, cada vez más, inquieta a muchos (33). Sea como fuere la Inteligencia artificial deberá ponerse al servicio de la política, sin sustituirla; en esas condiciones la determinación de los algoritmos y su composición no pueden quedar completamente sustraídos al conocimiento y decisión del pueblo a través de sus representantes.

En todo caso al margen de las pretensiones de los dataístas más radicales, que no parecen muy verosímiles, lo que sí es ya una realidad es el empleo de la IA en la vida política. No sólo en los casos de la utilización de las falsas noticias a través de redes sociales y a través de falsas cuentas que encubren robots (*bots*), sino también como acabamos de ver a través de la usurpación de los datos de 50 millones de cuentas de Facebook que se emplearon tanto para influir en las elecciones presidenciales norteamericanas, como en el resultado del Brexit (34). Urge adaptar nuestra legislación en lo que sea necesario para que tales cosas no ocurran; en buena parte todo tiene que ver con la protección de datos personales, pero como se puede comprobar la usurpación de datos personales no solo afecta a derechos fundamentales de las personas, sino que también afecta a la credibilidad y estabilidad de nuestras democracias.

2.3 **Libertad y seguridad**

La sociedad digital muestra un problema delicado en la articulación de la libertad y seguridad. Se trata de un tema recurrente a lo largo de la historia del mundo y lo es particularmente importante en toda democracia avanzada. Desde luego el problema existe en todos los países, pero en aquellos constituidos en dictaduras o en negadores de derechos huma-

(33) Ademas de a los autores citados en las nota deben verse las continuas advertencias de Elon Musk, el promotor de TESLA, sobre la urgencia de regular la IA, considerándola un peligro superior al de las armas nucleares en http://thehill.com/policy/technology/342345-elon-musk-we-need-to-regulate-ai-before-its-too-late. En esa misma urgencia de la regulación está Bill Gates y estaba Stephen Hawking (recientemente fallecido) que en enero de 2015 firmaron, junto a Elon Musk, una carta alertando de los peligros de la IA.

En un sentido que todavía no sabemos pero que es consciente de la relación entre Inteligencia Artificial, Big Data y democracia será interesante ver el próximo libro de Posner, Eric A., y Weyl E. Glen, «Radical Markets/ Uprooting Capitalism and Democracy for a Just Society» | Nook Book (eBook) | Barnes & Noble®, donde parece que aborda la cuestión del pago por el empleo de los datos no personales para evitar posiciones de monopolio.

(34) *Vid.* Koopman, Colin, en «How Democracy Can Survive Big Data», *The New York Times,* 22 de marzo 2018 en https://www.nytimes.com/2018/03/22/opinion/democracy-survive-data.html

nos el problema desaparece absorbido por la falta total de derechos y garantías.

En una democracia el problema se presenta en toda su importancia y dimensión. Como es sabido internet empezó siendo un intento de solucionar el problema estratégico importante de cómo responder a un ataque que anulara el centro del poder militar de un país, localizado en un punto determinado, y desactivase la capacidad de reacción del país entero. El protocolo internet fue la respuesta. Pues bien hoy esa respuesta está siendo puesta en cuestión en su finalidad inicial y en muchas otras.

El ataque de un virus («ransomware») informático en mayo de 2017 que se propagó por muchos países del mundo, entre ellos España, pone de manifiesto la necesidad de adoptar medidas de seguridad que eviten que se pongan en peligro sistemas vitales, no ya por razón de la defensa, sino de servicios públicos esenciales (redes de energía, telecomunicaciones, hospitales, etc.) (35).

Aparte de las medidas para prevenir esos ataques y la imposición a tal efecto de obligaciones a empresas que los gestionan, los gobiernos han de adoptar medidas para prevenir una de las posibles fuentes origen de tales ataques como podrían ser los terroristas. Eso lleva a la adopción de medidas que pueden acabar afectando a los derechos fundamentales a la libertad de expresión, información, privacidad, intimidad, etc.

Es el caso de algunos ***softwares***, como Pegasus del grupo NSO israelí, que parece haber vendido a Méjico y que sirve para el seguimiento y monitoreado de terroristas y criminales. Ahora bien, un empresario mejicano, crítico con el gobierno, denunció en 2017 que había sido empleado para su seguimiento lo que el Gobierno de Peña Nieto negó (36).

Sea como fuere la cuestión radica en cuáles son las garantías que han de aplicarse en la sociedad de la información. La legislación ha desarrollado muchos aspectos en relación con la intimidad y el domicilio, pero es preciso afrontar las cuestiones que tienen que ver con los ordenadores y los móviles que presentan problemas específicos en relación con las, por otra parte necesarias, medidas de seguridad frente al terrorismo o los ataques informáticos.

2.4 **El mercado y el Big Data**

El impacto de las tecnologías digitales en el mundo económico es asombroso. No hay más que ver cómo en la actualidad en el ***ranking*** de

(35) *Vid.* el informe sobre «Ciberseguridad, la protección de la información en un mundo digital». Ed. Fundación Telefónica y Ariel.

(36) *Vid.* The New York Times de 19 de junio de 2017: Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families en https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/

las 10 mayores empresas del mundo por capitalización bursátil, 7 son tecnológicas, lo que supone que en sólo diez años se ha producido un cambio radical al sustituir a las empresas de banca y energía que ocupaban dichos puestos, por otras completamente distintas (37). En definitiva, eso confirma la aparición de nuevos modelos de negocio y que los mismos son los más rentables y los que más futuro parecen tener. Es también significativo que Europa no tenga, al menos por el momento, empresas de referencia en esos campos comparables con las de los Estados Unidos. Finalmente debe destacarse cómo tales compañías están posicionándose y colonizando otros sectores conexos y son, por otra parte, las que mayores esfuerzos de inversión están haciendo en nuevas tecnologías e investigación del mundo digital.

En definitiva, nos enfrentamos a un cambio de modelo de negocios en el plano mundial dominado por pocas empresas tecnológicas americanas (38) que se extienden por todos los países del mundo y desde luego por Europa. Todo ello plantea, además, graves problemas fiscales en cuanto a su mínima tributación merced a técnicas de ingeniería fiscal que consiguen lo que se ha denominado «la erosión de la base imponible y el traslado de beneficios» (39).

Sin embargo el problema relevante a los efectos del presente trabajo consiste en la tendencia a la concentración y oligopolio de ámbito mundial de las nuevas compañías tecnológicas (básicamente los cinco grandes: Apple, Alphabet –Google–, Amazon, Facebook y Microsoft) en un horizonte de creciente aplicación de inteligencia artificial al Big Data del que esas mismas compañías son las mayores recolectoras de datos.

El reto que plantean es doble. Por una parte en relación con los riesgos para una competencia efectiva en su propio ámbito tecnológico y en sus aledaños; a la postre a lo largo y ancho del mercado mundial. Por otra en relación con los riesgos para la democracia misma a que antes se ha hecho referencia.

En relación con el mantenimiento de la competencia efectiva en el ámbito económico las cinco grandes tecnológicas que antes se han citado, tienen acceso directo a datos de sus clientes, ya como titulares, ya en cuanto responsables de sus subsidiarias que prestan servicios como titulares de redes sociales, buscadores o servicios de compra ampliamente difundidos y por tanto tienen capacidad para, a partir del conjunto de todos los datos que obtienen de sus clientes, poder aplicarles programas

(37) *Vid.* «Consulta pública sobre la estrategia digital para una españa» p. 16.

(38) Conocidas como GAFA (Google, Apple, Facebook y Amazon) a la que habría que añadir como quinta a Microsoft.

(39) *Vid.* OECD y sus propuestas y publicaciones sobre el BEPS (Base Erosion and Profit Shifting). Así «Action Plan on Base Erosion and Profit Shifting» o «La lucha contra la erosión de la base imponible y el traslado de beneficios» OECD 2013.

de IA que les permitan afinar mucho en sus políticas de venta y publicidad perfectamente adaptadas a los gustos y preferencias de sus clientes. También les permiten conocer las tendencias del mercado y prepararse para ella adelantándose a cualquier competidor o entrando en nuevos mercados.

Recientemente la Agencia de Protección de Datos española sancionó a Google por prácticas abusivas con su servicio de comparador al dar preferencia a los productos que ella misma comercializa a través de su servicio google-shop (40). En la misma línea se mueve el expediente iniciado por la Agencia Española de Protección de Datos contra Facebook y WhatsApp porque al ser adquirida la segunda por la primera le ha dado acceso a los datos de sus clientes (41). Similares acciones se están iniciando en Francia y Alemania.

El Big Data y su tratamiento supone un salto cualitativo muy importante que coloca a quien dispone de los datos y del conocimiento y técnicas para tratarlos en una situación de ventaja competitiva sin precedentes (42). En definitiva, las grandes empresas tecnológicas pueden comprometer seriamente el mercado y la competencia. Tal es el reto al que debe hacerse frente, pues al comprometer el funcionamiento del mercado se distorsionan las ventajas que del mismo se esperan.

La concentración asimétrica de conocimientos que proporciona el acceso a datos masivos y su tratamiento con inteligencia artificial por muy pocos actores del mercado obliga a una regulación, no muy diferente a la general empleada en defensa de la competencia, pero adaptada a sus singularidades. Aspectos como la determinación de la propiedad de los datos masivos, la reserva del uso de los datos para la misma entidad que los recolecta o la separación funcional de ambas actividades o la puesta a disposición de terceros de los mismos datos recolectados, son cuestiones sobre las que hay que adoptar posición (43); todo ello sin perder de vista muchas otras como el consentimiento en el uso de los datos, su forma de recolección, el carácter gratuito o no del consentimiento, su anonimización (44), etc.

---

(40) La Comisión impuso el 27 de junio de 201 a Google una multa de 2,42 mil millones de euros por abuso de posición dominante como motor de búsqueda por dar una ventaja ilegal a su propio servicio de compras comparativas.

(41) La Agencia Española de Protección de Datos (AEPD) ha impuesto sendas multas de 300.000 euros a Whatsapp y a Facebook por el trasvase y el tratamiento de datos personales de usuarios a partir de la compra de la primera por la segunda, en el 2014. Facebook ya anunciado su intención de recurrir. En Francia el supervisor de datos ha anunciado un expediente similar.

(42) *Vid.* Pasquale, Frank «The black Box Society: The Secret Algorithms that control Money and information» Ed. Cambridge: Harvard University Press, 2015.

(43) *Vid.* Posner, Eric A. y Weyl E. Glen «Radical Markets/ Uprooting Capitalism and Democracy…», *op. cit.* pendiente de publicación en la que, por algunas informaciones, parece que se aboga por que se pague una cantidad por los datos.

(44) *Vid.* la opinión de 10 de abril de 2014 del Grupo del artículo 29 sobre «Anonymisation Techniques».

El segundo reto al que se hacía referencia consiste en que la falta de competencia efectiva en la economía compromete también la democracia. No se trata aquí de reiterar lo que ya se ha indicado más arriba, sino de destacar otra faceta del mismo problema, pero desde el punto de vista de la relación entre la democracia y un mercado que, al funcionar de modo efectivo y permitir la competencia, no sólo se supone que es capaz de asegurar (si no hay fallos de mercado) el precio justo y la correcta asignación de recursos escasos, sino también el mantenimiento de la democracia al impedir monopolios que al distorsionar gravemente el mercado, comprometen también la democracia.

El sistema económico de un país y el sistema político están íntimamente interconectados. Una actividad económica controlada y dominada por unos pocos, acaba afectando a la calidad de la democracia. En los orígenes de la Sherman Act de Estados Unidos estaban no solo las luchas contra los monopolios, sino también la garantía de la propia democracia en aquel país. En Europa se teorizó del mismo modo por parte, incluso, de la propia Escuela de Friburgo (ordo-liberal) que achacaba a la concentración de poder económico en pocos grupos la destrucción de la república de Weimar y todas las derivas posteriores. Su tesis enfatizaba que no solo se trata de defender las libertades económicas por sí mismas, sino que las libertades económicas promueven y garantizan las libertades políticas. Y cuando no hay mercado sino monopolios, la libertad económica está comprometida.

Por eso el Estado no solo debe proteger a los individuos frente a los excesos y amenazas de los poderes públicos, sino que debe protegerles de las amenazas provenientes de determinados poderes privados (45). Con esa perspectiva se comprende que el Big Data y los tratamientos que de tales datos hagan las grandes compañías tecnológicas enormemente concentradas a nivel mundial se derivan no solo riesgos para el mercado, sino también riesgos para la democracia misma, que se añaden a los analizados más arriba.

Cuanto hasta aquí se ha dicho obliga a una reflexión sobre los datos y su propiedad por una parte y, por otra, su tratamiento. El debate acerca de si las grandes compañías recolectoras de datos –el nuevo oro negro o el petróleo de internet según algunos– deben pagar por ellos a las personas a que se refieren los mismos, puede ser uno de los grandes temas de debate en el inmediato futuro. Pero también debía serlo lo relativo a su empleo, pues si es un recurso esencial en la actualidad, alguna reflexión

(45) *Vid.* Gerber, D. J., «Constitutionalizing the Economy: German Neoliberalismus, Competition Law and the «New» Europe». The American Journal of Comparative Law, vol. 42, 1994, p. 27 (donde afirma que las ideas del neoliberalismo alemán se formalizan como respuesta a la crisis política y social de la República de Weimar y a la Alemania Nazi) y pp. 36 a 38; también Petersmann, Ernst-Ulrich, «Proposals for a new constitution for the European Union: building-blocks for a constitutional theory and constitutional law of the EU», *Common Market Law Review*, 32: 1123-1175, 1995, pp. 1154 y 1155.

merecería la cuestión de si no debía aplicarse la doctrina de las «*essential facilities*» que en el marco del Derecho de la competencia viene aceptándose como la única solución, cuando existe un recurso esencial que no puede reproducirse fácilmente y (46) que confiere un enorme poder de mercado a quien dispone del mismo (47).

Eso exige distinguir entre el acceso a los datos, con los problemas de su anonimización, si no se cuenta con el consentimiento de la persona a quien se refieren los datos, y la ideación de los modelos que sirven de base a la aplicación de la inteligencia artificial estableciendo los algoritmos adecuados. Estos últimos plantean la cuestión de los derechos de propiedad intelectual o industrial (48) de los autores que finalmente establecen el algoritmo.

La última cuestión tiene que ver precisamente con las posibilidades y dificultades de regulación de la inteligencia artificial. Dificultades por la presencia de los derechos de propiedad intelectual, pero como siempre pasa con los derechos es necesaria su articulación con los demás derechos. En ese contexto parecería que el empleo de algoritmos que pueden determinar o afectar a otros derechos fundamentales, como el derecho al trabajo en el acceso al mismo o en la extinción del contrato o empleo, no debería entregarse a un algoritmo para que ponga el sí o el no al acceso, cuando se hace en condiciones de concurrencia especialmente o al despido.

La IA no explica las razones de su decisión o propuesta de decisión sobre el acceso al trabajo o el despido; ni puede verbalizarlas o motivarlas explicando las razones que llevan a la propuesta. Solo conociendo el algoritmo y los datos concretos que se le han suministrado sobre la persona sobre la que propone la decisión podrían saberse las razones de la propuesta. La fórmula en que consiste el algoritmo debería, en algunos casos, poder ser conocida, en lo que se refiere al modelo sobre el que se construyó, las variables y ponderación de cada una de ellas, como también el tipo y clase de datos que, a partir del modelo, se han suministrado a la compu-

(46) *Vid.* sobre anonimización las «Orientaciones y garantías en los procedimientos de anonimización de datos personales» en la web de la Agencia Española de Protección de datos: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_y_garantias_Anonimizacion.pdf

(47) *Vid.* Istvan Nagy, Csongor, en «Refusal to deal and the doctrine of essential facilities in US and EC competition law: a comparative perspective and a proposal for a workable analytical framework», *European Law Review*, núm. 5, 2007, pp. 664-685; Díez Estella, Fernando, «La doctrina del abuso en los mercados conexos: del "Monopoly Leveraging" a las "Essential Facilities", *Revista de derecho mercantil*, núm. 248, 2003.

(48) El encaje de los algoritmos en uno u otro ámbito varía según los países, ofreciendo en el caso de Europa alguna dificultad, si bien, en todo caso, contarán con la protección que se deriva de su incardinación entre los secretos de empresa que regula el artículo 39 del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (Acuerdo sobre los ADPIC) (1994) en el seno de la OMC. *Vid.* Azuaje Pirela, Michelle, y Finol González, Daniel Ernesto, «Big Data, algoritmos y propiedad intelectual», en Anuario de propiedad intelectual, núm. 2016 (año 2017), pp. 257-275.

tadora para llegar al algoritmo, así como los datos suministrados de la persona sobre la que la computadora ha hecho la propuesta. Pero tal conocimiento puede chocar con los derechos de propiedad intelectual, industrial o con el secreto empresarial (49).

Desde luego en los casos en que pueda afectar a derechos fundamentales como el trabajo, la igualdad, etc., habría un derecho de los interesados afectados por la decisión en conocer el contenido del algoritmo, su lógica y todos los extremos que acaban de mencionarse. Entre otras cosas por razón de su eventual impugnación y de su derecho a la tutela judicial efectiva. No puede olvidarse que la experiencia hasta ahora con la IA y los algoritmos es que no están libres de errores, ni de sesgos y discriminaciones de los mismos programadores a los que un Estado no puede permanecer indiferente (50).

Otra cosa sucede con la IA dirigida a predecir las preferencias del público o a personalizar la publicidad; pues aquí no es fácil ver derechos o intereses de terceros que justifiquen el conocimiento de los algoritmos.

2.5 **Derechos fundamentales y libertades individuales en la sociedad digital**

Finalmente abordaremos aquí el último aspecto de los retos y oportunidades que suscita el mundo digital en relación con los derechos y libertades. Ese es el objeto de los distintos temas de que trata este libro por lo que no sería lógico analizar aquí cuestiones que van a ser objeto de reflexión con mucha mayor precisión a lo largo de los capítulos del presente libro. Procede solo señalar algunos rasgos que desde una visión general pueden caracterizar los riesgos que comporta la sociedad digital para los derechos y libertades de las personas.

Uno de los rasgos a destacar radica en el cambio mismo de percepción que se ha producido en apenas dos décadas en relación con los riesgos y oportunidades que implica la sociedad digital y el reflejo que eso ha tenido en la regulación y, en concreto, en la creciente demanda de una regulación pública. Ello nos lleva a la paradoja de que el reino de internet que parecía ser el del estado de naturaleza (51) acabe transformándose, a pe-

(49) Artículo 39 del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio (anexo 1c del Acuerdo de Marrakech por el que se establece la Organización Mundial del Comercio).

(50) *Vid.* O'Neil, Cathy «Armas de destrucción matemática. Cómo el Big Data aumenta la desigualdad y amenaza la democracia» ,Ed. Capitan Swing, 2017 pp. 131, 153 y 175

(51) La paradoja está en el propio origen de internet como un recurso militar. En todo caso la evolución en ese cambio la expresa mejor que nadie uno de los creadores de Internet Lanier, Jaron como puede verse en «¿Quién controla el futuro?» Ed. Debate, 2014, donde hace una amplia descripción de los cambios derivados de la difusión del empleo de Internet. Del mismo autor, acentuando su visión crítica, «Contra el rebaño digital» Debate, 2011 y, últimamente, en su

tición de sus habitantes, en el reino del contrato social (52). En definitiva en el descubrimiento del Estado, si bien un Estado que puede ser, él mismo, una fuente de interferencia en los derechos y libertades. La cuestión es qué Estado –qué poder público, qué intervención y qué alcance– queremos para la regulación de la sociedad digital.

Otro de los rasgos o novedades radica en que la sociedad digital amplía la dimensión subjetiva de la fuente de los riesgos para las libertades, que no provienen sólo, ni mayoritariamente, de los poderes públicos sino también de las empresas y otros ciudadanos. No se trata desde luego de una novedad absoluta, pues frente a una creencia algo simplificadora de que los derechos fundamentales solo existen frente al Estado, es sabido de siempre que hay derechos que, casi en su esencia, llevan ínsito el poderse invocar frente a los demás (53).

Si hasta ahora hemos examinado la incidencia de la sociedad digital desde distintas perspectivas, que no todas tienen que ver con la protección de datos de carácter personal (la democracia, el mercado, la igualdad, el hombre aumentado, etc.), en el presente apartado se trata de centrarnos en una visión general de los derechos y libertades que pueden quedar afectados por el tratamiento de los datos de carácter personal. Esta perspectiva de la afección de los derechos por el tratamiento automatizado de los datos personales constituyó la primera señal de alarma de que determinados usos de las nuevas tecnologías podían entrañar riegos para las libertades y los derechos. La alarma sobre los datos personales se adelantó así a las cuestiones, de más amplio espectro, que suscita lo que hemos llamado la sociedad digital. Y se adelantó al marcar una línea roja que el empleo de la informática no debería traspasar.

El Derecho de la UE en la Directiva 95/46/CE y el Convenio 108 del Consejo de Europa, de 28-1-1981 (54) se referían a los derechos que el tratamiento automatizado podía comprometer. Pero en la Carta de los derechos fundamentales de la Unión europea se cambia en su artículo 8 el

---

anunciado nuevo libro «Ten Arguments for Deleting Your Social Media Accounts Right Now», Ed. Henry Holt&Co.

(52) En realidad no es tal paradoja o, en todo caso, no es muy diferente de la que condujo a Rousseau desde defender las excelencias y ventajas del estado de naturaleza en el «Discurso sobre el origen y los fundamentos de la desigualdad entre los hombre» y en el «Emilio» a concluir legitimando el fin de ese ideal estado de naturaleza, con el sometimiento a normas, en «El Contrato Social»; si bien sobre la base de la común y general aceptación de tales normas creadas libre y precisamente por los hipotéticos firmantes de tal contrato.

(53) *Vid.* De la Quadra-Salcedo Fernández del Castillo, Tomás, «Derecho publico, derecho privado y derechos fundamentales», en *Revista General de Derecho Administrativo*, núm. 34, 2013; del mismo autor «El recurso de amparo y los derechos fundamentales en las relaciones entre particulares», Ed. Civitas, 1981.

(54) «Artículo 1.º Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales».

modelo, dando autonomía, en cierto modo, al derecho, al denominarlo como «derecho a la protección de los datos de carácter personal» sin describir en qué consiste su contenido, ni referirse en absoluto a los demás derechos clásicos.

En el nuevo Reglamento 2016/679 en su artículo 1.1 sobre la protección de la persona física respecto del tratamiento de los datos personales (sin aludir expresamente a los derechos clásicos y concretos a que se refiere con tal protección) y en el artículo 1.2 de lo que se habla es de la protección «*de los derechos y libertades fundamentales de la persona física y, en particular»,* de *«su derecho a la protección de datos»,* lo que supone que al nuevo reglamento de protección de datos no le basta con referirse a éstos, sino que vuelve a retomar y referirse directamente a los derechos y libertades fundamentales de la persona, de los que la protección de datos sería una parte. Tal vez una sinécdoque.

Todo ello no refleja otra cosa sino la evolución en la búsqueda de un *nomen iuris* para un nuevo derecho; búsqueda en la que la doctrina participó fijándose sobre todo en categorizar de forma más rigurosa la nueva garantía o el nuevo derecho con denominaciones autónomas como «autodeterminación informativa», «libertad informática», «habeas data», etcétera.

Sea como fuere el derecho a la protección de datos en sus sucesivas denominaciones no hace sino poner de manifiesto que está y sigue estando en proceso de construcción, porque los riesgos a proteger son dinámicos en cuanto varían en función de las nuevas aplicaciones.

En todo caso, los desarrollos del mundo digital y su empleo generalizado van ya más allá de los primeros riesgos atisbados, en la medida en que afectan a la democracia misma, al mercado, a los medios de comunicación, etc. Implican, además, otras dimensiones como el derecho al trabajo, a la desconexión, a la regulación de los perfiles o lo que se ha llamado el derecho al olvido que suponen una percepción más profunda sobre los riesgos existentes; y en cierto modo un opción moral y colectiva nueva sobre la sociedad que queremos y el concepto de persona humana y de humanidad que se sostiene (55).

No se pretende aquí analizar la cuestión de la concreta regulación de la protección «de los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales» (denominación del art. 1.2 del Reglamento 2016/679), sino destacar cómo en un momento más avanzado de la sociedad digital –que va mucho más allá

(55) *Vid.* a ese respecto Habermas, Jürgen, «El futuro de la naturaleza humana», Paidós, 6.ª imp., 2016, que, aunque referido a la genética, tiene reflexiones trasladables al ámbito de la sociedad digital. El hipotético hombre «mejorado» genéticamente suscita consideraciones sobre el futuro de la naturaleza humana que no son muy diferentes de las que pueden plantearse respecto del hipotético hombre «aumentado» o «potenciado» merced a aplicaciones de la sociedad digital.

del «uso de la informática» del artículo 18.4 de nuestra Constitución– la nueva regulación que se contiene en el Reglamento 2016/679 refleja en muchos momentos los nuevos riesgos que se derivan, no ya solo del tratamiento de los datos personales, sino de las nuevas técnicas de la sociedad digital.

Como antes se señalaba, el derecho a la protección de datos es un derecho en construcción, casi podríamos decir que en permanente construcción; al menos mientras la sociedad digital siga aportando y añadiendo nuevas técnicas y descubrimientos. Lo que en este apartado se quiere destacar son algunas de las nuevas aportaciones que el Derecho ha tenido que hacer durante estos años –concretadas en gran parte en el nuevo Reglamento 2016/669 de 27 de abril– ante la urgencia de dar respuesta a las nuevas técnicas y aplicaciones que, por entrañar nuevos riesgos, hacían necesario ampliar la regulación existente. Es el caso de los buscadores y el derecho al olvido, la igualdad y el tratamiento masivo de datos que permite predecir conductas y crear perfiles, las redes sociales y el consentimiento, el internet de las cosas, o la regulación de los tratamientos no consentidos ni autorizados específicamente por el Derecho.

Cada una de esas previsiones del Reglamento es la respuesta a la aparición de nuevas aplicaciones o servicios que multiplican los efectos y riesgos del tratamiento en forma no prevista o no prevista con suficiente claridad ni en el 18.4 de nuestra Constitución, ni en la derogada Directiva 95/46/CE.

2.5.1 Derecho al olvido

Es el caso, en primer lugar, del llamado derecho al olvido cuya construcción (56) viene determinada sobre todo por la creciente importancia de los buscadores. Sin buscadores los datos que pudieran existir en un archivo podían tener consecuencias en algún momento, pero no era algo por lo que los afectados se hubieran sentido inquietados. Una vez que los buscadores se generalizan y lo hacen con una enorme eficacia, el problema emerge con una fuerza arrolladora: la persona a que se refiere la sentencia del Tribunal de Justicia de la UE de 13 de mayo de 2014, como tantas otras antes y después, percibe de forma real y palpable como algo negativo que una determinada peripecia de su historia personal esté en la plaza pública a la vista de todos. Peor todavía que en la plaza pública, pues un exceso de información es ausencia de información, pero el nombre del Sr. X era buscado básicamente por aquellos que querían realizar un contrato, crear una sociedad, contratar un alquiler con dicho Sr. y en un buscador encontraban un dato de hacía ya

(56) Se trata en efecto de una construcción jurisprudencial del Tribunal de Justicia en asunto iniciado por la intervención de la Agencia española de protección de datos. *Vid.* STJUE 13 de mayo de 2014, Asunto C-131/12.

mucho tiempo que amenazaba con perseguirle toda la vida, comprometiendo sus expectativas de relaciones personales, comerciales y mercantiles.

La tensión entre el derecho a la información y el derecho a la intimidad, al buen nombre e imagen es evidente. Y la solución del conflicto no era tan fácil como pueda hoy parecernos, desde el momento en que se trataba de una información no ya veraz, sino cierta. Hasta la aparición del tratamiento de los datos y de los buscadores, el tiempo y del espacio, como decía la exposición de motivos de nuestra primera Ley Orgánica 5/1992, de 29 de octubre, eran los instrumentos naturales del olvido, que permitían a las personas continuar adelante sin llevar eternamente la carga de sus pequeños o grandes errores o, simplemente, de su historia.

Incluso en el caso de los autores de un delito que debía quedar registrado, era el propio Ordenamiento jurídico el que favorecía su olvido, pasado algún tiempo sin haber incurrido en delito alguno.

En esa perspectiva los buscadores en la sociedad digital hacen imposible el olvido de cualquier pequeño error o, sin ser error, de cualquier comportamiento del que su autor ha querido apartarse para siempre; el pasado se erige en fantasma vengador y en todo caso en condicionante del futuro, pues le persigue para siempre, sin la protección que la naturaleza le ofrecía: el tiempo y el espacio.

No se trata aquí de analizar ni la sentencia ni la regulación incorporada al artículo 17 del nuevo Reglamento 2016/679; se trata solo de subrayar que la regulación de tal derecho al olvido implica un modo de abordar la cuestión que tiene que ver con el conjunto de valores que inspiran las sociedades de los países de la UE. No es, desde luego y por ahora, la visión del problema que se tiene en los Estados Unidos de América. En cierto modo es una opción del legislador, pero que viene predeterminada porque el Tribunal de Justicia, supremo intérprete de los Tratados, ha entendido que de la vieja Directiva interpretada a la luz de los valores y principios de la UE se puede desprender tal derecho. Nada que reprochar a esa interpretación, muy al contrario, solo destacar el papel que en esa afirmación desempeña el conjunto de valores y principios de la Unión, que lleva a una conclusión –el reconocimiento del derecho al olvido– que es, en cierto modo, una opción por unos determinados valores que el Tribunal encuentra en la Carta o en los derechos y libertades del conjunto de los Estados miembros.

El hecho de que tenga su origen en una sentencia del Tribunal de Justicia, en veste de Tribunal Constitucional en cuanto supremo intérprete de los Tratados, hace que tendamos a verlo no como una opción, sino como algo que era obligado y que el Tribunal de Justicia no ha tenido más remedio que constatar. Pero siendo ello así, desde luego, no es menos cierto que esa constatación se hace desde una interpretación que se produce en un contexto de valores comunes y de comprensión de la per-

sona humana que surge de un entorno social y cultural que lleva a esa interpretación. Como dice el artículo 3 del Código civil en la interpretación de las normas se tendrá en cuenta *«el sentido propio de sus palabras, en relación con el contexto, los antecedentes históricos y legislativos, y la realidad social del tiempo en que han de ser aplicadas, atendiendo fundamentalmente al espíritu y finalidad de aquellas»*. Esa apertura del Derecho a la realidad social del tiempo y al espíritu y finalidad de las normas obliga a tomar en cuenta principios, valores y cláusulas en que la dignidad de la persona humana y los derechos que le son inherentes, así como el libre desarrollo de la personalidad (art. 10 CE), llevan a una solución como la encontrada por el Tribunal de Justicia en última instancia y, previamente, por nuestros Tribunales en relación con el derecho al olvido (57).

2.5.2 La elaboración y aplicación de perfiles

El segundo caso de respuesta del Derecho en relación con la protección de los derechos fundamentales y libertades públicas ante los avances y desarrollos de la sociedad digital lo encontramos en el Reglamento 2016/679 en relación con la elaboración de perfiles y la eventual adopción de decisiones basadas en los mismos (art. 22 del Reglamento). Son muchos los considerandos (58) y artículos (59) que el Reglamento dedica a la cuestión de la elaboración de perfiles. Particularmente importante es el artículo 22.1 en cuanto reconoce a todo interesado el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles. Derecho que sin embargo se excluye en tres supuestos previstos en el 22.2. Por su parte en el número 3 y en relación con los supuestos excluidos en el 22.2 se prevé la garantía como mínimo del derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. De ahí derivan algunos que ya está consagrado el derecho a una explicación, lo que no es evidente, pues se refiere solo a los supuestos excluidos y, además, no es claro el significado y alcance de la intervención humana.

La nueva regulación supone un avance importante, pero no puede considerarse totalmente satisfactoria, pues no se refiere al derecho a una explicación eficaz del algoritmo, ni evita que este pueda acabar siendo relevante en la decisión final, al margen de la dificultad de impugnar una decisión que, basada en un algoritmo, no supone una motivación conven-

(57) La Sentencia de 13 de mayo de 2014 se dicta en una cuestión prejudicial suscitada por la Audiencia Nacional en la que se preguntaba entres otras cosas por el alcance del derecho de cancelación y oposición.

(58) Considerandos 30, 38, 60, 63, 70, 71 a 73, 75 y 90.

(59) Artículos 4, 13.2 f), 14.2 g), 15.1 h), 21.1 y 2, 35.3, 47.2 e) y 70.2 f).

cional (60) pues exigiría impugnar el algoritmo mismo. Por otra parte se ha destacado mucho la existencia de prejuicios y discriminaciones directas, pero no se ha hecho tanto en relación con la cuestión de los errores de modelo base para la construcción del algoritmo o de los datos que se toman en cuenta en relación, todo ello, con su inadecuación al fin que se pretende o la licitud del fin (especialmente relevante en el caso de su eventual y discutible empleo por las Administraciones públicas) (61).

Tal vez sería necesario a esos efectos que, con carácter general, todo algoritmo dirigido a elaborar un perfil conllevara una memoria explicativa del fin y de los objetivos que se pretenden, así como la enumeración de las variables relevantes –12 por ejemplo– que tengan un peso conjunto más significativo (62). Eso está ya de alguna forma, aunque no es lo mismo, en la exigencia del artículo 13.2 f), 14.2 g) y 15.1 h) del Reglamento 2016/679 (63) tanto de informar, en el momento en que se obtengan datos personales para el tratamiento, sobre la lógica aplicada en los perfiles, como de hacerlo en cualquier momento. Añadir una memoria previa, general e igual para todos en que se exprese la finalidad y el objeto del algoritmo provee de un criterio funcional de crítica al mismo que puede ser relevante, sin afectar al secreto empresarial.

Se trata en definitiva de la respuesta del Derecho a las nuevas técnicas de inteligencia artificial que van más allá de la cuestión de la privacidad de sus datos personales. En efecto, en teoría, una decisión de negar un crédito, el acceso a un seguro, a un trabajo o unos estudios o un despido podría estar basado no ya en datos personales del solicitante, sino en *«perfiles»* obtenidos a partir de algoritmos y de miles o millones de datos personales, incluso anonimizados, que *«demostrarían»*, según el algoritmo, que el solicitante no debe ser admitido al crédito, el seguro, el trabajo o los estudios o despedido. Todo ello sobre la base de perfiles obtenidos a partir de millones de datos ajenos al solicitante pero que se aplican a la vista de los antecedentes de sus padres, el empleo de éstos, de sus estudios y su nivel cultural, el barrio en que viven los solicitantes en general, las multas de tráfico impuestas, las notas obtenidas, sus preferencias mu-

(60) *Cfr*. Goodman, Bryce y Flaxman, Seth en «European Union regulations on algorithmic decision-making and a "right to explanation"», en arXiv:1606.08813v3 [stat. ML] 31 Aug 2016.

(61) Puede recordarse el caso sobre la forma de establecer rankings de las Universidades, el modelo empleado y el peso de los distintos factores por la U. S. News que cuenta O'Neil, Cathy en «Armas de destrucción matemática…», *op. cit.*, pp. 66 y ss., y los errores y distorsiones del modelo que acabó imponiéndose durante mucho tiempo.

(62) Todo ello al margen de las directrices, recomendaciones y buenas prácticas sobre perfiles que el artículo 70.1 e) y g) del Reglamento prevé.

(63) En él se establece que el responsable del tratamiento facilitará al interesado información sobre «la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado».

sicales, las enfermedades padecidas, sus opiniones sobre diversos temas en redes sociales, etc., etc., etc.

En la elaboración del perfil no es preciso que se tengan en cuenta los datos personales del solicitante, sino los de millones de otras personas que llevan a la obtención de perfiles que permiten pronosticar con carácter general que el 75%, por ejemplo, de los que incurren en un determinado perfil, no cumplirán bien con sus obligaciones, fracasan escolarmente, contraen determinadas enfermedades, etc., por lo que la computadora, una vez introducidos los datos concretos del solicitante, desaconseja la admisión o contratación de quienes incurran en ese perfil.

En la entrevista de admisión de una persona antes de admitirla puede ser preguntada por muchos de esos datos sin advertirle previamente del significado y valor que cada uno de ellos representa para el algoritmo (64) lo que puede determinar que una respuesta no cuidadosa o no matizada puede determinar su no admisión sobre la base de un perfil que, incluso aunque esté bien hecho y libre de sesgos, condena al 25% que en ningún caso incurrirían en el pronóstico que se deriva del perfil.

Una persona concreta queda marcada no por lo que ella es o ha hecho, sino por lo que, estadísticamente, otros han hecho. Todo ello es inquietante y es la inteligencia artificial y los nuevos avances de la sociedad digital, lo que obliga al Derecho a dar una respuesta a un problema antes no contemplado. En efecto, no se trata ya del tratamiento de los datos del solicitante, pues es probable que ni siquiera sus datos hayan sido tratados para determinar el algoritmo, sino que al mismo se le aplica un perfil previamente establecido que determina que, a la vista de determinadas características de la persona que se somete a la entrevista o rellena un impreso con los datos que se le preguntan, dicho solicitante no debería ser admitido o aceptado a un trabajo, a unos estudios o a una póliza de seguro o de salud. La persona en cuestión cuando hace su solicitud o es entrevistada acepta y consiente normalmente facilitar los datos que le piden en ese momento; pero con esos datos puede quedar excluido al no encajar en el perfil de admisión.

Dejando aparte los perfiles que puedan establecerse por razones de mercadotecnia (salvo la mercadotecnia directa del artículo 21.2 del Reglamento) o publicidad, son especialmente relevantes los perfiles que pueden servir para acceder a un empleo, a un seguro, a unos estudios, etc.

Son muchos los derechos y libertades aquí en riesgo. Desde luego el derecho al trabajo, el derecho a la salud mediante la contratación de una póliza y los derechos de la personalidad. Junto a todo ello está también el derecho a la igualdad y al libre desarrollo de la personalidad, en el que nos

(64) Según la RAE algoritmo es un «conjunto ordenado y finito de operaciones que permite hallar la solución de un problema».

centraremos a continuación, no sin antes advertir que es posible que en relaciones entre particulares (Drittwirkung) (65) no siempre se pueda invocar el derecho a ser contratado para un trabajo o un seguro; pero ello no quita que incluso en esas relaciones sí pueda existir ese derecho (por ejemplo a no ser despedido sin causa o por causa de un perfil no explicado) especialmente cuando en la fórmula del perfil subyazca alguna forma de discriminación lo que no es inhabitual en los perfiles (66) al margen de la cuestión de oportunidad de reconstruir el concepto mismo de discriminación.

2.5.3 El derecho a la igualdad

La problemática de los perfiles debe ser examinada también con el prisma del derecho fundamental a la igualdad. Hasta ahora el derecho a la igualdad se concretaba en no sufrir discriminación por razón de nacimiento, raza, sexo, religión, opinión o cualquier otra condición o circunstancia personal o social. Lo que ocurre con los perfiles es que las razones de la exclusión basada en perfiles –suponiendo que no haya sesgos que incurran en alguna de las cinco primeras razones– podría no encajar en las categorías nominadas (las cinco primeras), quedando por ver si lo puede ser en las residuales, genéricas e innominadas del artículo 14 de la Constitución consistentes en «cualquier otra condición o circunstancia personal o social».

La persona que de acuerdo con un perfil no está indicada para ser admitida en un trabajo o está indicada para ser despedida no es claro si encaja en la idea de ostentar una determinada condición o circunstancia personal o social. Sin embargo, lo cierto es que el perfil que se toma en cuenta para admitirle o no, o despedirle –al margen del sexo, raza, religión o ideas– crea una nueva categoría o condición que hasta ahora no está claro si era personal o social, pero que desempeña los mismos efectos o consecuencias, estigmatizando a la persona que encaja en el perfil de no admisión o de despido, al margen de que ese perfil no pretenda afirmar

(65) *Vid.*, sobre la *Drittwirkung*, Quadra-Salcedo, Tomás, «El recurso de amparo y los derechos fundamentales», Ed. Civitas, 1981; también Alfaro Águila-Real, Jesús, «Autonomía privada y derechos fundamentales», en *ADC*, 1993, pp. 57-122; Bilbao Ubillos, Juan María, «La eficacia de los derechos fundamentales frente a particulares», *CEC*, Madrid, 1997, y «Prohibición de discriminación y relaciones entre particulares», en *Teoría y realidad constitucional*, 2006, pp. 147-198 y «Prohibición de discriminación y derecho de admisión en los establecimientos abiertos al público», en *Derecho Constitucional para el siglo XXI: actas del VIII Congreso Iberoamericano de Derecho Constitucional* (coord. por Joaquín Urías Martínez, Manuel Carrasco Durán, Manuel José Terol Becerra, Francisco Javier Pérez Royo), Vol. 1, 2006, pp. 819-842; Salvador Coderch, Pedro (coord.), «Asociaciones, democracia y Drittwirkung», en *Asociaciones, derechos fundamentales y autonomía privada* (Salvador Coderch, coord.), Madrid, 1997, pp. 55 y ss. Sobre el mismo tema en Alemania Hesse, Konrad, *Derecho Constitucional y Derecho Privado*, trad. e introduc. de Gutiérrez Gutiérrez, Madrid, 1995; y Von Münch, Ingo, «Drittwirkung de derechos fundamentales en Alemania», en *Asociaciones, derechos fundamentales y autonomía privada* (Salvador Coderch, coord.), Madrid, 1997, pp. 30 y ss.

(66) *Vid.* Cain Miller, Claire, «When Algorithms Discriminate», *The New York Times*, 9 de julio de 2015 en https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html?_r=0

que el 100% de quienes encajan en él vayan a incurrir en el defecto que determina recomendar no admitirle o despedirle. Bastará, posiblemente, que la probabilidad de incurrir en ese defecto sea del 51% (probablemente bastaría que fuera del 30%) para que se recomiende la no admisión.

Ello plantea el reto de interpretar si los perfiles han creado una nueva razón de discriminación objetiva en la medida en que permiten incluir en un colectivo –no predeterminado por las razones clásicas de sexo, edad, raza, etc.– construido sobre la base de razones de probabilidad estadística (pronóstico estadístico) de fallos o defectos (voluntarios o involuntarios) de comportamiento. Por tanto alguien podría argüir que el colectivo en sí mismo no carece de causa (causa como la raza, el sexo, la edad, etc.), sino que tiene una causa que lo hace legítimo. La cuestión es que admitir tal cosa sobre la base de un cálculo estadístico de probabilidades del 30% o del 51%, supone condenar al 70% ó 49 % restante respectivamente con un lastre que es sólo un pronóstico y que no ha hecho nada para merecerlo; por no entrar en los sesgos que puede tener la inteligencia artificial a la hora de establecer los perfiles o los datos que se han suministrado a la computadora para que llegue a tal conclusión (67).

Frente a estos nuevos retos el Reglamento reacciona a lo largo del articulado y de los considerandos poniendo límites al empleo de perfiles tanto a la hora de recolectar datos que sirvan para crear los perfiles como a la hora de aplicarlos. Así lo hace mediante distintas técnicas: la información al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración (68), la posibilidad de salir en cualquier momento del tratamiento a esos efectos si lo ha consentido mediante oposición del interesado, el derecho a no ser objeto de decisiones basadas únicamente en perfiles (art. 22), la obligación para el responsable de realizar estudios de impacto (art. 35), la obligación de la Autoridad de

(67) Sobre los sesgos puede verse. entre muchos otros O'Neil, Cathy, «Armas de destrucción matemática…», *op. cit.*, pp. 81 y ss.

(68) En el considerando 71 entre los fines de los perfiles se reconocen los de

[71] «analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar»;

«el responsable del tratamiento debe utilizar procedimientos matemáticos o estadísticos adecuados para la elaboración de perfiles, aplicar medida técnicas y organizativas apropiadas para garantizar, en particular, que se corrigen los factores que introducen inexactitudes en los datos personales y se reduce al máximo el riesgo de error, asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado y se impidan...»;

[91] «evaluación de impacto. Lo anterior debe aplicarse, en particular, a las operaciones de tratamiento a gran escala que persiguen tratar un cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados y entrañen probablemente un alto riesgo, por ejemplo, debido a su sensibilidad, cuando, en función del nivel de conocimientos técnicos alcanzado, se haya utilizado una nueva tecnología a gran escala y a otras operaciones de tratamiento que entrañan un alto riesgo para los derechos y libertades de los interesados».

control de contemplar la cuestión de la elaboración de perfiles en sus normas corporativas (art. 47) y la atribución de funciones (art. 70) al Comité Europeo de Protección de datos para emitir directrices, recomendaciones y buenas prácticas en relación con los criterios y requisitos de las decisiones basadas en perfiles, en virtud del artículo 22, apartado 1.

Todas esas previsiones tratan de poner límites al uso y aplicación de perfiles, aunque debe notarse que presuponen su existencia pues el artículo 22.2 b) deja la puerta abierta a su empleo, sin aplicar la previsión del apartado 1.º, cuando el Derecho de la Unión o el del Estado miembro lo autorice siempre que se establezcan medidas adecuadas para salvaguardar derechos y libertades. Esta escotilla que se abre, de impreciso alcance, refleja la dificultad de evitar el empleo de perfiles –probablemente por el derecho de las empresas de aplicar técnicas de IA a los datos que recolectan con funciones de, inicialmente, solo publicidad y mercadotecnia– pero ni está claro su alcance futuro al aplicarlos ni su eficacia para evitar sesgos, errores y discriminaciones.

Con todo subsisten al menos varias cuestiones de gran trascendencia. De una parte que el artículo 22.1 del Reglamento 2016/679, aunque reconoce al interesado el derecho a oponerse a una decisión basada únicamente en perfiles, no impide que el perfil sea uno de los elementos a tomar en cuenta en la decisión con lo que al final el perfil puede tener la última palabra. De otra que el tema de la elaboración de los perfiles y los criterios y algoritmos en que se basan o la determinación del Big Data a partir del cual se han construido no son objeto de ningún desarrollo, salvo la somera referencia en el artículo 70.1 f) a las directrices y recomendaciones y buenas prácticas en relación con la toma de decisiones basadas en perfiles (69). Nada sin embargo sobre el proceso mismo de elaboración de los perfiles, ni de su aplicación a una persona concreta, cuando son numerosos los expertos que han denunciado los sesgos y errores de todo tipo en que incurren muchos de esos algoritmos. Ello suscita la demanda creciente de regular un derecho a explicación que obligue a desvelar la lógica del algoritmo, tanto el modelo del que se partía como de otros aspectos del procedimiento de suministro de datos (70) a la computadora.

(69) *Vid.* Goodman, Bryce y Flaxman, Seth, «European Union regulations on algorithmic decision-making and a "right to explanation"», en https://arxiv.org/abs/1606.08813 del Archivo de la Cornell University Library; también el interesante informe y propuesta de Wachter, Sandra, Mittelstadt, Brent, y Floridi, Lucianen, en «Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation», en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469. También Chiel, Ethan, «EU citizens might get a "right to explanation" about the decisions algorithms make», en http://fusion.net/story/321178/european-union-right-to-algorithmic-explanation/

(70) *Vid.*, entre muchos otros, O'Neil, Cathy, «Armas de destrucción matemática. Cómo el Big Data aumenta la desigualdad y amenaza la democracia», Ed. Capitan Swing, 2017, pp. 131, 153 y 175.

Finalmente está la cuestión de los límites al empleo de perfiles en la Administración, ya que en ese contexto el mérito y la capacidad no parecerían ser compatibles con pronósticos. Si en las relaciones entre particulares su posición puede llegar a ser distinta, aunque ello admita excepciones, en el caso de la Administración la situación no puede ser la misma.

2.5.4 La regulación del consentimiento

El cuarto caso de respuesta del Derecho en relación con la protección de los derechos fundamentales y libertades públicas ante los avances y desarrollos de la sociedad digital que ofrece el Reglamento lo tenemos en el reforzamiento del consentimiento para el tratamiento de datos que se contiene en los artículos 5 a 9 del Reglamento 2016/679. Tal reforzamiento obedece, en gran parte, al desarrollo descomunal de las redes sociales y a los datos de carácter personal que en ellos se registran al inicio y, sobre todo, los que se van produciendo sobre la base de las opiniones (los *like)* que se van incorporando o los comentarios que allí se vierten (71).

De la importancia de todo ello tenemos un reciente ejemplo en el escándalo de Facebook y la cesión de sus datos a la empresa Cambridge Analytica que han servido para influir en las elecciones presidenciales americanas y en el referéndum para el Brexit.

Parece que no más de trescientos mil usuarios de Facebook habrían dado permiso para el tratamiento de sus datos, sobre la base de un programa experimental, pero, a partir de ahí Cambridge Analytica ha podido acceder a los datos personales de 50 millones de usuarios y de esa forma influir de forma significativa en el proceso democrático (72).

Las previsiones del Reglamento van dirigidas a precisar mucho más las condiciones para recabar y prestar el consentimiento, pero probablemente a la vista del escándalo haya que adoptar medidas adicionales. En todo caso el Reglamento amplía considerablemente las exigencias y requisitos para el consentimiento y la transparencia exigida a la hora de informar a los usuarios sobre la finalidad del tratamiento que se da a sus datos.

El funcionamiento de las redes sociales y su aparente gratuidad descansa en el valor de los datos que obtienen y que luego pueden servir para

(71) *Vid.* Megías Terol, Javier, «Privacy by design, Construcción de las redes sociales garantes de la privacidad», en *Derecho y redes sociales*, 2.ª ed., 2013 pp. 74 y ss.; también en la misma obra Martínez Martínez, Ricardo, «Protección de datos personales y redes sociales: Un cambio de paradigma», pp. 114 y ss.

(72) Según el Huffington Post del 20 de marzo de 2018 «300.000 usuarios pudieron descargarse la aplicación *thisisyourdigitallife*, que les sometía a un exhaustivo test de personalidad político, por lo que recibieron entre 2 y 5 dólares. Pero la app recabó información, no sólo de esos usuarios que habían dado su consentimiento a que se recogieran sus datos para fines académicos, sino los de sus contactos en Facebook, un total de 50 millones de perfiles que Kogan, según la red social, proporcionó a la consultora Cambridge Analytica a través de su empresa, Global Science Research».

venderlos a terceros o cederlos a empresas subsidiarias que a partir del tratamiento de tales datos, con técnicas de IA, permiten hacer estudios de mercado y de su evolución de gran exactitud o bien preparan campañas de publicidad personalizada en función de las preferencias y perfiles de los usuarios de tales redes.

Aunque las percepciones en torno al uso de las redes sociales y sus riesgos comienzan a cambiar, hasta ahora han sido vistas por la gran mayoría como una especie de ámbito privado y reservado. Por otra parte sin una clara conciencia de las consecuencias de las opiniones que en ellas se vierten o con indiferencia, cuando son utilizadas por jóvenes, de las consecuencias que pueden tener para su futuro.

No es el campo de la privacidad el único que ha experimentado daños como consecuencia del uso de las redes sociales (73), también otros derechos han sufrido las consecuencias o se han puesto en peligro otros derechos, bienes y valores a partir de la creencia de estar actuando en un ámbito privado (74). Es el caso de la propiedad intelectual (75) o el caso de nuevas conductas que ponen en peligro el honor y la seguridad de las personas con comportamientos nuevos y peligrosos en el caso de los menores (76) como el caso de los ciberacosos (*ciberbullying*) (77) o extorsión *(grooming*) que supone formas de agresión psicológica a otros, generalmente menores o adolescentes, cometidas a veces por otros menores y en ocasiones con resultados trágicos.

Todo ello obliga a establecer respuestas y, entre ellas, son importantes las relativas a la identificación del origen de la agresión, pero por otra parte abre un debate acerca de qué responsabilidad cabe a los titulares de las redes y plataformas en general (YouTube sería un ejemplo) para poner fin a conductas irregulares o agresivas o lesivas de derechos de terceros (por no hablar de terroristas) en cuanto tienen noticia de que está ocurriendo algo no admisible en su red. En casos patentes parece claro que la obligación de actuar puede no ser discutible, pero puede haber casos grises en los que atribuirle potestad de intervención puede equivaler a otorgar poderes de censura a un particular que el artículo 20.2 de la Constitución prohíbe.

---

(73) *Vid.* Herrán Ortiz, Ana Isabel, en «Las redes sociales digitales: ¿hacia una nueva configuración de los derechos fundamentales en Internet?» en *Revista Vasca de Administración pública*, núm. 87-88/2010, pp. 521-566.

(74) *Vid.* Martínez Otero, Juan María, «Derechos fundamentales y publicación de imágenes ajenas en las redes sociales sin consentimiento», *Revista Española de Derecho Constitucional*, núm. 106, Madrid, enero/abril (2016), pp. 119-148; también Upegui Mejía, Juan Carlos, «Libertad de expresión, redes sociales y derecho penal. Estudio del caso Nicolás Castro», en *Revista Derecho del Estado*, núm. 25, diciembre de 2010 (Universidad del Externado, Bogotá) pp. 159-192.

(75) *Vid.* Xalabarder Plantada, Raquel, en «Redes sociales y propiedad intelectual», en *Derecho y redes sociales*, *op. cit.*, pp. 357 y ss.

(76) *Vid.* Gil Antón, Ana María, «El fenómeno de las redes sociales y los cambios en la vigencia de los derechos fundamentales», *Revista de Derecho Uned*, núm. 10, 2012.

(77) Pardo Albiach, J., *Ciberacoso, la tutela penal de la intimidad, la integridad y la libertad sexual en Internet*, Valencia, 2010. pp. 56 y ss.

Habría que considerar también la cuestión de las noticias falsas (*fake news*) que difunden personas o *bots* (falsas cuentas que no corresponden a persona alguna, pero que sirven para difundir mensajes) y los medios de identificación con que se cuenta. El anonimato es desde luego un derecho, pero no puede servir para garantizarse la inmunidad. Una regulación más clara sería necesaria que respete el derecho al anonimato en el tráfico exterior, pero garantice la identificación en determinados supuestos. Todo ello sin perjuicio de detectar los «*bots*» en cuanto se pueda y bloquear su mensajes y noticias. Respecto de las demás noticias falsas no es fácil imponer a los titulares de las redes la obligación de verificar la noticia para retirarla –lo que no es claro que pueda hacer– pero sí la de señalar si tal noticia es reproducción de otra procedente de fuente autónoma que no sea repetición de la misma o si ha habido quejas de otras personas aludiendo a que la noticia es falsa.

Todo ello suscita cuestiones nuevas de fondo y algunas organizativas como la relativa a si el control de todo ello debería corresponder al poder judicial como todo lo que afecte a derechos fundamentales o si puede establecerse alguna Autoridad independiente que sea capaz de analizar los supuestos y proponer a un juez que resuelva sobre qué solución dar a los conflictos, de forma que el juez se encuentre con parte del trabajo hecho a la hora de resolver (78).

2.5.5 Las plataformas de la llamada economía colaborativa y el derecho al trabajo

No se trata aquí, a diferencia de los casos anteriores, de una cuestión que haya abordado el Reglamento, pero sí se trata de una cuestión que ha suscitado una gran controversia en el ámbito de los transportes y en el ámbito de los apartamentos turísticos. Se trata de lo que se ha dado en llamar la economía colaborativa (79) y ha suscitado entusiastas y detractores.

En el campo del transporte han sido los taxistas profesionales los que se ha opuesto en España y en la mayor parte de los países del mundo a este tipo de servicios que considera que es una forma de competencia desleal. Por su parte los clientes o usuarios del servicio se muestran muy satisfechos por su puntualidad, limpieza y calidad.

---

(78) *Vid.* artículo 158.1 de la Ley de propiedad intelectual que atribuye competencias a la sección 2.ª de la Comisión de Propiedad Intelectual –cuyos actos son impugnables ante la Audiencia Nacional– para la salvaguarda de los derechos de propiedad intelectual frente a su vulneración por los responsables de servicios de la sociedad de información en los términos previstos en los artículos 8 y concordantes de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Al Tribunal se le somete, para su decisión final, un acto que ha podido adoptarse con rapidez y por expertos en la materia.

(79) *Vid.* Montero Pascual, J. J. (Dir.), *La regulación de le economía colaborativa. Airbnb, BlaBlaCar y otras plataformas*, Tirant lo Blanch, Valencia, 2017.

En el ámbito de los apartamentos turísticos son los hoteleros las comunidades de propietarios –que sufren el trasiego diario de ocupantes nuevos, ocasionales y, a veces, ruidosos– y, en ocasiones, los Ayuntamientos quienes se quejan. Del mismo modo los usuarios obtienen precios más baratos, por lo que están satisfecho con las prestaciones que reciben.

Algunas Comunidades autónomas han establecido regulaciones limitativas al respecto y lo mismo han hecho algunos Ayuntamientos que se quejan de un exceso de turismo, especialmente el de Barcelona.

La UE no ha establecido ninguna normativa al respecto por lo que, hasta ahora deja que sean los Estados los que tomen iniciativas al respecto.

Ha sido sin embargo el Tribunal el primero que se ha pronunciado sobre la cuestión prejudicial suscitada por un Juzgado de Barcelona dictando el pasado 20 de diciembre de 2017 Sentencia en el asunto C-434/15 declarando que el servicio de UBER, no es un servicio de la Sociedad de la Información sino un servicio de Transporte por lo que queda excluido del ámbito de la Directiva 2006/123 de servicios. Con esa declaración UBER no puede aplicarse las ventajas que dicha Directiva supone para todos los servicios.

Ello no quita para hacer una reflexión acerca de cómo la sociedad digital abre la puerta a nuevas formas de actividad que tienen grandes efectos en el mercado de trabajo o en el sistema económico en general. En el caso de los taxistas, que eran los recurrentes en Barcelona, eran sus puestos de trabajo los que quedaban comprometidos. Con la sentencia citada queda en manos de las Comunidades autónomas establecer las reglas para que en ese ámbito de los transportes haya un cierto equilibrio de prestaciones.

En el caso de los apartamentos o pisos de alquiler el problema puede ser similar con la gran diferencia de que no estamos en el ámbito de los transportes.

Sea como fuere hay un impacto también en el sector hotelero que habrá que afrontar. El fenómeno de la economía colaborativa tiene defensores entusiastas (80) y otros detractores o al menos conscientes de los problemas que causa (81). En efecto, al margen de la pérdida de puestos de trabajo que pueda suponer, implicará también un cambio en las relaciones de trabajo o su desaparición y transformación en relaciones mercantiles cualquiera que sea su calificación (82). La cuestión es si se trata de relaciones mercantiles entre iguales y si una de las partes ostenta una posición de monopolio u oligopolio –el titular de la plataforma que hace de

(80) *Vid.* Rifkin, Jeremy, en «La sociedad de coste marginal cero: el internet de las cosas, los bienes comunes y el eclipse del capitalismo», Ed. Paidós Ibérica.

(81) Es el caso de Ferry, Luc, «La revolución transhumanista. Cómo la tecnomedicina y la uberización del mundo van a transformar nuestras vidas», Ed. Alianza, 2017 pp. 113 y ss., donde critica a Rifkin tanto por su visión benefactora de UBER, como por su adelanto en pronosticar el fin del capitalismo.

(82) *Vid.* Montero Pascual, Juan José, «La regulación de las plataformas colaborativas», en *Revista de privacidad y derecho digital*, núm. 9, año 2018.

intermediario entre el usuario y el propietario del coche o del apartamento– como para imponer a la otra las condiciones.

3. EL DERECHO FRENTE A LAS CONSECUENCIAS DE LA INCIDENCIA DE LAS TECNOLOGÍAS, SERVICIOS Y DISPOSITIVOS DIGITALES EN LA INTERPRETACIÓN Y APLICACIÓN DE LOS VALORES SUPERIORES DEL ORDENAMIENTO JURÍDICO Y EN LOS DERECHOS Y LIBERTADES FUNDAMENTALES

La perspectiva general adoptada en el presente trabajo debe concluir considerando el papel del Derecho ante las consecuencias, en muchos casos disruptivas, que se derivan del uso de las tecnologías y medios de la sociedad digital que es ya la sociedad en que vivimos. Ahora bien, la constatación que hemos hecho en los apartados anteriores es que el surgimiento y desarrollo de la sociedad digital con dispositivos, servicios, aplicaciones y con la inteligencia artificial (IA) traspasa y afecta al entero funcionamiento y articulación de las relaciones sociales, políticas y económicas de una sociedad tal cual era antes del advenimiento de tal sociedad digital. En realidad, afecta a todos los sectores de actividad (agricultura, industria, servicios), a casi todos los derechos de la persona, al funcionamiento del mercado y al funcionamiento mismo del sistema democrático.

La forma en que afecta a todo ello supone, en primer lugar, una mejora de todos esos ámbitos y campos de actuación lo que hace inevitable aprovechar sus enormes ventajas y posibilidades.

Ahora bien, a la vez que la sociedad digital presenta ventajas implica también la alteración de la forma de desarrollarse y funcionar todos esos ámbitos, relaciones y derechos; y lo hace creando riesgos de limitación de los derechos y libertades fundamentales, de alteración de las relaciones sociales, de alteración de funcionamiento del mercado y de alteración del propio sistema político. Esa afección a todos los elementos fundamentales que estructuran e informan nuestras sociedades hace obligatorio adoptar una perspectiva holística en el tratamiento de los retos que plantea la sociedad digital. Holística en cuanto un tratamiento separado de cada uno de los ámbitos que pueden ser afectados por la sociedad digital no reflejaría con precisión la dimensión del problema, pues no se limita a la suma de los riesgos y respuestas a dar en cada ámbito, sino que va más allá de dicha simple suma. La consideración separada de cada uno de los ámbitos y afecciones que en ellos se produce nos haría perder la perspectiva de conjunto, que no la percibimos con la mera suma del tratamiento individual de cada ámbito. La perspectiva de conjunto ofrece una visión más rica y completa en cuanto permite comprobar que estamos ante una sociedad, la digital, que determina y tiende a provocar cambios culturales y

civilizatorios (83), en el sentido de que propugna o tiende a cambiar la civilización entendida como *«conjunto de costumbres, saberes y artes propio de una sociedad humana»* que es el concepto de «civilización» de la Real Academia de la lengua.

Desde esa visión holística la respuesta del Derecho viene en cierta medida condicionada. Para empezar la respuesta del Derecho no sería completa si se limitara a proponer soluciones mediante la regulación de cada problema que se plantee en cada concreto ámbito. Tales regulaciones sectoriales deberán de existir (84), pero eso no significa que la dimensión holística a que se ha hecho referencia no aconseje una toma de posición general de la Constitución o del legislador sobre la cuestión de conjunto, estableciendo algunos principios y determinaciones generales, lo que nos lleva, en primer lugar, a la cuestión del contenido de esa toma de posición general. Asimismo obliga a considerar la cuestión de cuál debe ser el instrumento normativo para ese posicionamiento general; si de nivel constitucional o simplemente legal.

Antes de entrar en esa cuestión, deben subrayarse varias cosas.

La primera que la posición del Derecho –entendido aquí no tanto como ciencia o técnica, sino como el medio a través del cual se expresa la voluntad de lo que una comunidad considera que deben ser los criterios conforme a los cuales se organiza– debe ser la de favorecer, incentivar y sacar provecho de las tecnologías, instrumentos, programas y dispositivos que conforman el universo de la sociedad digital.

Por tanto, hay que evitar impedir o limitar su empleo, si no existe riesgo alguno para los derechos fundamentales y libertades que, de acuerdo con el artículo 10 de nuestra Constitución, son el fundamento del orden político y de la paz social. Ahora bien, precisamente porque se quiere potenciar el empleo y difusión de la sociedad digital –y en la medida que determinados usos de la misma pueden poner en peligro derechos, principios y valores fundamentales recogidos en nuestra Constitución– ello exige una regulación por el Derecho que, a la vez que garantiza el desarrollo y empleo de las técnicas e instrumentos propios de la sociedad digital, proteja dichos valores, principios y derechos.

La segunda cuestión a subrayar hace relación a que una regulación muy detallada, precisa e intervencionista en los momentos emergentes de la sociedad digital –y de sus técnicas e instrumentos– puede ser negativa en cuanto ahogue las posibilidades de desarrollo cuando todavía no se conocen bien todas sus posibilidades y efectos. En su lugar lo que hará

(83) En el Diccionario de la Real Academia el sufijo -torio, o -toria, en adjetivos denota relación con la acción del verbo base, en este caso civilizar.

(84) Pues, en todo caso, la solución en cada ámbito habrá de hacerse tomando en cuenta las características y peculiaridades de cada uno de ellos.

falta es establecer los principios generales de la regulación, así como determinar la conveniencia de emplear conjuntamente con regulaciones directas otras, en algunos casos, de autorregulación, preferentemente de autorregulación regulada (85), mediante las que con carácter previo se establezcan criterios desde los poderes públicos que deberán ser observados desde los distintos sectores de actividad.

La tercera cuestión tiene que ver con si es conveniente establecer algún organismo regulador para el desarrollo y funcionamiento de la sociedad digital, pues no siempre el legislador –ni el plano normativo– está en las mejores condiciones para culminar la regulación, por las peculiaridades técnicas que ofrece cada uno de los campos en que incide la sociedad digital y su constante evolución y progreso.

3.1 **Derechos, valores y principios que se quieren garantizar e instrumentos normativos para el desarrollo y funcionamiento de la sociedad digital**

La sociedad digital puede acabar provocando la puesta a disposición de unos pocos de unos instrumentos formidables de poder, dominación y control, incompatibles con los valores y principios superiores de nuestro ordenamiento: la libertad, la justicia, la igualdad y el pluralismo político.

Lo que para algunos, según se ha visto, es la tierra prometida del sometimiento a maquinas infalibles que dirijan la vida de los ciudadanos (86), no es sino una directa contradicción con los principios esenciales sobre los que descansa nuestro pacto social.

Sea o no, además, ese sometimiento a las máquinas una ensoñación imposible –o posible, pero, en todo caso, una pesadilla–, el modelo de un supuesto mundo feliz donde las máquinas y la inteligencia artificial sustituyan al ser humano, no se compadece con los valores superiores de nuestra convivencia, ni con la dignidad de la persona humana y los derechos fundamentales que le son inherentes.

Eso no supone que las máquinas y la inteligencia artificial no deban ser un poderoso medio para construir un mundo mejor y más justo, en el que los ciudadanos puedan lograr un más perfecto desarrollo de su personalidad y llevar a su plenitud la democracia. Las máquinas transforman los datos en informaciones accesibles y enormemente aprovechables, pero su

(85) *Vid.* Darnaculleta i Gardella, Mercè, en «La autorregulación y sus fórmulas como instrumentos de regulación de la economía», en *Regulación Económica*, Tomo I Fundamentos e Instituciones, Santiago Muñoz Machado y José Esteve Pardo (dir.), Iustel, 2009, pp. 631 y ss.

(86) *Vid.* los dataístas a que se refiere Harari en *Homo Deus*, *op. cit.*, y, según parece, el propio Harari. Pero en esa misma posición están los manifiestos de Asociaciones de Transhumanistas o posthumanistas en USA y en Europa, por lo que no se puede no considerar con seriedad la cuestión.

empleo sólo corresponde al conocimiento humano que es capaz de ponderar los juicios últimos morales y de valor.

El primer principio, la primera declaración, ante la emergencia de la sociedad digital que ha de hacerse, sea a nivel constitucional o legal, debe consistir en un compromiso doble. Por una parte el de potenciar al máximo, siempre en beneficio de los ciudadanos, el desarrollo, uso y empleo de la sociedad digital con todos sus medios e instrumentos. Por otra el de garantizar sin desfallecimiento todos los principios y valores fundamentales de nuestra convivencia recogidos en el artículo primero de la Constitución –y a lo largo de toda ella–, así como la dignidad de la persona humana con los derechos fundamentales que le son inherentes.

La igualdad es uno de esos derechos fundamentales que pueden quedar comprometidos con la aparición de técnicas que permitan el llamado aumento o potenciación de determinadas personas mediante su conexión a ordenadores con inteligencia artificial; lo que puede determinar la competencia en el mercado –incluido el mercado de trabajo– en condiciones desiguales.

Dado que la Constitución ya contiene esos principios, valores superiores y derechos fundamentales podría parecer innecesario cualquier instrumento normativo que insista en la proclamación de los mismos, incluida una reforma constitucional que tratase de reiterarlos formulándolos de nuevo en relación con su aplicación en las nuevas condiciones que se derivan del empleo de los medios digitales.

Sin embargo, no puede desconocerse que habría quien podría, por ejemplo, invocar su derecho a la producción y creación científica y técnica [art. 20.1 b) de la Constitución] –en relación con su libertad para emplear todos los medios que la ciencia y la técnica pongan a su disposición para el libre desarrollo de su personalidad– para sostener la imposibilidad de restringir o regular la sociedad digital ya que dificultaría su acceso a todas las posibilidades que las tecnologías le ofrecen. Ese concreto derecho del artículo 20.1 b) de la Constitución, invocado como un derecho fundamental, se pretendería contraponer al derecho de todos los demás a la igualdad o a no ver afectados sus derechos fundamentales por el empleo por el primero de su creación o de sus inventos.

Parecería así ser necesaria alguna determinación por parte del pueblo soberano o en su caso de los representantes del pueblo español, acerca de cuáles son los limites respectivos de los derechos y libertades cuando el ejercicio de alguno puede poner en cuestión los valores superiores del ordenamiento jurídico.

Parecería también necesaria una toma de posición omnicomprensiva de respuesta a los retos de la sociedad digital, porque nuestra Constitución, al igual que todas las Constituciones europeas, no contiene referencia alguna –por la época en que se aprobó– a la sociedad digital o a sus

medios o instrumentos, con la salvedad de la referencia que en el artículo 18.4 se contiene al uso de la informática. Referencia por cierto más bien defensiva frente a tal uso, si bien en la perspectiva de la protección de determinados derechos fundamentales. El artículo 18.4 CE habría sido así un adelantado de los problemas que provocan las nuevas tecnologías como presuntamente atentatorias a los derechos fundamentales.

Parece conveniente continuar reafirmando el compromiso con los derechos fundamentales, pero afirmando también el compromiso con la ciencia, sus avances y sus aplicaciones que no pueden presentarse como directamente contrapuestos a tales derechos fundamentales, siempre que, al contrario, se conciban al servicio de los mismos y de su concreción (derecho a la salud, la cultura, el medio ambiente, a la igualdad, etc.) en la medida que la sociedad digital puede contribuir decisivamente a hacerlos reales y efectivos (art. 9.2 de la CE).

No es la sociedad digital la que, directa y necesariamente, compromete los derechos, valores y principios fundamentales, sino determinados usos de los medios de tal sociedad que son los que se quieren regular.

Una norma constitucional o legal que proclame eso sería, así, muy conveniente para todo el desarrollo posterior de la regulación de la sociedad digital.

Ello nos lleva a la cuestión del rango de tal norma –constitucional o legal– lo que en buena parte corresponde a la prudencia política, pero no deja de ser oportuna alguna reflexión al respecto.

Desde luego sería muy necesaria una reforma constitucional si la actual Constitución impidiera al legislador infraconstitucional hacer una norma con contenidos regulatorios de la sociedad digital, lo que no parece ser el caso. Otra cosa es si alguna concreta determinación sobre el derecho de acceso a dicha sociedad o a sus precursores podría ser conveniente o necesaria; entendiendo por precursores el acceso a aquellas infraestructuras y soportes sin los cuales no es posible entrar o acceder a la sociedad digital.

3.2 **Sobre la existencia o no de obstáculos constitucionales para regular por Ley los derechos en la sociedad digital**

Lo cierto es que no parece que existan obstáculos constitucionales para que el legislador infraconstitucional pudiera regular los derechos en la sociedad digital con el argumento de que algunos otros derechos fundamentales reconocidos en nuestra Constitución (la producción y creación científica y técnica, por ejemplo) lo impiden en cuanto tal regulación suponga una restricción de los mismos. Al contrario, la normativa legal de que se habla lo que pretendería no es establecer limitaciones –en cuanto ablacio-

nes injustificadas de unos determinados derechos– sino encontrar sus límites (que no limitaciones o restricciones) en su articulación con los demás.

Ello no obstante, pudiera llegar a sostenerse por algunos que desde el punto de vista, por ejemplo, del derecho a la creación y producción científica y técnica o de la prohibición de censura previa (87) restringir su alcance no supondría determinar sus límites, sino una limitación, restricción o ablación –aunque fuera para proteger los demás derechos (intimidad, privacidad, honor, autodeterminación informativa, etc.) u otros valores o bienes constitucionales como la democracia o la competencia en el mercado– que exigiría una reforma constitucional.

No parece, sin embargo, que tal posición tenga fundamento, pues son los demás bienes y valores presentes en la Constitución los que han permitido que el Tribunal constitucional haya reconocido –sin que la Constitución lo haya recogido de forma específica en cada caso, salvo la genérica referencia en el artículo 10 al «respeto a los derechos de los demás»– que eventuales límites puestos por el legislador o por la jurisprudencia a algunos derechos fundamentales tienen su fundamento en la propia Constitución; en la necesidad de articular no sólo unos derechos con otros, sino también con otros bienes y valores.

En efecto, desde una interpretación sistemática de la Constitución cada derecho encuentra su límite en los demás derechos y en los derechos de los demás. Así por ejemplo, no es una limitación de la libertad de expresión la sanción civil o penal de la injuria, sino que es un límite o frontera natural del derecho; frontera determinada por otros derechos. Tampoco lo es la sanción penal por revelar secretos de la defensa –que no son en sí mismos ningún derecho fundamental, pero sí un bien constitucional– sin que nadie pueda invocar el derecho a dar veraz información de secretos militares para evitar esa sanción penal.

No habría, pues, estricta necesidad de una reforma constitucional para incorporar una referencia a la sociedad digital que permita limitar o regular algunos derechos con la finalidad de proteger otros por la incidencia de la sociedad digital. Por consiguiente, si no hay obstáculo constitucional para regular las condiciones de emergencia, desarrollo y aplicación de la sociedad digital –por razón de su incidencia en los demás derechos–, no parece necesaria, en principio, una reforma constitucional salvo que se

(87) La prohibición de censura previa del artículo 20.2 se vincula habitualmente con la libertad de expresión, pero no tendría por qué ser ese su único campo de aplicación. De hecho en el marco de la investigación biomédica hay limitaciones recogidas en el Convenio de Oviedo y en la Ley 14/2007, de 3 de julio, de Investigación biomédica que en su artículo 2 e) requiere previo y preceptivo informe favorable del Comité de Ética de la Investigación para autorizar el desarrollo de cualquier proyecto de investigación sobre seres humanos o su material biológico, lo cual podría ser interpretado como un tipo de censura en el ámbito de la investigación que sin embargo no es disconforme con la Constitución, en cuanto todo derecho tiene siempre sus límites en otros derechos o valores, siempre que no quede afectado su contenido esencial.

quisiera poner énfasis en la importancia y significado de la propia sociedad digital llevándola a la norma suprema.

No obstante de acometerse tal reforma constitucional, no puede olvidarse que todo texto constitucional se presta solo a proclamaciones breves y sumarias, que no añadirían nada demasiado significativo en una materia que exige muchos matices.

3.2.1 La limitada incorporación a la Constitución del concreto derecho de acceso a la sociedad digital como derecho fundamental

Cabe plantearse, por otra parte, si lo que hay que llevar al texto constitucional es algo más limitado, aunque relevante. En concreto el reconocimiento como derecho fundamental. en el capítulo primero del Título I de nuestra Constitución, del derecho de acceso a la sociedad digital, entendido básicamente como el derecho de acceso a lo que podríamos llamar sus precursores: es decir, a todos los instrumentos, dispositivos y posibilidades, que son la condición necesaria para beneficiarse de la sociedad digital.

Reconocimiento del derecho de todos a acceder a la sociedad digital– en el sentido indicado– que podría entenderse necesario para la realización efectiva de las posibilidades de igualdad y libre desarrollo de la personalidad de todos y cada uno; posibilidades de enorme relevancia individual y social en cuanto piedra angular de nuestros Estados de bienestar.

Desde ese punto de vista su incorporación como derecho fundamental al capítulo I del Título I de la Constitución, contribuiría a hacer efectivos todos los derechos, por una parte, y, por otra, sería una forma de exhibir ante el mundo los rasgos de una Constitución adecuada el tiempo que vivimos.

De todas formas, la efectividad de tal derecho de acceso a la sociedad digital no precisa, en rigor, de su incorporación a la Constitución como derecho fundamental, puesto que cualquier Ley sectorial –la Ley General de Telecomunicaciones, por ejemplo– podría reconocer en la práctica tal derecho (sin calificarlo como derecho fundamental) al incluirlo dentro del servicio universal, puesto que, en gran medida, el mismo se refiere básicamente a la disponibilidad y existencia de infraestructuras y servicios con capacidad, latencia o velocidad necesarias para soportar las demandas de servicios que la sociedad digital (servicios vinculados con coches inteligentes, cirugía a distancia, drones, internet de las cosas, ciudades inteligentes, etc.) exige hoy día.

En definitiva, la garantía del acceso a la sociedad digital no precisa, en rigor, de su incorporación al capítulo I del Título I de nuestra Constitución, sin perjuicio de lo que luego se dirá.

La otra función que tendría la incorporación a la Constitución del derecho de acceso a la sociedad digital como derecho fundamental sería la de

hacer exhibición o manifestación de tener una Constitución a la altura del tiempo en que vivimos. Ahora bien, esa función puede suscitar algunos problemas desde el momento en que plantearía de inmediato la cuestión de los medios de hacer efectivo ese derecho y la exigibilidad de tales medios; si bien tal objeción no tiene la misma fuerza según sea el capítulo o sección del Título I en que se añadiera la referencia a la sociedad digital.

3.2.2 Las secciones y capítulos del Título I de la Constitución en que se podría añadir las referencias al derecho de acceso a la sociedad digital de considerarlo conveniente

Las objeciones que puede suscitar la incorporación a la Constitución de determinaciones sobre la sociedad digital son muy diferentes según sea la concreta ubicación en la norma suprema en que se hiciera. En efecto en la sección primera del capítulo segundo del Título I se ubican los llamados derechos autonomía y los de participación política por lo que la ubicación del derecho de acceso allí puede provocar algunos problemas teóricos y prácticos. Los teóricos tienen que ver con las obligaciones de prestación que se derivarían de dicho reconocimiento y su coste. Los prácticos se derivarían del procedimiento agravado de reforma constitucional exigido.

La gran mayoría de los derechos fundamentales de la sección primera no exigen ninguna prestación por parte del Estado, con la excepción del derecho de acceso a la justicia y a la educación que presuponen una prestación de éste.

En el caso de la justicia bien justificado, porque a lo largo de la historia la construcción del Estado se ha hecho en buena medida en torno a la función judicial –el rey juez del antiguo testamento o la función judicial de los reyes en la edad media–. En el caso de la educación estamos ante una dimensión más moderna del Estado que se compromete con la igualdad garantizando, desde el principio, el acceso a la educación como condición esencial para poner, al menos, las bases de las condiciones de igualdad.

Que el acceso de todos a la sociedad digital es de enorme importancia no es discutible, pero ni tiene todavía la misma que tiene el derecho a la educación, ni podemos saber en este momento los compromisos de gasto que supone a menos que se acotara muy claramente el alcance de ese derecho de acceso circunscrito a lo que hemos llamado precursores. Ello podría desaconsejar situar el reconocimiento del derecho de acceso a la sociedad digital en la sección 1.ª del capítulo 2.ª del Título I de la Constitución. La ubicación, de considerarlo necesario, no sería en la sección 1.ª de ese capítulo 2.º Titulo I, sino en la 2.ª –en el que está el derecho de propie-

dad o la libertad de empresa– o en el capítulo tercero («De los principios rectores de la política social y económica») de ese mismo Título.

Por lo que hace a la sección 2.ª del capítulo segundo del Titulo I, en la misma se encuentran muchos derechos cuyo alcance y efectividad quedan deferidos a la Ley con lo que su posición queda, en el fondo, muy cercana a los principios rectores de la política social y económica del capítulo 3.º del Título I de la Constitución. Es verdad que el capítulo 3.º del Título I se considera por algunos poco más que como un capítulo programático con poca capacidad de obligar [lo que ni es ni puede ser considerado así (88)], pero la sección 2.ª del capítulo 2 no está muy lejos de ello, aun cuando existan diferencias más aparentes que reales. Por una parte, a los derechos de la Sección segunda se les aplica la garantía –frente el legislador– del respeto al contenido esencial; por otra a los derechos de la sección segunda no se les aplica la restricción de no poder ser invocados frente a los órganos judiciales del artículo 53.3 CE, si no es de acuerdo con las leyes que los desarrollen.

En lo que hace al contenido esencial, dicho concepto es muy impreciso y permite regulaciones muy restrictivas con tal de que el resultado final haga recognoscible el derecho tal como quede finalmente regulado. Por otra parte, en realidad, todos los preceptos de la Constitución tienen, en cierto modo, un contenido esencial. Cuando el Tribunal Constitucional se ha enfrentado a determinar qué significa la referencia del artículo 103 de la Constitución al estatuto de los funcionarios ha encontrado un, por así decirlo, contenido esencial que le llevó a declarar inconstitucional la Ley de medidas para la reforma de la función pública de 2 de agosto de 1984 (89); lo mismo ocurre constantemente, con todas sus sentencias sobre cuestiones de competencia entre el Estado y las Comunidades autónomas, donde anula normas con rango de Ley sobre la base de infracción de preceptos de la Constitución que ni siquiera están en el Título I. En definitiva, ningún precepto de la Constitución sea cual sea su posición en la misma, está a disposición del legislador para que éste haga con él lo que quiera en trance de aprobar las leyes.

En lo que hace a la imposibilidad de invocar el derecho si no es de acuerdo con lo que dispongan las leyes ante los órganos judiciales (que se

(88) *Vid.* De la Quadra-Salcedo Fernández del Castillo, Tomás,«Derecho Público tras la crisis económica en el Estado social y democrático: Estado de bienestar y servicios de interés general», en *Crisis y Constitución. XIX Jornadas de la Asociación de Letrados del Tribunal Constitucional*. Ed. Centro Estudios Constitucionales, 2015, pp. 82 y 83.

(89) La Sentencia del TC 99/1987, de 11 de junio, declaró nulo el artículo 15.1 de la Ley 30/1984 de medidas de reforma de la función publica, porque entendía que no podía dejar a disposición del ministerio competente en materia de funcionarios la determinación de qué puestos podían ser cubiertos por funcionarios o por otras formas de empleo público con base todo ello en el artículo 103.3, que se refiere al estatuto de los funcionarios. Si se violó tal artículo es porque tenía un contenido esencial, aunque la sentencia no lo formulara así. En todo caso, sin tratarse de derechos, la Constitución no queda al albur de cualquier interpretación.

contiene en el art. 53.3 en relación con los derechos del capítulo tercero del Título I), es cierto que tal exclusión no existe para los derechos de la sección 2.ª del Título I. Sin embargo para éstos últimos es la propia sección segunda la que los proclama, pero sólo en los términos que diga la Ley, por lo que, a la postre, su invocabilidad en sede judicial, aun no impedida por el 53.3, está en realidad vinculada a lo que diga la Ley. La única diferencia es que los particulares pueden invocarlos, incluso contra lo que dice la Ley, para que los órganos judiciales promuevan la cuestión de inconstitucionalidad. Sin embargo, en la práctica, la limitación de su alegabilidad para los derechos del capítulo tercero no ha impedido que los justiciables invoquen ante los Tribunales, no tanto su derecho, pero sí la inconstitucionalidad de las leyes que no los han respetado; ni ha impedido que jueces y tribunales, ante esas invocaciones, hayan planteado cuestiones de inconstitucionalidad, en muchos casos resueltas a favor de la lesión del principio rector.

En realidad los principios rectores de la política social y económica acaban denominándose literalmente en el propio texto constitucional en muchos artículos como derechos (al menos bajo su *nomen*) en el propio capítulo tercero del Título I. Por ello nada impide que, aun no pudiendo ser alegados por las partes sino de acuerdo con las leyes que los desarrollen, los jueces y tribunales puedan plantear *motu proprio* la cuestión de inconstitucionalidad sobre leyes que los desarrollen o sobre leyes que sin desarrollarlos no los tengan en cuenta. Tal cosa ha ocurrido muchas veces determinando la modificación de las leyes que desarrollan tales principios por considerarlas contrarias a la Constitución (90), especialmente cuando se ponen en relación con la igualdad o con los derechos de la sección 1.ª del capítulo 2.º, sin descartar que ocurra lo mismo si se ponen en relación con los derechos de la sección 2.ª de dicho capítulo 2.º En definitiva, estos derechos del capítulo segundo –en sus dos secciones y en el articulo 14– desarrollan, en cierto modo, una función de precursores de los principios rectores o derechos del capítulo 3.º del Título I de la Constitución, polinizándolos o activándolos como derechos fundamentales en determinadas circunstancias.

Por tanto, de considerarse necesaria una incorporación al texto constitucional del derecho de acceso a la sociedad digital o sus precursores, el capítulo tercero del Título I podría ser el adecuado (también la sección

(90) Así ha ocurrido en la STC 45/1989, de 20 de febrero de 1989, en trance de interpretar el principio de igualdad en el ámbito tributario para concluir que el principio de protección a la familia del artículo 39 CE lleva a concluir que la Ley del impuesto sobre la renta de 1979 era inconstitucional en cuanto perjudicaba a los casados respecto de los no casados. De igual modo ocurrió en la Sentencia 275/2005, de 27 de octubre, sobre la investigación de la paternidad en que la remisión al legislador en términos muy genéricos no ha impedido que el TC considerase en su Sentencia que se había violado la Constitución.

segunda del capítulo segundo). Se trata, por otra parte, de un capítulo fundamental (el tercero) al que el Tribunal Constitucional no ha dado en su jurisprudencia toda la relevancia y función esencial que cumple en cuanto manifestación del elemento más novedoso y característico de nuestra Constitución como expresión del contrato social fundamental sobre el que descansa la convivencia en los Estados de bienestar surgidos en Europa tras la segunda guerra mundial.

Podría haber una segunda razón para incorporar a nuestra Constitución los derechos relacionado con la sociedad digital: la de modernizar nuestra norma suprema poniéndola al nivel del tiempo que vivimos. En realidad, habría que subrayar que la función de esa incorporación sería simplemente esa –la de señalar o destacar la modernidad o postmodernidad de la Constitución– pero no tanto la de hacer efectivo el derecho de acceso por todos los medios a la sociedad digital.

La pregunta es –no sólo en el caso de si esta fuera la única razón, sino incluso si se atendiera a razones más de fondo– si tendría sentido poner en marcha un procedimiento de reforma agravada de la Constitución del artículo 168.1 si se pretendiera incorporar el derecho al capítulo 2.º sección 1.ª del Título 1.º de la norma suprema. Parece bastante claro que no sería muy lógico, ni es verosímil que nadie quisiera ponerla en marcha por esa exclusiva razón.

Otra cosa sería si lo que se quisiera es incorporar alguna referencia a la sociedad digital, concretamente, el derecho de acceso a la misma pero no a la sección 1.ª del capítulo segundo, sino a la sección segunda de dicho capítulo segundo del Título I o al capítulo tercero del mismo Título.

En ambos casos el procedimiento de reforma constitucional es el ordinario con el régimen de mayorías que establece el artículo 167. Si hay acuerdo amplio no habría demasiada dificultad para tal reforma, como lo puso de manifiesto una modificación más polémica como la del artículo 135 sobre el principio de estabilidad presupuestaria. En realidad corresponde a la prudencia política de los partidos considerar si es conveniente tal reforma, una vez que se constata que no es una reforma necesaria.

3.2.3 Regulación por Ley de la sociedad digital

Desde luego, una norma con rango legal puede regular perfectamente todos los aspectos de la sociedad digital. Ello suscita de nuevo la cuestión del rango de esa norma: ley orgánica o ley ordinaria. Probablemente lo mejor sería darle el carácter de ley ordinaria sin perjuicio de que aquellos artículos que se entendiera que más directamente implican un desarrollo de un derecho fundamental, siquiera fuese en su articulación con otros,

podrían llevarse a una Ley orgánica específica; sin perjuicio de que pudieran también incorporarse a una Ley orgánica preceptos sin ese carácter.

La cuestión no obstante reside en si estamos hablando de una única ley o de varias leyes, pues ambas alternativas son posibles. Que tenga que haber varias leyes es difícil discutirlo puesto que no es lo mismo la afección al Derecho de la competencia en la aplicación de la inteligencia artificial al Big Data, que las afecciones al derecho a la protección de datos, o a la regulación del transporte con coches inteligentes o al internet de las cosas, o a la regulación del voto electrónico, etc.

Será al hilo de la regulación de cada sector de actividad –y no solo en Ley, sino en la aplicación que de la misma hagan las Autoridades de regulación competentes– donde se puedan establecer con más precisión cuales son las medidas adecuadas.

La cuestión es, sin embargo, si, además de cada Ley sectorial debe haber una Ley general que establezca los principios y criterios conforme a los cuales deberá hacerse la regulación para preservar los derechos y valores constitucionales de forma general en todos los sectores. Una Ley tal sí puede ser conveniente para sentar los principios y criterios generales de articulación de la sociedad digital con los derechos fundamentales y con los demás bienes e intereses generales dignos de protección, sin perjuicio de la necesidad de que en cada sector de actividad las normas propias de cada uno, a la vista de sus problemas y requerimientos propios, establezcan las reglas pertinentes.

3.3 **Derecho, sociedad digital y autoridades de regulación**

El Derecho ante la sociedad digital ha de concretar la respuesta que la sociedad demanda para conciliar las oportunidades y desafíos de la misma con los derechos fundamentales y libertades públicas, así como con los principios, valores superiores y demás bienes constitucionales (91). Aho-

(91) Por bienes constitucionales han de entenderse aquellos bienes, valores y principios que, sin ser ellos mismos derechos fundamentales o libertades públicas, sirven para delimitar la frontera de cada derecho. Los secretos de la defensa o el secreto sumarial son, por ejemplo, un limite para la libertad de información que «delimita» tal libertad. En todos esos «bienes constitucionales», aun no siendo derechos fundamentales en sí mismos, existe siempre una conexión con los derechos fundamentales. En el caso del secreto sumarial la conexión con el derecho a una tutela judicial efectiva es evidente, pues se trata de garantizar la efectividad de la instrucción evitando la destrucción de pruebas, la puesta a disposición de la justicia de los responsables, etc. En el caso de los secretos de la defensa se trata de garantizar la soberanía que está conectada con los derechos de participación política y también, desde luego, con todos los derechos y libertades: desde el derecho a la vida e integridad física hasta el propio derecho a la tutela judicial efectiva, pues una agresión exterior que triunfe, priva de sustento al entero orden constitucional.

La jurisprudencia ha aceptado el término de bienes constitucionales en numerosa jurisprudencia. Así la STC 155/2017, de 21 de diciembre en relación con los límites de la capacidad de presentar enmiendas a los proyectos de Ley afirma: «*Esta doctrina constitucional preserva los derechos de las minorías parlamentarias y, en definitiva, los que a los representantes mismos confiere el artículo 23.2 CE (SSTC 136/2011, de 13 de septiembre, y 231/2015, de 5 de noviembre, FFJJ 8 de*

ra bien tal conciliación pudiera no producirse satisfactoriamente solo en el nivel normativo –sea constitucional, legal o reglamentario–, sino que probablemente debe llevarse al nivel más ejecutivo, de forma que sea necesario pensar en organismos, al modo de las autoridades de regulación que existen en muchos sectores de la acción pública, que puedan dar respuestas concretas y rápidas a los miles de conflictos, tensiones y dudas que puedan producirse en el devenir diario del desarrollo de la sociedad digital. Conflictos y tensiones entre proveedores de servicios de la sociedad digital y receptores de dichos servicios o, de forma más general, proveedores y personas privadas en relación con sus derechos fundamentales o, simplemente, sus derechos.

Ante tal problemática la cuestión se reduce a saber si únicamente deben ser los Tribunales ordinarios quienes conozcan de tales conflictos o es preferible que con carácter previo se interponga un órgano especializado que con los conocimientos y la experiencia de cada sector pueda dar provisionalmente respuesta a los conflictos que se puedan suscitar. La conveniencia sobre la interposición de tales organismos parece clara; ante la complejidad de los conflictos que pueden producirse entre partes en la sociedad digital el ciudadano no puede ser dejado ante la opción de resignarse y rendirse frente a lo que considera un ataque a sus derechos o contratar los servicios de un abogado para llevar ante los tribunales a las poderosas organizaciones que lideran la sociedad digital.

La única opción razonable es interponer el papel de organizaciones –autoridades, agencia, comisiones, etc.– que sean capaces de proteger al

---

una y otra resolución), por más que esa garantía no pueda extremarse en detrimento, a su vez, de otros bienes constitucionales igualmente dignos de tutela como son la propia autonomía de las asambleas (art. 72 CE) y la seguridad jurídica que la Constitución consagra en su artículo 9.3».

En la STC 53/1985, de 11 de abril sobre Proyecto de Ley Orgánica de reforma del artículo 417 bis del Código Penal sobre interrrupción voluntaria del embarazo califico la vida del nasciturus como «bien constitucionalmente protegido».

En el mismo sentido ha aceptado el concepto de bien constitucional en la sentencia 198/2012, de 6 de noviembre en la que ha afirmado:

«Aunque la demanda conecta en varias ocasiones la protección constitucional del matrimonio (art. 32 CE) con la de los diversos apartados del artículo 39 CE por considerar que estos últimos tienen su fundamento principal en el matrimonio tradicional, debemos recordar que matrimonio y familia son dos bienes constitucionales diferentes, que encuentran cabida en preceptos distintos de la Constitución por voluntad expresa del constituyente, de modo que «el texto constitucional no hace depender exclusivamente el concepto constitucional de familia a la que tiene su origen en el matrimonio… ni tampoco la limita a las relaciones con descendencia» (STC 19/2012, de 15 de febrero, FJ 5 y jurisprudencia allí citada). Por tanto, son dignos de protección constitucional los matrimonios sin descendencia, las familias extramatrimoniales o monoparentales (STC 222/1992, de 11 de diciembre) y, sobre todo, los hijos a los que el artículo 39 CE, que «refleja una conexión directa con el artículo 14 CE» (STC 154/2006, de 22 de mayo, FJ 8)».

El reconocimiento del concepto de bienes constitucionales como límites de los derechos y libertades o como determinantes de la inconstitucionalidad de la leyes se recoge en las sentencias del Tribunal Constitucional 65/2015, de 13 de abril; 244/2007, de 10 de diciembre; 14/2003 de 28 de enero; 205/1994, de 11 de julio y Autos del mismo Tribunal 43/2002, de 14 de marzo y 193/1993, de 14 de junio.

ciudadano de las intromisiones en sus derechos derivadas de los instrumentos, aplicaciones, etc. de la sociedad digital. Organizaciones que provistas de los medios y personal necesario dicten resoluciones resolviendo los problemas que plantea la sociedad digital; resoluciones que podrán llegar finalmente a los Tribunales ordinarios.

La cuestión que se plantea es cuádruple. La primera el carácter independiente de estas organizaciones, lo que no parece que deba ofrecer muchas dudas; la segunda si debe tratarse de una organización única para todos los sectores, pero limitada su función a resolver los problemas que se susciten en cada uno de ellos en relación sólo con los conflictos entre la sociedad digital en todas sus manifestaciones con los derechos fundamentales y bienes y valores de relevancia constitucional. La tercera si debe ser la misma que ya existe en cada uno de los sectores. La cuarta si debe ser cada autoridad sectorial, pero con una autoridad que coordine y de coherencia a las respuestas de cada una de las demás autoridades en lo relativo a derechos y libertades en la sociedad digital.

No parece que pueda ponerse en duda que una única organización para resolver en todos los sectores los conflictos de la sociedad digital no resulta aconsejable en la medida en que no serán fácilmente separables los conflictos que afecten exclusivamente a derechos y libertados por razón del desarrollo de la sociedad digital de los demás conflictos de distinta naturaleza que surjan en cada sector y que están encomendados a cada organización específica: Comisión Nacional del Mercado de Valores, Comisión Nacional de los Mercados y la Competencia, Consejo de Seguridad Nuclear o Sección segunda de la Comisión de Propiedad Intelectual. La única excepción a tal solapamiento sería la Agencia de protección de datos.

Por otra parte la resolución de tales conflictos de la sociedad digital exige un conocimiento técnico profundo de las peculiaridades de cada sector; y tal conocimiento lo tienen las Autoridades especializadas que en cada uno existen, siendo dudoso que una nueva Autoridad, exclusivamente centrada en las cuestiones relativas a las afecciones de la sociedad digital en los derechos, pueda llegar a tener un conocimiento suficiente de las peculiaridades de todos y cada uno de los sectores que le capacite para resolver de forma adecuada las incidencias que se presenten.

A ello se añade que tampoco es conveniente duplicar en cada sector lo ya existente, creando una nueva autoridad –limitada a los conflictos y problemas derivados de la sociedad digital–, sino más bien encomendar a las ya existentes también la solución de los problemas derivados más específicamente de los problemas relacionados con la incidencia de la sociedad digital en los derechos, libertades y otros bienes y valores superiores de nuestro ordenamiento.

El único problema que ello tendría podría ser el de la disparidad de soluciones que en cada sector se diera en relación con los demás. Tal inconveniente podría tratar de solventarse dejando que sean los Tribunales ordinarios y eventualmente el Tribunal Supremo, a través del recurso de casación, quien procure la unidad de criterios en todos los sectores. No parece sin embargo que la solución de cuál es el mejor criterio para resolver los conflictos sea solo estrictamente jurídica, por lo que dejar en manos de un órgano judicial decidir cuál debe ser el criterio común, en el caso de que sea posible un criterio común por concurrir idénticas circunstancias, no acaba de ser satisfactorio por la cantidad de complejas cuestiones técnicas concurrentes que un Tribunal no estaría en condiciones de resolver sin recurrir a expertos habida cuenta de la discrecionalidad técnica en la búsqueda de soluciones.

En su lugar podría considerarse, tal vez, si sería oportuno crear un Organismo independiente de la Administración del Estado –del tipo del Consejo de Seguridad Nuclear– (o, sin crearlo, atribuir tal función al Consejo de Estado, aumentando en dos las secciones ya existentes para no alterar el carácter impar de su Comisión permanente) encargándole la tarea de informar preceptivamente todas las propuestas de resolución de los demás organismos con competencias sectoriales en los asuntos en que estuvieran presentes cuestiones relativas a la incidencia de la sociedad digital en los derechos, libertades, bienes y valores superiores del Ordenamiento. De tal forma que la intervención de dicho Organismo procurara una cierta unidad de criterios en la forma de articular el desarrollo y despliegue de la sociedad digital con los derechos fundamentales, valores y bienes de relevancia constitucional. De esta forma sería cada Autoridad independiente la que mantendría la competencia, pero el carácter preceptivo del nuevo Organismo dotaría de una cierta coherencia a la actuación de todos ellos y permitiría al nuevo Organismo, en informes anuales, analizar los problemas planteados y proponer a las Cortes y al Gobierno recomendaciones para el futuro.

3.4 **El carácter internacional de la regulación**

Cualquiera que sea la regulación que se haga de la sociedad digital no puede prescindir de un dato relevante, como es el de la dimensión transnacional de la regulación. Resulta bastante inverosímil creer que cada Estado puede hacer una regulación efectiva cuando de lo que estamos hablando es de una sociedad que si por algo se caracteriza es por su desconexión de territorios concretos y determinados, por más que sus efectos se acaban produciendo sobre personas concretas localizadas en lugares determinados.

Toda regulación que se haga no puede perder de vista la vocación transnacional y en todo caso regional que ha de tener siempre la regulación de la sociedad de la información para ser eficaz.

Ello no impide que cada país debe ir conformando su propia visión sobre la forma de regular la sociedad digital. Pero debe hacerlo con la conciencia clara de que, en última instancia, dado el carácter transnacional de la sociedad digital, los logros más importantes han de conseguirse en las organizaciones internacionales o supranacionales.

4. LA INTELIGENCIA ARTIFICIAL FRENTE AL DERECHO

Una última reflexión debe hacerse en relación con la inteligencia artificial por las peculiaridades que presenta en su relación con el Big Data y su carácter e impacto disruptivos en muchos aspectos. Como se ha visto más arriba hay quienes piensan –los llamados dataístas– que el enorme avance logrado en el tratamiento de ingentes cantidades de datos, en el recurso al *machine learning* y en la investigación y elaboración de algoritmos permiten asegurar cambios radicales en muchos campos; desde le tratamiento de enfermedades, pasando por la ordenación de la economía, el papel de los jueces y tribunales y acabando en la política y el gobierno de nuestras sociedades que parecería que tienen sus días contados hasta ser sustituidas las decisiones humanas en dichos campos por los algoritmos o las máquinas. Ese es el tipo de horizonte que no es compatible con los valores que subyacen y soportan nuestro modelo de convivencia y, más bien, habría que luchar porque en todos los campos las máquinas ayuden al hombre a tomar decisiones y no sustituyan el proceso de adopción de las mismas que solo pueden realizarse sobre la base del conocimiento humano a partir de informaciones que, eso sí, pueden ser suministradas, con ventaja en muchos casos, por las máquinas.

Como es obvio, en lo que se refiere al manejo y tratamiento de los datos, las máquinas son imbatibles, pero en la determinación del algoritmo que analiza los datos y en función de ellos propone o recomienda una acción, han de tomarse en cuenta no sólo datos, sino previamente determinadas preferencias y referencias a valores para el control último de la fórmula o algoritmo; preferencias y valores que no son cuantificables, sin previa valoración y que, en todo caso, no quedan entregados a una máquina. Es el creador del algoritmo quien da a cada factor un peso determinado en la fórmula, incluso aunque la máquina sea capaz de aprender por sí misma (*machine learning*). Conforme a tal peso los resultados de la fórmula son unos u otros. Una alteración de milésimas a cada factor en la fórmula puede llevar a consecuencias distintas; y si la máquina es capaz de aprender por sí misma, nada impide que ratifique tendencias que han de corregirse, más

que confirmarse o ratificarse, salvo que exista algún control humano. En todo caso los algoritmos están llenos de sesgos que tiende a acentuar como numerosos estudios han demostrado. Sin duda ello se puede mejorar, pero demostraría que no está exento de riesgos (92).

Lo mismo ocurre en cuanto a los datos concretos que en cada caso se ponen a disposición de la máquina y que, si tienen sesgos, llevan a la máquina a determinar un algoritmo erróneo.

En definitiva, la inapelable exactitud matemática corresponde a los cálculos que se hacen por el computador a partir de los datos que se le suministran, pero no a la calidad misma de tales datos, ni al modelo inicial que se suministra al mismo; pero no se puede atribuir el algoritmo mismo en cuya realización se han podido incorporar todos los sesgos, prejuicios y errores que corresponden al ser humano. Ni siquiera es cierto que los avances autónomos o automáticos de los propios sistemas de inteligencia artificial, preparados para aprender por sí mismos –el *deep learning,* aprendizaje profundo, o *machine learning,* aprendizaje automático– puedan mejorar las respuestas a los problemas que encierran criterios de valor.

Uno de los campos en los que se pronostica que la IA y el Big Data puede tener resultados espectaculares –entre muchos otros– es el de la función judicial. Hay quien piensa que proporcionando a un ordenador centenares de miles de sentencias, por no decir millones, resolviendo controversias, éste nos podría proporcionar, en cuestión de segundos y sobre la base de los algoritmos de inteligencia artificial que el mismo ha podido establecer a partir de un modelo inicial, la única de respuesta posible en términos de Derecho a cada nuevo problema o conflicto planteado. De tal forma hay quien considera que la IA podría sustituir con ventaja el sistema judicial tanto por la rapidez de la respuesta como por la seguridad que proporcionaría.

Los juristas, en especial aquellos que desarrollan una actividad profesional no tendrán muchas dudas a ese respecto sobre la base de su propia experiencia. Experiencia que probaría que por iguales que parezcan dos asuntos nunca hay un caso igual a otro, por idéntico que pueda parecer.

La tentativa de extraer un patrón común del resultado de miles de casos semejantes para dar solución a problemas iguales que puedan producirse en el futuro no es la primera vez que se produce en la historia. Tal cosa tiene precedentes; así el emperador Justiniano con su Digesto (533 dc) que pretendía compendiar en el *Digesto* toda la jurisprudencia romana producida desde el siglo segundo antes de Cristo y ofrecerla para el futuro junto con su *Código* como el criterio único de solución de contro-

(92) *Vid.* O'Neil, Cathy, *Armas de destrucción matemática,* Capitan Swing, 2018.

versias, con prohibición incluso de interpretar el Digesto que se pretendía presentar como una obra definitiva y perfecta; perfecta no tanto por haberla encargado Justiniano, sino por recoger toda la sabiduría y justicia romana, depurada y perfeccionada durante siglos. Prohibición de interpretar lo que se suponía perfecto –la única respuesta posible– precisamente por ser perfecto, pues solo habría que aplicar el *Digesto*; solo se trataba de aplicarlo sin interpretación alguna.

Naturalmente esa compilación –que incluía la quintaesencia de la mejor jurisprudencia de más de cinco siglos de Derecho romano– que pretendía servir para dar respuesta a todos los conflictos posibles, no se hizo con algoritmos u ordenadores, inconcebibles para la época, pero sí sobre la base de las respuestas o sentencias que los más ilustres juristas habían dado a lo largo de los siglos. Respuestas o sentencias (*responsa prudentium*) a los más diversos conflictos. Tanta sabiduría depurada con los múltiples instrumentos y técnicas del derecho romano contendrían la única respuesta justa posible para cada caso que en el futuro se presentase (93). De ahí la prohibición de interpretar; prohibición fundada en la soberbia intelectual de creer que todo estaba ya dicho –una especie de fin de la historia del Derecho– puesto que nada nuevo podrían presentarse que no se hubiera ya resuelto en siglos y siglos de historia del Derecho recogidos en el Digesto.

Tal pretensión se reveló completamente inútil. Cada caso concreto tiene sus propios matices, como cualquier jurista conoce; y un pequeño matiz determina que la solución pueda ser la contraria a la adoptada en un caso anterior.

La misma pretensión renació en la Revolución francesa con la prohibición a los jueces de interpretar la Ley, que solo debían aplicar. En este caso la prohibición no descansaba en la soberbia intelectual de creer que la Ley fuese perfecta, sino en el dogma de la separación de poderes que entendía, desde Montesquieu (94) al menos, que el que interpreta la Ley

(93) Los romanos eran conscientes de que las decisiones de los jueces (prudentes) que resolvían las controversias que les remitía el pretor podían tener un sesgo: el propio de la clase social a la que pertenecían los prudentes que eran personas dotadas de cultura y capacidad y, por eso, mismo podían tender a dar como justas soluciones que solo eran conservadoras del *statu quo* de la clase dominante. El Edicto del Pretor, más sensible a las controversias de clase entre patricios y plebeyos, corregía para el futuro esos sesgos clasistas, para evitar el mantenimiento del *statu quo*.

La otra técnica de corrección de los sesgos –y de la diversidad de sentencias en función de cada juez o prudente– la constituían las *responsa prudentium* (esto es las sentencias y opiniones a los que se les había reconocido el *iura condere* o dar opiniones sobre los derechos a los que se reconocía autoridad (Ist. Just. 1,2,8 y Gayo I,7) de forma que vinculaban a los jueces cuando había coincidencia entre los pocos juristas a quienes se había reconocido el *ius publice repondendi* desde Augusto.

(94) De «bocas mudas que pronuncian las palabras de la ley» hablaba Montesquieu en el «Espíritu de las Leyes». Así debe ser, en principio, cuando la Ley es clara y precisa, para evitar confundir el papel del legislador con el del juez. Pero como la Ley no se adapta siempre, ni mucho menos, al caso concreto, hace falta indagar en su sentido para dar la respuesta justa y conforme con su espíritu, que no siempre se corresponde estrictamente con esa letra de la Ley. La IA sería

puede acabar por colocarse por encima de la Ley (95) si se le reconoce tal poder de interpretación.

Ni Justiniano, ni los revolucionarios franceses de primera hora, tuvieron el menor éxito. La inteligencia artificial y el Big Data parecerían pretender ahora hacer la misma apuesta sobre la base de la potencia de computación y la inmensidad de datos a tratar. Pero la apuesta no tiene garantía de éxito alguno, puesto que, de nuevo, surge el problema de los conceptos de valor que no pueden cuantificarse, ni permanecen iguales en el tiempo, así como la cuestión de qué datos –qué sentencias– se proporcionan a la computadora y cómo se clasifican y analizan sus términos y contenidos relevantes. Lo cierto es que al ponderar en el algoritmo el valor de cada factor y al proporcionar determinados datos y no otros se están congelando las soluciones e incentivando los prejuicios y sesgos del algoritmo.

Si a ello añadimos que un mismo concepto de valor aceptado de forma general por una sociedad en un momento determinado, depende sin embargo de la concurrencia de circunstancias de hecho, de detalles y de contexto que concurran en cada caso, la cosa de nuevo se complica todavía más; todavía más a medida que la sociedad evoluciona y cambia su forma de ver las cosas.

Por otra parte no solo el algoritmo o la fórmula tiene que estar bien compensada y el modelo y los datos masivos que se han suministrado para determinar la fórmula tienen que estar desprovistos de sesgos, sino que los datos de hecho del caso que se pretende que solucione la inteligencia artificial tienen que darse de forma completa e integral (la existencia de un trastorno mental transitorio en quien ha cometido un delito o si se trata de un caso de legítima defensa). Todo ello hace muy difícil concebir una sustitución de la función judicial por las computadoras. Mas todavía cuando la función judicial exige una motivación de las decisiones que es

---

la perfecta boca muda, si la justicia fuera pura matemática, pero como ya estableció Aristóteles en su Lógica y en la Retórica una cosa son las ciencias en relación con las leyes físicas y matemáticas y otra la «prudencia» para el saber de las relaciones y comportamientos humanos; de ahí para el Derecho la denominación de *prudentia iuris* o jurisprudencia con que todavía hoy se denomina no solo a las sentencias, sino al Derecho mismo.

(95) Tal es la posición de Robespierre que se plantea que los parlamentos judiciales u órganos judiciales no pueden interpretar las leyes para resolver las dudas que se susciten con ocasión de su aplicación. Esa posición se va a llevar a la legislación revolucionaria de los primeros años para prohibir a los jueces interpretar la Ley ante las dudas que puedan surgir en su aplicación. Ante esa prohibición y antes la dudas que puedan tener los jueces no les quedaba a estos otro remedio que el *referé*: remitir a la Asamblea legislativa sus dudas para que una especie de Comisión de ésta dijera cuál era la interpretación auténtica de la Ley. La inundación de *referés* no solo trababa la marcha de la justicia, sino que era imposible que fuera resuelta por la Comisión sin entrometerse en la función judicial. El Código de Napoleón dio un giro de 180º prohibiendo a los jueces dejar de interpretar la Ley acogiéndose al *referé*. De ahí llegó a nuestro Código civil con la imposición de la obligación de fallar a toda costa no sólo interpretando la Ley, sino echando mano de cualquier instrumento en Derecho para no dejar sin fallar caso alguno: «el Tribunal que rehúse fallar a pretexto de silencio, oscuridad o insuficiencia de la Ley incurrirá en responsabilidad» (art. 6 del Código Civil español inspirado en el código de Napoleón; articulo vigente hasta el 28 de julio de 1974).

también difícil que pueda hacer una computadora. Este puede decir la solución final binaria –inocente o culpable; estimación o desestimación; condena a pagar y hacer algo o absolución, etc.– pero difícilmente puede razonar la solución en los términos que se exigen.

En fin, son muchos los aspectos que no pueden ser apreciados por la maquina directamente. Por otro lado la Inteligencia artificial puede acabar petrificando la sensibilidad social sobre un tema, a menos que sea alterada o revisada por el hombre cada cierto tiempo.

Lo más incierto de todo es que quien suministra el modelo y los datos que sirven para configurar el algoritmo en materias o aspectos que implican juicios de valor puede estar vertiendo sus propios prejuicios. Y si no los vierte y el único criterio es el estadístico entonces petrifica la estadística vigente en un momento determinado, aunque no sea la de un solo instante, como la única verdad a la que se tiene que ajustar el futuro, cuando en muchas ocasiones el progreso y el avance se hace contra la opinión dominante.

La reflexión sobre la justicia y la IA que acaba de hacerse y que muestra con ejemplos históricos la imposibilidad de proclamar de nuevo el fin de la historia de la Justicia –por creer que hemos llegado al paraíso de la perfección o la exactitud– es aplicable a todas las dimensiones de la vida social y política. El dominio del hombre por los robots o las computadoras dotadas de inteligencia artificial desconoce que el trascendental, pero único, destino de éstas últimas es la de ayudar al hombre a servirse de ellas para lograr un mundo más mejor y más justo. Y en ese papel de auxiliares impagables su contribución ha de ser reconocida e impulsada.

5. EPÍLOGO

Es hora de recapitular cuanto hasta aquí se ha dicho, pero no en términos de reiterar, ni siquiera de forma sumaria, cuanto se ha ido analizando, sino de retener la atención sobre la trascendencia que tiene la emergencia de la sociedad digital en cuanto abre enormes posibilidades de aprovechamiento que no podemos despreciar, pero, a la vez, como siempre ocurre con todo lo humano, según destacara Berlin (96), genera nuevos riesgos. Riesgos no sólo para los derechos y libertades, sino también para la democracia y el mercado. Todo ello –derechos y libertades, democracia y mercado– obliga a repensar nuestra civilización desde la concepción de humanidad que corresponde a los tiempos que vivimos; a hacerlo para conseguir una mayor protección de los derechos fundamentales y una más profunda

(96) Isahia Berlin en su obra *El fuste torcido de la humanidad*, Ed. 62, 1992.

democracia y más eficiente mercado sobre la base de aprovechar las ventajas que para ello nos depara, precisamente, la sociedad digital.

Junto a ello también es preciso centrar la atención en dos aspectos especialmente: la inteligencia artificial vinculada al Big Data y las consecuencias del hombre aumentado o potenciado. No supone que los demás aspectos no sean igual de importantes e, incluso, que en el medio plazo sean más importantes; pero los dos señalados marcan las fronteras más avanzadas que, por lo que hoy sabemos, la ciencia está ya tocando, sin que quiera decir que vayan a ser las últimas.

El reto que nos plantea, con esa perspectiva, la sociedad digital es de enorme trascendencia: cuando parecía que todo estaba ya hecho hasta el punto de proclamar el fin de la historia, estamos en un momento crítico de la misma porque hemos de reconstruir la sociedad junto con todas las demás naciones eligiendo las bases sobre las que queremos hacer esa reconstrucción. Los enormes avances de la ciencia en el campo de las tecnologías digitales y del genoma, que parecen suponer el omega de nuestra civilización y la cultura, nos obligan a volver sobre el alfa de la condición humana; a una reflexión sobre el humanismo: el humanismo, el transhumanismo o el posthumanismo.

El concepto de humanismo está en cuestión desde diversas perspectivas, pero hay dos visiones filosóficas representadas por Heidegger y sus seguidores (Foucault, Sloterdijk, etc.) de un lado –que cuentan con el apoyo de muchas Asociaciones de transhumanistas o post-humanistas– y Habermas (máximo exponente hoy de la Escuela de Francfort) y otros (Sartre, Sandel, Fukuyama, Hottois, Ferry, etc.) (97), cuyas posiciones marcan dos formas distintas de ver qué es el hombre (98) y cada una conduce por caminos diferentes.

La diferencia de posiciones podía ser vista como una cuestión académica, pero no lo es en absoluto, una vez que el pensamiento de Heidegger, como él mismo reconoció a uno de sus discípulos, Karl Löwith (99), tenía directa relación con su nazismo declarado.

---

(97) *Vid.* Habermas, Jürgen, *El futuro de la naturaleza humana, ¿hacia una eugenesia liberal?*, Ed. Básica, 6.ª imp., 2016; Sartre, Jean Paul, *El existencialismo es un humanismo*, Ed. Edhasa, 1999; Sandel, Michel, *Contra la perfección. La ética en la era de la ingeniería genética.* Ed. Marbot, Barcelona, 2007; Fukuyama, Francis, *El fin del hombre: consecuencias de la revolución biotécnológica*, Barcelona, Ed. B, 2002; Hottois, Gilbert, *Le transhumanisme est-il un humanisme?*, Academie Royal de Bélgica, 2014; y Ferry, Luc, *La revolución transhumanista. Cómo la tecnomedicina y la uberización del mundo van a transformar nuestros días*, Ed. Alianza, 2017.

(98) De nuevo empleo la palabra hombre y no persona, pues desde Kant la pregunta es, en efecto, por el hombre y utilizar otra palabra políticamente más correcta en nuestros días puede perturbar el sentido del debate que se quiere recoger.

(99) *Vid.* Löwith, Karl en *Mi vida en Alemania antes y después de 1933: Un testimonio*, Ed. La balsa de la Medusa Visor, 1992, p. 79, donde cuenta la anécdota de cómo en un viaje a Italia le preguntó a Heidegger sobre la determinación de su posición política por su filosofía, a lo que Heidegger asintió reconociendo la necesaria relación. Es curioso que tanto Löwith como Hannah

El carácter crítico de la encrucijada en que estamos tiene que ver en nuestros días con la concurrencia de las tecnologías de la sociedad digital, con las investigaciones de las ciencias biomédicas y del genoma que están tocando las últimas fronteras que parecen hacer realidad su empleo no ya para curar enfermedades, minusvalías y lesiones, sino mejorar o aumentar al hombre mismo: el hombre aumentado. Tomar en estas condiciones una posición exige saber el contexto y las raíces filosóficas de las escuelas en presencia. Es ahí donde se hace necesario exponer sus fundamentos; muy especialmente los del pensamiento de Heidegger que, sin las connotaciones racistas y supremacistas, sigue en la actualidad teniendo enorme influencia en la filosofía.

El pensamiento de Heidegger tiene gran importancia porque es el primero que rompe con una visión del hombre capaz de libertad y de decisión para situarlo en una visión donde la técnica es lo que domina todo. En su obra «La pregunta por la técnica», establece que la técnica no es un instrumento del hombre para sus fines, sino que es el medio del «desocultamiento» es decir de la verdad a la que el hombre parece ser conducido o provocado por la técnica. La técnica como dominando al hombre (100). La técnica, dirá en otro momento, representa la culminación del olvido del Ser.

Todavía en 1976, muy poco antes de su muerte, en sus declaraciones al *Der Spiegel* (101), consideradas como su testamento político, pues ordena publicarlas después de su muerte, insiste una y otra vez en la técnica (102)

Arendt, sus mejores y primeros discípulos, fueran ambos judíos y acabaron distanciándose de su maestro completamente en el plano filosófico. Otro discípulo, también judío, Franco Volpi, se distanció en «Goodbye, Heidegger! Mi introducción censurada a los Beiträge zur Philosophie» recogido la Actas del I Congreso Internacional de Filosofía y Hermenéutica, 2008 y también en su libro, *Martin Heidegger: aportes a la filosofía*, Ed. Maia, 2010.

(100) En un pasaje de una de sus obras Heidegger cita el momento de la Odisea en que Ulises le dice a su hijo Telémaco –para que no se extrañen los pretendientes de Penelope, a los que se propone dar muerte, de por qué no están las armas de hierro habituales en el salón– que les explique que «el hierro, por sí mismo, arrastra al varón» si animados por el vino entran en disputa. Parece así que sea el hierro, la técnica, el *primum movens* del comportamiento humano.

(101) *Vid.* «Entrevista del *Spiegel* a Martin Heidegger», trad. y notas de Ramón Rodríguez, Tecnos, Madrid, 1996.

(102) «Mientras, a lo largo de los últimos treinta años, se ha hecho cada vez más claro que el movimiento planetario de la técnica moderna es un poder cuya capacidad de determinar la historia apenas puede apreciarse. Hoy es para mí una cuestión decisiva cómo podría coordinarse un sistema político con la época técnica actual y cuál podría ser».

Y más adelante al preguntarle por el calificativo de medias tintas que había empleado hablando de la democracia, de la expresión política de la concepción cristiana del mundo y también del Estado de Derecho, Heidegger le pide al entrevistador que aclare dónde ha dicho todo eso y, luego, continua:

«De «medias tintas» podría, sí, calificarlas porque no veo en ellas una efectiva discusión con el mundo técnico, porque tras ellas está siempre, a mi modo de ver, la idea de que la esencia de la técnica es algo que el hombre tiene en sus manos, lo cual, en mi opinión, no es posible. La técnica en su esencia es algo que el hombre, por sí mismo, no domina».

Más adelante concluye «Esto es precisamente lo inhóspito, que todo funciona y que el funcionamiento lleva siempre a más funcionamiento y que la técnica arranca al hombre de la tierra cada vez más y lo desarraiga».

por la importancia que la cuestión tiene en su filosofía, que tal vez es una deriva de Nietzsche al que dedicó tanto estudio (103). De ahí se explica también su obra de 1946 (104) *Carta sobre el humanismo*, con su crítica a Sartre por la publicación de su obra *El existencialismo es un humanismo*.

Desde esas raíces se comprende la posición de Sloterdijk –discípulo de Heidegger– ya directamente conectado con la ciencia del siglo XXI y de Harari.

Frente a ellos está la obra de Habermas y de muchos otros, incluido el propio Sartre a quien Heidegger fustiga en su *Carta sobre el existencialismo*. En todos ellos con sus diferencias no se niega la libertad del hombre, ni su voluntad, ni su conciencia. Desde ahí se puede construir un humanismo a la altura de nuestro tiempo actual, pero tampoco se pueden ignorar los retos que plantea el desarrollo del mundo digital y las posibilidades de mejora que abre. Es preciso establecer unas reglas –una regulación– y hacerlo a escala planetaria, pues si no servirán para poco.

En la búsqueda de esa regulación no valen ya los clichés que en otros momentos se hicieron sobre que lo progresista era estar con los inventos y lo conservador con el *statu quo*. Tal es la opinión de Volpi (105) –discípulo, él mismo, de Heidegger del que luego renegó– al reconocer que durante mucho tiempo la resistencia a los avances de investigación y la ciencia se vieron como una posición antiilustrada y oscurantista, pero que en la actualidad los últimos logros del mundo digital y de las biotecnologías obligan a todos a hacer una nueva reflexión más profunda.

Una reflexión que no pierda de vista los rasgos sobre los que se fundamenta la dignidad de la persona humana y su vida libre en sociedad.

Pero esa reflexión tiene la ambigüedad muy propia de Heidegger, pues no es tanto un lamento, sino una constatación que demuestra el destino del hombre como dominado por la técnica y preparado con ello, tal vez, para ser dominado por un Fhürer que sería el ventrílocuo del Ser.

(103) Pero con el anuncio de la muerte de Dios, Nietzsche se proponía que el hombre dejase de enfrentarse al mundo con el consuelo de la idea de Dios y afrontase su realidad tal como era: sin subterfugios; pero no desde luego para dejarse dominar por la técnica aceptándola como su destino inevitable.

(104) Allí dice en un momento: *«La esencia del materialismo se oculta en la esencia de la técnica, sobre la que ciertamente se escribe mucho, pero se piensa poco. En su esencia, la técnica es un destino, dentro de la historia del ser, de esa verdad del ser que reside en el olvido»*.

(105) *Vid.* VOLPI, FRANCO, «El hombre entre el nihilismo de la técnica y la responsabilidad éticopolítica», en *Konvergencias, Filosofía Culturas en Diálogo*, núm. 13, año IV, septiembre 2006, donde al final del trabajo acaba proponiendo *«un humanismo que, frente al carácter asimbólico de la técnica, se esfuerce por activar el sentido de responsabilidad del cual la humanidad es en principio capaz»*.

CAPÍTULO 2

DEL SER HUMANO AL POSTHUMANO

Stefano Rodotà
Universidad La Sapienza di Roma

Cuando en 1950 Norbert Wiener publica sus reflexiones sobre cibernética, ciencia y sociedad, escoge como título *El uso humano de los seres humanos*. En estas palabras encontramos algo que va más allá del conocimiento que tiene el científico de las consecuencias de su investigación. Está el eco de una época que ha cambiado, y no solo por la percepción lúcida de lo que habría determinado la tecnología. Acaba de terminar la Segunda Guerra Mundial y Wiener ya se encuentra entre los científicos que, con Robert Oppenheimer a la cabeza, se han dado cuenta de los riesgos del uso militar de la energía atómica y rechazan toda nueva colaboración con el Gobierno estadounidense. Será Guenther Anders, centrando su reflexión precisamente en la bomba atómica, quien en 1956 recoja la radicalidad de este pasaje, preguntándose en su libro más conocido si El hombre está anticuado. Y escribe: «Del mismo modo que un pionero, el ser humano desplaza sus propios confines siempre más allá, se aleja cada vez más de sí mismo; se «trasciende» cada vez más y, aunque no se traslada a una región sobrenatural, de todos modos, dado que franquea los límites congénitos de su naturaleza, pasa a una esfera que ya no es natural, al reino de lo híbrido y de lo artificial».

Muchas trasformaciones son ya visibles y justifican la consideración del cuerpo como «un nuevo objeto conectado», presentado incluso como una «nano-bio-info-neuromáquina», recordando aquel *homme machine* del que hablaban La Mettrie y D'Holbach en el siglo XVIII. Así se identifica el efecto de converger disciplinas diversas que concurren para definir una nueva dimensión de lo humano, con frecuencia representada como un

campo de batalla en donde combaten visiones irreconciliables. El tiempo por venir se describe como el de «nuestra invención final: la inteligencia artificial y el fin de la edad humana» (1). ¿Qué espacio quedaría entonces para esa actividad propiamente humana que consiste en la libre actuación y en poner reglas a la actuación? ¿Desaparecerán los derechos «humanos» y, con ellos, los principios de dignidad e igualdad, o bien se ampliarán a otras especies vivas y también al mundo de las cosas?

Al reconstruir la dimensión del ser posthumano se insiste en la absoluta libertad de la investigación científica y en el reconocimiento no condicionado del derecho a la tecnología, especificado a escala individual como derecho al uso legítimo de todas las oportunidades que la innovación científica y tecnológica pone a disposición de las personas. Entonces, ¿no hay ningún límite? Pero, precisamente debatiendo las tesis de Guenther Anders, Norberto Bobbio ponía de manifiesto cómo en ellas la fundación de una nueva moral asumía un significado absolutamente prioritario y cómo los remedios jurídico-institucionales estaban condicionados por el alcance de ese objetivo. Estos dos planos se han ido imbricando cada vez más al cambiar de un contexto en el cual el acento se ha desplazado de la consideración de la supervivencia física de la humanidad, tal y como implicaba la referencia a la bomba atómica, hacia una trasformación suya tan radical que lleva a un abuso del ser humano por parte del mundo de las máquinas. Entonces, si hay que mirar hacia la dirección de la construcción de un contexto institucional coherente con la novedad de los tiempos, son los principios de lo jurídico los que se deben tener en cuenta en esa fundación suya particular que les ofrece la última fase del constitucionalismo; en primer lugar, los de la igualdad y la dignidad, presentes no por azar, directa o indirectamente, en el conjunto del debate que se está desarrollando.

Estos temas han entrado en el discurso público al difundirse las técnicas de reproducción asistida y al emerger hipótesis extremas, como la de las madres-abuelas o la de la elección de una pareja de lesbianas sordomudas que recurren a esas técnicas para tener hijos también sordomudos. De ahí que se plantee la pregunta sobre qué derecho se debe «fabricar» el ser humano. ¿No estamos quizá ante la pretensión del ser humano de *play God*, de comportarse como si fuera dios, desbaratando el orden milenario de los sistemas de parentesco y del sucederse las generaciones?

El horizonte se ha dilatado, la definición del campo de lo posthumano ya no hace referencia solo a las innovaciones vinculadas a la biología y la genética, sino que es el resultado de la convergencia de diversas disciplinas y experiencias, que van desde la electrónica hasta la inteligencia arti-

(1) Barrat, J., *Our Final Invention: Artificial Intelligence and the End of the Human Era*, Dunne Books. St. Martin's Press (NY) 2013.

ficial, la robótica, las nanotecnologías y las neurociencias. Las trasformaciones asumen así un valor cualitativo inédito, aunque de ellas se pueda hacer el seguimiento de ascendencias incluso sorprendentes, como en las *Magnalia naturae* que Francis Bacon escribe en 1627 como apéndice a la *Nueva Atlántida*, indicando las perspectivas abiertas por la ciencia: «prolongar la vida; retardar la vejez; curar las enfermedades consideradas incurables; mitigar el dolor; trasformar el temperamento, la estatura, las características físicas; reforzar y exaltar las capacidades intelectuales; trasformar un cuerpo en otro; fabricar nuevas especies; realizar trasplantes de una especie a otra; crear nuevos alimentos recurriendo a sustancias que hoy no se usan».

Hoy se habla mucho de realidad «aumentada», considerando el modo en el que la electrónica trasforma el ambiente en el que vivimos, así como a nosotros mismos. Pero Bacon, en realidad, nos hablaba ya de una persona «aumentada», y esta es la terminología a la que recurren los tecnólogos. Se entra así en el campo del *human enhancement*, de una potenciación de la condición humana gracias a la eliminación de vínculos naturales y culturales que hace posible la ciencia, con una extensión de las oportunidades de vida.

¿Una persona aumentada o desposeída de esos tramos de los que creemos que la humanidad no se puede separar? Si apartamos la mirada de las premoniciones del pasado, entramos en anticipaciones proféticas y promesas tentadoras. Llegará un día, dicen los más radicales entre los transhumanistas, en el que el ser humano ya no va a ser un mamífero, se va a liberar del cuerpo, va a ser uno con el ordenador, de su cerebro se podrán extraer informaciones que luego se repliquen en un ordenador, y podrá acceder a la inmortalidad. Y la inteligencia artificial se presenta como aquella que nos va a liberar de las enfermedades y de la pobreza, dándonos la plenitud de lo humano, liberado de sus miserias. ¿Por qué, entonces, cuatrocientos científicos solicitan una atención crítica hacia la inteligencia artificial?

En ese documento se pone de manifiesto la creciente aparición de sistemas autónomos, vehículos autónomos, formas autónomas de producción, armas letales autónomas. Pero ¿autonomía con respecto a qué? El criterio de comparación es claro: con respecto a una situación en la cual las decisiones se confían al conocimiento y a la independencia de las personas. Ahora, sin embargo, la autonomía parece abandonar al ser humano y convertirse en carácter de las cosas, invirtiendo la perspectiva de un ser posthumano como «mejor que el humano» y presentándose más bien como ideología de la tecnociencia.

Pero ya vivimos el eclipse de la autonomía de la persona en la época del capitalismo «automático». Gracias a una ininterrumpida recopilación

de informaciones sobre las personas, la construcción de la identidad puede confiarse cada vez más a algoritmos, sustrayéndola a la decisión y al conocimiento individuales. «Tú eres quien Google dice que eres»: y sobre esta base la persona se conoce y se clasifica, se construyen proyecciones de sus posibles decisiones futuras, de modo que la persona corre el riesgo de ser valorada por sus propensiones y no por sus acciones. Así, la separación entre identidad e intencionalidad, además de ser una «captura» de la identidad por parte de otros, confirma una tendencia hacia un alejamiento progresivo de la identidad como fruto de la autonomía de la persona. Se empaña hasta desaparecer la fuerza del humano en la construcción de sí mismo, y es trabajosa la investigación de vías para reinventar la identidad en la época de la tecnociencia.

Son continuos los intercambios entre el ser humano, el posthumano y un mundo de las cosas que manifiesta una autonomía creciente. No carece de significado el paso de la Internet 2.0, la de las redes sociales, a la Internet 3.0, la Internet de las cosas. Y el mundo de las cosas está trasformado por la presencia heterogénea de los robots, que cada vez tienen menos referencia solo a la dimensión física. Aparecen robots virtuales, precisamente los algoritmos que permiten el funcionamiento de los ordenadores que gobiernan determinadas actividades, y robots sociales, que serían aquellos a los que ya se debe reconocer «una pequeña humanidad». ¿Pequeña como única posibilidad o primer paso hacia una «humanidad» integral de las máquinas?

El ser humano se distribuye, sale del área que culturalmente se le había atribuido, el mundo de las cosas se anima y, así, parece certificar el eclipse de lo que hemos llamado humanismo. ¿Es una nueva manifestación de aquel conflicto entre las dos culturas del que tanto se habló hace años? Más bien se anuncia un desafío definitivo. No es solo la asunción de apariencias de máquina por parte del ser humano. Es la creación de sistemas artificiales capaces de aprender, dotados de una forma de inteligencia propia que los hace capaces de someter la inteligencia humana, de crear una simbiosis máquina/persona que influya en la propia evolución de la especie.

Son dos situaciones distintas que, sin embargo, tienen en común el problema del umbral, superado el cual se pasaría de una dimensión a otra. En este entrelazamiento entre datos del presente y proyecciones hacia el futuro se sitúa la ardua construcción de un contexto de reglas y principios, de una RoboLaw capaz de maximizar los beneficios de la segunda revolución de las máquinas.

Se está manifestando una nueva forma social y, tal como ya sucedió en el pasado, sus efectos se miden enseguida por la relación entre condición posthumana y destino del trabajo. ¿Es una sociedad liberada del trabajo o

socavada por servidumbres más profundas? ¿Son exclusiones crecientes o un *fully automated luxury communism*? Estas preguntas remiten a un interrogante más radical que cada vez se manifiesta más explícitamente en los debates: estas trasformaciones ¿se producen bajo la bandera del beneficio o por el interés de la persona? Para afrontar este problema, la referencia no se puede buscar en la inteligencia artificial, sino en la colectiva, por lo tanto en la política y en las decisiones que ésta está llamada a asumir. El verdadero riesgo, de hecho, no es el de una política expropiada por la tecnociencia. Es su abandono a una deriva que la desresponsabiliza, que induce a concluir que verdaderamente la enfermedad y la pobreza son asuntos que ya se pueden delegar en la técnica y no problemas que haya que gobernar con el conocimiento consciente civil y político.

Esta política no puede carecer de principios; lo demuestra, por ejemplo, la cuestión del *human enhancement*, la potenciación de lo humano. Es un tema en absoluto abstracto, ya que el cuerpo se presenta no solo como objeto vinculado, sino como destinatario de intervenciones cada vez más invasivas. Una invasión que, por lo demás, no implica solo riesgos, sino que describe recuperaciones de funciones perdidas, acceso a nuevas oportunidades, enriquecimiento de los vínculos sociales.

¿Quién gobierna estos procesos? Vuelve aquí el tema de la libertad y de la autonomía y es evidente que la potenciación del ser humano no se puede resolver con la disponibilidad del cuerpo de otros, sean cuales sean sus motivaciones, culturales, paternalistas o autoritarias. Se ha debatido sobre la legitimidad de la decisión de una pareja de lesbianas sordomudas de tener un hijo también sordomudo. Libertad de elección, por lo tanto, pero siempre que las decisiones solo produzcan efecto en la esfera del interesado. Y esto pone en discusión la afirmación posthumanista de un derecho incondicional a recurrir a todo lo que pone a disposición la tecnociencia.

La potenciación del ser humano conoce además el principio de igualdad. ¿Qué criterio regirá el acceso a las oportunidades que ofrezca la tecnociencia? ¿La lógica de los derechos o la del mercado? Basta con pensar en la potenciación de la inteligencia y en las consecuencias de una situación en la que esta potenciación estuviese vinculada a la disponibilidad de los recursos necesarios para comprarla en el mercado. Ya no basta con decir que así nacería una sociedad de castas, puesto que históricamente esta forma social se basaba en una discriminación cultural, económica, social y religiosa que siempre se podía eliminar. Sin embargo, cuando está implicado el cuerpo nace una distancia humana, irredimible como tal.

A la cuestión de la igualdad se añade así la de la dignidad, que reaparece cuando las técnicas de potenciación implican formas de control externo, permanentes o transitorias. Aquí la regla no puede ser, de forma simplista,

la del consentimiento de la persona interesada, pues bien, se conocen los condicionamientos de la libertad de consentir. Lo que se puede admitir es una modificación o una potenciación transitoria, y por lo tanto reversible, sobre la base de las decisiones del interesado.

Estas vicisitudes del ser humano remiten a una consideración más general derivada de la observación según la cual la humanidad parece haber surgido de dos procesos en apariencia opuestos: la hominización, esto es, la evolución biológica, que ha producido el surgimiento de una sola especie humana con un proceso de unificación tendente al universalismo, y la humanización, es decir, la evolución que se ha articulado a través de las culturas con un proceso de diversificación tendente al relativismo. Universalidad y unicidad, por una parte; diferenciación propia de cada grupo humano, por la otra. En la época de una innovación científica que modifica las modalidades de la procreación y construye integraciones nuevas del mundo humano con el mundo animal y con el de las máquinas, estas categorías ya no nos darían una descripción de las dinámicas humanas en consonancia con la profundidad del cambio. El acento se debería poner con particular intensidad precisamente en la hominización, puesto que la profundidad del cambio en los procesos biológicos y su intersección con todo el conjunto de innovaciones científicas y tecnológicas parecen indicar una dirección que llevaría a una diversificación de la especie humana, incluso a la creación de nuevas especies. En los procesos de humanización, por el contrario, se perciben signos significativos de un movimiento hacia la unificación, de lo cual da testimonio precisamente la difusión de normas jurídicas comunes en los sectores en los que el ser humano está más visiblemente sometido a la prueba de la tecnociencia. Por lo tanto, es una inversión radical de perspectiva que también se ha descrito refiriéndose a la esperanza de que la humanidad conseguirá sustituir «la casualidad del proceso evolutivo por una reinvención autodirigida de la naturaleza humana». Son procesos que, de todos modos, nos llevan fuera de la lógica de la evolución darwiniana.

¿Podemos detenernos a contemplar este horizonte, que nos puede parecer desmesurado? ¿O debemos mirar más allá, volviendo a ese uso humano de los seres humanos citado al principio? ¿A quién incumbe la responsabilidad de este uso humano? De hecho, aunque se aceptase la tesis de una tecnología tendencialmente incontrolable porque sería productora autónoma de fines siempre nuevos, no se podría eludir un análisis de las fuerzas concretas que actúan, que orientan la investigación, la sostienen y la financian, dando a los complicados trayectos entre lo humano y lo posthumano la función de trasformar profundamente las propias relaciones sociales.

La difusión de la robótica, tal como ya sucedió con la electrónica, lleva a una concentración del poder en manos de sujetos que controlan la dimensión técnica. Con su exasperado énfasis en la expansión indefinida y libre del poder individual, el proyecto transhumanista termina por encarnar la lógica de una competitividad sin límites, de la cual cada uno está llamado a ser protagonista. Si sucumbe, es solo porque no ha sido capaz de aprovechar las oportunidades ofrecidas por la tecnociencia. La nueva revolución desvela así un alma antigua y muestra inquietantes continuidades con la lógica de un mercado competitivo incontrolado.

El ser humano, y su custodia, resultan así no ser una resistencia a lo nuevo, al temor al cambio, o una infravaloración de sus beneficios. Se presentan como conocimiento consciente de una transición que no se puede separar de los principios en los que el ser humano sigue reconociéndose, abriéndose no obstante a un mundo más amplio y en continua trasformación. No es empresa baladí, ni de unos pocos. Para los riesgos del futuro no basta con evocar el asunto de la bomba atómica, esperando que el tabú que lo acompañó se pueda transferir a los nuevos territorios. El compromiso necesario exige una trasformación cultural, una atención civil difundida, una acción pública coherente. Hablar de una política de lo humano es, entonces, exactamente lo opuesto a las prácticas corrientes que quieren apropiarse de cada aspecto de lo vivo.

CAPÍTULO 3

IDENTIDAD Y PERSONA EN LA SOCIEDAD DIGITAL (1)

JOSÉ LUIS PIÑAR MAÑAS
Catedrático de Derecho Administrativo de las Universidades de Castilla-La Mancha (excedente) y CEU San Pablo de Madrid

1. SOBRE EL DERECHO A LA IDENTIDAD

Decía el tristemente fallecido Stefano Rodotà que «profondissimo è divenuto il pozzo dell'identità» (2). Y en efecto, pese a que sigue siendo un tema poco tratado, con notables excepciones, el de la identidad se ha convertido en un tema especialmente controvertido sobre todo a partir de la irrupción de la innovación tecnológica en el marco de la sociedad digital.

(1) El presente trabajo tiene conexión con el Proyecto de Investigación *Protección de datos, seguridad e innovación: retos en un mundo global tras el Reglamento Europeo de protección de datos*, Referencia DER2016-79819-R, de la Convocatoria 2016 de Proyectos de I+D+I, del Ministerio de Economía y Competitividad, del que soy Investigador Principal.

(2) «Quattro paradigmi per l'identità», en *Nuova giurisprudenza civile commentata*, 2007. He utilizado el original que amablemente me facilitó el autor. También publicado en *El derecho a tener derechos*, Editorial Trotta, 2014, pp. 273 y ss.

La identidad se configura como el derecho a ser uno mismo y diferente de los demás. Se ha señalado [Giorgio Pino (3)] que el derecho a la identidad personal es el derecho a que la proyección social de la propia personalidad no sufra distorsiones como consecuencia de la atribución de ideas, opiniones o comportamientos diferentes a los que la persona ha manifestado en sus relaciones vitales. También se ha señalado que la persona no tiene o no debe tener la posibilidad de reescribir su propio pasado, lo que equivale a decir que no debería poder alterar su identidad. La Sala Primera del Tribunal Supremo, en su Sentencia de 15 de octubre de 2015 (4) ha señalado que «el llamado "derecho al olvido digital" ... no ampara que cada uno construya un pasado a su medida, obligando a los editores de páginas web o a los gestores de los motores de búsqueda a eliminar el tratamiento de sus datos personales cuando se asocian a hechos que no se consideran positivos. Tampoco justifica que aquellos que se exponen a sí mismos públicamente puedan exigir que se construya un currículo a su gusto, controlando el discurso sobre sí mismos, eliminando de Internet las informaciones negativas, "posicionando" a su antojo los resultados de las búsquedas en Internet, de modo que los más favorables ocupen las primeras posiciones. De admitirse esta tesis, se perturbarían gravemente los mecanismos de información necesarios para que los ciudadanos adopten sus decisiones en la vida democrática de un país».

No es fácil encontrar en el ámbito de las normas jurídicas un reconocimiento expreso al derecho a la identidad, que no está expresamente reconocido en nuestra Constitución. La Corte Constitucional Italiana ha establecido (por ejemplo Sentencia de 3 de febrero de 1994, n.º 13) que el derecho a la identidad se reconoce en el artículo 2 de la Constitución de 1947 (por el que se reconocen y garantizan los derechos individuales de la persona, tanto en cuanto sujeto singular como en el marco de las formaciones sociales en las que se desarrolla su personalidad). Por su parte, la Constitución portuguesa de 1976 reconoce expresamente en su artículo 33.1 (Derecho a la identidad, a la buena fama y a la intimidad) el derecho de todos «a la identidad personal, al buen nombre y reputación y a la reserva de su intimidad en la vida privada y familiar».

Según el Tribunal Europeo de Derechos Humanos, el derecho a la identidad está reconocido en el artículo 8 del Convenio Europeo de Derechos Humanos (por ejemplo Sentencia de 28 de enero de 2003, Peck

(3) *Il diritto all'identità personale. Interpretazione costituzionale e creatività giurisprudenziale*, Il Mulino, Bolonia, 2003.

(4) Corregidas ya las segundas pruebas de esta obra ha sido publicada la Sentencia del Tribunal Constitucional 58/2018, de 4 de junio, que declara nula la STS de 15 de octubre de 2015. En cualquier caso la doctrina que acabo de transcribir no resulta afectada sustancialmente. Puede verse mi comentario urgente en Abogacía Española: «Derecho al olvido y hemerotecas digitales»: https://www.abogacia.es/2018/07/23/el-derecho-al-olvido-y-las-hemerotecas-digitales/

c/ Reino Unido). En su Sentencia de 26 de junio de 2014, en los asuntos 65192/11 (Mennesson c/ Francia) y 65941/11 (Labassee c/ Francia) el Tribunal recuerda que el derecho a la propia identidad forma parte integral de la noción de vida privada. Advierte además que privar a alguien de su identidad supone privarle de todos sus derechos.

Por su parte, nuestro Tribunal Supremo ha señalado que el reconocimiento de la propia identidad forma parte del libre desarrollo de la personalidad (entre otras, Sentencias de Sala 1.ª, de 28 de febrero, 6 de marzo o 18 de julio de 2008).

2. UNA O VARIAS IDENTIDADES

De lo anterior cabría deducir que la identidad es la que es, sin posibilidad de ser alterada. Pero lo cierto es que no es del todo así. En el mundo físico, analógico si se quiere, el ser humano tiene una identidad formal u oficial, pública, que es la que se define a partir de las circunstancias y del entorno público y recognoscible de cada persona. Somos quienes somos en virtud de haber nacido con un determinado sexo (sin perjuicio de lo que luego veremos) en un determinado lugar un determinado momento. Se nos atribuye un nombre y se nos van asignando características que van configurando esa identidad pública u oficial: se nos asigna un nombre y unos apellidos, vivimos en un determinado lugar (nuestra dirección), se nos asigna un número identificativo, ocupamos o no un determinado puesto de trabajo, obtenemos un título… De Castro ya señaló que el nombre es el signo externo de la individualización de la persona (5). En relación con los menores esto es algo especialmente relevante. El artículo 3 de la Declaración de los Derechos de los niños y adolescentes, de 1959, dispone que «El niño tiene derecho desde su nacimiento a un nombre y a una nacionalidad». Uno de los mayores dramas de los menores en no pocos países es carecer de identidad, pues la carencia de identidad implica la carencia de personalidad y por tanto la carencia de derechos. De modo que contar con una identidad es presupuesto para la propia dignidad de la persona, para ser titular de derechos y obligaciones, para tener una existencia en el mundo del Derecho y por tanto en el de los derechos.

Pero también hay una identidad que se define en función de los elementos que cada uno quiere que se resalten o le definan. Y en este punto la privacidad asume un papel de primera magnitud, pues la privacidad

(5) *Derecho de la Persona. Apuntes de Derecho civil español, común y foral*, apuntes de Cátedra editados por la Delegación del SEU de la Facultad de Derecho de la Universidad Complutense, Madrid, 1945, p. 12.

nos permite mantener e incluso reivindicar o hacer valer la identidad que queremos para nosotros o la que realmente tenemos, y que paradójicamente define asimismo la identidad que queremos mostrar hacia fuera. La privacidad permite controlar mi yo y expresar el yo que quiero transmitir a los demás. Alguien puede dedicarse a la crítica rigurosa de cine de autor y disfrutar en privado viendo películas de ínfima calidad; dedicarse a la crítica literaria y desconectar en privado leyendo prensa rosa; ser o aparentar ser eficiente, serio, cabal y exigente personal al servicio de una Administración Pública o de una empresa y frecuentar reuniones de intercambio de parejas. De modo que debe quedar a la decisión de cada uno compartir o visibilizar más o menos ámbitos de su identidad. Con alguna excepción, como es obvio. Por un lado, el ámbito privado no compartido debe ser lícito para poder resultar intranscendente mantenerlo reservado o no; por otro, las personas de relevancia pública han de ser conscientes de que su ámbito privado, el que define su yo, debe ser forzosamente mucho más limitado que el de quienes no tienen esa relevancia, llegando incluso a existir ámbitos que para el *uomo qualunque* son admisiblemente privados y que para aquéllas son no ya admisiblemente sino obligatoriamente públicos. La identidad privada es mucho más limitada en relación con las personas de relevancia pública. Sería fácil ahora citar decisiones de los tribunales que así lo advierten. O recordar cómo el Tribunal de Justicia de la Unión Europea, en su conocida Sentencia de 13 de mayo de 2014, sobre derecho al olvido, obliga a llevar a cabo una ponderación entre el derecho a la protección de datos y el derecho a la libertad de información o de expresión, lo que en la práctica implica valorar, entre otras circunstancias, la relevancia pública del solicitante del olvido para determinar el alcance de la desindexación en que tal derecho consiste.

En definitiva, hay o puede haber una tensión entre la identidad pública que nos dan y la privada que nos damos. Y en gran medida la historia ha oscilado entre los intentos del poder por controlar, definir y tergiversar la identidad de las personas y la lucha del ser humano por alcanzar la propia identidad. Los poderes públicos, no siempre dictatoriales, se han valido de la posibilidad de alterar, tergiversar o manipular la identidad de las personas para convertirlas en amigos o enemigos. El nacismo y el estalinismo así lo hicieron. Pero también se pretendió diseñar en Italia una identidad de Pier Paolo Pasolini para, si no justificar, sí desdramatizar e incluso tolerar su muerte, como ha denunciado Rodotà (6).

(6) En *Pasolini: crónica giudiziaria, persecuzione e norte*, libro coordinado por Laura Betti, Garzanti, Milán, 1977, pp. 279-291. También recogido en Rodotà, *La vida y las reglas. Entre el derecho y el no derecho*, Trotta, Madrid 2010, pp. 317 y ss.

3. IDENTIDAD Y DEMOCRACIA

La democracia implica saber lo menos posible de las circunstancias que configuran la identidad de las personas. Pero también es saber lo necesario de cada persona en función de sus circunstancias para garantizar precisamente una convivencia democrática que respete la dignidad, la libertad y la igualdad de las personas. Una dictadura quiere saberlo todo de las personas. Necesita saberlo todo para conseguir el máximo control social y con ello la menor libertad y la igualdad que al poder le interese instaurar. El poder se basa en saber todo del otro, sea contrincante o súbdito, Fouchet lo sabía muy bien, y así lo narró, como solo él podía hacerlo, Stefan Zweif. Y en que se sepa lo menos posible de quien lo ostenta, del que además diseña una identidad inventada al objeto de doblegar el conocimiento de los súbditos. Alan Westin ha señalado con acierto que los estados totalitarios prefieren una administración opaca y un ciudadano visible, mientras que las democracias descansan sobre el control a un gobierno transparente y el respeto a la privacidad de la persona (7).

No es de ahora ni nuevo crear identidades totalmente falsas de quien ostenta el poder para impresionar, subyugar, asombrar o fascinar a los súbditos. Las identidades falsas condicionan la relación con el otro. La democracia se basa en que la identidad oficialmente pública esté configurada por los menos elementos posibles, mientras que la privada puede ser tan limitada o tan extensa como cada persona decida sin que por ello puedan derivarse consecuencias negativas para ella. Las dictaduras quieren saber si una persona es homosexual o tiene una determinada ideología; las democracias quieren que las personas puedan dar a conocer que son homosexuales o tienen una determinada ideología sin que para ellas derive de ello consecuencia alguna. Las dictaduras quieren heterodefinir la identidad de las personas y decidir las consecuencias que de ello derivan; las democracias quieren permitir que cada uno defina su propia identidad sin que de ello deriven consecuencias. Se decía que el derecho puede hacerlo todo menos cambiar un hombre en mujer; ahora debe afirmarse que el derecho puede hacerlo todo, incluso permitir que un hombre cambie a mujer. El Tribunal Constitucional Federal Alemán acaba de declarar, mediante sentencia de 10 de octubre de 2017 (8), que es inconstitucional la imposibilidad de inscribir a una persona con un tercer sexo diferente al masculino o femenino. Y ello derivado de la conjunción de los artículos 1 (1), 2 (1) y 3 (3) de la Ley Fundamental de Bonn de 1949. El primero dispone que «La dignidad humana es intangible. Respetarla y

(7) *Privacy and Freedom*, Atheneum, New York, 1967, p. 23.
(8) http://www.bundesverfassungsgericht.de/SharedDocs/Downloads/EN/2017/10/rs20171010_1bvr201916en.pdf?__blob=publicationFile&v=1

protegerla es obligación de todo poder público»; el segundo, que «Toda persona tiene el derecho al libre desarrollo de su personalidad siempre que no viole los derechos de otros ni atente contra el orden constitucional o la ley moral»; y el tercero que «Nadie podrá ser perjudicado ni favorecido a causa de su sexo, su ascendencia, su raza, su idioma, su patria y su origen, sus creencias y sus concepciones religiosas o políticas. Nadie podrá ser perjudicado a causa de un impedimento físico o psíquico» (9).

La Sentencia es de extraordinaria importancia para el derecho a la identidad. El Tribunal llama la atención acerca de la importancia de la identidad de género en la vida cotidiana: «La identidad de género desempeña un papel importante en la vida cotidiana: en parte, el género determina los derechos y obligaciones previstos por la ley; además, a menudo constituye la base para la identificación de una persona, y la identidad de género también es importante en la vida cotidiana, independientemente de las disposiciones legales. En gran medida, determina, por ejemplo, cómo se visten las personas o qué se espera de una persona en términos de su apariencia, educación o comportamiento» (10). Y la importancia que la propia identidad tiene para el libre desarrollo de la personalidad: la Ley Fundamental de Bonn también «protege la identidad de género de las personas a las que no se les puede asignar ni el género masculino ni el femenino. Estas personas podrían desarrollar su personalidad más libremente si se atribuyera menos importancia a la asignación de género en general… La asignación de género es un factor particularmente relevante sobre cómo perciben las personas los demás y cómo ven su propia personalidad» (11). Y resalta la importancia que tiene en la construcción de la propia identidad: «el reconocimiento del género en la ley del estado civil tiene un efecto de creación de identidad...; define los aspectos centrales de la identidad legalmente relevante de una persona» (12). En definitiva la identidad propia, la real en una democracia, no la que atribuye tasadamente la ley, es parte esencial del libre desarrollo de la personalidad y de la dignidad humana. Pero no basta con construcciones grandilocuentes, pues la identidad en definitiva condiciona la vida misma de la persona, su quehacer cotidiano. Su desarrollo normal y tranquilo como persona.

La Sala Primera de nuestro Tribunal Supremo, ya a partir de la Sentencia 929/2007, de 17 de septiembre, dejó de exigir la operación quirúrgica de reasignación sexual para admitir la pretensión de rectificación de la mención del sexo y el nombre en la inscripción de nacimiento en el Registro Civil. Algo que ha reiterado en las Sentencias 158/2008, de 28 de febre-

(9) Utilizo la traducción de Ricardo García Macho y de Karl-Peter Sommermann, edición del Bundestag, Berlin 2010. También disponible en https://www.btg-bestellservice.de/pdf/80206000.pdf
(10) Epígrafe (39).
(11) Epígrafe (40).
(12) Epígrafe (47).

ro, 182/2008, de 6 de marzo, 183/2008, de 6 de marzo, 731/2008, de 18 de julio y 465/2009, de 22 de junio. Así lo Recuerda el Auto de dicha Sala de 10 de marzo de 2016 (recurso 1583/2015) por el que plantea cuestión de inconstitucionalidad en relación al artículo 1 de la Ley 3/2007, reguladora de la rectificación registral de la mención relativa al sexo de las personas, por presunta vulneración de los artículos 15, 18.1 y 43.1, en relación al 10.1, todos ellos de la Constitución, en cuanto que solo reconoce legitimación a las personas mayores de edad para solicitar la rectificación de la mención registral del sexo y del nombre. En todas las sentencias se resalta la importancia de la identidad y su relación con la dignidad de la persona y el libre desarrollo de la personalidad. Como también, tal como ya hemos visto, ha destacado el Tribunal Europeo de Derechos Humanos y el propio Tribunal de Justicia de la Unión Europea (13).

Por otra parte el derecho, a veces, otorga consecuencias jurídicas a identidades no siempre acreditadas pero si deducibles de indicios contrastados. No otra cosa persigue la posesión de estado (14), que permite configurar la identidad de la persona.

4. IDENTIDAD FÍSICA E IDENTIDAD DIGITAL

La identidad a que vengo refiriéndome se construye fundamentalmente en el entorno de la realidad física. Pero puede asimismo trasladarse al entorno digital. En éste, en efecto, confluyen elementos que configuran tanto la identidad que cada uno quiere o pretende darse como la que se otorga. Lo que ocurre es que en el entorno digital la heteroformación de la identidad depende de factores que no siempre operan en el mundo físico o lo hacen de un modo muy diverso. Pues en el entorno digital las posibilidades de conformar desde fuera del propio sujeto su identidad y con ello su personalidad son sin duda mucho más numerosas, y cualitativamente diversas.

¿Cómo altera lo digital el concepto de persona y de identidad? Hoy ya se habla de identidad digital (15), de persona digital (16).

Como ya he señalado en otro lugar (17), la identidad *online* puede llegar a ser definida no desde la autonomía de la persona sino heteróno-

(13) El citado Auto de 10 de marzo de 2016 incluye un muy completo análisis de la jurisprudencia de ambos tribunales.

(14) *Vid.*, del Código Civil, artículos 113 (acreditación de la filiación), 131 (declaración de filiación). *Vid.* asimismo los artículos 132, 133, 137 y 140 del mismo Código Civil.

(15) Clare Sullivan, *Digital Identity: An Emergent Legal Concept The role and legal nature of digital identity in commercial transactions*, University of Adelaide Press, 2011. Puede consultarse en http://www.jstor.org/stable/10.20851/j.ctt1sq5wqb.1.

(16) Daniel J. Solove, *The digital person. Technology and privacy in the Information Age*, New York University Press, 2004.

(17) *Derecho e innovación tecnológica. Retos de presente y futuro*, CEU Ediciones, Madrid, 2018, pp. 14-15.

mamente. El poder de los algoritmos puede configurar la identidad de la persona, una identidad controlada, diseñada y vigilada. Lo que pone en cuestión el propio derecho al libre desarrollo de la personalidad. Una identidad cuya configuración puede limitarse en base al modo en que se reconducen e incluso definen los gustos o prioridades de las personas. Se puede perfilar con facilidad a las personas y puede limitarse el marco de su desarrollo personal en un proceso difícil de identificar y ante el que puede resultar aún más difícil resistirse, pues en definitiva el algoritmo va a adecuar procesos a nuestros gustos, por lo que no será fácil objetar las indicaciones que de ello deriven. Pero al mismo tiempo puede cercenar la apertura y diversificación de la personalidad y por tanto de la propia identidad, pues en definitiva se va empobreciendo la capacidad de apertura a lo diverso y nuevo. Dicho con otras palabras y por ejemplo, si en base a nuestros gustos y de acuerdo a técnicas de *online behavioral advertising* (publicidad comportamental en línea) se nos muestran y ofrecen productos (de todo tipo, música, ocio, viajes, consumo…) que encajan o coinciden con nuestras preferencias como consecuencia del seguimiento que se hace de nuestra vida en internet, lo cierto es que con gran probabilidad nos sentiremos cómodos con lo que se nos ofrece, pero se cerrará o al menos no se facilitará el acceso a otros productos que pueden enriquecer nuestra personalidad. Algo que a largo plazo y de forma casi desapercibida puede llegar a condicionar e incluso definir desde fuera la personalidad del ser humano, que poco a poco pasa a ser más controlable y maleable.

Porque en realidad la mayor parte de las innovaciones tecnológicas que están produciéndose en la actualidad tienen directa (las más de las veces) o indirecta relación con el tratamiento de datos de carácter personal. Ya hace años se habló de las RFID, las *cookies* o más recientemente del *cloud computing*. Hablamos ahora también de *big data,* internet de las cosas, *wearables, bitcoin, Blockchain,* robótica, drones, Inteligencia Artificial*, gene drive technology, data driven innovation,* ciudades inteligentes, realidad aumentada… Cualquiera de estos conceptos es imposible sin el uso de datos. En particular la Inteligencia Artificial. Bostrom (18) nos recuerda que Nilson (19), uno de los más importantes expertos en inteligencia artificial, considera que la llegada de la inteligencia artificial de nivel humano puede producirse entre 2030 y 2100.

Las anteriores consideraciones nos ponen sobre aviso de algo innegable: la convivencia de un entorno físico y un entorno digital puede dar

(18) Bostrom, N. *Superinteligencia. Caminos, peligros, estrategias*, Teell Editorial, S.L., 2016, p. 19.

(19) Nilsson, N.J. *The Quest for Artificial Intelligence: a History of Ideas and Achievements*, Cambridge University Press, Nueva York, 2009.

lugar a una diversidad de identidades, física una, digital otra (u otras). En el futuro digital, en realidad ya hoy, junto a la identidad física convive la identidad virtual, online: «en el futuro la identidad será la materia prima más valiosa para los ciudadanos y ésta existirá principalmente online» [Schmidt y Cohen (20)]. Se ha afirmado asimismo que la identidad es el nuevo dinero (21) y se ha puesto de manifiesto la importancia que para las finanzas tiene la identidad digital (22). Lo que a su vez nos debe hacer cuestionar el alcance mismo del sujeto de dicha identidad: la persona.

5. IDENTIDAD DE LA PERSONA

La identidad es del ser humano, no de la máquina. Es de la persona (23). Esta afirmación, que parecería obvia, no lo es tanto, y menos lo será en el futuro.

Según el Diccionario de la Real Academia Española, persona es «Individuo de la especie humana». El Diccionario Panhispánico del Español Jurídico define persona como «sujeto de derecho, susceptible de ser titular de derechos y de contraer obligaciones». El Código Civil no define a la «persona natural», aunque sí señala que «el nacimiento determina la personalidad» (art. 29) y que «la personalidad se adquiere en el momento del nacimiento con vida, una vez producido el entero desprendimiento del seno materno» (art. 30, según redacción dada por la disposición final 3 de la Ley 20/2011, de 21 de julio). Por su parte el artículo 32 dispone que «la personalidad civil se extingue por la muerte de las personas», sin perjuicio de los supuestos de declaración de fallecimiento a que se refieren los artículos 193 y siguientes.

La Carta de Derechos Fundamentales de la Unión Europea «sitúa a la persona en el centro de su actuación» (24) y no cabe duda de que es la persona la que debe ser el centro de cualquier regulación sobre el entorno digital.

Siendo como es válido el régimen del Código Civil y válidas son las definiciones de persona que acabo de transcribir, lo cierto es que el propio concepto de persona está sujeto a no pocas tensiones. Rodotà en el trabajo que se incluye en la presente obra señala que «muchas transformaciones justifican la consideración del hombre como un «nuevo objeto conectado», presentado incluso como una «nano-bio-info-neuro máquina», re-

(20) *El futuro Digital*, Ediciones Anaya, Madrid, 2014.

(21) Birch, David, *Identity is the New Money*, London Publishing Partnership, Londres, 2014.

(22) Foro Económico Mundial, *A Blueprint for Digital Identity. The Role of Financial Institutions in Building Digital Identity*, 2016. Disponible en http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

(23) No me ocupo en estos momentos de la posible identidad o identificación de las personas jurídicas.

(24) Así lo recuerda Rodotà, *El derecho a tener derechos*, *op. cit.*, p. 137.

cordando al «hombre maquina» del que en el siglo XVIII hablaban La Mettrie y D'Holbach». Lasalle (25) hace suyas las advertencias de la artista Hito Steyerl al señalar que la evolución tecnológica hace que no sepamos muy bien qué somos o, mejor dicho, quienes somos: si sujetos desorientados por el impacto de la tecnología u objetos geolocalizados, cosificados por el uso que hacemos de los dispositivos inteligentes.

Por otra parte, parece que una de las características de la persona es la limitación temporal de su existencia. Una hipotética superación de esta circunstancia, ¿nos permitiría seguir hablando de persona o por el contrario nos encontraríamos ante una realidad diferente? Si se declara «la muerte de la muerte» (26), ¿podemos seguir considerando personas a quienes se han despojado de una de sus propiedades trascendentales, ontológicas?

La máquina puede tener identificación, pero no identidad. Pero esta afirmación, ¿podría ser puesta en cuestión cuando la máquina se humanice? No ya los robots, sino los «replicantes», ¿pueden llegar a tener identidad? ¿Podrá en el futuro generarse un ser vivo, una persona, al margen del cuerpo humano? Por otra parte, el transhumano, ¿puede llegar a perder su identidad, pese a mantener su identificación? ¿Podría llegarse a producir una suerte de cruce de trenes, de modo que la máquina se dirija hacia una posible atribución de identidad en la medida que se humaniza, y el ser humano hacia la pérdida de su identidad en la medida en que se mecanice? Pues como recuerda Rodotà en este mismo libro, «llegará un día, dicen los transhumanistas más radicales, en que el hombre ya no será un mamífero, se librará del cuerpo, se hará uno con el ordenador, de su cerebro se podrán extraer informaciones luego replicadas con precisión en un ordenador, y tendrá acceso a la inmortalidad» (27). Julian Huxley propone por primera vez el concepto de transhumanismo (28) en 1957. Y podría pensarse que la propuesta que hace es incompatible con la identidad (29) y con la dignidad de la persona.

6. IDENTIDAD E IDENTIFICACIÓN

Por otro lado identidad e identificación no son lo mismo (30). La identificación, afortunadamente, no identifica la entera identidad de la perso-

(25) *Contra el populismo. Cartografía de un totalitarismo posmoderno*, Penguin Random House, Debate, Barcelona, 2017, p. 89.

(26) Cordeiro Mateo, José Luis y William Wood, David, *La muerte de la Muerte*, Editorial Deusto, Barcelona, 2018.

(27) «Del humano al posthumano», en este mismo libro.

(28) Julian Huxley, «Transhumanism», en *New Bottles for New Wine*, Chatto & Windus, Londres, 1957, pp. 13-17

(29) Héctor Velázquez Fernández, «Transhumanismo, libertad e identidad humana», *Thémata. Revista de Filosofía*. Número 41. 2009, pp. 577 y ss.

(30) Sobre identidad e identificación *vid.* Rodotà, «Cuatro paradigmas…», *op. cit.*, p. 275 de la publicación en *El derecho a tener derechos»*.

na sino sólo de los atributos de la misma necesarios para una relación jurídica segura. La identificación hace referencia a esos atributos o elementos que son necesarios para las relaciones jurídicas: el nombre, una imagen o dato biométrico (fotografía, huella dactilar, imagen del iris…), la edad, quizá un domicilio, y un número o código identificativo y diferenciado. La identificación no debe hacer referencia a elementos distintos, y a estos efectos superfluos, que no son necesarios para esas relaciones jurídicas. Que incluso pueden perturbarla pues pueden generar situaciones discriminatorias, que en algunas ocasiones han llegado a ser literalmente letales (31). Incluso la identidad que no es objeto de identificación formal es la que realmente define a la persona. Identidad que debe adaptarse a la identificación formal en caso de que de ella deriven o puedan derivar consecuencias jurídicas.

7. IDENTIDAD E INTERRELACIÓN DERECHO, TÉCNICA Y ÉTICA

La gestión de la identidad e incluso su definición misma en la sociedad digital requieren de una incuestionable interrelación entre el Derecho, la Técnica y la Ética.

En primer lugar el Derecho debe encontrar su lugar en la nueva situación. Como señala Rodotà (32), las nuevas realidades producidas por la ciencia y la tecnología, hacen que la sociedad pida al derecho seguridad, más que protección. Hemos pasado de una época de «valores generalmente compartidos» a una situación de «politeísmo de valores». Aparece una «demanda de certeza a toda costa» y «el derecho acaba tomando tintes autoritarios, representa una imposición y no el reflejo de un sentir común». La frontera entre el derecho y el no-derecho, entre la exigencia de certeza social y la identidad individual se hace evanescente, y se plantea un interrogante capital: «¿cuáles son las áreas en las que puede intervenir legítimamente la norma jurídica? ¿Cuáles son en definitiva los límites del derecho?».

La extensión de esos límites se ha denunciado por muchos, que advierten que el derecho no debe poner puertas al campo, limitar o restringir el avance de la técnica. Y esto sin duda es así, pero tampoco debe abrir o no cerrar la puerta al desalmado. En este sentido el diálogo entre derecho y técnica se impone. Como ha señalado Lorenzo Martín Retortillo, «la técnica no tiene porqué arrumbar al Derecho» (33), pero este deseo no siempre se cumple. Esteve Pardo ha llegado a decir incluso que «se está

(31) Véase, si no, Edwin Black, *IBM and the Holocaust*, Crown Publishers, Nueva York, 2001.
(32) *La vida y las reglas. Entre el derecho y el no derecho*, Trotta, Madrid, 2010, p. 12.
(33) Martín Retortillo, L., «Presentación», en *La autorización administrativa. La Administración electrónica. La enseñanza del derecho administrativo hoy. Publicaciones de la Asociación Española de Profesores de Derecho Administrativo*, Thomson Aranzadi, Cizur Menor, 2003, p. 10

estableciendo como una nueva división de poderes entre el poder establecido por la ciencia y el poder establecido por el derecho», de modo que «la ciencia está ocupando extensos territorios tradicionalmente atribuidos al derecho y efectivamente dominados por él hasta tiempos muy recientes» (34). En cualquier caso, las leyes sólo son posibles si van de la mano de la realidad social y tecnológica, no contra ellas, como ha advertido Marc Langheinrich (35).

Ese diálogo ha de ser, en realidad, un trílogo. Pues además del derecho y la técnica ha de darse voz a la ética. El diálogo entre ética y derecho no es nuevo y nada debo decir ahora sobre ello, pues excedería con mucho el alcance de estas páginas. Sí debo resaltar que, en efecto, el derecho por sí sólo no basta para hacer frente a los retos que el avance tecnológico, que la innovación, trae consigo, y que tanto pueden incidir en la configuración de la identidad digital. En ciertos ámbitos esta perspectiva está ya asumida. Esta es la razón de ser, por ejemplo, de los Comités de Ética en la Investigación (36) o de la aproximación ética a la protección de datos. No hace mucho el Supervisor Europeo de Protección de Datos ha creado un *Ethics Advisory Group* que acaba de hacer público su Informe 2018 (37) y que se enfrenta a situaciones trascendentales para el ser humano, que en realidad van más allá que el más limitado ámbito de la privacidad: cómo conectar las nuevas tecnologías a los valores europeos; consecuencias de la interacción entre el ser humano y las máquinas; la dignidad en situaciones de una autonomía en declive; el poder del mercado para definir qué significa ser humano; el dilema de la multitud de opciones que proporciona un ecosistema digital controlado por nuevas formas de automatización; nuevos desafíos que se plantean a las nociones tradicionales de titularidad y derecho de propiedad aplicadas a datos personales; o la innovación responsable en el ecosistema digital. Creo que merece la pena dedicar unas líneas a las reflexiones que el Grupo hace sobre la identidad. Destaca siete cambios *(«shifts»)* que definen el nuevo panorama para la ética digital, y de entre ellos el primero es el paso del individuo al sujeto digital *(«From the individual to the digital subject»).* Los otros seis cambios son el paso de la vida analógica a la digital, del gobierno por las instituciones a la «gubernamentalidad» a través de datos, de una *«risk society»* a una *«scored*

(34) *Técnica, riesgo y Derecho. Tratamiento del riesgo tecnológico en el Derecho ambiental*, Ariel Derecho, Barcelona, 2009, pp. 99 y 100.

(35) «Privacy by Design-Principles of Privacy-Aware Ubiquitous Systems», en la Revista *Ubicomp 2001: Ubiquitous Computing 2001*, pp. 273-291, disponible en http://www.vs.inf.ethz.ch/res/papers/privacy-principles.pdf.

(36) Ver el muy interesante Documento Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada (2014), *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans*. Disponible en http://www.pre.ethics.gc.ca/pdf/eng/tcps2-2014/TCPS_2_FINAL_Web.pdf

(37) https://edps.europa.eu/sites/edp/files/publication/18-01-25_eag_report_en.pdf

society», de la autonomía del ser humano a la convergencia entre humanos y máquinas, de la responsabilidad individual a la *«distributed responsability»,* de la justicia penal ex post a la justicia predictiva. Y como digo, el primero de tales cambios es el que tiene que ver con el sujeto digital. En el que la definición de la identidad adquiere una especial relevancia.

Por otra parte, el Grupo señala que una de las condiciones para el desarrollo éticamente sostenible de las tecnologías digitales es la libertad para desarrollar y expresar la propia identidad sin interferencias (38). También señala que a medida que las tecnologías de identificación mejoran a través, por ejemplo, del reconocimiento facial, el desafío de proteger la identidad de los sujetos digitales frente a algunos, al tiempo que se comparte con otros, se exacerba (39).

El Grupo de Ética del Supervisor Europeo propone, en fin, varias conclusiones, entre las que ha de destacarse la primera: «la dignidad de la persona permanece inviolable en la era digital. La vida en la era digital está cercana a enfrentarse con el principio básico de la personalidad: la dignidad. La experiencia digital transforma nuestra comprensión de la identidad personal, la experiencia humana y las interacciones sociales. La vida digital tendrá que ser compatible con la naturaleza inviolable de la dignidad humana» (40).

Esta perspectiva ética, este trílogo entre derecho, técnica y ética ha de traducirse también en el protagonismo que los principios han de tener en la regulación jurídica de la innovación y sus consecuencias sobre la identidad en la sociedad digital. En más de una ocasión he señalado (41) que cuanto más novedoso, más concreto, más específico es un tema más hemos de acudir a los principios, al objeto de evitar la obsolescencia del derecho. En una época en que la obsolescencia programada de los objetos y dispositivos es incluso considerada delito, como acaba de hacerse (enero de 2018) en Francia, debe evitarse la del derecho, y para ello debería evitarse hacer girar la regulación en torno a previsiones excesivamente pegadas a la realidad concreta que debe ser regulada. Lo que nos lleva a plantear la trascendencia de los principios generales en la regulación.

En este punto voy a permitirme transcribir (42) unas líneas de mi Maestro, Eduardo García de Enterría, relativas a los principios del Derecho, sacadas de su memoria de Cátedra para la Complutense, en 1961:

> «La meditación científica sobre el Derecho no es una operación abstracta y puramente culturalista que no tenga nada que ver con la vida real del Dere-

(38) Informe 2018, *cit.*, p. 21.
(39) Informe *cit.* p. 26.
(40) Informe *cit.*, p. 30.
(41) Últimamente en *Derecho e innovación tecnológica…*, *op. cit.*, pp. 16 y ss.
(42) Como ya he hecho en *Derecho e innovación tecnológica…*, *op. cit*, pp. 17 y ss.

> cho (como la astronomía no influye para nada en el comportamiento de los astros), sino que es ella misma un trozo de esta vida real del Derecho. Bien entendido esto no es la expresión de un pío deseo, sino un hecho efectivo y de común experiencia, pues es notorio que «todo gran jurista ha dejado su huella en la historia» (De Castro), pero en la historia del Derecho vivido y no sólo en la de la ciencia.
>
> Ahora bien, la ciencia jurídica no tiene otra misión que la de desvelar y descubrir, a través de conexiones de sentido cada vez más profundas y ricas, mediante la construcción de instituciones y la integración respectiva de todas ellas en un conjunto, los principios generales sobre los que se articula y debe, por consiguiente, expresarse el orden jurídico. Este, en la sugerente expresión de Simonius, "está impregnado de principios hasta sus últimas ramificaciones", de modo que en hacer patente esa oculta y profunda vida de los principios está la augusta función del científico del Derecho, y no en ofrecer clasificaciones o sistematizaciones geométricas, lógicas o nemotécnicas de la materia de las leyes. Una ciencia jurídica puramente exegética (aunque quisiese incluir los "principios incluidos por el legislador en sus normas") no podría responder nunca a la clásica objeción de Von Kirchmann: "tres palabras rectificadoras del legislador convierten bibliotecas enteras en basura"; el que esto no haya sido así y las obras de los grandes juristas de la historia no sólo no sean basura, sino que hayan adquirido un permanente y eficaz valor clásico, es justamente porque en ellas se ha acertado a expresar un orden institucional de principios jurídicos no sometidos a la usura del tiempo.
>
> La superioridad del Derecho Romano sobre otros sistemas jurídicos históricos anteriores o posteriores estuvo justamente, no ya en la mayor perfección de sus leyes (acaso las de Licurgo, o las de cualquier otro de los grandes legisladores mitificados fuesen superiores), sino en que sus juristas fueron los primeros que se adentraron en una jurisprudencia según principios, la cual ha acreditado su fecundidad, e incluso, paradójicamente, su perennidad, y hasta su superior certeza, frente a cualquier código perfecto y cerrado de todos los que la historia nos presenta (43).»

Las palabras de García de Enterría nos permiten concluir que ante la innovación tecnológica hemos de volver a los principios, a lo esencial, pues de otro modo corremos el riesgo de movernos en un escenario cambiante, improvisando soluciones que terminan por quedar obsoletas antes incluso de ser plenamente aplicadas, desbordadas por la evolución, inmisericorde para el derecho, de los avances de la técnica.

8. CONTROL DE LA IDENTIDAD EN LA SOCIEDAD DIGITAL

Si compleja es la definición y control de la identidad de las personas en el mundo físico, más lo es, como ya he apuntado, en el entorno digital.

(43) *Reflexiones sobre la Ley los principios generales del Derecho*, Civitas, Madrid, 1984, pp. 33-35.

Donde además son muchos los factores, además de los que ya he señalado más atrás, que pueden alterar la identidad y la percepción que de la misma otros pueden tener. ¿Hasta qué punto la realidad aumentada puede definir nuestra identidad? ¿Hasta dónde llega nuestra identidad? ¿Es la que nosotros queremos mostrar o la que los demás muestran de nosotros? En el entorno digital puede llegar a ser difícil, incluso para algunos imposible, ser uno mismo, es decir mantener la propia identidad. Byung-Chul Han considera que el «*homo digitalis*» «mantiene su identidad privada», es un «*alguien penetrante* que se expone y solicita la atención» si bien actúa de forma aislada, sin noción de «nosotros». Los medios digitales aíslan a las personas, que actúan como un enjambre, no como una comunidad (44), y que sin embargo se expone en una transparencia cuasi pornográfica (45).

Quizá Han tenga razón en lo que se refiere al mantenimiento de la identidad privada, pero no cabe duda de que expuesto o no voluntariamente a la visión virtual de los demás, el que él llama *homo digitalis* está claramente expuesto a la posible pérdida no sólo de su privacidad sino de su identidad misma. Por eso en el entorno digital, en la sociedad digital, es imprescindible reforzar los esfuerzos, técnicos y jurídicos, para preservar la identidad y la privacidad. Lo que puede llegar a exigir un esfuerzo muy considerable. ¿Qué alcance puede llegar a tener, incluso económicamente, preservar nuestra identidad en el entorno digital? Se ha señalado que en 2014 en Reino Unido se invirtieron más de tres mil trescientos millones de Libras para intentar garantizar la seguridad de la identidad digital (46).

9. CONCLUSIÓN. DERECHO, TECNOLOGÍA Y ÉTICA PARA LA PROTECCIÓN DE LA IDENTIDAD DIGITAL

Y en este panorama casi desolador el derecho, la tecnología y la ética, como antes señalaba han de ir de la mano para proteger la identidad digital y en consecuencia la dignidad misma de la persona.

El derecho ha de aportar los principios. Como hemos dicho la identidad de la persona se configura hoy en la sociedad digital en torno al tratamiento de datos personales. Por lo que resulta de especial relevancia la aprobación del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección

(44) *En el enjambre*, Herder, Barcelona, 2016, p. 28.
(45) Biung-Chul Han, *La sociedad de la transparencia*, Herder, Barcelona, 2014.
(46) Mitchell, Alan, y Smith, *Economics of Identity The size and potential of the UK market for identity assurance*, Economics of Identity White Paper. The Open Identity Exchange/Ctrl-Shift, Octubre 2015. Disponible en https://www.ctrl-shift.co.uk/wp-content/uploads/2014/06/Ctrl-Shift-and-OIX-Economics-of-Identity.pdf

de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE: Reglamento general de protección de datos (47), plenamente aplicable desde el 25 de mayo de 2018 (48). Como he señalado en otra ocasión (49) el Reglamento supone la apuesta europea por el máximo respeto a la protección de datos en base al reconocimiento que de tal derecho contiene el artículo 8 de la Carta Europea de los Derechos Fundamentales (50). Supone el cambio a un nuevo modelo de protección de datos (51) que está llamado a ser la referencia global en protección de datos. No sólo por la influencia que el texto pueda tener en los marcos y desarrollos normativos de no pocos países, sino por la extraordinaria amplitud de su ámbito de aplicación territorial (art. 3.2). Las más grandes empresas multinacionales que basan en el tratamiento de datos gran parte de su actividad (Google, Facebook, Amazon, Microsoft, Linkedin, Yahoo, y tantas otras) van a tener que adaptarse obligatoriamente al nuevo Reglamento Europeo. Ya sólo esta consecuencia es de un alcance y trascendencia hasta ahora desconocidos. Y se inscribe en un proceso de globalización de la protección de datos que va consolidándose sin pausa en los últimos años y que resulta imprescindible para conseguir que la tutela de la protección de datos no se quede en meras palabras o buenas intenciones en la sociedad digital. Que además resulta especialmente protegida, y con ella el control sobre la identidad digital, a través de la definición de principios como el de responsabilidad proactiva, privacidad desde el diseño y privacidad por defecto.

Por otra parte, son de extraordinaria importancia diversas Sentencias del Tribunal de Justicia de la Unión Europea que afectan directamente a grandes multinacionales y que decididamente advierten que la normativa europea de protección de datos tiene un alcance tal que no está dispuesta a que la defensa de la privacidad ceda cuando los tratamientos de datos puedan llevarse a cabo desde fuera de las fronteras europeas. Me refiero a las Sentencias de 13 de mayo de 2014, Asunto C-131/12,

(47) *DOUE* n.º L 119, de 4 de mayo de 2016.

(48) Sobre el Reglamento, entre otras obras, *vid.* Piñar Mañas, J. L. (Dir.), Álvarez Caro, M. y Recio Gayo, M. (Coords.) *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Editorial REUS, Madrid 2016; López Calvo, José, *Comentarios al Reglamento Europeo de Protección de Datos*, SEPIN, Madrid, 2017.

(49) «Sociedad, innovación y privacidad», en *Información Comercial Española*, n.º 897, julio-agosto 2017, pp. 71 y ss.

(50) 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

(51) Así lo he señalado en «Introducción. Hacia un nuevo modelo europeo de protección de datos», en Piñas Mañas (dir.), *Reglamento General de Protección de Datos...*, *op. cit.*, pp. 15 y ss.

Google Spain, S.L. y Google Inc. vs. Agencia Española de Protección de Datos y Mario Costeja González, en la que, como es sabido, se exige a Google Inc. que atienda el derecho al olvido de una persona que la solicita en España; de 6 de octubre de 2015, asunto C362/14, *Maximillian Schrems,* por la que se declara inválida la Decisión 2000/520/CE de la Comisión Europea, de 26 de julio de 2000, sobre la adecuación de la protección conferida por los principios de puerto seguro; y de 8 de abril de 2014, asunto C 594/12, *Digital Rights Ireland,* por la que se declara inválida la Directiva 2006/24/CE, de retención de datos (52).

El control sobre la propia identidad en la sociedad digital se pretende fortalecer tecnológicamente con iniciativas tales como el sistema *Self Sovereign Identity* (53), por el que, en base al principio de autodeterminación informativa en relación con los propios datos, y con la participación de diversos actores en el mundo digital puede garantizarse con mayor fiabilidad la identidad de las personas a través sobre todo de la emisión de testimonios relacionados con los atributos que definen la identidad.

En fin, desde la perspectiva ética el Grupo de Trabajo sobre Ética del Supervisor Europeo ha advertido que los encuentros directos entre personas en el mundo digital son reemplazados cada vez más por perfiles algorítmicos remotos. Como consecuencia, las cualidades psicológicas, espirituales, culturales, sociales, morales y de otra índole de las personas tienden a detectarse más a menudo a través de datos personales, tomados de múltiples fuentes. Hoy en día, la identidad a menudo se establece a través de construcciones y patrones digitales. Sin embargo, en la nueva era digital, debemos recordar que los datos no agotan ni la identidad personal ni las cualidades de las comunidades a las que pertenecen los individuos, que la protección de datos no solo trata sobre la protección de datos, sino principalmente sobre la protección de las personas que hay tras los datos. Las personas son representadas digitalmente, lo que puede traer consigo nuevas formas de vulnerabilidad. Ante esta situación el Grupo resalta que la protección de datos no es un asunto meramente técnico o legal. Es profundamente humano (54).

(52) *Vid.* Piñar Mañas, José Luis, y Recio Gayo, Miguel, *El derecho a la protección de datos en la jurisprudencia del Tribunal de Justicia de la Unión Europea*, La Ley-Wolters Kluwer, Madrid, 2018.

(53) *Vid.* por ejemplo *Self Sovereign Identity. A guide to privacy for your digital identity with Blockchain*, disponible en https://medium.com/@AlexPreukschat/self-sovereign-identity-a-guide-to-privacy-for-your-digital-identity-5b9e95677778

(54) Ethics Advisory Group, *Informe 2018,* pp. 11-12.

CAPÍTULO 4

ROBOTS, INTELIGENCIA ARTIFICIAL Y PERSONA ELECTRÓNICA

Moisés Barrio Andrés
Letrado del Consejo de Estado. Doctor en Derecho.
Profesor de Derecho Digital. Abogado y Árbitro

1. INTRODUCCIÓN

Los robots y los sistemas de inteligencia artificial, que nosotros englobamos conjuntamente dentro del concepto de «robot» (o también «sistema robótico»), están entrando rápidamente en los entornos domésticos, empresariales y públicos. Los robots ya ayudan a realizar cirugías, ciertos drones entregan paquetes, y los coches y camiones están empezando a conducirse de forma autónoma. Y, próximamente, las administraciones públicas y los tribunales de justicia tendrán que lidiar con procedimientos relativos a los mismos. Incluso, a medio plazo, los robots interactuarán progresivamente de manera autónoma e independiente del control huma-

no, con la posibilidad de que las personas se hibriden con robots para mejorar o restablecer sus funciones fisiológicas (*cyborg*).

Si bien la revolución de la informática primero y de Internet después ha transformado y alterado diversas industrias, la incorporación de sistemas robóticos capaces de tomar decisiones autónomas, acumular conocimientos a partir de datos no estructurados (1) y actuar físicamente en el mundo puede ser altamente perturbadora, tanto en los entornos existentes como mediante la creación de productos y servicios innovadores y novedosos. Al mezclar esta disrupción técnica con las presiones económicas y demográficas y los cambios en el flujo global del comercio, el efecto de la robótica y la inteligencia artificial será de gran alcance: en el hogar, en el trabajo y en nuestras ciudades, hospitales, granjas, supermercados y en las infraestructuras de las que dependemos, por citar sólo una gavilla de entornos.

Esta revolución conlleva nuevos desafíos a los que las normas existentes no dan respuesta. Es necesario abordar no sólo cuestiones técnicas, sino también sociales, económicas, de salud, éticas y jurídicas con el objeto de garantizar la libertad, autonomía y seguridad de los seres humanos, esclareciendo cuestiones tales como cuál es la condición jurídica del robot, si deben tener o no un régimen especial de derechos y obligaciones, quién asume la responsabilidad de las acciones y omisiones de los sistemas robóticos autónomos e impredecibles, o el conjunto mínimo indispensable de medidas organizativas, técnicas y legales para asegurar su desarrollo seguro y minimizar los riesgos a los que están expuestas las personas. La seguridad jurídica es crucial para el propio desarrollo de la tecnología y del mercado de la robótica, que alcanzará los 45 billones de dólares para el año 2020, y desde 2017 a 2020 se instalarán más de 2 millones de robots en fábricas de todo el mundo (2).

En efecto, el Derecho tiene que brindar un marco legal de referencia a los operadores del sector, quienes están seriamente preocupados por las implicaciones de sus actividades y, además, necesitan disponer de una cobertura jurídica ante potenciales creaciones que superen los confines de los laboratorios. Por otro lado, el Derecho está obligado a elaborar una regulación avanzada que pueda impulsar el desenvolvimiento de la robótica y asegurarle un desarrollo congruente con los valores propios del ordenamiento jurídico.

Entre las distintas iniciativas reguladoras (3), cabe destacar la importante Resolución del Parlamento Europeo, de 16 de febrero de 2017, con

(1) Sobre su problemática, *vid*. Barrio Andrés, Moisés: *Internet de las Cosas*. Editorial Reus, Madrid, pp. 80 y ss.

(2) Informe «World Robotics 2017 Industrial Robots» de la International Federation of Robotics, de 27 de septiembre de 2017.

(3) *Vid*. su estudio detallado en Aransay Alejandre, Ana María: «Antecedentes y propuestas para la regulación jurídica de los robots», en Barrio Andrés, Moisés (dir.): *Derecho de los Robots*. Editorial Wolters Kluwer, Madrid, 2018, pp. 89 y ss.

recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)), que recoge las principales líneas de trabajo para el legislador al respecto, entre las que destacamos:

a) la creación de una Agencia Europea de Robótica e Inteligencia Artificial;

b) la elaboración de un código de conducta ético voluntario que sirva de base para regular quién será responsable de los impactos sociales, ambientales y de salud humana de la robótica y asegurar que operen de acuerdo con las normas legales, de seguridad y éticas pertinentes. Prevé por ejemplo la exigencia de que los robots incluyan interruptores para su desconexión en caso de emergencia. Y recoge la necesidad de crear una Carta sobre Robótica;

c) promulgar un conjunto de reglas de responsabilidad por los daños causados por los robots;

d) crear un estatuto de persona electrónica;

e) estudiar nuevos modelos de empleo y analizar la viabilidad del actual sistema tributario y social con la llegada de la robótica;

f) integrar la seguridad y la privacidad como valores de serie en el diseño de los robots; y

g) crear un Registro Europeo de los robots inteligentes.

Se hace, así, evidente la urgente necesidad de definir las condiciones de legitimidad jurídica de los nuevos sistemas robóticos y establecer con precisión un régimen claro de derechos y obligaciones. La primera y esencial cuestión tiene que ver con la existencia de un marco jurídico que garantice un progreso tecnológico que refuerce el libre desarrollo de la personalidad y los derechos fundamentales, al tiempo que impida que la tecnología se convierta en una vía para hacer a las personas menos humanas y más pasivas, con una autonomía reducida, con una dependencia creciente y una pérdida de la capacidad de iniciativa con una eventual situación de subordinación irreversible que pueda expropiar la libertad y la humanidad misma.

Su análisis jurídico debe enmarcarse dentro de una nueva rama jurídica autónoma, el Derecho de los Robots (*Robot Law*), para dar respuesta a estos insólitos desafíos y situaciones disruptivas, lo cual hemos desarrollado recientemente en otra obra, precisamente titulada *Derecho de los Robots* (4), a la que también me remito para una referencia bibliográfica *in extenso*. Ahora bien, y como también hemos defendido (5) al hilo de la autonomía científica y académica del Derecho de Internet, se postula aquí un Derecho de los Robots que a la vez adapte el Derecho general –en

(4) Barrio Andrés, Moisés (dir.): *Derecho de los Robots*. Editorial Wolters Kluwer, Madrid, 2018.
(5) Barrio Andrés, Moisés: *Fundamentos del Derecho de Internet*. Editorial Centro de Estudios Políticos y Constitucionales, Madrid, 2017, pp. 147 y ss.

cuanto que previamente vigente–, y, en la medida de lo necesario, genere un Derecho nuevo como ya está sucediendo en los Estados Unidos al hilo del uso doméstico de drones y coches sin conductor por ejemplo (6).

En todo caso, la robótica es la próxima tecnología transformadora de nuestro tiempo. Pero la robótica posee un conjunto de rasgos estructurales diferentes a los de Internet (7): combina, posiblemente por primera vez, la *promiscuidad de la información* (8) con la *capacidad de causar daño físico* (9). Los robots muestran un comportamiento cada vez más prometedor, permitiendo realizar un número creciente de tareas que eran, hasta fechas recientes, insospechadas, y los hace cada vez más presentes en multitud de entornos públicos y privados.

De hecho, estamos siendo partícipes de la incorporación gradual a nuestras vidas de los llamados asistentes virtuales, cuya misión es facilitar la vida cotidiana a las personas. Pueden ser antropomorfos o no, o incluso no tener ninguna forma tangible como es la aplicación Siri® de Apple. Estos productos son auténticos «cerebros globales», porque utilizan contenidos disponibles en Internet y no están, por ello, sujetos a las limitaciones de sus diseñadores. Igualmente ya están disponibles humanoides como Pepper® (10), cuyo propósito es ser un compañero emocional del propietario, en el sentido de hablar y entender las emociones humanas, o incluso ser capaz de expresar algunas.

En efecto, la inminente presencia generalizada de la robótica en la sociedad, como fue el caso de Internet en su momento, va a alumbrar profundas tensiones sociales, culturales, económicas y, por supuesto, jurídicas, que comienzan a desbordar los contornos tradicionales del Estado constitucional. Por todo ello, la robótica lleva ínsita un inevitable cambio de paradigma legal, que va a provocar transformaciones estructurales en el Derecho, sus instituciones y operadores jurídicos. Se avecina un auténtico *tsunami digital*, que puede dar un vuelco a los instrumentos jurídicos que garantizan la identidad e incluso la libertad de las personas.

Por todo ello, en el próximo epígrafe expondremos los contornos de la propia robótica y sus caracteres singulares como punto de partida para analizar después si cabe atribuir a los robots más avanzados una personalidad electrónica independiente.

---

(6) *Vid.* el listado en Barrio Andrés, Moisés (dir.): *Derecho de los Robots*, *op. cit.*, p. 84, nota. 48.

(7) Barrio Andrés, Moisés: *Fundamentos…*, *op. cit.*, pp. 38 y ss.

(8) Con esta denominación se alude a que los nodos en la red a la que están conectados los sistemas robóticos están compartiendo continuamente información con numerosos otros nodos (como una persona que tiene relaciones sexuales con muchas personas diferentes). La metáfora de la «promiscuidad» también sugiere la vulnerabilidad a la infección (por analogía a la enfermedad venérea), en este caso al sabotaje informático y la consecuente causación del daño.

(9) Un hecho cierto es que los drones ya han provocado accidentes, y es ocioso incluir aquí una relación de casos expuestos en los medios de comunicación.

(10) *Vid.* https://www.ald.softbankrobotics.com/en/robots/pepper/

2. ROBOTS, INTELIGENCIA ARTIFICIAL Y DERECHO

Resulta indiscutible que los avances en robótica e inteligencia artificial tienen cada vez más difusión y aplicación en la sociedad. La plena integración de estas tecnologías disruptivas en las vidas cotidianas no es tan lejana como en principio podría parecer. Los científicos y aficionados, a la sazón primeros precursores de la revolución de Internet, han acogido la robótica con júbilo. El propio Departamento de Defensa de los Estados Unidos, que aportó el soporte y subvención pública de la red ARPANET –la «abuela de Internet»– y de su tecnología que hicieron posible lo que hoy conocemos como Internet, viene financiando desde hace varias décadas múltiples proyectos robóticos (11). Incluso hace ya más de doce años que algunas de las mismas universidades que operaban los primeros nodos de la red ARPANET participaron en un concurso para construir vehículos no tripulados (12).

También el sector privado ha mostrado un creciente interés en la robótica. Los grandes señores de Internet han dirigido también su atención hacia la robótica y sus tecnologías constitutivas. Así, por ejemplo, Google ha adquirido al menos nueve empresas de inteligencia artificial por cantidades que ascienden a billones de dólares, al tiempo que ha desarrollado Firefly®, un prototipo de automóvil sin conductor. Por su parte, Amazon compró en 2012 una empresa de robótica para ayudar a automatizar sus almacenes (13), y a finales de 2014 anunció un plan para entregar algunos paquetes por medio de drones. En la actualidad, existen varios fondos de capital de riesgo especializados en financiar proyectos de esta naturaleza. Incluso algunos bufetes de abogados disponen ya de departamentos completos alrededor de la robótica y la inteligencia artificial.

En definitiva, la robótica (que también incluye a la inteligencia artificial), como la siguiente tecnología transformadora después de los ordenadores e Internet, representa una realidad que ya lleva un tiempo entre nosotros. No obstante, la robótica posee un conjunto diferente de cualidades esenciales. Estos atributos, y las experiencias que ocasionan, generan un elenco sustantivo de cuestiones jurídicas disruptivas, algunas de las cuales pueden ser resueltas por las técnicas del Derecho de Internet, si bien otras desbordan su marco al no tener un previo parangón. Por todo ello, el siguiente objeto de atención en nuestro estudio será identificar tales características únicas, para examinar en el próximo epígrafe la viabilidad de una personalidad electrónica para los robots. Previamente vamos

(11) *Vid.* en detalle, Singer, Paul: *Wired for War: the robotics revolution and conflict in the 21st century.* Editorial Penguin Press, Nueva York, 2009.

(12) *Vid.* http://archive.darpa.mil/grandchallenge/

(13) A comienzos de 2018 Amazon emplea más de 100.000 robots, frente a los escasos 1.000 en 2013.

a perfilar un concepto de robot que nos permita diferenciarlo del conjunto de artefactos preexistentes.

2.1 **Concepto**

Con el término «robot» se alude a toda una serie de ingenios que comprenden, desde androides y otras formas de inteligencia artificial con aspecto humanoide cada vez más sofisticados y aplicables a infinidad de tareas, hasta meras máquinas que realizan autónomamente algunas tareas domésticas. En definitiva, se incluyen en esta categoría los robots asistentes, los drones de uso militar o civil, los automóviles sin conductor, los *rovers* o robots de exploración espacial, ciertos aparatos de utilización médica, los ya clásicos de uso industrial, los robots imprimibles cuyas piezas están fabricadas con impresoras 3D, las ropas tecnológicas (*wearables*) y otros dispositivos de mejora del cuerpo humano (*cyborgs*), o incluso los nanorobots que emplean la nanotecnología para insertarse en el cuerpo humano con el objetivo de combatir determinados tipos de enfermedades.

No obstante, existe una imposibilidad sustancial de apuntar una noción suficientemente precisa de robot que responda a las múltiples formas de implementación robótica existentes y que sean inventadas en el futuro. De hecho, esta dificultad es una constatación común y un punto de partida constante, aunque negativo, de cualquier reflexión o estudio sobre el tema. En esta búsqueda de un rasgo característico, la doctrina pone con frecuencia el acento en la capacidad de los robots de ejecutar tareas de manera automatizada, o bien en la autonomía de la máquina frente al control humano, en la movilidad en el ambiente o, incluso, en el dato exterior de su apariencia como figura humana.

Pero sí hay un cierto consenso en destacar que los auténticos robots tendrían una serie de características distintivas desde el punto de vista técnico, condensadas en la capacidad de recoger datos mediante sensores (*sentir*), de procesar los datos en bruto (*pensar*) y de planificar y cumplir acciones mediante conocimientos e informaciones adquiridas, generalmente en función de objetivos prefijados (*actuar*). En cambio, serían atributos solo eventuales la capacidad de comunicación con un operador, con otros robots o con una red externa, y la de aprendizaje.

De este modo, un robot *strictu sensu* sería aquel «*objeto mecánico que capta el exterior, procesa lo que percibe y, a su vez, actúa positivamente sobre el mundo*». Es lo que los profesores Pfeifer y Scheier (14), con expresión exacta, bautizaron como el paradigma de «sentir–pensar–

(14) Pfeifer, Rolf y Scheier, Christian: *Understanding Intelligence*, Editorial MIT Press, Cambridge, 1999, p. 37.

actuar», que permite sustantivar a los robots de otras tecnologías. Por ejemplo, un ordenador portátil con una cámara puede, hasta cierto punto, captar y procesar el entorno exterior. Pero el portátil no actúa sobre el mundo físico. Un coche de control remoto con una cámara detecta y afecta físicamente a su entorno, pero depende del conductor humano para su pilotaje.

En suma, la esencia de un robot o sistema robótico es que la tecnología combine los apuntados tres atributos de sentir, pensar y actuar.

Por lo que se acaba de mostrar, y como sostienen prestigiosas voces autorizadas como Singer (15) o Calo (16) en los Estados Unidos o Palmerini (17) en Europa, los robots son máquinas que se construyen sobre el señalado paradigma de «sentir–pensar–actuar». Es decir, son dispositivos fabricados por el hombre con tres componentes seminales:

a) *sensores* que vigilan el entorno y detectan cambios en él,

b) *procesadores* o *inteligencia artificial* que deciden cómo responder, y

c) *actuadores* que operan sobre el entorno de manera que refleje las decisiones anteriores, provocando algún tipo de cambio en el mundo alrededor de un robot.

Cuando estos factores actúan conjuntamente, entonces el artefacto deviene en robot, y adquiere la funcionalidad de un organismo artificial, capaz de operar independientemente, libre de la intervención humana (o de otra índole) y, por extensión, libre de condicionantes externos.

Un artilugio no actúa, y por lo tanto no es un robot, simplemente proporcionando información en un formato digital. Debe *ser* de alguna manera. Un robot en el sentido más genuino y completo del término existe en el mundo como un objeto corpóreo con la capacidad de interactuar físicamente. Aunque esta aproximación no deja de tener inconvenientes y excluye los programas informáticos y los ordenadores de la noción de robot (a pesar de su capacidad para percibir e interactuar con el entorno físico a través de interfaces de usuario o actuadores (18)), en todo caso la línea entre cualquier inteligencia artificial y los robots es borrosa en parte porque muchos de los problemas éticos y de regulación que surgen en el marco de la robótica también aparecen en el contexto de la inteligencia artificial.

(15) Singer, Paul: *Wired for War…*, *op. cit.*, p. 67.

(16) Calo, Ryan: «Robots and ethics», en Lin, Patrick (coord.): *Robot ethics: the ethical and social implications of robotics*, Editorial MIT Press, Cambridge, 2012, p. 187.

(17) Palmerini, Erica: «Liability and risk management in robotics», en *Digital Revolution: Challenges for Contract Law in Practice Nomos*, vol. 1, núm. 1, 2016.

(18) Sobre los mismos, *vid.* Barrio Andrés, Moisés: *Internet de las Cosas*, *op. cit.*, pp. 35 y ss.

No obstante, para nosotros no es tan importante la distinción entre los robots y los agentes de inteligencia artificial. A medida que avanza la innovación, la diferenciación entre estos dos tipos de tecnologías puede ser mucho menos importante para el Derecho de lo que parece en la actualidad. Todavía no conocemos si los límites entre estas dos tecnologías se desdibujarán cada vez más o, por el contrario, se separarán gradualmente. A nuestro juicio, no existirá una distinción útil entre ambos tipos de ingenios, que se fundirán en una única categoría. Así viene sucediendo en el Derecho de Internet con la propia red telefónica e Internet, que progresivamente se están fusionando en un único medio de intercambios digitales diversos que proporciona un espacio infinito para la creación de nuevas aplicaciones y plataformas, y donde el cobre ha dado paso a la voz IP.

A la postre, el robot (o sistema robótico), en cuanto entidad dotada de una *materialización física* pero también de un *sistema de software* que procesa información, presenta la potencialidad y los riesgos de ambos mundos, el físico y el virtual. Combinando estos dos rasgos característicos, en particular, se está en capacidad de asegurar el desarrollo de un amplio espectro de funciones útiles, pero también de exponer al usuario, así como a otras personas, al riesgo de lesiones en caso de interacción defectuosa en la esfera física y moral.

Clave en esta noción es poner de relieve cómo las características que más sobresalen en la robótica van a depender esencialmente de cómo las personas vayan a usarla. A menudo los usuarios emplean la tecnología de maneras que sus diseñadores no preveían ni pretendían. Esto es especialmente así en lo que lo que Zittrain llama «tecnologías generativas» (19), definidas como «*la capacidad de un sistema para producir cambios imprevistos a través de contribuciones sin filtrar provenientes de audiencias amplias y variadas*», y que ofrecen múltiples entornos y posibilidades de innovación y un extraordinario progreso en el desarrollo de formas de expresión artística y política. Lo que parece particularmente destacado sobre la robótica cambiará con el tiempo a medida que las personas trabajan con y por medio de la nueva tecnología.

Los rasgos apuntados por Calo han sido relativizados por Balkin (20) en una sugestiva polémica reciente. Indica este último autor cómo, a medida que nuestro mundo se llena de robots, nuestras vidas y relaciones de poder social, político y económico también cambiarán, planteando nuevas e inesperadas aplicaciones de la robótica y los consiguientes desafíos para el Derecho. Además, la tecnología, al igual que el Derecho, media las rela-

(19) Zittrain, Jonathan: «The Generative Internet», en *Harvard Law Review*, Vol. 119, 2006.
(20) Balkin, Jack: «The path of robotics law», en *California Law Review Circuit*, Vol. 6, 2015.

ciones sociales entre los seres humanos, incluidas las relaciones de poder y control. Debido a que estas relaciones están siempre evolucionando, la evaluación de lo que es más interesante o preocupante acerca de la robótica puede variar también. A causa de que el uso de la robótica en la vida social evoluciona, y porque la gente encuentra continuamente nuevas maneras de emplear la tecnología para bien o para mal, el autor reputa inútil congelar ciertas características de la robótica en uso en un momento particular y calificarlas de «esenciales». Tales características tienen que ser «*necesariamente puestas en estrecha conexión con los modos de utilización de los robots por las personas físicas y jurídicas*».

En cualquier caso, se trata de una aproximación técnica a efectos de centrar el objeto de nuestro estudio. Lo que resulta relevante, a efectos jurídicos, no es tanto la arquitectura técnica como las posibilidades y riesgos que la robótica genera y circunscribe. Del mismo modo que los debates en torno a Internet no se centran en la conmutación de paquetes como tal o en el protocolo TCP/IP, sino en la comunicación masiva, asíncrona y sin distancias que esta tecnología permite, lo importante son las cualidades singulares que caracterizan a la robótica y a la inteligencia artificial como tecnología transformadora, a cuya exposición dirigiremos nuestros próximos pasos.

2.2 **Características**

Al igual que los rasgos seminales de Internet interactúan con el Derecho en formas novedosas y originan problemas jurídicos insospechados, así también las características esenciales de la robótica están alumbrando situaciones jurídicas disruptivas.

Una sistematización que goza de gran predicamento en la doctrina es la propuesta por el propio Calo (21), para quien la robótica entrañaría tres propiedades privativas (o *transformativas*, como le gusta decir):

a) corporeidad (frente al *software*, el robot es material o con una materialidad corpórea);

b) impredecibilidad (a diferencia de una simple máquina, el robot piensa y decide con cierta autonomía); y

c) impacto social (que en determinados androides lleva a las personas a preocuparse por su situación o, incluso, hasta por sus «derechos»).

A tales propiedades vamos a atender de forma inmediata.

(21) Calo, Ryan: «Robots as legal metaphors», en *Harvard Journal of Law and Technology*, Vol. 30, núm. 1, 2016, y Calo, Ryan: «Robots in American Law», en *University of Washington School of Law Research Paper*, núm. 2016-04, 2016.

2.2.1 Corporeidad

Mientras que la robótica también se basa en datos como Internet, el robot en principio exige además una *materialización corpórea*.

Los robots funcionan con *software* específico y procesan información sensorial (y de otro tipo). Muchos sistemas robóticos están asimismo conectados a Internet para complementar sus funcionalidades, o incluso para ejecutar funciones básicas (lo que se denomina *cloud robotics*). Los robots, sin embargo, difieren de los ordenadores y del *software* precisamente en que están diseñados para actuar *sobre* el mundo *off-line*. La capacidad de actuar físicamente sobre el mundo «real» se traduce, a su vez, en el potencial de dañar físicamente a las personas o a las cosas.

De este modo, subraya el autor, los robots combinan, posiblemente por primera vez en la historia, la promiscuidad generativa de los datos que recolectan y atesoran con la capacidad de causar daño físico. La encarnación corporal alumbra un desafío de primer orden a los principios estructurales sobre los cuales se erige la sociedad digital, basada en el dato, y la reconducción de los eventuales daños a una perspectiva sobre todo de pérdida económica. Por ejemplo, en Europa el artículo 82 del nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos europeo), y en España el artículo 19 de la todavía vigente Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), reconocen el derecho de los interesados a ser indemnizados cuando, como consecuencia del incumplimiento de lo dispuesto en la normativa sobre protección de datos por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos.

Además, en el Derecho de Internet los diversos ordenamientos jurídicos han venido a admitir generosos regímenes de exclusión de responsabilidad para los proveedores y plataformas de Internet intermediarias por las actividades de sus usuarios, principiando por la sección 230 de la Communications Decency Act norteamericana de 1996 (22), en cuya virtud, por ejemplo, la red social Facebook no será responsable de un fraude cometido por uno de sus muchos usuarios a través del servicio, ya que expresamente declara que el proveedor no será tratado como editor u orador (23). En Europa, el sistema de exclusión de responsabilidad se

(22) 47 U. S. C. § 230.

(23) La § 230(c)(1) dispone que «[n]*o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*».

prevé en los artículos 12 a 15 de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la Sociedad de la Información, en particular el comercio electrónico en el mercado interior (DCE), y en España el régimen se contiene en los artículos 13 a 17 de la Ley 34/2002, de 11 de julio, de servicios de la Sociedad de la Información y de comercio electrónico (LSSI), todo cual fue objeto de estudio en nuestra tesis doctoral.

Sin embargo, estas limitaciones de responsabilidad ampliamente conocidas en el Derecho de Internet no serían aplicables aquí para inmunizar a los fabricantes de plataformas robóticas que puedan producir daños físicos. Siendo así crucial la cuestión de la responsabilidad jurídica por los daños que eventualmente ocasione la actuación de los robots, cabe apuntar que, cuanto más autónomos sean estos, más problemático será considerarlos como simples instrumentos en manos de otros agentes responsables (como el fabricante, el operador, el propietario, el usuario, etc.), ya que la causación del daño es *consecuencia de su programación*, o más precisamente, del efecto conjunto de su *hardware*, sistema operativo y *software*. Esta combinación de elementos es la que permite al robot interactuar con su entorno y provocar efectos físicos en el mundo.

Con todo, la «esencialidad» de este rasgo ha sido impugnada acertadamente por Balkin (24), quien observa que puede llevarnos a descuidar la diversidad de sistemas que emplean la inteligencia artificial y el autoaprendizaje y que también pueden causar daños físicos sin ser robots *stricto sensu*. Así, los algoritmos de autoaprendizaje pueden aumentar o disminuir las temperaturas en una casa, encender dispositivos, bloquear o desbloquear puertas y avisar a los servicios de policía y bomberos. Los algoritmos pueden comprar y vender valores bursátiles; pueden crear proyecciones holográficas que parezcan y actúen como personas; pueden amenazar, entretener, copiar, difamar, defraudar, advertir, consolar o seducir. Estos diversos efectos cruzan las fronteras entre lo físico, lo económico, lo social y lo emocional.

Por lo que se acaba de notar, a nuestro juicio resulta imprescindible dotar a los sistemas robóticos y de inteligencia artificial de *cajas negras* como las de los aviones y otros medios de transporte para registrar toda la actividad del sistema y las órdenes recibidas. Así, ante un incidente, se podrá determinar sin margen de error que sucedió y quién, o qué, fue el responsable.

(24) Balkin, Jack: «The path of robotics law», *op. cit.*, pp. 50 y ss.

2.2.2 Impredecibilidad

En la actualidad, las máquinas llevan a cabo una variedad de tareas que las personas podrían realizar, y no se opta por ello en atención a razones de coste, de preferencia o de comodidad. Es muy conocido el empleo de robots en ambientes extremos e inaccesibles al hombre, como en los planetas del sistema solar o en las profundidades marinas. Piénsese, también, en los robots que se destinan a desactivar explosivos o para llevar a cabo tareas industriales en atmósferas con condiciones ambientales desfavorables o contaminantes, así como en androides como Zenbo® capaz de cuidar personas, o incluso más limitadamente con el creciente auge de robots limpiafondos de piscinas.

Bajo el rasgo de la impredecibilidad, o del *comportamiento emergente* como lo denomina el propio Calo (25), se hace referencia a sistemas que, más que simplemente repetir las instrucciones, se adaptan interactivamente a las circunstancias. La doctrina, de modo unánime, sí reconoce esta nota como sustantivadora y esencial. Además, el comportamiento autónomo es un objetivo claramente declarado de la robótica y la inteligencia artificial, materializando directamente el componente de *impredecibilidad* incluido en la definición que nos servía para comenzar.

Como explora la obra de Arkin (26), una máquina que es lo suficientemente versátil como para «aprender» de los errores, podría impedir a sí misma (y a la gente) cometer esos errores en el futuro. Además, debido a que un sistema autónomo aprende de un comportamiento previo, mejorará el desempeño de una tarea a través del tiempo, incluso sin ayuda. Es importante destacar que tal comportamiento puede conducir a soluciones que ningún ser humano hubiera podido lograr por sí solo. Algo que se asemeja a la creatividad, pero puede conducir asimismo a soluciones erráticas.

La perspectiva de *sistemas autónomos, impredecibles y físicamente encarnados* va a ser la que plantee los desafíos jurídicos más acuciantes y dificultosos. Así, en materia de responsabilidad civil, habrá que distribuir las potenciales responsabilidades de los diferentes sujetos concernidos, incluyendo al propietario, al usuario (que le pudo también dar una orden indebida), al distribuidor, al fabricante del *hardware*, al diseñador del sistema operativo o al programador del *software*, por nombrar sólo algunas posiciones jurídicas.

Al propio tiempo, los mecanismos por los cuales los ordenamientos jurídicos suelen tipificar el ilícito involucran conceptos profundamente

(25) Calo, Ryan: «Robots in American Law», *op. cit.*, p. 40.
(26) Arkin, Ronald: *Governing lethal behavior in autonomous robots*. Editorial Chapman and Hall, Londres, 2009.

humanos, como es el dolo (responsabilidad penal) o la diligencia debida (responsabilidad civil), todos los cuales están ausentes cuando se construye un sistema para ser impredecible por diseño. La responsabilidad objetiva puede ser una solución tradicional, pero probablemente necesite calibraciones ante situaciones hoy inéditas, e incluso puede resultar inapropiada en el campo del Derecho Penal.

Incluso, como nota Balkin (27), el *software*, especialmente el empleado en sistemas robóticos, es bastante probable que tenga errores o produzca resultados no previstos. Los errores pueden ser difíciles de detectar y pueden originarse a través de la combinación de múltiples modificaciones y adiciones de variados equipos. Puede ser extremadamente difícil esclarecer la responsabilidad de los *bugs* que surgen de las múltiples capas de desarrollo de *software* de diversa procedencia. Y, en la medida en que los robots y los sistemas de inteligencia artificial aprenden a modificar su propio código, las cuestiones de responsabilidad se vuelven aún más difusas.

Profundizando en esta idea, Matthias (28) y Palmerini (29) advierten cómo en la puesta en funcionamiento de complejos sistemas compuestos, las funciones y las competencias de diversas personas se superponen y están íntimamente interconectadas; y quien contribuye en un segmento de la operación conjunta con frecuencia no tiene el control sobre la misma, y, a veces, incluso, tampoco conoce la estructura ni comprende el funcionamiento del dispositivo en su totalidad. La capacidad de interacción y de manipulación del ambiente y la imprevisibilidad de los comportamientos han provocado una fricción con el fundamento común de las reglas de responsabilidad por daños y con los modos tradicionales de los cuales el ordenamiento jurídico se vale para atribuirla, basados en la culpa y en la relación de causalidad. De la dificultad para asignar la responsabilidad en los sistemas complejos, pero principalmente de la reconocida incompatibilidad entre la *ratio* de este tipo de reglas y el modo de operación de los productos robóticos, se desprende la necesidad de romper con los modelos existentes y razonar según esquemas innovadores propios de una nueva disciplina jurídica como sería el Derecho de los Robots.

Para complicar más la cuestión, muchos robots y sistemas de inteligencia artificial estarán permanentemente conectados a Internet y continuamente recibirán nueva información y nueva programación de múltiples fuentes. Los coches sin conductor, por ejemplo, podrían ser diseñados como parte de una gigantesca red de vehículos interactivos, envián-

(27) Balkin, Jack: «The path of robotics law», *op. cit.*, p. 63.

(28) Matthias, Andreas: «The responsibility gap: ascribing responsibility for the actions of learning automata», en *Ethics and Information Technology*, Vol. 6, núm. 3, 2004.

(29) Palmerini, Erica (coord.): *Law and Technology. The challenge of regulating technological development*. Editorial Pisa University Press, Pisa, 2013.

dose constantemente información sobre el estado local del tráfico. Las actualizaciones periódicas del sistema operativo pueden descargarse en cada automóvil sin el conocimiento del usuario final (30).

De hecho, cabe esperar que algunos de los sistemas más útiles y ampliamente utilizados estén *siempre* conectados a la nube y a Internet (*cloud robotics*). Esto significa que estos sistemas no serán entidades autónomas, sino que serán constantemente actualizados mediante la comunicación con otros robots y sistemas de inteligencia artificial, así como con diversas fuentes centralizadas y descentralizadas de información. Aparte de los problemas de seguridad que presenta la robótica en la nube, también complica y difumina responsabilidad por accidentes.

Por último, la cualidad que venimos comentando también generará múltiples beneficios, con las consiguientes afecciones jurídicas. Por ejemplo, los robots y los sistemas de inteligencia artificial crearán nuevas invenciones y obras de propiedad intelectual. La pregunta es quién disfrutará de los derechos de propiedad intelectual. Por el momento, y como analizó pioneramente Rogel Vide (31) hace más de treinta años, una obra del espíritu ha de pertenecer, necesariamente, a una persona y nunca a una máquina, que, por versátil y sofisticada que sea, es objeto y no sujeto de derechos.

2.2.3 Impacto social

Finalmente, cabe apuntar cómo, en un grado mayor que cualquier otra tecnología en la historia, los robots tienen un impacto o valor social (32) para las personas.

El psicólogo Peter Kahn (33) ha concluido una serie de experimentos para esclarecer qué piensan las personas acerca de los robots. Los resultados han llevado al autor a formular una sorprendente conclusión: los robots pueden pertenecer a una categoría ontológica completamente nueva. Los participantes no tienden a pensar que los robots personificados están vivos, pero tampoco los consideran objetos. Más bien, los partícipes en esos estudios están inclinados a atribuir estados mentales a los robots, e incluso adoptan comportamientos que serían impensables al tratar con un mero objeto. El trabajo, financiado en gran parte por la National Science

(30) Boeglin, Jack: «The costs of self–driving cars: reconciling freedom and privacy with tort liability in autonomous vehicle regulation», en *Yale Journal of Law and Technology*, Vol. 17, núm. 1, 2015.

(31) Rogel Vide, Carlos: *Autores, coautores y propiedad intelectual*. Editorial Tecnos, Madrid, 1984, pp. 59 y ss.

(32) Turkle, Sherry: *Alone together. Why we expect more from technology and less from each other*. Editorial Basic Books, Nueva York, 2011.

(33) Kahn, Peter: «The new ontological category hypothesis in human–robot interaction», en *Proceedings of the seventh annual* ACM/IEEE *international conference on Human–Robot Interaction*, Boston, Massachusetts, 2012.

Foundation norteamericana, ha puesto de relieve que además ninguna categoría ontológica existente captaría adecuadamente la robótica.

Cabe señalar, una vez más, que esta tendencia no es exclusiva de la robótica; también es aplicable a los sistemas de inteligencia artificial *stricto sensu*. La película 2013 de Spike Jonze, *Her*, trata sobre un hombre que se enamora de un sistema operativo basado en una inteligencia artificial, no de un robot. Los robots pueden hacer que los usuarios los consideren vivos porque se mueven; pero los sistemas de inteligencia artificial pueden lograr que las personas los vean como vivos porque hablan. Y si la pretendida singularidad sería el antropomorfismo, lo cierto es que el ser humano ha asociado el poder del habla con la característica de humanidad mucho más que con la capacidad del movimiento como desarrolló la propia filosofía griega.

En una dirección algo divergente, Balkin (34) expresa que el problema no es que las personas *confundan* a los robots con los seres vivos, porque por lo general no lo hacen. Más bien, el problema es que, a través de sus interacciones con robots y sistemas de inteligencia artificial, las personas están dispuestas a *sustituir* a los animales o seres humanos por robots en *ciertos* contextos y para *determinados* propósitos. Y lo denomina «efecto de sustitución», ya que «*las personas hacen que una entidad se interponga por un ser humano o un animal y tratan a la entidad como tal, pero sólo de cierta manera. En otras palabras, las personas tratan a los robots y agentes de IA como "animales de propósito especial" o como "seres humanos de propósito especial"*».

De todo ello se deriva la posible viabilidad de dotarles de una personalidad electrónica independiente, a cuyo análisis dedicaremos el próximo epígrafe.

3. ¿UNA PERSONALIDAD ELECTRÓNICA PARA LOS ROBOTS?

Como se sabe, el ser humano es, por su propia naturaleza, el protagonista de la vida social y, con ella, del Derecho. La persona humana es la razón de ser del Derecho, pues el fin de éste es la realización de la justicia en la sociedad –«*ubi societas, ibi ius*»– y la sociedad se compone de personas. Actualmente es un valor jurídico incontestable el de que esa sociedad es la humana, y todos los hombres, por el mero hecho de serlo, tienen personalidad jurídica y son sujetos, no objetos, para el Derecho. Es decir, todo ser humano es por naturaleza *sujeto del Derecho* (objetivo), y también es *sujeto de derechos* (subjetivos). Ahora bien, en la Historia esta idea no ha llegado a aceptarse pacíficamente y sin ambages, y no ha sido

(34) Balkin, Jack: «The path of robotics law», *op. cit.*, p. 57.

plenamente asimilada por la sociedad hasta tiempos relativamente recientes (35).

Así, en las épocas primitivas era persona solamente el que formaba parte de una sociedad muy restringida: la de la familia –*gens*, *Sippe*– o la política –el Estado, en sus diversas formas–. Incluso en la Roma antigua el extranjero no sólo carece de todo derecho, sino que es considerado enemigo (*hostis*), de modo que la pena más grave es la de destierro, por la que queda el sujeto a merced del primero que le encuentre. Pero también dentro del Estado no todos son personas, ya que la personalidad se define por el estado civil, de manera que solamente algunos –los ciudadanos libres y *sui iuris*– son personas en pleno sentido de la palabra. Los demás –libertos, esclavos– lo son en menor grado o carecen completamente de derechos, siendo equiparados a las cosas. Con todo, los juristas romanos son plenamente conscientes del significado de la persona para el ordenamiento jurídico como sujeto de derechos.

La Iglesia católica sostiene la igualdad esencial de todos los hombres a quienes Dios ha dotado sin discriminación alguna de un alma inmortal. Pero este principio ideal tarda en imponerse en la práctica y la esclavitud se mantiene durante mucho tiempo en los países cristianos, hasta que, ya en el siglo XIX, se impone el Estado de Derecho y el sistema constitucional de gobierno. El Código prusiano de 1794 autoriza todavía explícitamente el comercio de negros, en Estados Unidos la abolición de la esclavitud lo fue a merced de la decimotercera enmienda, aprobada en 1865, y en España la esclavitud es abolida legalmente en la península en 1837, aunque en sus colonias fue algo más tardía (36). No obstante, bien entrado el siglo XIX se dan aún casos de ventas masivas de esclavos de guerra, y a lo largo de ese siglo subsistió (37), en general en las colonias europeas, la esclavitud prohibida en las metrópolis coloniales.

La filosofía de la Ilustración, que va a inspirar el pensamiento europeo moderno y contemporáneo, fundamenta la personalidad jurídica de todo ser humano de manera autónoma, sin referencias externas a una determinada concepción religiosa o estado social. «*Los seres irracionales*» –afirma Kant en su *Fundamentación de la Metafísica de las Costumbres* (38)– «*tienen solamente un valor relativo, como medios, y, por ello, se llaman «cosas»; en cambio, los seres racionales son llamados «personas», pues su naturaleza les distingue ya como fines en sí mismos, esto es,*

(35) *Vid.* ALBALADEJO GARCÍA, MANUEL: «La distinción entre comunidad y sociedad», en *Actualidad civil*, núm. 3, 1995.

(36) En Puerto Rico lo fue por Leyes de 4 de julio de 1870 y de 22 de marzo de 1873, y en Cuba por Real Decreto de 7 de octubre de 1886.

(37) AMBROSI, CHRISTIAN: *L'Europe de 1789 á 1848*. Editorial PUF, París, 1972, pp. 213-214.

(38) KANT, INMANUEL: *Die Metaphysik der Sitten en Werkausgabe*. Editorial Suhrkamp Verlag, Frankfurt, 1979, tomo VIII, pp. 33 y ss.

algo que no está permitido emplear simplemente como medio». El personalismo ético de cuño kantiano, recuerda Larenz (39), atribuye al hombre –precisamente porque es persona en sentido ético– un valor en sí mismo, no como medio para fines de otros, y, en este sentido, una dignidad. De ello se sigue que todo ser humano tiene, frente a cualquier otro, el derecho a ser respetado como persona, a no ser perjudicado en sí mismo ni en su ámbito de actuación. Esta relación de respeto mutuo es, según esta concepción, la relación jurídica fundamental que está en la base de toda convivencia en una comunidad jurídica y de toda relación jurídica particular.

Por eso, como advirtió pioneramente entre nosotros Federico de Castro (40), no acaban de ser exactas aquellas definiciones de la persona que la identifican con la capacidad jurídica general o de Derecho o con la aptitud para ser sujeto de derechos y obligaciones, porque éstas son las consecuencias o repercusiones necesarias en el mundo jurídico de la existencia de personas humanas, pero la persona no es creación del Derecho. Por el contrario, el principio de que todo hombre lo es constituye un postulado anterior y superior al mismo ordenamiento jurídico, al que éste debe someterse. Aquí encontramos una radical diferencia entre la persona física y la jurídica, cuya existencia depende de que la ley la reconozca o no porque no lleva en sí misma su necesidad. La personalidad puede ser reconocida a sujetos que no son personas físicas, pero no le puede ser negada a éstas. Como precisa el citado autor (41), más exacto que hablar de clases de personas sería hablar de persona sólo para la persona física, y de personificaciones o realidades sociales personificadas para la persona jurídica.

El Código Civil ya se basa en estas ideas, como no podía ser menos, dada la ideología liberal en que se desenvuelve la Codificación. Destina su Libro I a tratar «De las personas» y en los dos Capítulos de su Título II regula respectivamente las personas físicas y las jurídicas, sin que haya de darse a esta equiparación más alcance que el puramente sistemático, pues no desconoce el Código la diferencia existente entre unas y otras. Al dedicar a esta materia sus primeras normas, demuestra el Código que coloca a la persona humana en el puesto central de todo el ordenamiento jurídico.

Estas reflexiones encuentran su acomodo en el propio artículo 10 de nuestra Constitución de 1978, a cuyo tenor:

> «1. La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social.

---

(39) Larenz, Karl: *Derecho justo. Fundamentos de ética jurídica*. Editorial Civitas, Madrid, 1985, pp. 60 y ss.

(40) De Castro y Bravo, Federico: *Derecho Civil de España*. Editorial Instituto de Estudios Políticos, Madrid, 1952, tomo II, pp. 31 y ss.

(41) De Castro y Bravo, Federico: *Derecho Civil de España*, *op. cit.*, p. 34.

2. Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.»

En el caso de los robots, algunos de los cuales tienen ya un aspecto parecido al de los seres humanos, con rasgos, miembros y movimientos incluidos, dando lugar a los robots androides o humanoides, existiendo también robots con aspecto de animales, que pueden servir como mascotas, y dadas sus capacidades de aprender, percibir el entorno y decidir de forma autónoma, progresivamente asistiremos a sistemas robóticos que serán capaces de negociar, comparecer ante las administraciones públicas o los tribunales, e incluso cometer algún delito. Si la inteligencia artificial derrotó a Gary Kasparov en 1997 (42), no es extraño que puedan concertar relaciones jurídicas, actuar en el tráfico y causar daños físicos y morales.

Por ello, autores como Calo aluden a «*una nueva categoría de sujeto jurídico a medio camino entre persona y objeto*». La calificación es «*a mitad de camino*», *parcial*, porque la asignación de *status* puede ser incompleta, contextual, inestable y, sobre todo, oportunista. Los ciudadanos puede tratar al robot como una «persona» (o «animal») para algunos propósitos y como un objeto para otros. La nota de sustitución, como advierte Balkin, tiene su pleno sentido porque, en muchos casos, el sustituto no es completamente idéntico a la cosa que viene a reemplazar. Por el contrario, es sólo provisional, en ciertos contextos o para concretos fines.

El Derecho parte de la distinción básica entre personas y cosas, siendo posteriormente reconvertida en la tríada didáctica de personas–cosas–acciones tan cara al Derecho romano. El Derecho, es verdad, se hace «*a causa de las personas*» como reza la *Instituta* de Justiniano (1, 2, 12), moralizando el modelo Gayano, en 1, 8, que reza «*veamos primero lo de las personas*», pero, con sólo personas, no hay Derecho del que hablar. El Derecho surge de las controversias sobre las cosas. Y las controversias mismas, si son propiamente jurídicas, son las acciones.

Sin embargo, a causa de la irrupción de los robots, para algunas voces éstos deberían ser calificados de «seres sensibles» ya que gozan de inteligencia y pensamiento. Sus defensores advierten que cuanto más antropomórfico es el robot, más personas tienden a compartir la culpa con el robot por el fracaso y el elogio por el éxito. Esta nueva realidad filosófica y social

(42) Más recientemente, en octubre de 2017 una división de Google, –Google Deep Mind– anunció que una máquina de su creación, denominada «AlphaGo Zero», había ganado a su predecesora (una versión anterior de la máquina –AlphaGo–) por un contundente 100 a 0. Tanto la primera como la segunda versión son máquinas diseñadas para jugar a un juego de mesa conocido como «Go».

hunde sus raíces en el previo debate de la Ilustración generado por la formulación tajante de los animales–máquina del racionalismo cartesiano (43).

En esta dirección, Darling (44) ha analizado recientemente si la forma en que las personas parecen reaccionar frente a las máquinas antropomorfas sugiere la necesidad de extender un *conjunto limitado de derechos legales a los robots sociales*, o al menos prohibiciones contra su abuso, aun cuando no sean reputados como seres vivos o sensibles a un nivel racional. «*Tal vez,* –dice la autora–, *no queramos ser el tipo de sociedad que tolera la crueldad con una entidad que consideramos como casi humana*». Darling apunta el interés de proteger a los ciudadanos frente al dolor que incluso puede ocasionar la visión de tal abuso. En suma, esta dirección minoritaria trae a colación los avances en la protección de los animales para plantear su aplicación a los robots humanoides.

A juicio de la opinión dominante, tanto en nuestro país como en los derechos comparados (45), sólo del hombre puede decirse, traduciendo a Hermogeniano en el *Digesto* (1, 5, 2), que en razón suya está constituido todo el Derecho (*hominum causa omne ius constitutum sit*), que nuestras Partidas traducen elegantemente como sigue: «*por causa, razón y favor de las personas se hacen y componen los derechos*». El Derecho necesita un *sujeto*, que es el ser humano, para aquello que tenga trascendencia socio–jurídica. El robot sería un *objeto*. Del mismo modo, la dignidad del individuo humano implica la posesión ineludible de unos bienes jurídicos resultantes de su propia condición. Son los llamados «derechos de la personalidad». Así lo reconoce el precitado artículo 10.1 de la Constitución de 1978 cuando establece que «*[l]a dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son el fundamento del orden político y social*».

No obstante, ya estamos asistiendo al debate acerca de crear o no una nueva categoría de sujeto jurídico, a medio camino entre la persona y el objeto o cosa. De hecho, el propio Parlamento de la Unión Europea en la Resolución antes citada de 16 de febrero de 2017 ha propuesto admitir una nueva «personalidad electrónica» para aquellos supuestos en los que los robots tomen decisiones autónomas inteligentes. Esta configuración no sería una ficción muy diferente de la personalidad jurídica atribuida a determinadas entidades en los ordenamientos jurídicos continentales desde hace décadas.

---

(43) *Vid.* sobre este tema Rescigno, Francesca: *I diritti degli animali. Da res a soggetti*. Editorial Giappichelli, Turín, 2005.

(44) Darling, Kate: «Extending legal protection to social robots: the effects of anthropomorphism, empathy, and violent behaviour towards robotic objects», en Calo, Ryan; Froomkin, Michael y Kerr, Ian (coords.): *Robot law*. Editorial Edward Elgar Publishing, Nueva York, 2016.

(45) *Vid.* nuestro estudio Barrio Andrés, Moisés: «Hacia una personalidad electrónica para robots», en *Revista de Derecho Privado*, núm. 2/2018.

Incluso, en los últimos tiempos, como recuerda Rogel Vide en una obra recién publicada (46), algunas Constituciones como las de Bolivia o El Ecuador, inspiradas en un pensamiento que podría decirse panteísta, han asignado derechos a la Pachamama, a la Madre Tierra. Yendo más allá todavía, Nueva Zelanda ha atribuido personalidad jurídica a un río, después de habérsela asignado a una montaña, designando representantes legales que puedan velar por el uno y la otra. En la línea de personificar todo, ha llegado a considerarse como persona a un ídolo hindú.

En nuestra opinión, la *personalidad electrónica* –que no persona electrónica– puede ser reputada como un enfoque plausible al problema, tanto para los robots dotados de un cuerpo como para los robots *software* que exhiben un cierto grado de autonomía e interactúan con las personas, en cuanto que tendrían la posibilidad de ser titulares de relaciones jurídicas con sus correspondientes derechos y obligaciones, y tener un cierto reconocimiento jurídico de su subjetividad, fundamentalmente en derechos de naturaleza patrimonial, pero no los constitucionales ni los de la personalidad, absolutamente consustanciales a la dignidad de los seres humanos tal y como recuerdan textos internacionales recientes como la Declaración universal de la UNESCO sobre bioética y derechos humanos de 2005 o la Carta de los Derechos Fundamentales de la Unión Europea de 2000.

Ciertamente junto al ser humano el Derecho conoce, desde hace siglos, otros sujetos de derechos distintos: se trata de organizaciones sociales a las que el ordenamiento jurídico dispensa un protagonismo en las relaciones jurídicas similar al que corresponde al ser humano (asociaciones, sociedades, corporaciones, fundaciones, etc.). Tales sujetos de Derecho, que no son seres humanos, reciben la consideración jurídica de personas, de forma que se produce una importante modificación del concepto de «persona», al que se da en Derecho un significado distinto del ordinario, de carácter más formal y preciso: para el Derecho, persona ya no es sólo el ser humano como posible sujeto de derechos, sino que también aparecen las personas jurídicas encarnadas en algunas organizaciones sociales a las que el ordenamiento jurídico atribuye esa cualidad.

El concepto de «persona» entonces se convierte en *sujeto de derechos*. Y se distingue entre *persona física* (el ser humano) y las *personas jurídicas* (sujetos de derechos distintos del ser humano). Incluso, la distinción más tarde será disuelta por autores como Kelsen (47), quien, tras haber subrayado que «*la así llamada persona física no es por lo tanto un hombre, sino la unidad personificada de las normas jurídicas*

(46) *Vid.* Rogel Vide, Carlos: *Personas, animales y derechos*. Editorial Reus, Madrid, 2018, pp. 81 y ss.

(47) Kelsen, Hans: *Teoría pura del Derecho* (2.ª ed., 1960), trad. de R. J. Vernengo, Editorial UNAM, México, 1982, p. 198.

que atribuyen deberes y derechos al mismo hombre», concluye destacando que «*la así llamada persona física es una persona jurídica*», un puro centro de imputación de situaciones jurídicas. En esta construcción, la persona no es una realidad natural, sino una construcción jurídica creada por la ciencia del Derecho, un concepto auxiliar en la descripción de hechos jurídicamente relevantes. Para el autor, «*la llamada persona física es una persona jurídica*». Construcción que, por lo demás, deja entrever una conexión directa con el planteamiento de Schmitt, quien expresa que la persona sólo podría existir socialmente como persona jurídico-política, como sujeto de un ordenamiento político.

Para nosotros, al menos la noción de «personalidad jurídica», entendida como *aptitud para ser titular, activo o pasivo, de relaciones jurídicas*, es la opción jurídica menos radical para atribuir derechos y obligaciones a los sistemas robóticos más avanzados, sin necesidad de por el momento crear una nueva categoría de sujeto jurídico a medio camino entre persona y objeto, como por otra parte se está realizando respecto a los animales, calificados ahora de «seres sensibles» (o de «seres vivos dotados de sensibilidad»). De este modo, la personalidad jurídica procede, en la persona individual, del mero hecho de ser persona (humana), condición que es anterior al propio Derecho, mientras que en la persona jurídica la atribución de aquella aptitud no deja de ser, en último término, un expediente técnico o de oportunidad para hacer posible el logro de los fines colectivos y durables que persiguen ciertas organizaciones sociales. Por todo ello, no hay inconveniente en que el Derecho pueda reconocer la (ficticia) personalidad jurídica del robot, como instrumento jurídico a fin de que los sistemas robóticos más avanzados puedan tener, como mínimo, obligaciones y algún tipo de personalidad legal, o incluso, como acabamos de sostener anteriormente, la posibilidad de ser titulares de relaciones jurídicas con sus correspondientes derechos y obligaciones, y tener un cierto reconocimiento jurídico de su subjetividad, fundamentalmente en derechos de naturaleza patrimonial. Ello no parece más anómalo que el considerar que un ser humano es una "cosa" como sucedía en la esclavitud, o la segregación racial, o establecer un sistema de protección para los animales que se usan en experimentos científicos.

A la postre, las referidas propiedades de corporeidad, impredecibilidad e impacto social de los sistemas robóticos, por si mismas y sobre todo en combinación, van a resultar relevantes para una extraordinaria variedad de contextos jurídicos (v. gr., Derecho Penal y proceso penal; responsabilidad civil; propiedad intelectual; libertad de expresión; privacidad; Derecho de contratos; tributos o incluso derecho marítimo, por citar sólo una muestra). Estas cualidades esenciales o distintivas de los robots y sus repercusiones en el Derecho nos llevan a defender la viabilidad de una

disciplina propia, el Derecho de los Robots, lo cual ha sido objeto específico de una obra recientemente publicada (48).

4. CONCLUSIÓN

En nuestra opinión, resulta apremiante la construcción de un Derecho de los Robots como marco jurídico e institucional resultante de la dialéctica entre los principios fundamentales del Estado constitucional de Derecho y la dinámica del desarrollo e implantación de sistemas robóticos y de inteligencia artificial, considerada no solo desde el punto de vista de las realizaciones ya adquiridas, sino de las hipótesis que señalan la necesidad de tener en cuenta un futuro disruptivo cada vez más próximo.

Esta pretensión se encuentra cada vez más respaldada por la conciencia de que un entorno legal claro, transparente y predispuesto a recoger las novedades robóticas apenas delineadas puede constituir un incentivo al desarrollo de este sector de progreso, que exige asimismo equipos interdisciplinares que también atiendan a los marcos jurídicos pertinentes y al contexto socio-técnico en el que se desplegarán los robots. La experiencia pone de manifiesto que tener en cuenta los requisitos sociales, jurídicos y éticos está lejos de ser una práctica estándar en la industria en proyectos complejos de ingeniería de última generación. Para que los robots alcancen su plena utilidad, tendrán que implementar un conjunto completo de requisitos funcionales, de seguridad, jurídicos, sociales y éticos.

Además, el marco jurídico de la *Robot Law* requiere una actualización continua. En primer lugar, tiene que abordar los efectos secundarios inesperados que las intervenciones regulatorias destinadas a salvaguardar determinados derechos o valores puedan tener sobre otros. En segundo lugar, debe mantenerse alerta ante la necesidad de poner al día, ampliar o cambiar el ordenamiento jurídico a la luz de los cambios en la sociedad y los sistemas de valores que se producen a través del proceso de conformación mutua de tecnologías, procesos sociales y perspectivas normativas.

Y todo ello en una disciplina jurídica que, como antes señalábamos, a la vez adapte el Derecho general –en cuanto que previamente vigente–, y, en la medida de lo necesario, genere un Derecho nuevo que respete los principios estructurales de dignidad, libertad e igualdad en el marco del mantenimiento de la democraticidad total de los sistemas robóticos.

Finalmente, para nosotros el reconocimiento de una «personalidad jurídica electrónica» para los sistemas robóticos más avanzados resulta viable para atribuir derechos y obligaciones a los mismos, sin necesidad de por el momento crear una nueva categoría de sujeto jurídico a medio ca-

(48) *Vid.* Barrio Andrés, Moisés (dir.): *Derecho de los Robots*. Editorial Wolters Kluwer, Madrid, 2018.

mino entre persona y objeto, como por otra parte se está realizando respecto a los animales, calificados ahora de «seres sensibles» (o de «seres vivos dotados de sensibilidad»). Por todo ello, no hay obstáculo jurídico en que el Derecho pueda reconocer la personalidad jurídica electrónica del robot en cuanto que tendrían la aptitud de ser titulares de relaciones jurídicas con sus correspondientes derechos y obligaciones, y tener un cierto reconocimiento jurídico de su subjetividad, fundamentalmente en derechos de naturaleza patrimonial, pero no los constitucionales ni los de la personalidad, absolutamente consustanciales a la dignidad de los seres humanos. Ello no parece más anómalo que el considerar que un ser humano es una «cosa» como sucedía en la esclavitud, o la segregación racial, o establecer un sistema de protección para los animales que se usan en experimentos científicos.

CAPÍTULO 5

LAS GENERACIONES DE DERECHOS HUMANOS ANTE EL DESAFÍO POSTHUMANISTA

ANTONIO ENRIQUE PÉREZ LUÑO
Profesor Emérito de la Universidad de Sevilla

1. ¿UN PLANTEAMIENTO. LOS DERECHOS HUMANOS EN LA ERA DE LA POSTHUMANIDAD: DE LA COMPUTOPÍA, AL *HOMO VIDENS* Y AL *HOMO DEUS*?

El inicio del Nuevo Milenio ha propiciado una reflexión, cada vez más extensa e intensa, sobre los impactos de la tecnociencia en distintos aspectos de la sociedad, la cultura, la economía y el sistema jurídico-político. Los últimos y espectaculares avances de la inteligencia artificial de la tecnobiología, de la robótica y la neurociencia, han sido considerados como el fin de la Era humana (1), como el advenimiento de un mundo

(1) BARRAT, J.: *Nuestra invención final: La inteligencia artificial y el fin de la Era humana*, Paidos, México, 2017.

transhumano (2), o posthumano (3) y, por consiguiente, como la suplantación de los derechos humanos por unos derechos posthumanos (4), lo que podría implicar la extinción de los derechos y libertades en su acepción tradicional, o la extensión de esos derechos a otros seres vivos (*Animal-Rights*) o a entes artificiales (*Robot-Rights*).

La revolución técnico científica conduce al planteamiento de un supuesto radical: que el futuro del género humano ya no será el resultado de decisiones políticas, basadas en valores y en derechos, sino que responderá, al diseño de los tecnólogos fundado en los datos inapelables derivados de las Nuevas Tecnologías (NT) y de las Tecnologías de la Información y Comunicación (TIC). Todo ello, conduce a presagiar un porvenir de la humanidad que ya no dependerá de la actividad de los Estados y de las Organizaciones Internacionales, sino de los avances tecnocientíficos que se vayan logrando en Silicon Valley.

La revolución tecnológica se plantea como un reto ineludible para el estudio actual de los derechos humanos, afectados en su significación, fundamento y en su realización y garantía por unos desarrollos técnico-científico que están cuestionando los propios valores de la dignidad, la libertad, la autonomía, la identidad y la igualdad, que constituían el centro de gravedad en torno al cual se nucleaba el entero sistema de los derechos y libertades.

Para un correcto enfoque de la nueva situación que hoy contextualiza la categoría de los derechos humanos, conviene tener presente algunos de los hitos principales que jalonan el debate sobre la irrupción tecnológica en la esfera de los derechos. Para ello, parece obligado recordar que fue el pionero de la cibernética Norbert Wiener quien en 1948 definía esta nueva disciplina como la ciencia de la comunicación y el control en los seres vivos y en las máquinas. Wiener fue consciente de las importantes aplicaciones, pero también de los riesgos, que confortaba la tecnología cibernética como un nuevo mecanismo de control social y, por tanto, como un pode-

(2) Diéguez, A.: *Transhumanismo. La búsqueda tecnológica de mejoramiento humano*, Herder, Barcelona, 2017.

(3) Harari, Y. N.: *Homo Deus: Breve historia del mañana*, Debate, Madrid, 2016. Las expresiones «transhumanismo» y «posthumanismo», designan a movimientos de la ciencia y de la cultura de nuestro tiempo. En numerosas ocasiones, estos términos son asumidos y empleados de forma indistinta, como sinónimos. Ambas expresiones aluden a la reivindicación del derecho a investigar y utilizar, con plena libertad, los avances de la tecnociencia, para conseguir la mejora o potenciación de las capacidades físicas y mentales de las personas. Al propio tiempo, estos movimientos se proponen transcender los límites naturales, biológicos o sociales que actualmente condicionan el pleno desarrollo de la existencia. Ahora bien, desde algunos enfoques teóricos, se establece una diferencia básica entre estos dos términos. Se indica, así, que mientras los transhumanistas sostienen que la tecnociencia debe contribuir a la mejora, pero no a la suplantación de la especie humana, los posthumanistas postulan la superación de la humanidad actual por una superhumanidad, como resultado final del proceso de desarrollo tecnocientífico.

(4) Rodotà, S.: *Dall'umano al postumano*, Ponencia presentada al Conversatorio sobre: «Derecho y derechos en la sociedad digital», Texto inédito que debo a la deferencia del Prof. Dr. Tomas de la Quadra Salcedo.

roso instrumento de limitación de las libertades cívicas. Por ello, propugnó un «uso humano de los seres humanos», es decir, la garantía de que el tratamiento cibernético de determinados comportamientos sociales no entrañaría la abolición de la responsabilidad humana en las proyecciones sociales de la tecnología.

Wiener concluía su reflexión indicando que el tiempo apremiaba y que había llegado el momento de la decisión entre el bien y el mal (5).

Entre las figuras más representativas de la primera etapa de interacción entre las NT, los procesos políticos y las libertades, destaca la del profesor Yoneji Masuda, de la Universidad de Aomori, fundador y presidente del «Institute for the Information Society» y ex director del «Japan Computer Usage Development Institute»; uno de los pioneros y máximo artífice de la informatización de la sociedad japonesa y, por ello, uno de los más cualificados estudiosos de la sociedad informatizada. Masuda opuso a la siniestra imagen del «Estado automatizado», o sea, la organización política totalitaria apoyada en el control tecnológico, la «Computopía» (*computer-based utopia*), es decir, la sociedad libre a través de las computadoras y de la información. La futura sociedad informatizada o Computopía será, a tenor de cuanto anticipaba Masuda, «una *sociedad sin clases*, libre de un poder dominante y cuyo núcleo social serán las comunidades voluntarias».

Para que no se confunda su Computopía con un sueño inalcanzable e ilusorio, carente de cualquier posible incidencia en la realidad de un futuro ya inminente, Masuda establecía aquellos principios o condiciones que deberán observarse para llevarla a la práctica. Tales principios hacían referencia a: 1.º) el reconocimiento del derecho de todos los ciudadanos, sin ningún tipo de discriminación o excepciones, a participar directamente en la decisión de los asuntos que les afecten; 2.º) el espíritu de «sinergia», es decir, de cooperación y de sacrificio voluntario y altruista de los intereses egoístas en función del bien común, como exigencia ética y jurídica que debe presidir todo el sistema social; 3.º) la garantía del derecho de las personas y los grupos para conocer y acceder a todas las informaciones que les conciernan; 4.º) la distribución equitativa entre todos los ciudadanos de los beneficios y cargas que comporta la vida social; 5.º) búsqueda de las soluciones a través del acuerdo participativo y de la persuasión en los distintos conflictos y tensiones que puedan plantearse; y 6.º) la cooperación de los ciudadanos en la puesta en marcha de las soluciones adoptadas sin que, por tanto, sea necesario acudir a la coacción acompa-

(5) Wiener, N.: *Cibernetics*, MIT Press, Cambridge (Mass.), 2.ª ed. 1961, pp. 11 y 107. Sobre esta obra, *vid.* Pérez Luño, A. E., *Cibernética, Informática y Derecho*, Publicaciones del Real Colegio de España, Bolonia, 1976, pp. 17 ss y 39.

ñada del castigo por la fuerza de la ley, como sucede en las sociedades actuales.

Masuda pensaba, al concluir su diseño de la futura Computopía, que nos dirigimos a un nuevo milenio, en el que ese modelo de sociedad será una realidad y «cuyo monumento histórico serán sólo unos cuantos *chips* de un centímetro cuadrado metidos en una cajita. Pero esta cajita almacenará muchos datos históricos, incluyendo el expediente de cómo cuatro mil millones de ciudadanos del mundo vencieron la crisis energética y la explosión demográfica, lograron la abolición de las armas nucleares y el desarme completo y crearon una rica simbiosis entre Dios y el hombre sin la compulsión del poder o la justicia, sólo con la cooperación voluntaria de los ciudadanos para poner en práctica sus aspiraciones globales comunes» (6).

La prognosis de Masuda constituyó un estímulo pionero para una reflexión *more* tecnológico de las principales cuestiones jurídicas y políticas actuales. A partir de su ejemplo se han ido multiplicando los estudios y experiencias sobre esta materia. Conviene, no obstante, advertir que no todos los trabajos dirigidos a evaluar el impacto de las NT y las TIC sobre los derechos y libertades se han mostrado optimistas sobre los efectos de dicha proyección. Entre las actitudes críticas destaca la sustentada por Giovanni Sartori. En su obra *Homo videns* expresa abiertamente su temor de que la telepolítica, en lugar de contribuir a la madurez de los ciudadanos, debilite su responsabilidad política. El flujo de informaciones y su crecimiento cuantitativo no se están traduciendo en la ampliación del conocimiento, ni en el desarrollo de la capacidad crítica de los ciudadanos. La TV, en opinión de Sartori, «empobrece drásticamente la información y la formación del ciudadano... el video-ser desactiva nuestra capacidad de abstracción y, con ella, nuestra capacidad de comprender los problemas y afrontarlos racionalmente» (7). Sartori responsabiliza a los nuevos medios tecnológicos y, en particular, a la TV de haber creado un post-pensamiento, que supone la anulación del pensamiento crítico. Sartori denomina a quienes hoy detentan las NT de la información «hombres-bestias», y los acusa de exaltar una comunicación perenne, que incapacita para articular ideas claras y diferentes. Lejos de forjar ciudadanos libres y responsables, las NT han promovido una *Lumpenintelligentia,* un proletariado intelectual sin ninguna consistencia intelectual (8).

---

(6) Masuda, Y.: *La sociedad informatizada como sociedad post-industrial*, trad. cast. de J. Ollero y F. Ortiz Chaparro, Fundesco & Tecnos, Madrid, 1984, pp. 172 ss. *Cfr.*, en relación con las tesis de Masuda, Pérez Luño, A. E., *Nuevas tecnologías, sociedad y derecho. El impacto socio-jurídico de las N. T. de la información*, Fundesco, Madrid, 1987, pp. 137 ss.

(7) Sartori, G.: *Homo videns. La sociedad teledirigida*, Taurus, Madrid, 1998, p. 127.

(8) *Ibid.*, p. 147.

La reflexión política responsable exige, según Sartori, dosis adecuadas de reposo y ponderación. Estas condiciones resultan incompatibles con la forma de operar de las NT, que propician respuestas urgentes y conclusiones simples y simplificadoras. Lo que debe conducir a un juicio más equilibrado sobre los beneficios, sin duda importantes, de las NT para el reforzamiento de los derechos de participación política en las sociedades democráticas.

Wiener, Masuda y Sartori, han estudiado, desde distintas perspectivas y con distintas valoraciones, los impactos de la tecnociencia en distintas esferas de la vida social y política y en el ejercicio de las libertades. En todo caso, ninguno de estos trabajos planteaba cuestionar la noción tradicional de humanidad, que era objeto de las implicaciones tecnológicas, ni se replanteaban la propia idea de los derechos y libertades, como atributos inherentes de la persona humana, en su nueva radicación tecnocientífica. Ese cambio revolucionario es, precisamente, el que protagoniza el debate sobre las libertades y la tecnología en estos últimos años. Ahora el problema ya no reside en evaluar las implicaciones de la tecnociencia en el mundo natural y social, sino que el reto consiste en la propia modificación interna de la propia vida humana como resultado de la revolución tecnicocientífica. De lo que se trata hoy es de proyectar la tecnociencia a una modificación del cuerpo, del cerebro y de la mente humana.

Yuval Noah Harari ha estudiado esta problemática y afirma que, la revolución que se avecina, no está en el mundo externo sino en el propio mundo interior de los seres humanos. El desarrollo de la inteligencia artificial, la neurociencia y la ingeniería de *Cyborgs,* permitirá conectar el cerebro humano con estas nuevas entidades tecnocientíficas. De este modo, se conseguirá ampliar el conocimiento humano hasta límites insospechados y, dado que el conocimiento engendra poder, le permitirá maximizar sus potencialidades.

La muerte, que durante milenios ha sido considerada como un fenómeno metafísico producto de designios divinos, aparece hoy como un problema técnico, que puede ser resuelto a través de soluciones técnicas y, por ello, no es descartable imaginar un futuro de personas inmortales.

De este modo, las prerrogativas divinas de omnisciencia, omnipotencia y de eternidad son ahora atributos que se hallan al alcance de la nueva humanidad. De ahí, concluye Harari que estamos siendo una de las últimas generaciones de *Homo Sapiens* que será sustituido por el *Homo Deus*.

Piensa Harari que, a través de determinados cambios en el mapa genético, así como en la estructura biológica y hormonal de los seres humanos, se podrá conseguir una modificación cualitativa en sus principales características y habilidades. Durante millones de años la evolución de las es-

pecies ha seguido una selección natural, ahora dicho proceso puede ser sustituido por un diseño inteligente, que permita la creación de seres super-humanos.

Harari, plantea una posibilidad, todavía más radical, la de sustituir la vida orgánica, que gravita en torno al carbono, por la vida inorgánica, basada en el silicio. Se podrán generar, entonces, entes artificiales dotados de una vida inorgánica. Estas circunstancias conducen, en definitiva a vislumbrar un universo nuevo en el ámbito social cultural económico y político.

Concluye Harari que el camino hacia esa revolución tecnocientífica resulta imparable e irreversible. Se va a producir una sustitución de la humanidad actual por una posthumanidad y la pregunta que queda abierta, es si esa posthumanidad será mejor o peor que la actual (9).

2. EL ENFOQUE GENERACIONAL DE LOS DERECHOS

De cuanto se lleva expuesto se desprende que la categoría de los derechos humanos no constituyen un concepto fijo e inalterable, sino que se halla sometida a un constante cambio y que, en particular, se ha visto notablemente aceptada por los desarrollos técnico-científicos. Una concepción generacional y, por tanto, histórica de los derechos humanos puede juzgarse sorprendente y paradójica. Muchos ciudadanos de las sociedades democráticas actuales juzgan los derechos humanos como un valor eterno consustancial a su experiencia cívica. El paradigma generacional de los derechos humanos se dirige a disipar el sueño ilusorio de imaginar derechos más allá de la historia.

Los derechos humanos, en su acepción estricta, surgieron en el clima cultural ilustrado de la Modernidad. Fueron formulados entonces como categorías que pretendían expresar las exigencias intemporales y perpetuas de la naturaleza humana; como un conjunto de facultades jurídicas y políticas propias de todos los hombres y en todos los tiempos. Ese paradigma eleático concebía los derechos humanos como unas verdades, cuya evidencia podía demostrarse a través de los dictámenes de la recta razón.

Las circunstancias jurídico-políticas y la propia evolución cultural, que han caracterizado el sucesivo devenir de los derechos y libertades desde la época moderna hasta el presente, han determinado una decantación del enfoque de los derechos humanos. Si en su gestación y primeras manifestaciones fueron contemplados *sub specie aeternitatis*, hoy no pueden dejar de ser concebidos *sub specie historiae.* Las profundas transformaciones económicas, científicas y tecnológicas acaecidas desde el periodo de la Ilustración hasta el presente han tenido sus consiguientes repercusiones en la

(9) Harari, Y. N.: *Homo Deus: Breve historia del mañana, op. cit., passim.*

esfera social, jurídica y política. Los Estados de derecho, que tienen uno de sus elementos constitutivos en el sistema de libertades, han experimentado importantes mutaciones y adaptaciones institucionales, con inmediata repercusión en la esfera de los derechos cívicos. Asimismo, la Comunidad internacional ha vivido en su seno cambios y evoluciones, cuya incidencia en el estatuto de los derechos humanos ha sido profunda y relevante.

3. LAS GENERACIONES DE DERECHOS HUMANOS

La mutación histórica de los derechos humanos ha determinado la aparición de sucesivas «generaciones» de derechos. Los derechos humanos como categorías históricas, que tan sólo pueden predicarse con sentido en contextos temporalmente determinados, nacen con la modernidad en el seno de la atmósfera iluminista que inspiró las revoluciones burguesas del siglo XVIII (10).

Este contexto genético confiere a los derechos humanos unos perfiles ideológicos definidos. Los derechos humanos nacen, como es notorio, con marcada impronta individualista, como libertades individuales que configuran la primera fase o generación de los derechos humanos. Dicha matriz ideológica individualista sufrirá un amplio proceso de erosión e impugnación en las luchas sociales del siglo XIX. Estos movimientos reivindicativos evidenciarán la necesidad de completar el catálogo de los derechos y libertades de la primera generación con una segunda generación de derechos: los derechos económicos, sociales, culturales. Estos derechos alcanzan su paulatina consagración jurídica y política en la sustitución del Estado liberal de Derecho por el Estado social de Derecho.

La distinción, que no necesariamente oposición, entre ambas generaciones de derechos se hace patente cuando se considera que mientras en la *primera* los derechos humanos vienen considerados como derechos de defensa (*Abwehrrechte*) de las libertades del individuo, que exigen la auto limitación y la no injerencia de los poderes públicos en la esfera privada y se tutelan por su mera actitud pasiva y de vigilancia en términos de policía administrativa; en la *segunda*, correspondiente a los derechos económicos, sociales y culturales, se traducen en derechos de participación (*Teilhaberechte*), que requieren una política activa de los poderes públicos encaminada a garantizar su ejercicio, y se realizan a través de las técnicas jurídicas de las prestaciones y los servicios públicos (11).

(10) PECES-BARBA, G.: *Tránsito a la modernidad y derechos fundamentales*, Mezquita, Madrid, 1982.
(11) *Cfr.* PÉREZ LUÑO, A. E.: *Derechos humanos, Estado de Derecho y Constitución*, Tecnos, Madrid, 11.ª ed., 2017, pp. 84 ss.

4. LOS DERECHOS HUMANOS DE LA TERCERA GENERACIÓN: LOS DERECHOS DE LA ERA TECNOLÓGICA

La revolución tecnológica ha redimensionado las relaciones de los seres humanos con la naturaleza, las relaciones de los seres humanos entre sí y la relación del ser humano para consigo mismo. Estas mutaciones no han dejado de incidir en la esfera de los derechos humanos. Se ha producido, de este modo, un fenómeno bifronte: de una parte, las NT y las TIC han generado importantes desarrollos y mejoras en las condiciones vitales de la humanidad, contribuyendo a reforzar, en ocasiones, el disfrute y ejercicio de determinados derechos; pero como reverso a estos avances, determinados usos o abusos tecnológicos han supuesto una grave amenaza para las libertades, lo que ha exigido la formulación de nuevos derechos o actualización y adecuación a los nuevos retos de los instrumentos de garantía de derechos ya existentes. Estas cuestiones constituyen el objeto nuclear de la que hoy se considera como tercera generación de los derechos humanos (12).

a) **Los derechos relativos al medio ambiente, la calidad de vida y la paz**

En el curso de estos últimos años pocas cuestiones han suscitado tan amplia y heterogénea inquietud como la que se refiere a las relaciones del *hombre con su medio ambiental*, en el que se halla inmerso, que condiciona su existencia y por el que, incluso, puede llegar a ser destruido. La plurisecular tensión entre naturaleza y sociedad corre hoy el riesgo de resolverse en términos de abierta contradicción, cuando las nuevas tecnologías conciben el dominio y la explotación sin límites de la naturaleza como la empresa más significativa del desarrollo. Los resultados de tal planteamiento constituyen ahora motivo de preocupación cotidiana. El expolio acelerado de las fuentes de energía, así como la contaminación y degradación del medio ambiente, han tenido su puntual repercusión en el hábitat humano y en el propio equilibrio psicosomático de los individuos. Estas circunstancias han hecho surgir, en los ambientes más sensibilizados hacia esta cuestión, el temor de que la humanidad pueda estar abocada al suicidio colectivo, porque como *l'apprenti sorcier*, con un progreso técnico irresponsable ha desencadenado las fuerzas de la naturaleza y no

(12) *Cfr.* Pérez Luño, A. E.: *La tercera generación de derechos humanos*, Thomson/Aranzadi, Cizur Menor (Navarra), 2006; Riccobono, F. (ed.): *Nuovi diritti dell´età tecnologica* (Atti del Convegno tenuto a Roma presso la Libera Università Internazionale degli Studi Sociali, 5 e 6 maggio 1989, Giuffrè, Milano, 1991; Rodríguez Palop, M. E.: *La nueva generación de derechos humanos. Origen y justificación*, Dykinson, Madrid, 2.ª ed., 2010; Saladin, P.: *Grundrechte im Wandel*, Stämpfli, Bern, 3.ª ed., 1982.; Sommermann, K. P.: «El desarrollo de los derechos humanos desde la declaración universal de 1948», en el vol. col. *Derechos Humanos y Constitucionalismo ante el Tercer Milenio*, ed. a cargo de A. E. Pérez Luño, Marcial Pons, Madrid, 1996.

se halla en condiciones de controlarlas. En estas coordenadas debe situarse la creciente difusión de la inquietud ecológica.

La ecología representa, en suma, el marco global para un renovado enfoque de las relaciones entre el hombre y su entorno, que redunde en una utilización racional de los recursos energéticos y sustituya el crecimiento desenfrenado, en términos puramente cuantitativos, por un uso equilibrado de la naturaleza que haga posible la calidad de la vida. La inmediata incidencia del ambiente en la existencia humana, la contribución decisiva a su desarrollo y a su misma posibilidad, es lo que justifica su inclusión en el estatuto de los derechos fundamentales. Por ello, no debe extrañar que la literatura sobre el derecho medioambiental, derecho y ecología, y el derecho a la calidad de vida constituyan uno de los apartados más copiosos en la bibliografía actual sobre los derechos humanos. Y parece poco razonable atribuir este dato al capricho, o a la casualidad.

Un fenómeno especialmente inquietante que amenaza a la vida humana y supone una degradación de la calidad de vida, es el que dimana de la consciencia universal de los peligros más acuciantes que se derivan del desarrollo de la industria bélica. La potencialidad de los armamentos de destrucción masiva sitúa a la humanidad ante la ominosa perspectiva de una hecatombe de proporciones mundiales capaz de convertir nuestro planeta en un inmenso cementerio. Los esfuerzos de las organizaciones internacionales en pro del desarme y del desmantelamiento de las industrias bélicas y los arsenales nucleares, sólo han alcanzado metas parciales. De ahí, que la temática de la paz haya adquirido un protagonismo indiscutible en el sistema de las necesidades insatisfechas de los hombres y de los pueblos de nuestra época y que tal temática entrañe una inmediata proyección subjetiva. Prueba elocuente de ello constituye la monografía de Wolfgang Däubler *Stationierung und Grundgesetz* (13), que mas allá de su título constituyó un replanteamiento del entero catálogo de los derechos fundamentales de la *Grundgesetz* asumidos desde la perspectiva de la paz y el desarme. Por ello, tiene razón Vittorio Frosini cuando estima que el pacifismo, como ideología política, representa ahora una novedad en la evolución de la consciencia cívica de Occidente (14). Existe, además, un nexo de continuidad entre la inquietud por la paz y por la calidad de vida. Tal nexo viene dado por cuanto de amenaza inmediata para esos dos valores suponen los riesgos de la energía nuclear. De ahí, la oportunidad de la

(13) Däubler, W.: *Stotionierung und Grundgesetz*, Rowohlt, Reinbek bei Hamburg, 2.ª ed. 1983.

(14) Frosini, V.: «Mitología e ideología del pacifismo», en su vol. *Constituzione e società civile*, Edizioni di Comunità, Milano, 1975, p. 157.

obra de Alexander Rossnagel (*Radioaktiver Zerfall der Grundrechte?*) (15), cuyo provocativo título posee la virtualidad de enfrentamos con uno de los problemas más urgentes que hoy se plantea a la tutela de los derechos y libertades. Porque, en efecto, se cierne un peligro de desintegración de los derechos humanos agredidos por las consecuencias inmediatas (conflicto atómico, o contaminación nuclear del ambiente), o mediata (medidas de seguridad generalizadas limitadoras o suspensivas de las libertades), que se derivan de la utilización de las tecnologías radiactivas.

b) **Los derechos en el ámbito de las tecnologías de la información y la comunicación (TIC)**

En el *plano de las relaciones interhumanas* la potencialidad de las modernas tecnologías de la información y la comunicación (TIC) ha permitido, por vez primera, establecer unas comunicaciones a escala planetaria. Las nuevas tecnologías (NT) han posibilitado que los seres humanos de nuestro tiempo puedan establecer una comunicación sin límites en el espacio, sin límites en las personas y en tiempo real. Internet constituye la gran revolución de nuestro tiempo y sus efectos se proyectan también en la esfera de las libertades.

No puede soslayarse, en efecto, que el contexto en el que se ejercitan los derechos humanos es el de una sociedad donde la Red ha devenido el símbolo emblemático de nuestra cultura, hasta el punto de que para designar el marco de nuestra convivencia se alude reiteradamente a expresiones tales como la «sociedad de la información», la «sociedad informatizada» o la «era de Internet». Las TIC y la NT, han propiciado nuevas formas de ejercicio de los derechos y pueden contribuir a un reforzamiento del tejido participativo de las sociedades democráticas. La ciberciudadanía y la teledemocracia constituyen el nuevo horizonte de los derechos. Pero como todas las conquistas de la técnica y de la ciencia, sus posibilidades emancipatorias no escapan de riesgos y, por ello, tienen también su reverso (16).

El control electrónico de los documentos de identificación, el proceso informatizado de datos fiscales, educativos y médicos, el registro y gestión de las adquisiciones comerciales realizadas con tarjetas de crédito, así como de las reservas de viajes, representan algunas muestras bien conocidas de la omnipresente vigilancia informática de nuestra existencia habitual. Nuestra vida individual y social corren, por tanto, el riesgo de hallarse sometidas a lo que se ha calificado, con razón, de «juicio universal

(15) Rossnagel, A.: *Radioaktiver Zerfall der Grundrechte?*, C. H. Beck, München,1984.
(16) Pérez Luño, A. E.: *¿Ciberciudadani@ o* Ciudadani@.com?, Barcelona, Gedisa, 2004.

permanente» (17). Ya que, en efecto, cada ciudadano fichado en un banco de datos se halla expuesto a una vigilancia continua e inadvertida, que afecta potencialmente incluso a los aspectos más sensibles de su vida privada; aquellos que en épocas anteriores quedaban fuera de todo control por su variedad y multiplicidad.

Es sabido que la etapa actual de desarrollo tecnológico, junto a avances y progresos indiscutibles, ha generado nuevos fenómenos de agresión a los derechos y libertades. En esas coordenadas se está iniciando un movimiento de la doctrina jurídica y de la jurisprudencia de los países con mayor grado de desarrollo tecnológico tendente al reconocimiento del derecho a la libertad informática y a la facultad de autodeterminación en la esfera informativa (18). En una sociedad como la que nos toca vivir en la que la información es poder y en la que ese poder se hace decisivo cuando, en virtud de la informática, convierte informaciones parciales y dispersas en informaciones en masa y organizadas, la reglamentación jurídica de la informática reviste un interés prioritario. Es evidente, por tanto, que para la opinión pública y el pensamiento filosófico, jurídico y político de nuestro tiempo constituye un problema nodal el establecimiento de unas garantías que tutelen a los ciudadanos frente a la eventual erosión y asalto tecnológico de sus derechos y libertades.

En la situación tecnológica propia de la sociedad contemporánea todos los ciudadanos, desde su nacimiento, se hallan expuestos a violaciones de su intimidad perpetradas por determinados abusos de la informática y la telemática. La injerencia del ordenador en las diversas esferas y en el tejido de relaciones que conforman la vida cotidiana se hace cada vez más extendida, más difusa, más implacable.

c) **Los derechos en la esfera de la bioética y de las biotecnologías**

De igual modo, las nuevas tecnologías han contribuido decisivamente, a posibilitar un conocimiento más radical del propio ser humano. Durante milenios el hombre ha sido un desconocido para sí mismo. Desde la perspectiva de los avances científicos y tecnológicos de nuestro tiempo, no

(17) Frosini, V.: *Cibernética, derecho y sociedad*, trad. cast. de C. Salguero-Talavera y R. Soriano, con Prólogo de A. E. Pérez Luño, Tecnos, Madrid, 1982, p. 36.

(18) Denninger, E.: «El derecho a la autodeterminación informativa», trad. cast. de A. E. Pérez Luño, en el vol. col. *Problemas actuales de la documentación y la informática jurídica* (Actas del Coloquio Internacional celebrado en la Universidad de Sevilla, 5 y 6 de marzo de 1986), a cargo de A. E. Pérez Luño, Tecnos & Fundación Cultural Enrique Luño Peña, Madrid, 1987, pp. 268 ss.; Frosini, V.: *Il diritto nella società tecnologica*, Giuffrè, Milano, 1981; Lucas Murillo de la Cueva, P.: *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990.; Pérez Luño, A. E.: *Nuevas tecnologías sociedad y derecho, cit.*

pueden dejar de considerarse como meras elucubraciones ingenuas e insuficientes las teorías y conjeturas rudimentarias, que desde la medicina, la biología, la psicología y la filosofía se venían haciendo sobre el significado y la estructura de la naturaleza humana (19).

En los últimos años los avances de la ingeniería genética, la biotecnología y la neurociencia, han permitido trasladar desde la incertidumbre y la penumbra de las elucubraciones a la seguridad de los datos científicos, el conocimiento de la vida humana. Los estudios sobre el genoma humano y la consiguiente revelación del mapa genético de nuestra especie constituyen un nuevo marco de referencia para el estudio y la propia tutela de los derechos humanos (20). Estos progresos no se hallan exentos de riesgos. El desarrollo biotecnológico, junto a avances indiscutibles para la mejora del derecho a la salud y a la prolongación de la vida humana, ha generado nuevos fenómenos de agresión a los derechos y libertades. Esta circunstancia ha promovido un movimiento de la doctrina jurídica, la legislación y la jurisprudencia de los países con mayor implante tecnológico tendente al reconocimiento de derechos y facultades subjetivas frente a eventuales abusos que afecten a la esfera bioética y frente a determinadas experiencias biotecnológicas. Entre esos derechos, tiene importancia especial el referente a la tutela de la intimidad de los datos sanitarios procesados a través de las nuevas tecnologías. Son importantes también los esfuerzos por establecer instrumentos de tutela en el ámbito de la experimentación biotecnológica, que pueden agredir esferas de la libertad y de la identidad de las personas. Los debates sobre la manipulación genética, el tratamiento de embriones, clonación…, son algunas de las cuestiones mas candentes de esta nueva frontera de los derechos. No puede tampoco omitirse la trascendencia que para el alcance de los derechos humanos del presente poseen las polémicas sobre cuestiones bioéticas tan candentes como la problemática del aborto, la eutanasia y el derecho a una muerte digna (21).

---

(19) *Cfr.* Casado, M.: *Bioética, Derecho y Sociedad*, Trotta, Madrid, 1998.; De Castro Cid, B.: «Biotecnología. Derechos humanos: una compleja interacción circular», en el vol., col., a cargo de A. M.ª Marcos del Cano, *Bioética y derechos humanos*, UNED, Madrid, 2011, pp. 47 ss.; Gracia, D.: *Fundamentos de Bioética*, Eudema, Madrid, 1989.; Martínez Moran, N.: (ed.), *Biotecnología, Derecho y dignidad humana*, Comares, Granada, 2003.; Martínez Moran, N.: «La dignidad humana en las investigaciones biomédicas,» en el vol., col., a cargo de A. M.ª Marcos del Cano, *Bioética y derechos humanos*, UNED, Madrid, 2011, pp. 145 ss.

(20) Porras del Corral, M.: *Biotecnología, derecho y derechos humano*s, CajaSur, Córdoba, 1996.

(21) Álvarez, S.: *Derechos fundamentales y protección de datos genéticos*, Diykinson, Madrid, 2007, *passim.;* Malem Seña, J.: «Privacidad y mapa genético», en *Isonomía*, n. 2., 1995, pp. 23 ss.; Pérez Luño, A. E.: «Biotecnologías e intimidad», en su vol., *La tercera generación de derechos humanos, cit.*, pp. 129 ss. y la bibliografía allí citada.

5. CONCLUSIÓN: LOS DERECHOS DE LA TERCERA GENERACIÓN ANTE EL DESAFÍO POSTHUMANISTA

Conviene advertir, al enfilar el último tramo de estas reflexiones, que las generaciones de derechos humanos no entrañan un proceso meramente cronológico y lineal. En el curso de su trayectoria se producen constantes avances, retrocesos y contradicciones que configuran ese despliegue como un proceso dialéctico. No debe escapar tampoco a la consideración de esta problemática, que las generaciones de derechos humanos no implican la sustitución global de un catálogo de derechos por otro; en ocasiones, se traduce en la aparición de nuevos derechos como respuesta a nuevas necesidades históricas, mientras que, otras veces, suponen la redimensión o redefinición de derechos anteriores para adaptarlos a los nuevos contextos en que deben ser aplicados.

Una concepción generacional de los derechos humanos implica, en suma, reconocer que el catálogo de las libertades nunca será una obra cerrada y acabada. Una sociedad libre y democrática deberá mostrarse siempre sensible y abierta a la aparición de nuevas necesidades, que fundamenten nuevos derechos. Mientras esos derechos no hayan sido reconocidos por el ordenamiento jurídico nacional y/o internacional, actuarán como categorías reivindicativas, prenormativas y axiológicas. Pero los derechos humanos no son meros postulados de «deber ser». Junto a su irrenunciable dimensión utópica, que constituye uno de los polos de su significación, entrañan un proyecto emancipatorio real y concreto, que tiende a plasmarse en formas históricas de libertad, lo que conforma el otro polo del concepto. Faltos de su dimensión utópica los derechos humanos perderían su función legitimadora del Derecho; pero fuera de la experiencia y de la historia perderían sus propios rasgos de humanidad. Se ha dicho, en expresión afortunada, que es necesario aprender la lección de la realidad presente, para ser capaces de orientarla hacia un mundo mejor del futuro (22).

Los derechos de la tercera generación cumplen ese cometido de ser puente entre la realidad científico tecnológica del presente y sus proyecciones de futuro. Suponen, por tanto, la respuesta más adecuada y eficaz a los nuevos retos de la tecnociencia. Porque, como se ha indicado *supra*, se dirigen a extraer la máxima potencialidad de los desarrollos científicos y tecnológicos y, al propio tiempo establecen un sistema de garantías para que esos desarrollos no se produzcan a costa de las libertades. Incumbe a los derechos humanos de la tercera generación una doble tarea: aprove-

(22) Frosini, V.: *L'uomo artificiale. Etica e diritto nell'era planetaria*. Spirali, Milano, 1986, p. 133. En fecha reciente, Jürgen Habermas ha insistido y elucidado esa dimensión «utópico-real» de los derechos humanos en su ensayo: «La idea de dignidad humana y la utopía realista de los derechos humanos», en *Anales de la Cátedra Francisco Suárez*, n. 44, 2010, pp. 105 ss.

char, en la mayor medida posible los avances de la tecnociencia para la mejora de las condiciones de la vida humana y evitar la degradación o contaminación tecnológica de las libertades (*liberties pollution*).

En lo que atañe a la primera función, se alude hoy en distintos contextos científicos y tecnológicos a una «realidad aumentada», es decir al aumento y potenciación de capacidades humanas gracias a usos convenientes de las NT y las TIC, lo que se traduce en un fortalecimiento y mejora de la calidad de vida. Gracias a ello, se pueden superar determinados vínculos, barreras y limitaciones naturales y culturales, con la consiguiente extensión de las capacidades vitales. Los derechos humanos de la tercera generación contribuyen así a orientar el progreso técnico-científico hacia la consecución de una de las aspiraciones seculares de la humanidad. En diversos *Diálogos* platónicos se reitera la idea de que el ser humano aspira a la *pleonexia*, o sea, al aumento y la potenciación, vivir es crecer ilimitadamente, cada vida es un intento de expansión hasta lo infinito, el límite nos es impuesto, es una resistencia que nos impone la naturaleza o la sociedad.

Una utilización adecuada de las NT y las TIC, y, en definitiva, de todos los avances científicos y tecnológicos debe contribuir a superar esas barreras y limitaciones. Los derechos humanos de la tercera generación han surgido, precisamente, para hacer posible el uso de la tecnociencia dirigido a superar barreras y límites, pero respetando siempre los valores y los derechos de la condición humana. De este modo, contribuyen, decisivamente, a hacer efectivo el valor del pleno desarrollo de la personalidad, proclamado en los textos constitucionales de orientación liberal democrática, tal como acontece en el artículo 10.1 de la Constitución española vigente.

La tercera generación de derechos humanos se concibe, y en eso consiste su segunda tarea, como la garantía de que los avances de la sociedad tecnocientífica no se conseguirán a costa de la negación de los valores de la propia humanidad. Para el logro de este cometido denuncian las trampas liberticidas que subyacen a determinados postulados posthumanistas o transhumanistas. Así, en lo que hace referencia al impacto posthumanista sobre determinados valores y derechos humanos, revelan cuanto sigue.

La dignidad humana fue concebida por Kant en el «reino de los fines». De este modo, se considera que la persona humana es un fin en sí misma y que no puede ser instrumentalizada para la consecución de otros fines u objetivos (23). Frente a ello, el discurso posthumanista acepta hoy

(23) Pérez Luño, A.: «Kant y los derechos humanos» en su libro, *La Filosofía del Derecho en perspectiva histórica*, Servicio de Publicaciones de la Universidad de Sevilla, Sevilla, 2009, pp. 117 ss.

la manipulación e instrumentalización de los seres humanos en función de un pretextado progreso tecnológico.

En nombre de la tecnociencia se pretende colonizar todos los aspectos de la vida humana. Se suplantan los esfuerzos de cada individuo para construir y afirmar su propia personalidad, por una tendencia a la cosificación. Esa tendencia implica un desplazamiento desde la Internet 2.0, o sea, la de las personas y las redes sociales, a la Internet 3.0 que es la de las cosas. El control externo, la instrumentalización y la cosificación de la vida desembocan en la aniquilación de la personalidad y, por consiguiente, de la dignidad humana.

Como un derecho inmediatamente fundado en la dignidad humana, la *intimidad*, se halla amenazada en el discurso posthumanista, por determinados programas de la neurociencia que pueden invadir los estratos mas reservados de la persona. De otro lado, existen ya experiencias de *Big-Data*, que permiten un uso y un control masivo de informaciones referentes a un número ilimitado de personas y a un número ilimitado de situaciones (24). Con ello puede llegar a convertirse en una pretensión ilusoria el respeto a la vida privada.

En estrecha relación con estos fenómenos la *identidad* corre el riesgo de ser abolida, porque determinadas investigaciones neurocientíficas anticipan programaciones de la conducta. A partir de ello, ciertos rasgos peculiares e irrepetibles que definen la identidad de cada persona, podrán ser disueltos en identidades en serie. De igual modo, la biotecnología y la ingeniería genética, mediante determinadas técnicas de clonación o de intervenciones en los genes, pueden reemplazar la reproducción natural de los seres humanos, por diseños planificados de identidades preconcebidas.

No menos inquietante resulta la posibilidad de que a través de la ingeniería de *Cybor*g y de una *Interface* que conecte no solo el cerebro humano con la inteligencia artificial, sino distintos cerebros humanos entre sí, se posibilite una transferencia del pensamiento, la memoria, los deseos y las experiencias de cada sujeto a otros. De este modo, la propia personalidad humana dejaría de fundarse en una identidad peculiar e irrepetible, para proyectarse y transmitirse a un número ilimitado de sujetos.

El posthumanismo puede significar también el eclipse de la *libertad*, en la medida en que la neurociencia permite programar la conducta humana, con la consiguiente abolición del libre albedrío. El derecho a la libertad, considerado en nuestra cultura como la posibilidad de actuar sin condicionamientos o determinismos, sin controles ni mediatizaciones, sean de carácter paternalista o autoritario, se ve ahora como una caracte-

(24) *Cfr.* Garriga Domínguez, A.: *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, Dykinson, Madrid, 2015.

rística que abandona al ser humano y se convierte en libertad de las cosas. La libertad se ve condicionada por algoritmos, sustraída a la decisión y la conciencia individual, con lo que cada persona puede ser identificada, controlada y clasificada. Se pueden, a través de los algoritmos, establecer una previsión sobre conductas y decisiones futuras y así se corre el riesgo de que la persona pueda ser evaluada por sus propensiones y no por sus acciones (25).

El eclipse de la libertad tendría importantes implicaciones, no solo en el ámbito ético y político, sino que supondría una reelaboración de conceptos jurídicos fundamentales, como los de: responsabilidad, culpa, negligencia, buena fe…

Desde posiciones transhumanistas y posthumanistas se reclama una libertad para la investigación y el aprovechamiento, sin ningún tipo de trabas o límites, de todos los avances de la tecnociencia. Esta pretensión resulta incompatible con cuanto entraña la garantía de los derechos y libertades, que postula que ninguno de los derechos es absoluto e ilimitado. Y que, por tanto, debe ceder ante determinados valores y derechos que, en caso de conflicto, se consideren prevalentes. Por este motivo, determinadas experiencias de la tecnociencia, por su incompatibilidad con el núcleo básico de los valores y derechos humanos, no pueden ser admitidos como el uso de un derecho de libertad tecnológica sino que entrañan un abuso del derecho.

El planteamiento posthumanista afecta también al concepto de *autonomía*, concebida como la posibilidad de cada persona para establecer y desarrollar sus propios planes de vida, sin injerencias, ni controles externos. Hoy el posthumanismo pretende sustituir la autonomía de las personas, por la autonomía de las cosas. Así, se alude, a sistemas autónomos, vehículos autónomos, mecanismos autónomos de producción, armas autónomas, sistemas de reproducción autónomos, es decir, de autoreproducción… El mundo de las cosas evoluciona y se transforma por el desarrollo de la robótica. Los robots asumen, cada vez más tareas antes reservadas al ámbito estrictamente humano. Se hace referencia incluso a los denominados «robots sociales» a los que se les debe reconocer una cierta dimensión de humanidad, que puede ser el primer paso hacia una humanidad integral de la máquina. Para el estudio de las realidades y posibilidades de la robótica se ha acuñado un *Robot-Law*, que se ocuparía de la interacción entre los seres humanos y los robots y de la incidencia de la robótica en el ámbito de los derechos y libertades (26).

(25) *Cfr.* Rodotà, S.: *Dall'umano al postumano, cit.*

(26) De Asis, R.: *Una mirada a la robótica desde los derechos humanos*, Dykinson, Madrid, 2015.

Se asiste así a la posibilidad ominosa, de que determinadas decisiones fundamentales para la vida, sean sustraídas a la voluntad autónoma de los seres humanos, para ser asumidas por el poder impersonal y difuso de las cosas. Pero se deja en la penumbra a las fuerzas o poderes que pueden controlar la autonomía de las cosas y la robótica, en función de sus propios intereses.

La difusión de la tecnociencia se proyecta, asimismo, en la esfera de la *igualdad*. Los costes del acceso a los principales desarrollos de las biotecnologías, de la robótica y de la inteligencia artificial abren una brecha entre tecno-ricos y tecno-pobres. La fractura social se agudiza y el discurso actual posthumanista se aleja, cada vez más, de la imagen idílica de la Computopía imaginada por Masuda y a la que se aludió *supra*, según la cual el desarrollo de las NT y las TIC conducirían a una sociedad más justa e igualitaria.

No huelga omitir, que la implantación de la robótica puede conducir al desempleo de enormes masas de población laboral y su consiguiente empobrecimiento, así como a su inutilidad desde el punto de vista económico. No parece posible que esas masas encuentren un empleo adecuado en la sociedad tecnológica del conocimiento. En ella, por el propio desarrollo tecnológico y, en particular, de la inteligencia artificial y, según se desprende de actuales postulados posthumanistas, será cada vez mas innecesaria la aportación humana. El posthumanismo responde a los intereses de un mercado no controlado y al de las élites tecnocráticas, en detrimento de los derechos de las personas.

En la teoría y en la práctica de los derechos de la tercera generación se expresa la herencia de la cultura humanista, adaptada a las exigencias de la sociedad tecnológica. La tercera generación de derechos ofrece un marco adecuado para responder a los principales retos, aquí reseñados, del desafío posthumanista, a partir de la clarificación, la denuncia y la alternativa de sus principales dogmas y postulados.

1) En primer término, desde la tercera generación de los derechos, se puede cuestionar la pretensión de objetividad, neutralidad y asepsia de la teoría posthumanista. Esta se presenta como un conjunto de tesis e ideas irrefutables, avaladas por los desarrollos de la ciencia y la tecnología.

Hace ya algunos años, Jürgen Habermas en su lúcida obra: *Ciencia y técnica como ideología*, denunció la pretensión tecnocrática de presentar determinado tipo de conocimientos y propuestas, sedicentemente tecnocientíficos, cuando en realidad ocultan opciones prácticas e intereses. La ideología tecnocrática trata de sustraer al debate científico y político

particulares intereses, presentados como teorías, cuando en realidad suponen meras propuestas ideológicas (27).

Los principales argumentos posthumanistas se presentan, en la actualidad, como verdades tecnocientíficas irrefutables e inexorables. No obstante, un análisis crítico de esas propuestas, revela que ese discurso responde a la pretensión ideológica de escamotear las grandes elecciones y decisiones sobre el presente y el futuro de la condición humana y del desarrollo tecnológico al debate político. Tiene razón Stefano Rodotà cuando se pregunta si las transformaciones previstas y auspiciadas por el posthumanismo, se plantean en nombre del beneficio económico o del interés de las personas (28). Para responder estos retos, que afectan a la humanidad en su conjunto, no debe acudirse a la inteligencia artificial, sino a las opciones de la sociedad política.

El carácter ideológico de las propuestas posthumanistas se evidencia también cuando, a través de ellas, se propugna expropiar de la decisión colectiva ética y política, las cuestiones vitales de toda sociedad, como la educación, la sanidad o la pobreza. Los poderes que apoyan y financian la investigación tecnocientífica, no son anónimos, se trata de personas entidades o corporaciones reales y concretas, con intereses e ideologías fácilmente comprobables, que no pueden eludir su responsabilidad social y política.

2) Resulta, al propio tiempo necesario clarificar el sentido del prefijo «post», que se incluye en la expresión «posthumanismo». Dicho prefijo puede asumir dos significados diferentes: puede aludir a la sucesión cronológica o al perfeccionamiento de las concepciones o movimientos que le preceden; o bien, expresar la abolición de los mismas.

De cuanto hasta aquí se lleva dicho, se desprende que el posthumanismo, asume la segunda acepción indicada. Por ello, el posthumanismo no implica la mejora de la tradición humanista, sino que supone su negación, abolición o suplantación. El posthumanismo, por tanto, entraña un antihumanismo, por lo que aludir a una generación de derechos humanos antihumanistas implica una evidente *contradictio in términis*.

Si se parte de esta premisa, resulta evidente que no puede aludirse a la aparición de nuevos derechos procedentes del posthumanismo, ya que esta ideología representa, precisamente, la negación de la cultura humanista. Como se ha tenido ocasión de exponer reiteradamente, los derechos de la tercera generación se inscriben en el marco evolutivo de las generaciones de derechos humanos y, por eso mismo, son incompa-

(27) Habermas, J.: *Technik und Wissenschaft als Ideologie*, Suhrkamp, Frankfurt a. M., 1968, pp. 27 ss. (existe trad. cast. Tecnos, Madrid, 1984).

(28) Rodotà, S.: *Dall´umano al postumano, cit.*

tibles con el discurso posthumanista, cuyos presupuestos ideológicos resultan contrarios a la tradición de los valores y derechos fundamentales. Los derechos de la tercera generación, representan la crítica y la alternativa al posthumanismo en la medida en que se dirigen a encauzar el uso de las NT y las TIC conforme con los principios de la tradición humanista.

3) Por último, el carácter ideológico de las tesis posthumanistas se evidencia en su pretensión de reputar al humanismo como una experiencia cultural periclitada y conclusa. Desde las premisas posthumanistas se pretende desconocer que el proyecto jurídico-político humanista es todavía una promesa incumplida para amplios sectores de nuestro mundo, que no se han emancipado de la ignorancia, del hambre o de la opresión. Se produce así la situación paradójica de que, mientras se está reclamando un proyecto posthumanista, grandes sectores de la población mundial se hallan condenados a una condición de infrahumanidad.

No creo aventurado conjeturar que, en nuestro inmediato futuro, el discurso posthumanista se hallará en el núcleo del debate científico, económico, social, cultural, ético y jurídico-político. Pienso, en definitiva, que el paradigma de los derechos de la tercera generación es un marco idóneo para esos debates, con la plena conciencia de que como advirtió Jürgen Habermas: «al desafío de la técnica, no se le puede responder sólo con la técnica» (29).

(29) Habermas, J.: *Technik und Wissenschaft als Ideologie, cit.*, p. 118.

II

CIUDADANÍA DIGITAL

CAPÍTULO 6

CIUDADANÍA Y GOBERNANZA DIGITAL ENTRE POLÍTICA, ÉTICA Y DERECHO

ALESSANDRO MANTELERO
Profesor Asociado de Derecho Privado - Politecnico di Torino

1. INTRODUCCIÓN

La noción moderna de ciudadanía ya no se centra exclusivamente en la relación entre una persona y un territorio [¿qué territorio en un mundo de Internet? (1)], sino que reúne las condiciones necesarias para ejercer los derechos fundamentales y participar en la vida democrática (2). En este sentido, la ciudadanía digital no se centra necesariamente en la per-

(1) Véase, *inter alia*, REIDENBERG, J. R.: «Technology and Internet Jurisdiction», *University of Pennsylvania Law Review*, núm. 153(6), 2005, pp. 1951-1974; IRTI, N.: *Norma e luoghi. Problemi di geo-diritto*, Laterza, Roma-Bari, 2001; POST, D.: «The 'Unsettled Paradox': The Internet, The State, and the Consent of the Governed», *Indiana Journal of Global Legal Studies*, núm. 5(2), 1998, pp. 521-543.

(2) Véase VROMEN, A.: *Digital Citizenship and Political Engagement The Challenge from Online Campaigning and Advocacy Organisations*, Palgrave Macmillan, London, 2017.

tenencia a una comunidad y se ha convertido en un componente de la dimensión legal y política de la vida individual y social (3).

Desde esta perspectiva, las dos nociones de ciudadanía digital y gobernanza digital son en gran parte complementarias. Por un lado, el debate existente en la literatura sobre la ciudadanía digital se centra en la participación, tanto en el área política como en la económica. Por otro lado, la idea de la gobernanza digital se concentra en el uso de las soluciones de las TIC que se han adoptado para llevar a cabo las tareas tradicionales del sector público.

La ciudadanía digital (4) y la gobernanza digital (5) representan las dos caras de la misma moneda. En una democracia, tanto el gobierno (digital) como la ciudadanía (digital) están estrechamente vinculados. En este sentido, estas nociones no son nuevas en sí mismas. La novedad se debe, en todo caso, al impacto de la revolución digital en los entornos tradicionales de la relación social entre los ciudadanos y entre los ciudadanos y la administración pública.

En este sentido, esta transformación es parte del cambio más amplio inducido por la comunicación, los servicios en línea y la *datafication* (6). Estos tres elementos fundamentales han cambiado significativamente la interacción social y la manera en que se llevan a cabo las actividades tradicionales. Por lo tanto, también la esfera pública se ha visto afectada por este cambio.

Sin embargo, este nuevo paradigma no es un mero cambio tecnológico, ya que el advenimiento de la sociedad de la información ha afectado la forma en que se establecen las relaciones humanas. El nuevo entorno digital plantea, por lo tanto, nuevas cuestiones relativas a su regulación, el acceso a los servicios privados y públicos en línea, la transparencia en la acción pública y las nuevas formas de participación ciudadana. Todos estos temas se analizan en los siguientes capítulos, mientras que el presente capítulo se centra en los principales temas relacionados con los datos de los ciudadanos y su uso (7).

Aunque existe un dominador común a la ciudadanía digital y la gobernanza digital, estos dos componentes de nuestra sociedad basados en da-

---

(3) Véase Rodotà, S.: *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma-Bari, 1997, pp. 164-165.

(4) Véase, *inter alia*, Mossberger, K. *et alii: Digital citizenship: the internet, society, and participation*, MIT Press, Cambridge, Mass., 2010.

(5) Véase Milakovich, M. E.: *Digital Governance: New Technologies for Improving Public Service and Participation*, Routledge, London-New York, 2012.

(6) Véase Castells, M.: *The Rise of the Network Society, The Information Age: Economy, Society and Culture*, Vol. I, Blackwell, Cambridge, MA-Oxford, 1996.

(7) La brecha digital, que puede afectar tanto a la ciudadanía digital como a la gobernanza digital, no se trata en este capítulo; véase Warschauer, M.: *Technology and Social Inclusion. Rethinking the Digital Divide*, MIT Press, Cambridge, Mass., 2003; Compaine, B.M.: *The digital divide: facing a crisis or creating a myth?*, MIT Press, Cambridge, Mass., 2001. Para otras referencias, véase 'https://socialmediacollective.org/2015/08/13/reading-list-on-the-digital-dividedigital-inclusion/'.

tos tienen orígenes diferentes y un distinto desarrollo a lo largo de los años, que han planteado diversas cuestiones.

Sin embargo, en la última década, se ha producido una convergencia entre estas dos trayectorias en el contexto de la actual sociedad del Big Data (8). La transparencia, la no discriminación, la participación en decisiones algorítmicas, así como la interacción entre las operaciones de tratamiento de datos llevadas a cabo por entidades privadas y públicas, llevan ahora a juristas y legisladores a analizar tanto la ciudadanía digital como la gobernanza bajo el prisma del procesamiento de datos.

Al mismo tiempo, la regulación del tratamiento de datos está evolucionando hacia una noción más amplia, enfocada hacia una dimensión colectiva del uso de los datos. Esto impulsa al legislador a abordar los desafíos del nuevo paradigma que comporta el Big Data de una manera que ya no se reduce a la dimensión individual, sino que abarca cuestiones relativas a la gobernanza de la sociedad y al papel de los ciudadanos. También se tiene en cuenta la necesidad de profundizar sobre la interacción entre los diferentes derechos fundamentales.

En las dos primeras secciones, este capítulo examina, por un lado, esta evolución del tratamiento de datos llevado a cabo por la administración pública con fines sociales y, por otro lado, el concomitante desarrollo de la regulación de protección de datos. La tercera sección señala cómo esta evolución va a converger en la era del Big Data y lleva necesariamente a los responsables políticos a considerar el procesamiento de datos desde una dimensión más amplia. Esta nueva dimensión implica cuestiones sociales y legales del uso de datos e impulsa a los responsables políticos a adoptar formas más articuladas de evaluación del impacto del uso de la información en la sociedad en general.

2. EL TRATAMIENTO DE DATOS PARA FINES SOCIALES: DE LAS OFICINAS DE ESTADÍSTICA DEL GOBIERNO A LA COLABORACIÓN ENTRE EL SECTOR PÚBLICO Y PRIVADO

El desarrollo, en los países occidentales, del estado de bienestar entre los años 1960 y 1970 requirió la recopilación y organización de una gran cantidad de datos para evaluar las condiciones de las personas y proporcionar servicios sociales. Para abordar esta necesidad, las agencias gubernamentales y las oficinas estadísticas pasaron del papel a los bits. Inicia-

(8) Véase, *inter alia*, Mantelero, A. y Vaciago, G., «Legal Aspects of Information Science Data Science and Big Data» en M. Dehmer y F. Emmert-Streib (dirs.): *Frontiers in Data Science*, CRC Press, Boca Raton, 2017; Mayer-Schönberger, V. y Cukier, K.: *Big Data. A Revolution That Will Transform How We Live, Work and Think*, John Murray, London, 2013, p. 78; Bollier, D.: *The Promise and Perils of Big Data*, Aspen Institute, 2010 'http://www.aspeninstitute.org/sites/default/files/content/docs/pubs/The_Promise_and_Peril_of_Big_Data.pdf'.

ron un proceso de digitalización de la información disponible y planearon el desarrollo de bases de datos para varias finalidades (registros de la población, registros de propiedades, archivos policiales etc.). Además, debido a la naturaleza de la tecnología disponible (mainframes) y para ser más eficientes, los gobiernos se orientaron hacia la creación de archivos computarizados centralizados (véase, por ejemplo, la propuesta presentada, en 1966, por el Social Science Research Council en los EE.UU. para establecer un centro federal de datos y la propuesta similar de la Oficina Central de Estadística de Suecia a principios de los años sesenta) (9).

Esta primera ola de digitalización y *datafication* de nuestra sociedad (10) incrementó el papel ya existente de las agencias gubernamentales en la realización de análisis estadísticos y confirmó su liderazgo en el gobierno de datos. Con el paso de los años, los organismos públicos nacionales y regionales adoptaron progresivamente este enfoque basado en el tratamiento automatizado de datos para los procesos de adopción de decisiones.

Aunque este cambio de paradigma generó algunas preocupaciones entre los ciudadanos (11), este proceso ocurrió en todos los países industrializados, independientemente de sus orientaciones políticas. Esta fue una profunda transformación de los procesos administrativos e impactó en la relación entre la administración pública y los ciudadanos. Tres condiciones principales lo hicieron posible: la dimensión del aparato gubernamental, la disponibilidad de datos y la confianza de los ciudadanos en el gobierno (12).

La centralización de datos y la creación de amplias bases de datos automatizadas fueron posibles ya que a lo largo de los siglos los Estados adoptaron formas y procedimientos para recopilar información de los ciudadanos para diversas finalidades relacionadas con la soberanía y su ejercicio, así como con la organización de una administración pública eficiente.

Además, la soberanía y el poder administrativo establecido por la ley preveían organismos públicos con facultades de legitimar la recopilación de datos de las personas sin ninguna posibilidad de negociación con los ciudadanos, salvo la negociación a nivel político en los casos de gobiernos democráticos que la hicieron posible.

Por lo tanto, los únicos límites a la recopilación de datos fue la presencia de una fuerte oposición de los ciudadanos. Un ejemplo en este sentido fue la reacción contra el procesamiento automatizado de datos informatizados que caracterizó a muchos países entre los años sesenta y los seten-

(9) Véase Bennett, C.J.: *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Cornell University Press, Ithaca, 1992, pp. 45-55.

(10) Véase Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, 1973 'http://epic.org/privacy/hew1973report/'.

(11) Véase la siguiente sección 3.

(12) Véase Krotoszynski, R.J. Jr.: *Privacy Revisited. A Global Perspective on the Right to Be Left Alone*, Oxford University Press, Oxford, 2016.

ta. Esto abrió el camino a las regulaciones relativas a la protección de datos. Estas regulaciones y la primera ola de digitalización representaban los dos elementos del acuerdo político alcanzado en ese momento: los ciudadanos aceptaron una recopilación de datos extensa y automatizada a cambio de salvaguardas específicas de sus derechos previstas por la ley.

De distinto modo, el sector privado no tenía el mismo poder que la administración pública, ya que no habría podido imponer la recopilación de datos. Por lo tanto, la *datafication* en las empresas privadas comenzó como una especie de efecto colateral de la actividad principal llevada a cabo por ellas: se recopiló información para apoyar las cadenas de suministro, la logística y la gestión de los pedidos, de manera funcional a la organización básica de las actividades comerciales.

La revolución del *marketing* directo que ocurrió entre los años ochenta y los noventa modificó esta actitud inicial, desvelando los valores económicos de esta información, principalmente respecto los perfiles de los clientes (13). Las nuevas formas de *marketing* basadas en la creación de perfiles reemplazaron la comercialización de pedidos por correo, pasada de moda, y se movieron hacia soluciones automatizadas basadas en datos almacenados en archivos electrónicos.

Esto aumentó significativamente el valor económico y competitivo de los archivos de información y motivó a las compañías a invertir en extensos procesos de recopilación de datos y software de análisis de datos. Este nuevo enfoque colmó la brecha entre los sectores público y privado. En los años ochenta, cuando se adoptaron las primeras posiciones comunes sobre protección de datos a nivel europeo, la recopilación de datos ya no era una actividad circunscrita a la relación entre el gobierno y los ciudadanos, sino que también afectaba a las empresas y los clientes.

Aunque las empresas privadas no fueron los principales actores de la primera etapa de la *datafication,* se convirtieron en los principales actores de la segunda ola de *datafication,* que empezó con la comercialización de Internet y ha seguido hasta las actuales aplicaciones algorítmicas y dispositivos IoT (14). La digitalización de negocios tradicionales y de los servicios o productos proporcionados por estos negocios (comercio electrónico), la provisión de nuevos servicios en línea *(e-business)* y un número creciente de servicios gratuitos hacen posible que las empresas re-

(13) Véase Petrison, L.A., Blattberg, R.C. y Wang, P.: «Database Marketing. Past, Present, and Future», *J. Direct Marketing*, núm. 11(4), 1997, pp. 115-119; Solove, D.J.: «Privacy and Power: Computer Databases and Metaphors for Information Privacy», *Stan. L. Rev.*, núm. 53(6), 2001, pp. 1405-1407.

(14) Véase King, G.: «Preface: Big Data is Not About the Data!» en Álvarez, M.R. (dir.): *Computational Social Science: Discovery and Prediction*, Cambridge University Press, Cambridge, 2016.

copilen grandes cantidades de datos y desarrollen nuevos negocios y modelos de negocio basados en la explotación de datos.

Este nuevo escenario, donde la recopilación de datos del sector privado es omnipresente, ha inducido un cambio en la relación entre el gobierno, las empresas privadas y los ciudadanos. La administración pública y los gobiernos locales están cada vez más interesados en asociarse con empresas privadas para tener un acceso más fácil a la información personal que quieren utilizar para diferentes propósitos (por ejemplo, estrategias de prevención del delito) (15) o para proporcionar servicios de datos intensivos a ciudadanos a un menor coste, externalizándolos a empresas privadas.

Esto también es evidente en un sector crucial de la vida democrática, como los sistemas de vigilancia social. El caso de la NSA (16) fue una clara representación de las posibles consecuencias de monitorizar la interacción en línea utilizando datos en manos de empresas privadas (17). De esta manera, los gobiernos obtienen información con la «cooperación» indirecta de los usuarios, que probablemente no habrían dado la misma información a las entidades públicas si así lo solicitaran.

Los proveedores de servicios recopilan datos personales en gran parte en virtud de acuerdos privados (políticas de privacidad) y con el consentimiento de los usuarios y lo hacen para fines específicos (18). Puesto que los gobiernos explotan esta práctica mediante el uso de acuerdos y órdenes judiciales para obtener la divulgación de esta información, este mecanismo oculta a los ciudadanos el riesgo y la dimensión del control social que pueden realizar los gobiernos.

---

(15) Véase Mantelero, A. y Vaciago G.: «The "Dark Side" of Big Data: Private and Public Interaction in Social Surveillance: How data collections by private entities affect governmental social control and how the EU reform on data protection responds», *Computer Law Review International*, núm. 14 (6), 2013, pp. 161-169.

(16) Véase, *inter alia*, European Parliament: *Resolution of 4 July 2013 on the US National Security Agency surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' privacy*, Bruxelles, 2013, 'http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0322+0+DOC+XML+V0//EN'; European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs: *The US National Security Agency (NSA) surveillance programmes (PRISM) and Foreign Intelligence Surveillance Act (FISA) activities and their impact on EU citizens*, Bruxelles, 2013, pp. 14-16 'http://info.publicintelligence.net/EU-NSA-Surveillance.pdf'; European Parliament, Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs, Civil Liberties, Justice and Home Affairs: *National Programmes for Mass Surveillance of Personal data in EU Member States and Their Compatibility with EU Law*, Bruxelles, 2013, pp 12-16 'http://www.europarl.europa.eu/committees/it/libe/studiesdownload.html?languageDocument=EN&file=98290'.

(17) Véase Council of Europe: *Guidelines for the cooperation between law enforcement and internet service providers against cybercrime*, Strasbourg, 2008 'http://www.coe.int/t/informationsociety/documents/Guidelines_cooplaw_ISP_en.pdf'.

(18) Véase Reidenberg, J.: «The Data Surveillance State in the US and Europe», *Wake Forest Law Review*, núm 49, 2014, pp. 583-608.

3. LOS DESAFÍOS DE UNA SOCIEDAD BASADA EN DATOS

El nuevo entorno de datos descrito en la sección anterior y la nueva dinámica de las relaciones entre la administración pública y las empresas privadas que procesan grandes cantidades de datos socavaron necesariamente el papel atribuido históricamente a las agencias estadísticas, en un mundo en el que muchísimos datos se producen en base a una gran variedad de sensores y dispositivos. Este aumento en el número de fuentes de datos y en la cantidad de información disponible, ha sugerido la sustitución parcial del enfoque estadístico tradicional y de los servicios estadísticos gubernamentales por el análisis social proporcionada por las empresas privadas. Este fue el caso del análisis de la difusión de la gripe por medio de Google Flu Trends y, más recientemente, el caso de Uber.

Esta colaboración entre servicios públicos y empresas privadas no es nueva, ya que en varios sectores existe una interacción similar con beneficios mutuos y sin ningún impacto negativo en los ciudadanos. No obstante, las colaboraciones relativas a la gobernanza de datos no están circunscritas al servicio (como cuando un servicio de transporte es proporcionado por una empresa privada en lugar de un servicio público) ya que también se refieren al uso de los datos necesarios para acceder al servicio y de las informaciones generadas por el servicio.

En este contexto, existe una creciente necesidad de salvaguardar a las personas y las comunidades del riesgo potencial de decisiones políticas relacionadas con la gobernanza digital que puedan minar la autodeterminación de los ciudadanos a corto y largo plazo. Las empresas privadas pueden recopilar información extensa sobre los ciudadanos, debido a la asociación público-privada mencionada, sin ninguna libertad de elección para el interesado, ya que las empresas privadas actúan en nombre de organismos públicos que están autorizados por ley a usar datos sin consentimiento individual (19).

En estos casos, si no se adoptan medidas específicas que limiten cualquier uso adicional de esta información, existe el riesgo que la oferta de servicios más económicos a la administración pública por parte de las empresas más grandes del sector de las TIC sean el medio para acceder a los datos de los ciudadanos, de la misma manera que los servicios gratuitos de correo electrónico y de acceso a las redes sociales fueron el medio para recabar los datos de los particulares.

Los movimientos de ciudadanos, así como las estrategias de gobernanza digital adoptadas por la administración local pueden mitigar este riesgo, de manera que los proveedores de servicios no estén autorizados a

(19) Véase artículos 6(1)(c) y 6(1)(e) RGPD.

extraer información adicional de los datos que tratan, como un subproducto de sus servicios.

Sin embargo, las decisiones sobre cómo abordar estos problemas no pueden dejarse en manos de gobiernos individuales, o de grupos locales, que pueden verse afectados por la falta de conciencia, la subestimación de las posibles consecuencias o el desequilibrio de poder. Por esta razón, es importante proporcionar un marco legal que proteja adecuadamente el derecho individual y colectivo (20) a la protección de datos, apoyando el gobierno de datos. Además, este derecho debería colocarse en un contexto más amplio, que también tuviera en cuenta las consecuencias sociales y éticas del uso de datos (21).

Esta necesidad es aún más relevante en el contexto del Big Data, donde el análisis de los datos se utiliza para ayudar a quienes toman decisiones o (en algunos casos) sustituye las decisiones humanas. La ciudadanía digital implica un control efectivo, público y democrático de estas aplicaciones.

Varios casos de sesgo en la utilización de los datos y la complejidad del uso de esta nueva herramienta para la toma de decisiones instan a adoptar un enfoque más consciente respecto los proveedores de servicios y el desarrollo de servicios. En este sentido, los beneficios prometidos del análisis en tiempo real, el enfoque holístico en relación con los datos de las comunidades, la capacidad predictiva del *Big Data analytics* no deberían restringir la reflexión sobre los límites y los riesgos de estas tecnologías.

Por lo tanto, de acuerdo con el principio de proporcionalidad, es importante definir en primer lugar si estos servicios representan un beneficio para las comunidades, si el análisis de datos en tiempo real y masivo basado en correlaciones es necesario en todos los casos y es mejor que un mecanismo más elaborado y de análisis científico, que esté basado en el enfoque estadístico tradicional.

Los *data obesitas* (22) y las conclusiones basadas en las correlaciones entre los datos pueden considerarse políticamente deseables, pero pueden no ser necesariamente efectivas para una mejor gestión de las comunidades de ciudadanos. Desde esta perspectiva, la ciudadanía digital asume la dimensión del compromiso cívico en las decisiones sobre la forma y la intensidad de las operaciones de procesamiento de datos que deberían implementarse para proporcionar beneficios potenciales a las comunidades.

El primer paso de este proceso de uso de datos es, por lo tanto, un compromiso cívico o debate político. Posteriormente, cuando se asume

(20) Véase Mantelero, A.: «Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection», *Computer Law and Security Review*, núm. 32 (2), 2016, pp. 238-255.

(21) Véase la siguiente sección 3.2.

(22) Véase Hildebrandt, M.: «Learning as a machine: Crossovers between humans and machines», *Journal of Learning Analytics*, núm. 4 (1), 2017, p. 10.

una decisión en el sentido de la necesidad de adoptar una solución específica basada en datos, un segundo paso del proceso se caracteriza por una mayor reflexión sobre la manera de poner en práctica dicha elección.

En esta segunda etapa, es fundamental analizar aspectos como el diseño de los servicios o productos, la naturaleza de los datos procesados, la naturaleza de los proveedores de servicios externos y sus posibles propósitos concurrentes (23). Al respecto, el enfoque centrado en el diseño, expresamente adoptado por el legislador de la UE en el reciente Reglamento General de Protección de Datos (RGPD) (24), puede proporcionar una base legal para este análisis (25). Proporcionalidad, minimización de datos y preferencia por soluciones orientadas a la privacidad son algunos de los elementos que pueden concurrir en la definición de un mejor entorno digital, más respetuoso con los ciudadanos y sus derechos.

Para abordar estos problemas, se podría sugerir la adopción de modelos basados en la propiedad, enfatizando la propiedad de los datos de los ciudadanos o de sus organizaciones representativas. Sin embargo, los modelos que enfatizan la noción de propiedad respecto de los datos corren el riesgo de socavar el control sobre la información que las leyes de protección de datos reconocen a las personas, independientemente del hecho de que hayan proporcionado su información a terceros.

El régimen legal existente ha creado una especie de circulación controlada de información personal, donde los elementos cercanos a la noción de propiedad (por ejemplo, transferencia de información personal a terceros, explotación económica de la información personal) coexisten con un control persistente de los datos personales por los interesados (26). Este modelo regulatorio contrasta con la idea de una propiedad pura, donde el acto de disposición excluye cualquier forma de control en nombre de los propietarios originales, que no mantienen un control residual sobre el objeto transferido a terceros.

La preferencia por un enfoque diferente, fiel al marco de la regulación europeo en tema de derechos de la personalidad, se confirma en el RGPD donde disposiciones específicas reconocen a los interesados un control sobre su información, aunque se haya transferido la información a un responsable del tratamiento (27). Esto es coherente con el enfoque basado en los derechos fundamentales y el RGPD construye además un nivel adicional sobre la responsabilidad del responsable de los datos (28).

---

(23) Véase artículo 26 RGPD (corresponsables del tratamiento).

(24) Sobre el Reglamento General de Protección de Datos, vedase Piñar Mañas, J.L. (Director): *Reglamento General de Protección de datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016.

(25) Véase artículo 25 RGPD (Protección de datos desde el diseño y por defecto).

(26) Véase capítulo III RGPD.

(27) Véase la nota 26.

(28) Véase el principio de responsabilidad proactiva (artículo 5 (2) RGPD).

La responsabilidad proactiva implica que los responsables del tratamiento no pueden utilizar los datos de los interesados sin ninguna restricción, por el contrario, deben tener en cuenta adecuadamente los intereses de los afectados. Esto es diferente de lo que sucede en un modelo de propiedad. Además, la responsabilidad proactiva supone una evaluación de los riesgos potenciales relacionados con el procesamiento de datos y la adopción de medidas técnicas, organizativas y contractuales adecuadas para prevenir o mitigar los riesgos y poder demostrar el cumplimiento de las disposiciones legales que imponen estas medidas.

Otro desafío que debería considerarse en el entorno digital actual es la transparencia y la igualdad de trato en relación con el papel que desempeñan las empresas privadas en la interacción con las administraciones públicas en el procesamiento de datos de los ciudadanos. Las empresas privadas se ven frecuentemente afectadas por la falta de transparencia sobre la manera en que se procesan los datos, como se demostró en el debate sobre la transparencia de los algoritmos. Esto se debe principalmente a razones competitivas y de protección de la propiedad intelectual, pero contrasta con el enfoque adoptado por las oficinas de estadística y la necesidad democrática de conocer los detalles de los algoritmos que sirven de base para las decisiones públicas (29).

En caso de colaboración entre la administración pública y las empresas privadas en el tratamiento de datos para la gobernanza digital, esta falta de transparencia puede afectar los datos en manos de las empresas privadas e impactar negativamente en el análisis de la información que proporcionan a la administración pública.

Estas limitaciones que afectan los archivos privados y su uso para el apoyo a la toma de decisiones no excluyen necesariamente la interacción entre las empresas privadas y la administración pública en la gestión de datos, pero instan a exigir y mantener un alto nivel de responsabilidad a las empresas privadas involucradas en estas formas de interacción. Para abordar este desafío y garantizar un uso democrático de los datos, las salvaguardias contractuales específicas, las auditorías externas y los comités internos (según los modelos de los comités de ética o de las juntas de revisión institucional) pueden aumentar el nivel de responsabilidad proactiva y de transparencia en el uso de datos. Al mismo tiempo, estas soluciones también pueden contribuir a involucrar las potenciales partes interesadas en el proceso de diseño del uso de los datos para finalidades públicas.

(29) Restricciones pueden justificarse cuando hacer público el algoritmo puede tener un impacto negativo en la capacidad de la administración pública de llevar a cabo sus tareas (esto es el caso de los algoritmos de vigilancia predictiva).

3.1 **Las leyes de protección de datos como un instrumento para la democracia digital en el contexto de la era de la información**

A lo largo de los años y aún hoy, varias preguntas –descritas en la sección anterior– han surgido en relación con la revolución informática y la progresiva *datafication* de nuestra sociedad. Estas preocupaciones acerca de las consecuencias que pueden afectar a la democracia digital y la gobernanza de los datos han originado una respuesta legal en muchos países.

En una sociedad cada vez más basada en la explotación de los datos, frente al riesgo de una distribución asimétrica del poder relacionado con la información y las posibles consecuencias en términos de discriminación y control social, la respuesta legal se centró en la regulación del uso de datos. Esto llevó a los legisladores a la adopción de regulaciones relativas a la protección de datos.

En un contexto en el que las personas ya no están representadas solo por su cuerpo físico sino también por su representación digital generada por la base de datos, la protección de datos «fulfils the task of ensuring the «habeas data» required by the changed circumstances - and thereby becomes an ineliminable component of civilisation, as has been in the history for the habeas corpus» (30). En este sentido, desde sus orígenes, la noción de protección de datos se basa en la idea de control sobre la información, como lo confirma la literatura de ese período (31).

Por estas razones, las leyes dieron a los individuos la oportunidad de tener un cierto nivel de control sobre los datos recopilados, proporcionando una respuesta a la creciente preocupación de los ciudadanos sobre la gobernanza digital y el uso democrático de la información (32). En este sentido, el propósito de estas reglamentaciones iniciales no fue necesariamente difundir y democratizar el poder sobre la información, sino aumentar el nivel de transparencia sobre el tratamiento de datos y salvaguardar el derecho de acceso a la información.

La notificación obligatoria de nuevas bases de datos, la creación de registros públicos de bases de datos y el modelo basado en las autorizaciones fueron los elementos fundamentales de estas nuevas reglamentacio-

(30) Véase Rodotà, S.: «Privacy, Freedom, and Dignity: Conclusive Remarks at the 26th International Conference on Privacy and Personal Data Protection» 2004 «http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/export/1049293».

(31) Véase Westin, A.F.: *Privacy and Freedom*, Atheneum, New York, 1970; Breckenridge, A.C.: *The Right to Privacy*, University of Nebraska Press, Lincoln, 1970; Solove, D.J.: *Understanding Privacy*, Harvard University Press, Cambridge, Mass., 2008.

(32) Véase Mayer-Schönberger, V.: «Generational development of data protection in Europe?» en P.E. Agre y M. Rotenberg (Directores), *Technology and privacy: The new landscape*, MIT Press, Cambridge, Mass., 1997, pp. 221-227; Bennett, *op. cit.;* Secretary's Advisory Committee on Automated Personal Data Systems: *Records, Computers and the Rights of Citizens*, 1973 «http://epic.org/privacy/hew1973report/»; Miller, A.R.: *The Assault on Privacy Computers, Data Banks, Dossiers* (University of Michigan Press, Ann Arbor, 1971; Brenton, M.: *The Privacy Invaders*, Coward-McCann, New York, 1964; Packard, V.: *The Naked Society*, David McKay, New York, 1964.

nes, necesarios para que los ciudadanos supieran quién tenía el control de la información y para controlar el tratamiento de datos. Otro componente clave fue el derecho de acceso, que permitió a los ciudadanos preguntar a los responsables del tratamiento sobre la forma en que se utilizaba la información y, en consecuencia, sobre el ejercicio de su poder sobre la información. Este marco regulatorio se completó con la creación de autoridades independientes de protección de datos, con el fin de salvaguardar los derechos de los ciudadanos, ejercer el control sobre los responsables de tratamiento y reaccionar contra los abusos.

Finalmente, en esa etapa, no existía un espacio de autonomía en términos de negociación sobre la información personal, dado que la recopilación de información se llevaba a cabo principalmente por entidades públicas para fines relacionados con el interés público y era obligatoria en virtud de la ley.

El siguiente período, desde mediados de los años 80 hasta los 90, se caracterizó por un cambio en el paradigma normativo, debido a nuevos escenarios tecnológicos, sociales y económicos. Los ordenadores personales emergieron en el mercado a finales de los 70 para convertirse en algo común durante los años 80. Esta fue la nueva era de la computación distribuida, en la que mucha gente compró ordenadores para recopilar y procesar información. La capacidad computacional ya no era un privilegio exclusivo de los gobiernos y las grandes empresas, sino que se convirtió en accesible para muchas entidades y consumidores.

Esta transformación y el incremento contemporáneo del marketing directo originaron nuevas demandas de la sociedad hacia el legislador, ya que los ciudadanos querían tener la oportunidad de negociar sus datos personales y obtener algo a cambio. Aunque en Europa la protección de datos se mantuvo dentro del contexto de los derechos fundamentales (33), el objetivo principal de esta nueva ola de regulaciones fue buscar intereses económicos relacionados con el libre flujo de datos personales (34), afirmando una tendencia, que aún está presente, y que se ha reforzada aún más, si cabe, en los últimos años (35).

---

(33) Véase Council of Europe: *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 1981 «http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CL=ENG'; OECD, *Annex to the Recommendation of the Council of 23rd September 1980: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* 'http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#preface».

(34) Véase los Considerandos de la Directiva 95/46/CE de 24 de octubre; Poullet, Y.: «EU data protection policy. The Directive 95/46/EC: Ten years after», *Computer Law and Security Review*, núm. 22 (3), 2006, p. 207; Simitis, S.: «From the Market to the Polis: The EU Directive on the Protection of Personal Data», *Iowa L. Rev.*, núm. 80, 1995, p. 445.

(35) Véase la Estrategia para el Mercado Único Digital propuesta por la Comisión Europea «http://www.consilium.europa.eu/es/policies/digital-single-market/».

Tanto el modelo teórico de los derechos fundamentales, basado en la autodeterminación individual, como la creciente economía impulsada por los datos destacaron la importancia de reconocer un papel activo al sujeto de los datos en la gobernanza de los mismos. Esto ya no constituye una tarea exclusiva y un privilegio de los responsables de los datos, sino que debe involucrar necesariamente a los interesados que, de forma autónoma y sin restricciones ilegítimas, deben poder decidir si y como se tratan sus datos. Sin embargo, esta autonomía en la gestión de los datos se refiere a la información tratada por entidades privadas, mientras que el sector público mantiene su derecho a procesar información personal en virtud de la ley y con la finalidad de llevar a cabo sus tareas.

3.2 **El advenimiento del Big Data y el nuevo cambio de paradigma**

El advenimiento de la analítica del Big Data ha creado un nuevo escenario tecnológico, con consecuencias directas en términos de gobernanza digital y adecuación del marco legal que regula el procesamiento de datos. El uso de análisis de datos para extraer nuevos valores de los datos tiene dos consecuencias principales: el riesgo de una distribución asimétrica del poder de información y el surgimiento de una nueva dimensión colectiva del tratamiento de datos.

En cuanto a la primera consecuencia, el elemento innovador del Big Data no es ni la ingente cantidad de datos procesados ni los varios parámetros que suelen mencionarse con la dominación de 3V (velocidad, variedad y volumen). El elemento clave, que representa un nuevo paradigma en el análisis de datos, se refiere al enfoque predictivo adoptado por estas tecnologías. En este sentido, el Big Data identifica conjuntos de datos extremadamente grandes que pueden analizarse computacionalmente para extraer inferencias sobre los interesados, tendencias y correlaciones. Además, los resultados proporcionados por el *software* de análisis *(Big Data analytics)* y basados en estas correcciones son cada vez más utilizados por quienes deben adoptar decisiones con la finalidad de facilitar sus elecciones entre las posibles soluciones alternativas.

Con este telón de fondo, tres elementos asumen importancia para beneficiarse del análisis basado en el Big Data: grandes cantidades de datos, *analytics* y expertos en datos. Por lo tanto, los datos no son suficientes, pero se requieren inversiones importantes en software (y hardware) para analizar datos *(analytics)* y la disponibilidad de recursos humanos califi-

cados para definir el diseño correcto del análisis y proporcionar una interpretación precisa de los resultados (36).

En este escenario, las grandes empresas basadas en datos (p. ej. Google o Amazon), así como los gobiernos o intermediarios en flujos de información (p. ej. motores de búsqueda, proveedores de Internet, intermediarios de datos) están en la mejor posición para maximizar sus archivos informativos y extraer inferencias que no están disponibles para otras entidades. Esto crea una distribución asimétrica de la información y del conocimiento basado en la información.

Las políticas de datos abiertos adoptadas por muchos organismos públicos y, en un número más limitado, por empresas privadas solo pueden aparentemente disminuir esta concentración de poder respecto la información, ya que el acceso a la información no es equivalente al conocimiento. Una gran cantidad de datos crea conocimiento si los titulares de los datos disponen de las herramientas de interpretación adecuadas para seleccionar la información relevante, reorganizar e interpretar los datos y los resultados de los *analytics*. Sin estas habilidades, más datos solo producen confusión y menos conocimiento al final, con información interpretada de manera incompleta o incorrecta. Por estas razones, una mayor disponibilidad de datos no es suficiente para democratizar la distribución del poder sobre la información en el contexto de Big Data (37).

Otro elemento que caracteriza y distingue esta nueva forma de concentración del control de la información está relacionada con la naturaleza de las finalidades del tratamiento de datos: el procesamiento de datos ya no se centra en usuarios únicos (creación de perfiles individuales), sino que aumenta por escala y trata de investigar las actitudes y comportamientos de grandes grupos y comunidades. Las nuevas tecnologías y el poderoso *software* de análisis permiten recopilar y analizar grandes cantidades de datos para tratar de identificar patrones en el comportamiento de grupos de individuos y tomar decisiones que afectan las dinámicas internas de estos grupos, con consecuencias que afectan los intereses colectivos de las personas involucradas.

Además, estos grupos son diferentes de los considerados en la literatura sobre privacidad de grupo (38); de hecho, estos grupos son creados por los responsables del tratamiento, que seleccionan conjuntos específicos de

---

(36) Véase Bollier, *op. cit.*; Cohen, J.E.: «What Privacy is For», *Harv. L. Rev.*, núm. 126, 2013, pp. 1924-1925; Boyd, D. y Crawford, K.: «Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly», *Inf., Comm. & Soc.*, núm. 15(5), 2012, pp. 666-668.

(37) Véase Dwork, C. y Mulligan, D.K.: «It's not Privacy and It's not Fair», *Stan. L. Rev. Online*, núm. 66, 2013, pp. 35-40.

(38) Véase Taylor, L. *et alii* (Directores): *Group Privacy: New Challenges of Data Technologies*, Springer, Cham 2017.

información. Los responsables moldean los conjuntos de personas que se propusieron investigar: las personas cuya información contribuye a la creación de estos grupos dinámicos pueden ser cambiadas de un grupo a otro, según su comportamiento. Finalmente, estos algoritmos de Big Data recopilan informaciones sobre varias personas, que no conocen a los otros miembros del grupo y, en muchos casos, no saben de su pertenencia a un grupo (39). Este es el caso de los perfiles de grupos de consumidores (40), productos de puntuación predictiva (41) y aplicaciones de vigilancia predictiva (42).

Este enfoque sobre categorías homogéneas de personas lleva a quienes deben tomar decisiones a adoptar soluciones comunes para todos los individuos clasificados dentro del mismo grupo generado por los algoritmos de Big Data. Sin embargo, estos no son los grupos sociológicos tradicionales (p. ej. minorías o grupos políticos) o grupos creados por sus miembros (p. ej. asociaciones), que conocen su pertenencia y conocen (o pueden conocer) a los otros miembros. Los grupos generados por medio de los algoritmos se crean de forma autónoma mediante esta herramienta informática y pueden ser modificados de forma continua y sin esfuerzo.

Este escenario resalta nuevos aspectos de la ciudadanía digital, ya que señala el surgimiento de una dimensión colectiva del uso de datos (43), que va más allá de la protección de datos individuales y aborda cuestiones relacionadas con el impacto social de las políticas de datos.

Lo importante de esta dimensión colectiva depende del hecho de que el enfoque de la clasificación mediante algoritmos modernos no se centra únicamente en individuos, sino en grupos o grupos de personas con características comunes (p. ej. hábitos del cliente, estilo de vida, comportamiento en línea y fuera de línea, etc.). Las decisiones basadas en datos se

---

(39) Véase Hildebrandt, M.: «Defining Profiling: A New Type of Knowledge?» en M. Hildebrandt y S. Gutwirth (Directores), *Profiling the European Citizen. Cross-Disciplinary Perspective*, Springer, Dordrecht, 2010, pp. 19-20; Gandy, O.H. Jr.: «Exploring Identity and Identification in Cyberspace», *Notre Dame J. L. Ethics & Pub. Pol'y*, núm. 14, 2000, pp. 1085-1100.

(40) Véase Calo, R.: «Digital Market Manipulation», *George Washington Law Review*, núm. 82, 2014, pp. 995-1051.

(41) Véase Federal Trade Commission: *Data Brokers: A Call for Transparency and Accountability*, 2014 «https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf»; Rieke, A. *et alii: Civil Rights, Big Data, and Our Algorithmic Future. A September 2014 report on social justice and technology*, 2014 «http://bigdata.fairness.io/wp-content/uploads/2014/09/Civil_Rights_Big_Data_and_Our_Algorithmic-Future_2014-09-12.pdf».

(42) Véase Walter, L. *et alii: Predictive Policing. The Role of Crime Forecasting in Law Enforcement Operations*, The RAND Corporation, 2013 «http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf»; Ferguson, A.G.: «Predictive Policing: The Future of Reasonable Suspicion», *Emory L. J.*, núm. 62, 2012, pp. 259-325; van Brakel, R. y De Hert, P.: «Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies», *Journal of Police Studies*, núm. 20(3), 2011, pp. 163-192.

(43) Véase Mantelero, *op. cit.*

refieren a grupos de individuos y solo afectan indirectamente a los miembros de estos grupos.

Con este telón de fondo, la ciudadanía digital, en términos de participación en las decisiones que pueden afectar a una comunidad, así como la gobernanza digital y los asuntos políticos convergen al abordar esta dimensión colectiva del tratamiento de datos. Un ejemplo en este sentido es el conocido caso de la ciudad de Boston y su aplicación para *smartphone* StreetBump para detectar baches pasivamente: la aplicación tenía un problema de cualidad de los datos recopilados debido al sesgo generado por la baja penetración de los *smartphones* entre los residentes de bajos ingresos y de personas mayores. Si bien la administración de Boston tomó en cuenta este sesgo y resolvió el problema en otros casos similares, funcionarios públicos menos meticulosos podrían subestimar los sesgos y tomar decisiones potencialmente discriminatorias (44). Los mismos problemas surgen en muchos otros casos, como los relacionados con el software de vigilancia predictiva y los tratamientos de evaluación de riesgos adoptados en las sentencias penales de EE.UU. (45).

El impacto en los derechos individuales, pero también la presencia de intereses supraindividuales, riesgo de discriminación, gobernanza de datos, gestión comunitaria, todos estos temas surgen en estos casos, confirmando la convergencia y fusión de diferentes cuestiones sociales y políticas en las decisiones sobre el uso de los datos.

En este contexto, el reglamento existente sobre protección de datos de la Unión Europea (Reglamento General de Protección de Datos), que desempeña un papel central en estrategias de procesamiento de datos, mantiene un enfoque tradicional, que parece ser en parte inadecuado en el contexto de Big Data.

Por un lado, el RGPD muestra un cambio parcial del enfoque regulatorio de la autodeterminación del sujeto de datos a la responsabilidad de los responsables de tratamiento y de las personas involucradas en el procesamiento de datos (responsabilidad proactiva). La responsabilidad proactiva y el enfoque basado en el riesgo adoptado en el Reglamento representan el núcleo del nuevo marco de protección de datos de la UE y elementos importantes para abordar los posibles impactos negativos del uso del análisis de datos.

---

(44) Véase Crawford, K.: «The Hidden Biases in Big Data», *Harv. Bus. Rev.*, April 1, 2013, «https://hbr.org/2013/04/the-hidden-biases-in-big-data».

(45) Véase U.S. Department of Justice-Criminal Division, Office of the Assistant Attorney General: «Annual letter», 2014, pp. 6-13 «http://www.justice.gov/criminal/foia/docs/2014annual-letter-final-072814.pdf»; Administrative Office of the United States Courts - Office of Probation and Pretrial Services: «An Overview of the Federal Post Conviction Risk Assessment», 2011, «http://www.uscourts.gov/uscourts/FederalCourts/PPS/PCRA_Sep_2011.pdf».

Por otro lado, la respuesta a los desafíos de la sociedad algorítmica parece ser limitada e incompleta. El RGPD sigue enfocado en la dimensión individual de la protección de datos, mientras que el uso cada vez mayor del *Big* Data *analytics* en los procesos de adopción de decisiones ha aumentado la importancia de investigar aspectos relacionados con los grupos de individuos y la sociedad en general (46). Además, en estos casos los daños potenciales no están restringidos a los riesgos conocidos en tema de privacidad (p. ej. uso ilegítimo de informaciones personales, seguridad de los datos), sino que se requiere adoptar un enfoque más amplio para salvaguardar el derecho de los ciudadanos en la era digital actual.

Tal como lo demuestra el debate en curso sobre la ética de los datos y las diversas iniciativas en este tema, es necesario abordar las cuestiones éticas y sociales planteadas por los usos de los algoritmos. En este sentido, las soluciones de vigilancia predictiva, por ejemplo, no son solo una cuestión de protección de datos o cumplimiento de la ley, sino que se refieren a las formas de sociedad y relaciones entre los ciudadanos y la administración que queremos adoptar en el futuro. Por lo tanto, las decisiones políticas sobre tecnologías similares instan a tener en cuenta también esta dimensión más amplia del uso de datos, la que impacta en los valores éticos y sociales (47).

Por estos motivos, la evaluación de impacto relativa a la protección de datos (art. 35 RGDP) debería evolucionar hacia una evaluación más amplia y más compleja que es la Privacy, Ethical and Social Impact Assessment (PESIA) (48).

Esta evaluación sobre el cumplimiento del uso de datos con valores éticos y sociales es más complicada que la evaluación tradicional de protección de datos. De hecho, los valores principales (p. ej., la integridad de los datos) que se utilizan para realizar una evaluación en el contexto de la seguridad de los datos y la gestión de informaciones se basan en la tecnología y por lo tanto se pueden generalizar en diferentes contextos sociales. Al contrario, utilizando valores sociales y éticos, la situación es diferente: estos están necesariamente basados en el contexto y cambian de una comunidad a otra, por lo que es difícil identificar el punto de referencia que debe adoptarse en este tipo de evaluación de riesgos.

Este tema se aborda claramente en las directrices sobre el Big Data adoptadas por el Consejo de Europa. Al establecer un marco para el uso

(46) Véase Raab, C.: «Regulating Surveillance: The Importance of Principles» en K. Ball *et alii* (Directores), *Routledge Handbook of Surveillance Studies*, Routledge, London, 2012, pp. 377-385; Raab, C. y Wright, D.: «Surveillance: Extending the Limits of Privacy Impact Assessment» en D. Wright y P. De Hert, *Privacy Impact Assessment*, Springer, Dordrecht, 2012, pp. 363-383.

(47) Véase Piñar Mañas, J.L.: *Derecho e innovación tecnológica. Retos de presente y futuro*, CEU Ediciones, Madrid, 2018.

(48) Véase Mantelero, A.: «AI and Big Data: a blueprint for a human rights and ethical impact assessment», *Computer Law and Security Review*, 2018, en prensa.

del *Big Data analytics* orientado a la protección de datos, el Consejo de Europa insta tanto a los responsables de tratamiento como a los encargados a «adequately take into account the likely impact of the intended Big Data processing and its broader ethical and social implications» a fin de salvaguardar los derechos humanos y las libertades fundamentales, en consonancia con los principios de la Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (49).

Además, estas directrices reconocen la naturaleza relativa de los valores sociales y éticos y, en este sentido, requieren que los usos de los datos no entren en conflicto con los «ethical values commonly accepted in the relevant community or communities and should not prejudice societal interests, values and norms» (50). Aunque las directrices reconocen las dificultades para definir los valores que deben tenerse en cuenta al llevar a cabo un modelo que es similar al PESIA, sin embargo, señalan algunos pasos prácticos para identificar estos valores. Sugieren que «the common guiding ethical values can be found in international charters of human rights and fundamental freedoms, such as the European Convention on Human Rights», siguiendo la posición de los expertos en privacidad que han examinado este tema (51).

Dada la naturaleza de la evaluación social y ética, que es dependiente del contexto, y el hecho de que las Cartas internacionales solo pueden proporcionar una orientación de alto nivel, las Directrices combinan esta sugerencia general con una opción más personalizada, representada por «ad hoc ethics committees» (52). Estos comités, que en algunos casos ya existen en la práctica, deberían identificar los valores éticos específicos que deben salvaguardarse con respecto a un uso dado de datos cuando la evaluación de riesgo destaca «a high impact of the use of Big Data on ethical values». Las soluciones proporcionadas por estos comités serán más detalladas y basadas en el contexto especifico de cada aplicación que hace uso de los datos.

---

(49) Véase Consejo de Europa: *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, Strasbourg, 2017, Sección IV, párrafo 1.1.

(50) Véase Consejo de Europa, *op. cit.*, Section IV, párrafo 1.2.

(51) Véase Wright, D.: «A framework for the ethical impact assessment of information technology», *Ethics Inf. Technol.*, núm. 13, 2011, pp. 201-202.

(52) Véase Consejo de Europa, *op. cit.*, Section IV, párrafo 1.3 («the assessment of the likely impact of an intended data processing described in Section IV.2 highlights a high impact of the use of Big Data on ethical values, controllers could establish an ad hoc ethics committee, or rely on existing ones, to identify the specific ethical values to be safeguarded in the use of data»).

4. CONCLUSIONES

Este capítulo intenta crear un puente entre la primera y la segunda parte de este libro. Mientras que la primera parte se centra en la dimensión individual (naturaleza humana, identidad, identidad digital y derechos individuales) la segunda se refiere a la dimensión pública y colectiva de los derechos digitales (ciudadanía digital, transparencia de la administración pública, participación ciudadana, gobernanza y justicia digitales) Este capítulo, centrándose en los procesos de digitalización y *datafication* de nuestra sociedad, ha destacado cómo el tratamiento de datos desempeña un papel central en el desarrollo de la ciudadanía digital y cómo la presente sociedad algorítmica insta a vincular la dimensión individual y colectiva del uso de datos.

Desde esta perspectiva, la ciudadanía digital puede hacerse efectiva en términos de participación en la vida democrática solo si las personas, como individuos y grupos, han otorgado su derecho a su propio desarrollo y a su relación sin restricciones injustificadas por parte de entidades privadas o públicas. Esto destaca la dimensión sociopolítica de los datos, ya que la información se utiliza para analizar, organizar y dar forma a la sociedad.

En este sentido, la relevancia de la protección de datos va más allá de la dimensión individual y se convierte en un elemento constitutivo de la ciudadanía (53). La ausencia de cualquier estigma social y control generalizado es la condición previa para cualquier forma de ciudadanía digital y esto es aún más cierto en la sociedad actual, donde existe el riesgo de que la «verdad algorítmica» prevalezca sobre las decisiones democráticas.

Desde esta perspectiva, las cuestiones colectivas relacionadas con el impacto ético y social del uso de datos deben abordarse adecuadamente para desarrollar modelos de gobernanza de datos que los tengan en cuenta. La evaluación de estos impactos sociales a través de un debate abierto y participativo sobre la dirección que debe tomarse para equilibrar la eficiencia, los derechos y los intereses sociales es necesariamente parte de nuestra idea de democracia y fundamental para una ciudadanía digital efectiva.

En este sentido, treinta y cuatro años después, las ideas de Bobbio siguen vivas y nos sugieren cómo abordar los efectos de la transformación digital sobre la ciudadanía y el tema central relacionado con el control de la información sobre los ciudadanos: «l'ideale del potente è sempre stato quello di vedere ogni gesto e di ascoltare ogni parola dei suoi soggetti (possibilmente senza essere visto né ascoltato): questo ideale oggi è raggiungibile […] La vecchia domanda che percorre tutta la storia del pensiero politico: "Chi custodisce i custodi?" oggi si può ripetere con quest'alta

(53) Véase Rodotà, S.: *Tecnopolitica*, Laterza, Roma-Bari, 1997, p. 152.

formula: "Chi controlla i controllori?" Se non si riuscirà a trovare una risposta adeguata a questa domanda, la democrazia, come avvento del governo visibile, è perduta. Più che di una promessa non mantenuta si tratterebbe in questo caso addirittura di una tendenza contraria alle premesse: la tendenza non già verso il massimo controllo del potere da parte di cittadini ma al contrario verso il massimo controllo dei sudditi da parte del potere» (54).

(54) Bobbio, N.: *Il futuro della democrazia*, Einaudi, Torino, 1995, p. 19.

CAPÍTULO 7

EL ACCESO ELECTRÓNICO A LOS SERVICIOS PÚBLICOS: HACIA UN MODELO DE ADMINISTRACIÓN DIGITAL AUTÉNTICAMENTE INNOVADOR

Isaac Martín Delgado
Profesor Titular de Derecho Administrativo
Director del Centro de Estudios Europeos «Luis Ortega Álvarez»
Universidad de Castilla-La Mancha

1. PLANTEAMIENTO

Vivimos momentos de cambio. La sociedad, la economía, la cultura, la ciencia, la política e, incluso, el Derecho, están experimentando una paulatina transformación en sus reglas de funcionamiento como consecuencia de una causa común: el uso de las Tecnologías de la Información y las Comunicaciones (en adelante, TIC) por las personas y por las estructuras de las que éstas forman parte. Ello ha supuesto que, en cierto modo, el Estado entre en crisis, lo cual afecta a la propia Administración, que necesita legitimarse ante los ciudadanos (1).

Desde el plano teórico, la digitalización de su organización y de sus procedimientos de actuación nos sitúa ante un eventual cambio de paradigma en la concepción de las relaciones entre ésta y los ciudadanos. Efectivamente, la Administración surgida tras la Revolución Francesa, entendida como organización burocrática fuertemente jerarquizada con la encomienda monopolística de concretar el interés general y de ejecutar la Ley, está dando paso a una Administración, fruto de la Revolución Tecnológica, cuyas notas características tradicionales se están diluyendo en beneficio de una potencial mayor participación de los ciudadanos en la gestión de la cosa pública y de una posible flexibilización en la burocracia interna y externa, con el subsiguiente desplazamiento parcial del centro decisorio del Estado a los ciudadanos.

En consecuencia, hablar hoy en día de Administración Pública es, necesariamente, hablar de Administración electrónica. Este concepto se define convencionalmente como «el uso de las tecnologías de la información y las comunicaciones en las administraciones públicas, combinado con cambios organizativos y nuevas aptitudes, con el fin de mejorar los servicios públicos y los procesos democráticos y reforzar el apoyo a las políticas públicas» (2). La definición, más allá del hecho de que pone de manifiesto que el uso de las TIC no es un fin en sí mismo, da muestra de dos circunstancias. De un lado, permite intuir su alcance: su implantación en la Administración lo abarca todo, desde la organización administrativa hasta los derechos de los ciudadanos, desde la constitución y funcionamiento de los órganos colegiados hasta la notificación de las resoluciones, desde la transparencia hasta los contratos públicos. En segundo lugar, supone un cambio no tanto en el fondo como en las formas: se trata de usar las TIC para mejorar la administración, como función, y la Adminis-

(1) Sobre el Estado en crisis y la crisis de legitimidad de la Administración, puede verse Ramió, C.: *La Administración Pública del futuro (Horizonte 2050). Instituciones, política, mercado y sociedad de la información*, Tecnos, Madrid, 2017, pp. 12-13 y 91 y ss.

(2) Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre *El papel de la administración electrónica en el futuro de Europa*, COM (2003) 567 final, p. 7.

tración, como organización pública y persona jurídica. Y, si esto es así, es decir, si cambia la forma de organizarse y la forma de actuar de la Administración, puede cambiar toda ella. Estamos, sin duda –al menos desde el punto de vista teórico– ante un nuevo modelo de Administración Pública.

Todas las transformaciones que están experimentando nuestras organizaciones públicas tienen dos elementos en común: de un lado, el uso de las TIC, que es la premisa que los hace posible; de otro, el acceso y la utilización de la información pública como herramienta para el cambio, que constituye el auténtico motor de la innovación. Administración electrónica, transparencia y reutilización de la información en poder del sector público constituyen el triple eje de este nuevo modelo de Administración Pública.

Sin embargo, este proceso no es aséptico. Ni las tecnologías ni las decisiones políticas de aprovechamiento de las mismas son neutras; además, su implantación en la Administración puede tener consecuencias negativas si el Derecho no asegura el mantenimiento de las garantías jurídicas necesarias para la protección de los derechos de los ciudadanos. Éste es el principal reto que se plantea en relación con el proceso de digitalización de la Administración: lograr una mayor eficacia en el ejercicio de la función de administrar sin restringir el ámbito de protección de los ciudadanos frente al poder público.

Nos encontramos en nuestro país en un proceso permanente de reforma de la Administración española en relación con dos de sus aspectos esenciales: la organización y el procedimiento administrativo. Desde que la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y de Procedimiento Administrativo Común reconociera la validez legal del documento electrónico e incluyera la posibilidad de que las Administraciones hicieran uso de los medios electrónicos, hasta las actuales Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común (LPAC) y 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP), se han sucedido diferentes e importantes reformas normativas que incorporan las TIC como herramienta de cambio. Fue el caso, significativamente, de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAE), pero también lo es el de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno (LTBG), la Ley 37/2007, de 16 de noviembre, sobre Reutilización de la Información del Sector Público (LRISP) y la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP) (3). La mayor parte de estas medidas normativas fueron

(3) Para un examen de las implicaciones del uso de las TIC en relación con estas normas, puede verse el volumen colectivo Martín Delgado, I. (Dir.): *La reforma de la Administración electrónica: una oportunidad para la innovación desde el Derecho*, Instituto Nacional de Administración Pública, Madrid, 2017.

consecuencia del Informe de la Comisión para la Reforma de las Administraciones Públicas, un ambicioso proyecto de reforma administrativa impulsado en 2012 y cerrado en 2016 (4).

Tal proceso sigue su curso, como pone de manifiesto la reciente apertura del procedimiento de elaboración de un nuevo Plan Estratégico de Impulso y Transformación de la Administración Pública 2018-2020 (5), cuyo Eje 1, con el título Transformación digital de la Administración, plantea como objetivo estratégico la transformación integral de la Administración para convertirla en una Administración digital a través de la puesta a disposición de los diferentes usuarios de herramientas informáticas que permitan desarrollar un modelo de relación con los ciudadanos, las empresas y otras Administraciones Públicas más fluido y abierto.

Sin embargo, es evidente que los resultados no son los esperados –el nuevo Plan, que se lanza apenas finalizada la ejecución del Informe CORA, es la prueba más evidente de ello–. Más allá de que no se ha logrado aún la tramitación de la totalidad de los procedimientos de las diferentes Administraciones Públicas por medios electrónicos –principalmente, en los gestionados por la Administraciones autonómicas y, sobre todo,

(4) http://transparencia.gob.es/transparencia/dam/jcr: b1c69477-9882-41a5-9f6d-5cbb46fa12b4/reforma-AAPP. PDF (Última fecha de consulta: 19/03/2018). La Comisión para la Reforma de las Administraciones Públicas fue creada por Acuerdo del Consejo de Ministros el 26 de octubre de 2012. Se organizó internamente en cuatro Subcomisiones –Duplicidades Administrativas, Simplificación Administrativa, Gestión de Servicios Comunes y Administración Institucional–, que realizaron su trabajo durante poco más de 6 meses, tras los cuales presentó el 21 de junio de 2013 un informe que integraba un total de 217 propuestas (no pocas de las cuales eran indicaciones a las Comunidades Autónomas, por carecer el Estado de competencia sobre la materia) que buscaban eliminar duplicidades, simplificar procedimientos, mejorar la gestión de servicios y medios y racionalizar la Administración, en particular la institucional. Partiendo del constante aumento del gasto público en los últimos años, y teniendo en cuenta la considerable disminución de ingresos, lo que había generado un importante déficit estructural en el conjunto de las Administraciones Públicas, el Informe CORA proponía una reforma estructural de la Administración Pública española en clave eminentemente económica –no en vano, el principal marco legislativo de la misma era la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera– que condujera a la reducción del déficit y al aumento de la eficacia y la eficiencia en la gestión de la cosa pública. En relación con la Administración electrónica, el Informe CORA insistía en la idea de que «la reforma de la Administración parte, consecuentemente, de la necesidad de mejorar su eficacia (…). Entraña una Administración basada en los conceptos de transparencia, accesibilidad y capacidad de respuesta a las nuevas ideas y demandas de los ciudadanos. Una Administración al servicio de los ciudadanos. En definitiva, no sólo se trata de mejorar la eficiencia sino también de cambiar el enfoque de la Administración. Con innovaciones como la Administración electrónica no sólo se persigue hacer lo mismo a través de Internet, sino también usar Internet para hacer cosas nuevas». Más allá del exhaustivo trabajo realizado, del seguimiento de la ejecución de las medidas previstas y de las reformas normativas proyectadas y puestas en práctica, el Informe no presentaba un proyecto de reforma estructural de las Administraciones Públicas en lo que se refiere al paso de la Administración tradicional a la Administración digital. Se trataba más bien de una planificación conjunta por Ministerios de iniciativas para implementar la Administración electrónica en cumplimiento de la LAE, de una auditoría interna de la Administración General del Estado que afectaba parcialmente a la Administración autonómica y a la Administración local para perfeccionar diferentes aspectos organizativos, de una Planificación estratégica que buscaba avanzar en el camino hacia la modernización administrativa.

(5) *Vid.* http://transparencia.gob.es/transparencia/dam/jcr:2b9d399a-d49a-4aa3-9f95-68efa1e52f7c/Lineas-reforma-adminstrativa-2018-2020.pdf (Última fecha de consulta: 15/03/2018).

por los entes locales–, más bien poco ha cambiado en la forma de diseñar la organización administrativa, de estructurar el empleo público y, en general, de prestar servicios a los ciudadanos por medios electrónicos. Nuestra organización sigue anclada, en su esencia, en los años 80, el procedimiento es la principal y casi única forma de actuación de la Administración y algunas de las garantías clásicas de los ciudadanos están en claro retroceso.

Resulta por ello necesario llevar a cabo una reflexión de conjunto acerca del modelo de Administración Pública que queremos implantar en nuestro país .

En estas páginas se buscará ofrecer una serie de reflexiones generales en este sentido que tienen por objeto apuntar ideas concretas, a modo de premisas que pueden ayudar a llevar a cabo esa transformación digital necesaria.

A tal fin resulta imprescindible tener muy presente en todo momento una triple exigencia de carácter preliminar:

— Se ha de partir de un concepto concreto de Administración electrónica o, si se quiere, de Administración digital, que no se centre únicamente en el uso de los medios electrónicos, sino que considere los mismos como instrumentos para el cambio. Las TIC no son un fin en sí mismo, sino una herramienta imprescindible para la innovación del interior de la Administración y para la eficacia en la prestación de servicios a los ciudadanos.

— Se ha de optar por un concepto de ciudadano que, lejos de ser considerado como simple destinatario de actos administrativos, se sitúe en el centro de la actuación administrativa.

— Se ha de buscar, tanto con carácter general como en cada concreto proyecto de digitalización, el equilibrio entre Tecnología y Derecho –y, por ende, entre tecnólogos y juristas–, logrando que la transformación digital no se haga a costa de los derechos y garantías de las partes implicadas y que las exigencias jurídicas no supongan un freno a la innovación.

Dadas las características de la presente obra colectiva, en este trabajo se seguirá una metodología expositiva poco convencional desde la perspectiva del lenguaje empleado y del estilo de planteamiento de las proposiciones. Partiendo de la realidad necesitada de mejora y sobre la base de ideas previamente exploradas en anteriores estudios, apunta una serie de tesis –que, ciertamente, necesitarían de ulterior profundización y desarrollo– para contraponerlas con la situación actual de nuestro sistema. Precisamente por ello, con la salvedad de los casos concretos que pretenden ejemplificar lo que no debería hacerse, las reflexiones no se centrarán en el Derecho positivo, sino en el deber ser, esto es, buscan ofrecer al Legislador y a los actores públicos algunas pistas que pueden resultar de

utilidad en su tarea de innovar la Administración. Todas ellas se centrarán, sin embargo, en la cuestión relativa al acceso a los servicios públicos por parte de los ciudadanos o, lo que es lo mismo, en la organización y el procedimiento administrativo desde la perspectiva del interesado en el contexto de adopción de actos administrativos. Se descarta conscientemente ampliar el enfoque, puesto que muchas de las cuestiones interrelacionadas con este ámbito –tales como participación, interacción con los ciudadanos a través de redes sociales, derecho de protección de datos de carácter personal o acceso a la información pública y rendición de cuentas– serán objeto de análisis en otras partes de la obra.

En definitiva, estas páginas podrían calificarse como trabajo esquemático de prospección, construcción y diseño: partiendo del interior más profundo de la Administración (minería administrativa), se apuntan algunas ideas necesarias para el rediseño de la organización y el procedimiento administrativo (ingeniería administrativa) con el fin de que el ejercicio de las competencias administrativas frente a los interesados resulte lo más sencillo posible para aquélla y para éstos, desde el respeto absoluto a la Ley y a sus derechos (arquitectura administrativa).

2. CINCO TESIS SOBRE LA INNOVACIÓN ADMINISTRATIVA DE LA ORGANIZACIÓN Y EL PROCEDIMIENTO DESDE LA PERSPECTIVA DEL ACCESO DE LOS CIUDADANOS

2.1 **Mejorar el acceso exige empezar por el principio. ¿Y qué es el principio sino el interior de la Administración?**

Transformar desde dentro es la premisa imprescindible para que se note por fuera. El derecho de los ciudadanos al uso de los medios electrónicos para relacionarse con la Administración es la culminación de toda una labor previa de cambio. Hacerlo factible exige repensar cómo ésta se organiza y cómo actúa internamente. Y ello supone no quedarse únicamente en pasar del formato presencial al formato electrónico en la tramitación del procedimiento administrativo, sino avanzar hacia el rediseño de la organización, del personal a su servicio y del propio procedimiento, teniendo en cuenta, además, el conjunto del ordenamiento jurídico, el conjunto de la organización administrativa, el conjunto de los procedimientos de actuación.

Es demasiado habitual la inercia del Parlamento a legislar por islas, en función de la procedencia de la correspondiente iniciativa y del Ministerio que la lidera, sin tomar en consideración las normas ya existentes. Conectar leyes relacionadas entre sí desde la perspectiva de la aplicación de los medios electrónicos en la actuación administrativa resulta no sólo conveniente, sino fundamental. No menos infrecuente es seguir anclados en el

modelo papel a la hora de diseñar la regulación (6), de modo tal que la Administración continúa siendo el centro de la regulación y del diseño de su actuación.

Por otra parte, innovar la Administración exige no dejar de lado a quienes hacen que actúe: los empleados públicos. Seguimos teniendo una estructura organizativa pensada para mover papel, no para gestionar información por medios electrónicos. El rediseño de la organización administrativa no puede hacerse manteniendo el actual esquema de selección de personal y de distribución de puestos de trabajo.

En consecuencia, un Plan de Reforma que busque ser considerado verdaderamente tal debe integrar organización y procedimiento, pero también personal al servicio de las Administraciones tomando como referencia la clave tecnológica. Una transformación global en clave innovadora pensada para el ciudadano a través de reformas normativas previamente planificadas requiere la integración de todos los ámbitos de actuación de la Administración.

En el contexto de la transformación digital del interior de la Administración, la estandarización y la automatización de procesos es una estrategia imprescindible. Efectivamente, si puede hacerlo –bien– una máquina, es preciso que lo haga una máquina. Decidir por defecto y sin necesidad de que intervengan personas físicas en el proceso decisorio, allí donde sea factible y no se perjudique ni a derechos o intereses de terceros ni al interés público, es una opción más eficiente y más sencilla para el ciudadano. Si hoy en día seguimos necesitando con carácter general presentar una solicitud en un registro, esperar un tiempo para recibir respuesta –en el mejor de los casos– tras la oportuna valoración de la misma por el órgano competente para resolver o para entenderla desestimada y poder plantear reclamación o recurso es precisamente porque no estamos automatizando los procesos de gestión de la información ni los trámites necesarios para resolver la misma.

En todo caso, automatización no debe significar ni opacidad del proceso de toma de decisiones ni merma del derecho de defensa: saber cómo «razona» el sistema de información que sirve para la adopción de la reso-

(6) Como puede apreciarse claramente en la nueva LCSP, que incluso hace uso de terminología desfasada que, además, no se corresponde con el lenguaje de la LPAC ni de la LRJSP. Sobre esta cuestión, Martín Delgado, I.: «¿Por qué no estamos innovando la organización y el procedimiento en la contratación pública a través del uso de los medios electrónicos?, en http://www.obcp.es/index.php/mod.opiniones/mem.detalle/id.296/relcategoria.121/relmenu.3/chk.a10c595409d9425b7219c4f6a9638cc4 (Última fecha de consulta: 12/03/2018). Más en profundidad, «El uso de los medios electrónicos en la contratación pública» en Gimeno Feliú, J. M. (dir.), *Estudio sistemático de la Ley de Contratos del Sector Público*, Thomson-Aranzadi, Cizur Menor, 2018, pp. 1657 a 1714.

lución, conocer los motivos concretos que le han llevado a ella y no a otra deberá quedar asegurado (7).

Todo ello exige tener presente una realidad: no innovar tiene consecuencias –y no sólo jurídicas–. La falta de medios para cumplir con las obligaciones impuestas por la Ley no puede seguir siendo una excusa. La pérdida de oportunidad derivada de la ausencia de innovación, junto con la no reducción del gasto público por vía del aumento de la eficiencia, tiene un claro coste económico para la Administración. Pero también lo tiene para los propios ciudadanos. Es más, en el contexto de la transformación digital de la Administración deberían igualmente cuantificarse los costes de la no reutilización de soluciones tecnológicas y herramientas informáticas (art. 41.2 LRJSP), así como los efectos –no meramente económicos– de acudir al sector privado para dotarse de instrumentos tecnológicos (8).

Transformar el interior de la Administración para hacerla accesible a los ciudadanos exige, en última instancia, garantizar la seguridad y la protección de otros derechos de éstos. Sin esa transformación, necesariamente previa, no podrá hablarse de acceso electrónico de los ciudadanos a los servicios públicos como auténtico derecho.

2.2 **Un acceso configurado para el ciudadano, un acceso pensado con el ciudadano. Si las plataformas privadas de comercio electrónico funcionan, ¿por qué nos sigue costando acceder a la Administración por medios electrónicos?**

El error que puede conllevar un enfoque excesivamente centrado en la propia organización administrativa a la hora de transformar digitalmente la Administración es el olvido del ciudadano y la introducción de rigideces innecesarias en las relaciones entre éste y el poder público. Piénsese, por señalar algunos ejemplos, en la resistencia en determinados casos a hacer uso de sistemas de identificación y firma más flexibles para realizar trámites con la Administración en contextos donde sería perfectamente posible, en la insistencia en replicar en formato electrónico los rituales que venían llevándose a cabo en la actuación basada en papel, o en el re-

(7) Sobre la automatización de las decisiones administrativas y, en particular, sus garantías mínimas, puede verse MARTÍN DELGADO, I: «Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada», en *Revista de Administración Pública*, núm. 180, 2009, pp. 353-386.

(8) Para RAMIÓ, el diseño y la gestión de las tecnologías de la información debería ser una responsabilidad de las instancias centrales y de un colectivo de personal que no esté expuesto a las tensiones e incentivos de las actividades corruptas y, junto con ello, debería evitarse externalizar los centros gestores de nuevas tecnologías –más allá de supuestos puntuales debidamente justificados–, para no incurrir en el riesgo de pérdida del control, *La Administración Pública del futuro…*, *op. cit.*, pp. 152 y 153.

curso permanente al procedimiento administrativo como cauce formal de tales relaciones.

La idea, contenida en la Exposición de Motivos de la LAE, de adentrarse en el domicilio de ciudadanos y empresas sigue siendo válida. Es obvio que nadie quiere tener a la Administración en su casa, pero no menos evidente es que, en un contexto en el que el ciudadano podrá hacer prácticamente todo lo necesario para la vida ordinaria desde el punto de vista logístico sin moverse del sofá, la Administración no puede renunciar a hacerse presente en la forma en que a aquél le resulta más sencilla.

Sin embargo, seguimos optando por modelos que implican que el ciudadano venga a la Administración y no que ésta vaya al ciudadano (9). La inercia se aprecia muy claramente en relación con el sistema de notificaciones administrativas: se ha optado por domicilios virtuales con más garantías –Dirección Electrónica Habilitada Única y sede electrónica– pero de más difícil acceso y gestión ordinaria por los interesados. Más aún, el espacio natural de relaciones con la Administración –la sede electrónica–, sigue exigiendo el desplazamiento –virtual– del ciudadano para la sustanciación de cualquier trámite. Son muy anecdóticos aún los supuestos en los que un trámite puede realizarse a través de una app móvil.

En definitiva, la transformación digital de la Administración ha de llevarse a cabo no sólo desde la lógica diseño para los ciudadanos, sino también desde la clave diseño con los ciudadanos. Y, en todo caso, ha de hacerse partiendo del cumplimiento de una premisa inexcusable: no implicar el traslado de la carga del trámite de aquélla a éste (como ocurre, por ejemplo, en el acceso a notificaciones). Lo contrario dificulta el acceso y afecta a las garantías de los derechos de los ciudadanos.

2.3 **No necesitamos procedimiento –tal y como lo entendemos ordinariamente– para todo. Tenemos trámites, pero ¿ofrecemos servicios?**

Nuestro modelo de organización administrativa se ha basado tradicionalmente en el diseño de procedimientos e instrumentos de control complejos (10), pensados desde la óptica de la Administración sobre la base del principio de legalidad y no tanto desde la perspectiva del ciudadano. El procedimiento administrativo es la mayor prueba de ello: entendido como conjunto de trámites formalizados que tienen por objeto permitir a

(9) En este sentido, puede verse el excelente trabajo de Alamillo Domingo, I.: «La regulación de la tecnología. La superación del modelo papel como elemento de transformación digital innovadora», en Martín Delgado, I. (Dir.): *La reforma de la Administración electrónica: una oportunidad para la innovación desde el Derecho*, INAP-Investiga, Madrid, 2017, pp. 79 a 129.

(10) Para Ramió, unos y otros son «tan complejos y barrocos que matan toda la posibilidad de innovación y coartan de forma grave la eficacia y la eficiencia», *La Administración Pública del futuro…*, *op. cit.*, p. 148.

la Administración recopilar la información necesaria –por sus propios medios o a través del requerimiento de información al ciudadano interesado o a terceros– para adoptar una decisión en el ejercicio de las competencias legalmente atribuidas, implica en no pocas ocasiones rigideces hoy en día innecesarias. Es evidente que no puede renunciarse al procedimiento administrativo para el ejercicio de competencias complejas, pero no menos cierto es que, allí donde resulte posible, se ha de transformar la lógica de ejercer competencias a la de prestar servicios. Y ello exige acudir a modelos de actuación no procedimentalizados (11). Efectivamente, toda la complejidad interna administrativa no tiene por qué proyectarse necesariamente sobre las relaciones entre Administración y ciudadanos. Del mismo modo en que a los clientes de las empresas de comercio electrónico les resulta indiferente cómo éstos se organizan internamente para producir el bien o prestar el servicio que aquéllos les demandan, para los ciudadanos no es necesariamente relevante el conocimiento de la forma de organización interna, ni el reparto competencial, ni los procesos decisorios. La complejidad es un obstáculo al acceso.

Por ello puede prescindirse del procedimiento entendido como cauce para recabar información en determinadas circunstancias. Si el ordenamiento jurídico reconoce un derecho al ciudadano y la Administración posee toda la información que le permite certificar el cumplimiento de los requisitos a tal fin, la consecuencia lógica es reconocer el derecho por defecto y dar acceso a su ejercicio. Si la ponderación que ha de llevar a cabo la Administración al adoptar la decisión no precisa de intervención de terceros, puede hacerse por medio de procesos distintos del procedimiento administrativo.

Un ejemplo claro de ello es el caso del acceso a la información pública, configurado, de un lado, como un deber de la Administración de publicar determinada información a través de medios electrónicos y, de otro, como un derecho subjetivo de los ciudadanos que se ejerce a través de presentación de solicitud y tramitación del correspondiente procedimiento. Aunque no puede desconocerse que es el procedimiento la técnica más garantista desde la perspectiva del cumplimiento del principio de legalidad de la actuación administrativa, como instrumento de participación de los ciudadanos en la toma de decisiones públicas y como técnica de protección de los derechos de los ciudadanos, particularmente el derecho de defensa, no menos cierto es que, cuando no concurran otros derechos o

(11) Muy sugerentes en este sentido son las ideas que plantea Berning Prieto, A.D.: «La Administración electrónica y los servicios públicos digitales al albor de los progresos de la Unión Europea y el Horizonte Europa 2020». Su relación con las leyes 39/2015, de procedimiento administrativo común de las administraciones públicas y 40/2015, de régimen jurídico del sector público», en martín delgado, I. (Dir.): *La reforma de la Administración electrónica: una oportunidad para la innovación desde el Derecho*, INAP-Investiga, Madrid, 2017, pp. 17 a 48.

intereses, públicos o privados, afectados por el derecho de acceso, es decir, cuando la información ha de ser facilitada sin necesidad de ponderar límites, podría prescindirse del procedimiento y facilitar la vía de acceso a la misma (12). Lo mismo ocurre en relación con el ejercicio de otros derechos donde la Administración carece de potestad discrecional y cuenta con todos los datos e información necesarios para decidir el reconocimiento de los mismos (piénsese en la gratuidad de libros para padres con hijos en edad escolar, en las bonificaciones fiscales por maternidad, en el reconocimiento de trienios de los empleados públicos…); la Administración, lejos de esperar a la presentación de la solicitud en ejercicio del derecho, puede actuar de oficio –en algunos casos, incluso, de forma automatizada– y, tras comprobar la concurrencia de los requisitos, reconocer el mismo y dar las instrucciones precisas para su materialización.

En definitiva, «la sencillez es accesible» (13) y la complejidad es un obstáculo. Y, en demasiadas ocasiones, el procedimiento es complejo. El procedimiento tiene pleno sentido en el contexto de las relaciones presenciales de épocas pasadas, donde la información estaba en poder de aquél o de terceros y no de éstas o, incluso en el caso de que fuera al contrario, el intercambio de información resultaba difícil. En cambio, en el contexto de la revolución tecnológica, la información fluye de forma rápida y sencilla y, en la mayor parte de los casos, se encuentra en poder de la Administración. Ello ha de derivar, necesariamente, en una inversión de los términos y, en consecuencia, ha de afectar a la forma en la que la Administración actúa: el formulario no es imprescindible en todos los casos –más aún cuando es excesivamente complejo (14), rompiendo con el tra-

(12) Así lo ha hecho el Ayuntamiento de Madrid en su ordenanza de transparencia, cuyo artículo 23 prevé un sencillo trámite de petición de información con deber de dar respuesta sin necesidad de identificación ni de tramitación de procedimiento administrativo en sentido estricto. https://www.bocm.es/boletin/CM_Orden_BOCM/2016/08/17/BOCM-20160817-30. PDF (última fecha de consulta: 01/04/2018).

(13) Sunstein, C.: *(Más) simple. El futuro del Gobierno*, Marcial Pons, Madrid, 2014, p. 13.

(14) Ciertamente paradigmático es el asunto resuelto por la Audiencia Nacional en su Sentencia de 31 de octubre de 2017 (Rec. 270/2015). En el marco de una convocatoria de ayudas a la investigación de la Secretaría de Estado de Investigación, Desarrollo e Innovación, que exigía la presentación junto con la solicitud –y como parte integrante de la misma– de un *curriculum vitae* abreviado del investigador principal, una de las solicitudes presentadas por un profesor (conocido y reputado Catedrático de Derecho Administrativo) fue objeto de exclusión por no cumplir los requisitos establecidos en aquélla. La causa de exclusión era puramente formalista: el *curriculum* breve, que debía seguir un formato normalizado, no podía superar las 4 páginas y el presentado llegaba a 7. La Audiencia Nacional estima el recurso por entender que el órgano actuante llevó a cabo una interpretación de la normativa aplicable sumamente formalista sin dar la posibilidad al solicitante de subsanar el defecto de forma y precisa que «la advertencia en un formulario de que los defectos formales del curriculum no son subsanables no puede prevalecer frente a la previsión expresa de esa posibilidad en la convocatoria y con carácter general en el artículo 23.5 de la Ley 38/2003, de 17 de noviembre General de Subvenciones» (F. J. 6.º). En cualquier caso, la reflexión que suscita este supuesto debe ser más profunda: el sometimiento de la presentación de solicitudes a estrictos requisitos de forma, muchos de los cuales en no pocas ocasiones carecen de sentido, por medio de la técnica de los formularios, más pensada para la Administración que para el ciudadano, tiene efectos perjudiciales para éste.

dicional principio de antiformalismo del Derecho Administrativo–; ha de invertirse la carga de obtención de la información; puede prescindirse del procedimiento en determinados supuestos (15).

2.4 **El acceso universal requiere neutralidad tecnológica y búsqueda de soluciones comunes. ¿Nos lo creemos?**

Como ha sido señalado con anterioridad, la tecnología no es neutra. Tampoco lo son las opciones tecnológicas de la Administración. Intentar acceder con determinados dispositivos y herramientas, por mucho que su uso esté cada vez más generalizado, sigue siendo difícil. Lejos de avanzar hacia la neutralidad, da la sensación de que estamos caminando en sentido contrario. De hecho, la LPAC no recoge uno de los derechos que reconocía la LAE: el derecho a la elección de las aplicaciones o sistemas para relacionarse con las Administraciones Públicas siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos (16). La falta de neutralidad no sólo puede tener consecuencias sobre las decisiones administrativas, sino también sobre el acceso de los ciudadanos a los servicios públicos por medios electrónicos por riesgo de desigualdades y discriminación.

Un ejemplo de esta inercia es la exigencia de sistemas robustos de identificación y firma electrónica basados en certificado digital para cualquier trámite ante la Administración. En este sentido, ha de valorarse muy positivamente la opción de la LPAC de restringir la necesidad de firma electrónica sólo para determinados trámites, considerando suficiente para el resto la identificación, así como la flexibilidad en los instrumentos de identificación y firma que introduce. Pero habrá que esperar a ver cómo son aplicadas estas previsiones en la práctica para determinar si se ha parado tal tendencia o, por el contrario, sigue plenamente vigente. En todo caso, el certificado electrónico reconocido continúa siendo la base de la política de identificación y firma de las Administraciones Públicas. Teniendo en cuenta las previsiones de los artículos 9 a 11 LPAC, la decisión de la Administración acerca de cuándo exigir identificación y cuándo firma, así como sobre el concreto tipo de sistema de identificación y autenticación de la voluntad exige en relación con trámites y procedimientos,

(15) Sobre la evolución del procedimiento administrativo en general y una visión crítica de la regulación del procedimiento en la LPAC en particular, puede verse Barnés, J.: «La Ley 39/2015, de procedimiento administrativo, desde una perspectiva histórica y comparada», en Velasco Rico, C. (Dir.), *Reflexiones sobre la reforma administrativa de 2015*, Marcial Pons, Madrid, pp. 31 a 80.

(16) Fuertes, M.: *Neutralidad de la red: ¿realidad o utopía?*, Marcial Pons, Madrid, 2014. También, Boix Palop, A. «La neutralidad tecnológica como exigencia regulatoria en el acceso electrónico a los servicios administrativos», *Revista General de Derecho Administrativo*, núm. 16, 2007.

no es enteramente libre. Efectivamente, deberá respetar siempre tanto los requisitos exigidos para la presentación de solicitudes pensados para garantizar derechos de los ciudadanos, como el principio de proporcionalidad. Por señalar un ejemplo, el principio de proporcionalidad lleva a dudar de la legalidad –por desproporcionada– de la exigencia de los medios de identificación y firma incorporados en el sistema cl@ve para la presentación de una simple solicitud de acceso a información pública en ejercicio del derecho reconocido en la LTBG, sobre todo si se tiene en cuenta que en otros ámbitos resulta posible hacer uso de otros sistemas más flexibles además de los citados (por ejemplo, para confirmar el borrador de la renta o pagar una multa).

Por otro lado, igualmente constituye un obstáculo al acceso la multiplicidad de soluciones tecnológicas –en muchos casos, no interoperables– para canalizar las relaciones entre Administración y ciudadanos en el contexto del ejercicio de las competencias. Puede apreciarse en relación con este extremo una cierta colisión entre la opción por la uniformidad de la Administración General del Estado y la flexibilidad que se deriva del principio de potestad de autoorganización que incorpora el principio de autonomía.

Necesitamos soluciones comunes, pero no impuestas. Es claro que la solución tecnológica común –aquélla que resulte la más sencilla, accesible y eficiente– es lo más eficaz, necesario por razones de interoperabilidad y razonable desde la perspectiva de la simplificación del acceso al servicio por los ciudadanos. Pero no puede tenderse a ella a través de la imposición, sino que ha de promoverse desde la colaboración. El caso de la Disposición Adicional Segunda LPAC es claramente conflictivo al pretender imponer el uso obligado de algunas plataformas y herramientas tecnológicas estatales bajo determinadas circunstancias (17).

(17) Este precepto establece que «[*p*]*ara cumplir con lo previsto en materia de registro electrónico de apoderamientos, registro electrónico, archivo electrónico único, plataforma de intermediación de datos y punto de acceso general electrónico de la Administración, las Comunidades Autónomas y las Entidades Locales podrán adherirse voluntariamente y a través de medios electrónicos a las plataformas y registros establecidos al efecto por la Administración General del Estado. Su no adhesión, deberá justificarse en términos de eficiencia conforme al artículo 7 de la Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera. En el caso que una Comunidad Autónoma o una Entidad Local justifique ante el Ministerio de Hacienda y Administraciones Públicas que puede prestar el servicio de un modo más eficiente, de acuerdo con los criterios previstos en el párrafo anterior, y opte por mantener su propio registro o plataforma, las citadas Administraciones deberán garantizar que éste cumple con los requisitos del Esquema Nacional de Interoperabilidad, el Esquema Nacional de Seguridad, y sus normas técnicas de desarrollo, de modo que se garantice su compatibilidad informática e interconexión, así como la transmisión telemática de las solicitudes, escritos y comunicaciones que se realicen en sus correspondientes registros y plataformas*». A través de una resolución administrativa (Orden PRE/710/2016, de 12 de mayo, por la que se publica el Acuerdo de la Comisión Delegada del Gobierno para Asuntos Económicos de 31 de marzo de 2016, sobre condiciones adicionales a cumplir por las Comunidades Autónomas adheridas al Fondo de Financiación a Comunidades Autónomas, compartimento Fondo de Liquidez Autonómico 2016) se ha obligado a las Comunidades Autónomas y a los entes locales suscritos al mismo, antes de la entrada en vigor de la LPAC (y, por tanto, de su Disposición Adicional 2.ª) a suscribir las plataformas y aplicaciones desarrolladas por

Soluciones comunes son aquéllas pensadas colectivamente y planteadas para todas las Administraciones que han de asumirlas y para todos los ciudadanos que deben usarlas. Establecer como único criterio el de eficiencia económica, sin tener en cuenta que algunas Comunidades Autónomas han desarrollado sus propias soluciones tecnológicas –en algunos casos, de mayor calidad que las estatales– es más que discutible (18). Sobre todo cuando la LRJSP prevé vías alternativas para compartir tecnologías y reutilizar sistemas y aplicaciones en sus artículos 156 y 157 (19). El Tribunal Constitucional, en su reciente Sentencia 55/2018, de 24 de mayo, ante un recurso de inconstitucionalidad planteado por la Generalitat de Cataluña, ha procedido a realizar una interpretación conforme de la D.A. 2.ª en el sentido de considerar que no atribuye al Ministerio de Hacienda una herramienta de control de las decisiones tecnológicas de las Comunidades Autónomas, sino que trata de favorecer «la difusión de las nuevas tecnologías de la información y la comunicación en la organización y procedimientos administrativos con la ambición de no multiplicar el número de plataformas electrónicas ni los costes consecuentes» a través de una obligación meramente formal como técnica de colaboración interadministrativa. Llega incluso a apuntar que «hay variadas fórmulas mucho menos restrictivas para compaginar la generalización de los medios electrónicos con la eficiencia y la estabilidad presupuestaria. Por ejemplo, el diseño e implantación de plataformas electrónicas compartidas bajo la

---

la Administración General del Estado para cumplir con las obligaciones en materia de Administración electrónica. Entre las obligaciones del Acuerdo está la relativa a la suscripción de un convenio para la prestación mutua de soluciones básicas de administración electrónica para ganar eficiencia, evitar gasto duplicado y reducir costes de funcionamiento. Así pues, las Comunidades Autónomas deberán suscribir con la Administración General del Estado el Convenio para la prestación mutua de soluciones básicas de administración electrónica, lo que les permitirá usar los sistemas ya disponibles por parte de la Administración General del Estado. Asimismo, la Comunidad Autónoma asume el compromiso de trabajar de forma activa con el fin de mejorar la eficiencia de los procedimientos administrativos y reducir costes de funcionamiento a través de los siguientes instrumentos: adherirse al uso de las plataformas y registros para la gestión electrónica de los procedimientos facilitados por la Administración General del Estado (particularmente, en materia de registro electrónico de apoderamientos, registro electrónico, archivo electrónico único, plataforma de intermediación de datos y punto de acceso general electrónico de la Administración); facilitar la integración de las Entidades Locales del territorio de esa Comunidad Autónoma en las plataformas, sistemas y soluciones tecnológicas estatales; integrar los registros de la Comunidad Autónoma en el Sistema de Intercambio de Registros, de manera que los intercambios se hagan sólo por medios telemáticos, sin movimiento de papel; utilizar los medios telemáticos para la obtención de datos, información y certificados que obren en poder de la Administración, para evitar que los tengan que presentar los ciudadanos (en especial, la Plataforma de intermediación).

(18) Para un profundo análisis sobre los problemas que plantea la citada Disposición, puede verse Fondevila Antolín, J.: «Estado de derecho o el *imperium* de la deslealtad institucional: breves consideraciones sobre la imposición por el Estado central a las Comunidades Autónomas de su adhesión a sistemas y plataformas electrónicas estatales», en Martín Delgado, I. (Dir.): *La reforma de la Administración electrónica: una oportunidad para la innovación desde el Derecho*, INAP-Investiga, Madrid, 2017, pp. 527 a 546.

(19) Sobre la cuestión relativa a la reutilización y transferencia de tecnologías puede verse puede verse Martínez Gutiérrez, R.: «Relaciones interadministrativas por medios electrónicos. Interoperabilidad», en Gamero Casado, E.: *Tratado de Procedimiento Común y de Régimen Jurídico Básico del Sector Público*, Tirant lo Blanch, Valencia, 2017, pp. 2910 y ss.

dirección de una comisión mixta, compuesta por representantes de los tres niveles territoriales». Aunque, en última instancia, este precepto puede ser leído como garantía para posibilitar el ejercicio de los derechos de los ciudadanos por medios electrónicos al forzar a todas las Administraciones a disponer de las soluciones tecnológicas para ello –propias o ajenas–, la tecnología no puede justificar el olvido del Derecho, en este caso, del principio de autonomía.

2.5 **El acceso ha de ser configurado como un auténtico derecho y debe ir acompañado de garantías. ¿Y si nos tomamos en serio el cumplimiento de la ley?**

Desde la LAE, la configuración del acceso a los servicios públicos por medios electrónicos como un derecho ha sido la tónica dominante. Sin embargo, tal reconocimiento, aunque ha llevado consigo el establecimiento del correspondiente deber de dotarse de herramientas e instrumentos para satisfacer el mismo, no se ha visto acompañado de la previsión de garantías para los supuestos de incumplimiento, lo cual explica en parte el lento avance hacia la transformación digital de la Administración y hacia la incorporación definitiva por los ciudadanos del uso de los medios electrónicos en sus relaciones con aquélla.

Es más, en relación con lo afirmado anteriormente respecto de la opción por sistemas controlados por la Administración, la LPAC implica un cierto retroceso en los derechos de los ciudadanos, pues ha dejado de lado la fuerte opción del Legislador de 2007 por el derecho a relacionarse con las Administraciones por medios electrónicos y, además, ha renunciado a introducir garantías del cumplimiento de las obligaciones derivadas del régimen jurídico de la Administración electrónica. Efectivamente, disgrega completamente el catálogo de derechos de los ciudadanos en sus relaciones con la Administración por medios electrónicos al eliminar el reconocimiento del genérico derecho antes citado y al diferenciar entre derechos de las personas en sus relaciones con las Administraciones Públicas y derechos del interesado en el procedimiento administrativo.

Entre los primeros, regulados en el artículo 13, se contemplan dos de los derechos ya recogidos por la LAE: el derecho a la obtención y utilización de los medios de identificación y firma electrónica y el derecho a la protección de datos de carácter personal y, en particular, a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas. Junto con ello, se añaden otros dos nuevos derechos. De un lado, el derecho «*a comunicarse con las Administraciones Públicas a través de un Punto de Acceso General electrónico de la Administración*»; de otro, el derecho a «*a ser asisti-*

dos en el uso de medios electrónicos en sus relaciones con las Administraciones Públicas».

Tal derecho a comunicarse con las Administraciones a través del Punto de Acceso General Electrónico resulta ciertamente vago en cuanto a su reconocimiento y contenidos y, desde luego, más limitado aún en cuanto a su alcance (20) (más allá de que supone, una vez más, optar por soluciones tecnológicas en poder de la Administración), lo cual es ciertamente criticable por la centralidad que le atribuye la nueva regulación. Aunque el artículo 14 mantiene el carácter voluntario del uso de los medios electrónicos al establecer que «*las personas podrán elegir en todo momento si se comunican con las Administraciones Públicas para el ejercicio de sus derechos y obligaciones a través de los medios electrónicos o no*» y conserva la posibilidad de modificar la opción inicial al señalar que «*el medio elegido por la persona para comunicarse con las Administraciones Públicas podrá ser modificado por aquella en cualquier momento*», resulta evidente que la ausencia del reconocimiento de un derecho general a relacionarse con la Administración por medios electrónicos con sustantividad propia y no meramente instrumental hace perder fuerza a la posición del ciudadano ante la Administración. De un lado, el nuevo derecho se está restringiendo únicamente a un género de relación, como es la comunicación; de otro, se determina un único instrumento a tales efectos, el punto de acceso electrónico, cuya configuración, además, depende de la propia Administración, puesto que ni la LPAC ni la LRJSP regulan condición alguna de creación ni requisitos mínimos que haya de respetar su funcionamiento. A todo ello ha de añadirse que la LPAC no define qué ha de entenderse por Punto de Acceso General Electrónico de la Administración, de modo tal que no resulta posible concretar con claridad en qué se traduce el derecho a comunicarse con las Administraciones a través del mismo.

La pregunta que puede plantearse, ante esta regulación, es qué ocurrirá en los casos en los que una Administración carezca de un Punto de Acceso General Electrónico. La primera consecuencia es que no resultaría exigible el cumplimiento del deber de relacionarse con la Administración por medios electrónicos. La segunda que, al tratarse de una obligación de prestación, concreta y especial, no sometida a ninguna condición, quedaría abierta la posibilidad de presentar recurso por inactividad en vía contencioso-administrativa con el fin de lograr la condena a su creación o a la adhesión a algunos de los existentes previa firma del correspondiente

(20) *Vid.* Cotino, L.: «El derecho y del deber de relacionarse por medios electrónicos (art. 14). Asistencia en el uso de los medios electrónicos a los interesados (art. 12)», en Gamero Casado, E. (Dir.), *Tratado de Procedimiento Común y de Régimen Jurídico Básico del Sector Público*, Tirant lo Blanch, Valencia, 2017, pp. 475 a 531.

convenio. En cualquier caso, el hecho de que se restrinja el ámbito objetivo de aplicación del derecho y el que se planteen dudas sobre su contenido y alcance es la prueba de que esta opción no es la mejor. Aunque se esté pensando en la carpeta ciudadana como herramienta para facilitar el acceso a los trámites a los interesados, con independencia de la Administración actuante, identificar el proyecto con el derecho a costa de reducir sus dimensiones es una solución manifiestamente mejorable.

Por otro lado, la protección de los derechos de los ciudadanos requiere como premisa claridad y precisión en las normas. Justo lo contrario de lo que ocurre en relación con el derecho y el deber de asistencia en el uso de los medios electrónicos. Efectivamente, a pesar de que el artículo 13 LPAC reconoce el derecho a ser asistido en el uso de medios electrónicos a todas las personas, en realidad, el artículo 12 introduce un doble matiz que restringe su alcance: se refiere sólo a los interesados («*asistencia en el uso de medios electrónicos a los interesados*» es su título) y, además, configura el deber de asistencia de las Administraciones Públicas sólo para los interesados que no estén obligados al uso de los medios electrónicos, excluyendo expresamente a quienes sí lo están que, paradójicamente, pueden encontrarse más necesitados de asesoramiento y asistencia precisamente al no poder optar por el medio presencial y la tramitación en papel.

Y, finalmente, exige protección del reconocimiento. Dos son los casos más evidentes en los que se pone de manifiesto la ruptura del principio de mantenimiento de las garantías: el de la subsanación de las solicitudes y el del aviso complementario de notificación.

Efectivamente, resulta problemática la regulación contenida en el artículo 68.4, en virtud del cual *«[s]i alguno de los sujetos a los que hace referencia el artículo 14.2 y 14.3 presenta su solicitud presencialmente, las Administraciones Públicas requerirán al interesado para que la subsane a través de su presentación electrónica. A estos efectos, se considerará como fecha de presentación de la solicitud aquella en la que haya sido realizada la subsanación».* Una simple lectura del mismo pone de manifiesto que los sujetos obligados pueden perder, de facto, el derecho de subsanación. Efectivamente, el hecho de que se señale como fecha de presentación de la solicitud aquélla en la que materialmente se haya procedido a la subsanación mediante la presentación por medios electrónicos puede implicar que, en los casos en los que el requerimiento de subsanación llegue tarde, el plazo para presentar solicitudes haya expirado, con lo que la subsanación sería extemporánea. Son varias las dudas en relación con este extremo. En primer lugar, no resulta claro qué habrá de hacerse en los supuestos en los que la Administración detecta el defecto de forma cuando haya terminado el plazo de presentación de

solicitudes. ¿Será necesario notificar el requerimiento de subsanación, aun cuando, materialmente, no resulta posible ésta? ¿Se notificará directamente la preclusión del trámite o la extemporaneidad de la solicitud? Junto con ello, en segundo lugar, la solución no puede ser la misma cuando la imposibilidad de requerir subsanación se deba a que el interesado ha presentado defectuosamente su solicitud en fechas próximas a la finalización del plazo respecto de cuando lo haya hecho con antelación suficiente. Dicho sencillamente, el incumplimiento del deber de diligencia de la Administración a la hora de apercibirse del defecto formal en la presentación de la solicitud habrá de tener consecuencias para ella misma y no para el administrado. En cualquier caso, permítaseme insistir en ello, es claro que una regla de esta naturaleza rompe con el principio de mantenimiento de las garantías procedimentales existentes en las relaciones presenciales ante el uso de los medios electrónicos.

Respecto de las notificaciones, la LPAC, partiendo de una premisa acertada –evitar al ciudadano, que resulta indirectamente obligado a recibir notificaciones a través de medios electrónicos que no maneja habitualmente, la carga de consultar periódicamente su DEHU o identificarse en la sede para comprobar si tiene alguna notificación–, ha optado por introducir la obligación para la Administración de enviar un aviso complementario al dispositivo electrónico (móvil, normalmente) o a la dirección de correo deseados si aquél así lo indica. Así se deriva de lo dispuesto tanto en el artículo 41.1 cuando prevé la posibilidad del interesado de identificar un dispositivo electrónico y/o una dirección de correo electrónico a los efectos de recibir en ellos un aviso complementario de notificación, como en el artículo 41.6, de conformidad con el cual se establece el correlativo deber de las Administraciones Públicas de enviar ese aviso complementario –exigible también en el caso de práctica de notificaciones en papel–. Sin embargo, el teórico derecho a recibir tal aviso y la supuesta obligatoriedad de practicarlo quedan desarticulados y pueden resultar más aparentes que reales si se tiene en cuenta que el propio artículo 41.6 precisa en su inciso final que la falta de práctica de este aviso no impedirá que la notificación sea considerada plenamente válida, algo ya anticipado en la Exposición de Motivos mediante el empleo de la cláusula «*siempre que esto sea posible*». Nuevamente, queda en manos de la Administración actuante el cumplimiento de una obligación, sin que el incumplimiento tenga consecuencias jurídicas. La garantía fundamental que permite justificar el desplazamiento de la carga de la Administración al interesado (se pasa de ser aquélla la que acude al domicilio de éste a pedir a éste que acuda a la «oficina virtual» de aquélla o a un buzón de titularidad pública) es precisamente la confianza en que el destinatario de una notificación electrónica recibirá en los dispositivos electrónicos o en su buzón de co-

rreo electrónico ordinario que utiliza habitualmente un aviso complementario de notificación. Suprimir los efectos invalidantes de la notificación en ausencia de este aviso –ni siquiera se exige excepcionalidad en la omisión– es, sencillamente, poner en situación de indefensión al interesado cuando esto ocurra, sobre todo si se tiene en cuenta que no hay motivos técnicos ni jurídicos para no practicarlo. Efectivamente, el uso de los medios electrónicos en la gestión interna del procedimiento administrativo es obligatorio; las Administraciones disponen de medios –gestores de expedientes– que permiten tal posibilidad; el ciudadano confía en su práctica; no hacerlo produce indefensión e implica imponer sobre el interesado una carga desproporcionada.

En todo caso, más allá de estas cuestiones conflictivas –que ponen de manifiesto las limitaciones al acceso por medios electrónicos a los trámites administrativos–, ha de afirmarse que, junto con el derecho general a relacionarse con las Administraciones a través de medios electrónicos, debe prestarse la debida importancia a los otros derechos. Efectivamente, el acceso no es el único derecho. Sin herramientas, sin dispositivos al alcance de todos, no hay Administración digital al servicio del ciudadano. También resulta fundamental el archivo y la gestión de la información como garantía de la satisfacción de otros derechos (21). Asegurar la integridad de la información almacenada, su confidencialidad y, sobre todo, el acceso a la misma cuando sea necesario, es fundamental. También lo es el tratamiento electrónico automatizado de los datos que se contienen en los documentos electrónicos.

Por último, la excepción al derecho no puede ser la regla. Dicho sencillamente, la obligatoriedad no es el único camino. Desde la introducción de la posibilidad de obligar a determinados colectivos a relacionarse con la Administración por medios electrónicos en el ámbito tributario en aplicación de la habilitación contenida en la LAE, la opción por la obligatoriedad ha sido un recurso frecuente y continúa en aumento. Así lo hace el artículo 14 LPAC y son numerosos los supuestos de normas de carácter reglamentario que optan por ella. La negatividad de la obligación tiene sus límites y es menos eficaz que promover el uso voluntario por vía de la sencillez.

En definitiva, más allá de la opción por obligar a aquéllos colectivos que verdaderamente tienen garantizado el acceso y el conocimiento del uso de los medios electrónicos, en este periodo de transición de la Administración en papel a la Administración electrónica la regulación de las

(21) Para un estudio exhaustivo análisis sobre la proyección del uso de los medios electrónicos en la gestión documental puede verse Valero Torrijos, «La tramitación del procedimiento administrativo por medios electrónicos, en Almeida Cerreda y Míguez Macho (Dirs.), *La actualización de la Administración Electrónica*, Andavira, Santiago de Compostela, 2016, pp. 199 y ss.

relaciones entre ésta y los ciudadanos ha de fundamentarse en el reconocimiento de un derecho de carácter voluntario, acompañado de herramientas que fomenten su ejercicio. Un derecho, además, pensado para ser ejercido no en contextos habilitados específicamente y diseñados tomando como referente la Administración, sino el ciudadano. Un derecho cuya regulación no entre en colisión con la relativa a otros derechos (22).

3. A MODO DE CONCLUSIÓN: SUPERAR LAS «ANTÍTESIS» PARA AVANZAR HACIA UN MODELO DE ADMINISTRACIÓN DIGITAL AUTÉNTICAMENTE INNOVADOR

La realidad de la Administración digital en nuestro país pone de manifiesto que estamos aún lejos del cumplimiento de las ideas que acaban de ser expuestas.

Antítesis, como es sabido, es contrariedad de dos juicios. Una contrariedad que puede apreciarse claramente en las Exposiciones de Motivos y Preámbulos de nuestras normas y sus contenidos, pero, peor aún, entre la norma y su aplicación práctica. En cierto sentido, el concepto de Administración electrónica o digital tiene aún mucho de oxímoron en la práctica.

(22) Una de las novedades más relevantes de la LPAC, contenida en su artículo 28 y pensada precisamente para simplificar la presentación de solicitudes en ejercicio del derecho a no presentar datos y documentos no exigidos por las normas aplicables al procedimiento de que se trate que ya estén en poder de las Administraciones Públicas o hayan sido elaborados por ellas, corre el riesgo de verse anulada. El ejercicio de este derecho requiere el consentimiento por parte del titular de los datos a que el órgano actuante los recabe o consulte, consentimiento que, de conformidad con el citado precepto, se presumirá otorgado salvo oposición expresa del interesado. Ello ha de ser valorado muy positivamente, puesto que, de lo contrario, la ausencia de consentimiento expreso impide el acceso a la información y se desaprovechan las posibilidades que ofrecen las TIC. La contrapartida del mismo es la obligación de todas las Administraciones de dotarse de instrumentos adecuados para acceder por medios electrónicos a tal información. Uno de ellos es la denominada Plataforma de Intermediación, un servicio de verificación y consulta de datos que permite la comprobación automatizada de información obrante en los archivos de las Administraciones Públicas, previa identificación de quien solicita el acceso (que deberá estar convenientemente autorizado para ello) y acreditación de la finalidad del mismo, con constancia de la información consultada y garantías de protección de datos de carácter personal. Sin embargo, la presunción del consentimiento puede plantear problemas desde la perspectiva del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Tanto en su Considerando 32 como en su articulado señala que el consentimiento debe darse mediante acto afirmativo y claro (como ocurre en el caso en el que se marca una casilla en un formulario web), de tal modo que ni el silencio ni la inacción deben poder constituir consentimiento. Se da, pues, una contradicción entre este Reglamento europeo (una vez que entre en vigor) y la previsión del artículo 28, que llevaría en su caso a la inaplicación del precepto nacional en virtud del principio de primacía. Aun así, considero que cabría una interpretación conforme en el sentido de que si, en atención a las circunstancias concurrentes en el caso, el ciudadano ha llevado a cabo un acto afirmativo claro de consentir ese uso, es decir, si de su actuación consistente en la no presentación de documentos se puede deducir que está consintiendo inequívocamente que la Administración recabe la información, entender consentido el acceso ante tales circunstancias no vulneraría lo establecido en el Reglamento. En este caso no se estaría ante un simple silencio o inacción, sino ante una especie de omisión voluntaria indicadora del deseo de que sea el órgano actuante el que obtenga a la información requerida en la normativa aplicable.

El análisis de la realidad normativa, principalmente, de la LPAC y la LRJSP, pone de manifiesto que, lejos de innovar, estamos transformando la burocracia en papel en burocracia electrónica, en el peor sentido de la palabra. Más allá de que la burocracia sigue siendo un sistema válido de organización de las tareas administrativas (atribución de funciones a personas cualificadas por razón de ellas sobre la base del principio de jerarquía), no puede en ningún caso constituirse en un obstáculo a la innovación. Junto con ello, ambas normas están pensadas para blindar la legalidad de la actuación administrativa y dar cobertura normativa a soluciones desarrolladas por la Administración General del Estado, en lugar de situar al ciudadano en el centro de la actuación administrativa. Puede, además, observarse en nuestro ordenamiento jurídico un fenómeno excesivamente frecuente: las contradicciones entre normas, que empujan en sentidos diferentes constituyen del mismo modo un obstáculo evidente.

En definitiva, no pocas de las recientes opciones del Legislador son auténticas «antítesis», pues contradicen las premisas y las ideas expuestas en estas páginas (23).

Junto con todo lo anterior, faltan estrategias y miradas a largo plazo a la hora de reformar la Administración (24). Los importantes esfuerzos llevados a cabo por la CORA, cuyo informe es modélico en relación con algunos extremos, no eran sino cambios a corto plazo que no implicaban una reforma estructural de la organización administrativa ni un rediseño del procedimiento.

Todo ello trae consigo un claro impacto negativo sobre los derechos de los ciudadanos, que se enfrentan –por medios electrónicos, eso sí– a entramados burocráticos complejos y poco accesibles (sin posibilidad de opción en algunos casos por estar incluidos entre los sujetos obligados a hacer uso de los mismos), que han de soportar tiempos y trámites totalmente contrarios a la necesidad de obtener lo que esperan de forma rápi-

(23) La doctrina administrativista ha sido unánime a la hora de, más allá de valorar los aspectos positivos que toda reforma normativa conlleva, criticar la falta de innovación de la Administración y la mayor complejidad introducida en relación con algunos extremos en relación con las novedades legislativas recientes. *Vid.* Valero Torrijos, J.: «La reforma de la Administración electrónica, ¿una oportunidad perdida?», *Revista Española de Derecho Administrativo*, núm. 172, 2015, pp. 13 a 26; Gamero Casado, E.: «Panorámica de la Administración electrónica en la nueva legislación administrativa básica», *Revista Española de Derecho Administrativo*, núm. 175, 2016, pp. 15 a 27; y Menéndez Sebastián, E.: *Las garantías del interesado en el procedimiento administrativo electrónico. Luces y sombras de las nuevas Leyes 39 y 40/2015*, Tirant lo Blanch, Valencia, 2017 (en particular, p. 24).

(24) Para Ramió, «El problema estructural de las administraciones públicas de todo el mundo es una absoluta falta de identidad estratégica. Ni cuando se plantean reformas se observa mucho más allá del presente y solo se diagnostican los problemas de un pasado inmediato y todas las medidas prescriptivas que se proponen, en el marco o no de una reforma administrativa, son a muy corto plazo. Es evidente que durante los últimos 50 años las administraciones públicas han experimentado muchos cambios, pero estos han sido muy escasos respecto a modificar de forma drástica su paradigma conceptual», *La Administración Pública del futuro, op. cit.*, p. 21.

da y sencilla, que han de asumir costes directos e indirectos por falta de innovación.

En definitiva, en todo proceso de transformación –y más aún en el caso de la transformación digital, por los nuevos retos que plantea– resulta clave una premisa: asegurar el mantenimiento de las garantías de los ciudadanos.

La innovación para la mejora de la Administración es el fin; la tecnología es el método. El reto que se deriva de las posibilidades que ofrecen las TIC en relación con la organización y el procedimiento administrativo y la participación de los ciudadanos en la vida democrática consiste en traducir la innovación tecnológica en innovación administrativa. Modernizar la Administración no es lo mismo que innovarla. Incorporar las tecnologías en los procesos de actuación y en la estructura organizativa es simplemente modernizar; aprovechar esas mismas tecnologías para cambiar procesos y estructuras, explorando y explotando todas las posibilidades que conllevan y adaptándolas a las necesidades de los ciudadanos es innovar. Con ello, además, se realiza en mayor medida el fin que constitucionalmente tiene encomendada la Administración Pública –servir con objetividad los intereses generales y actuar de acuerdo con el principio de eficacia– y se da cumplimiento a uno de los principales derechos del ciudadano –el derecho de buena administración–.

En esta lógica, la Ley es la premisa necesaria, pero no suficiente. El convencimiento de que su aplicación práctica, desde el ejercicio del liderazgo político, resulta fundamental para una mejor y más eficaz, a la vez que más abierta, gestión de la cosa pública es condición imprescindible para alcanzar los objetivos de mejorar los servicios públicos y reforzar los procesos democráticos. Además, la Ley no es el único instrumento para la transformación digital; los planes y programas, las políticas públicas, los *nudges* [entendidos como «enfoques que influyen en las decisiones preservando la libertad de elección» (25)] y, en definitiva, la estrategia, son elementos claves, como también lo es la continuidad de la misma y su alcance global. Igualmente esencial es la elaboración de tales estrategias contando con los actores implicados: ciudadanos, empresas, empleados y directivos públicos, dirigentes políticos. Y, desde luego, desde la colaboración entre Ministerios y con las Administraciones autonómica y local y con análisis de costes y beneficios, sobre la base de datos y no de intuiciones políticas, con evaluaciones serias de implantación no limitadas a la autosatisfacción.

(25) Sunstein, C.: *(Más)* simple, *op. cit.*, p. 48.

En definitiva, resulta preciso revisar en profundidad las estrategias, valorar las diferentes opciones, evaluar los resultados, impulsar una legislación que funcione. E informar de todo ello al ciudadano.

La innovación, entendida como la incorporación transformadora de novedades para la mejora de una concreta realidad, no es estática. Antes al contrario, se trata de un proceso continuo, siempre abierto, en constante evolución. Un proceso que, además, conlleva una triple exigencia: moral –cambio de mentalidad–, formal –rediseño de la organización y del procedimiento– y jurídica –cumplimiento de las obligaciones contenidas en las nuevas leyes–. Sólo así «electrónico» o «digital» dejarán de ser adjetivos (en no pocas ocasiones, obviados y puestos entre paréntesis) para fusionarse con el sustantivo al que acompañan.

Lo electrónico no es mejor por ser electrónico, sino por las posibilidades de innovación que trae consigo. Ha llegado el momento de tomarse la Administración electrónica como lo que realmente es: el modelo de Administración del siglo XXI.

CAPÍTULO 8

LOS RETOS DE LA REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL: ALGUNAS APORTACIONES DESDE LA PERSPECTIVA EUROPEA

JOSÉ VIDA FERNÁNDEZ
Profesor Titular de Derecho Administrativo
Universidad Carlos III de Madrid

1. INTRODUCCIÓN

Resulta sintomático que en la mayoría de las aproximaciones jurídicas a la inteligencia artificial (IA) y a la robótica siempre se haga mención a las conocidas Leyes de la Robótica formuladas por Isaac Asimov (1). El hecho de que unas Leyes inventadas para un relato de ciencia ficción constituya el punto de referencia más sólido para el tratamiento jurídico de la IA y de los robots inteligentes pone de manifiesto las dificultades que presenta el análisis de estas cuestiones que se resisten a un tratamiento serio y convencional.

Por esta razón considero oportuno comenzar con una advertencia sobre los planteamientos visionarios que suelen adoptarse en muchas de las reflexiones de todo orden (políticas, sociológicas, filosóficas y, por supuesto, jurídicas) que se formulan sobre la IA y la robótica, y que suelen derivar en idealizaciones en torno a la creación de androides superinteligentes que actúan al margen de la voluntad humana.

Debe tenerse en cuenta que este tipo de planteamientos generan, en primer lugar, una evasión de la realidad actual en que se encuentran la IA y la robótica. Sin descartar que esos escenarios puedan llegar a darse en un futuro, es necesario concentrar la atención en el estado presente en que se encuentran estas tecnologías y en su evolución a corto plazo para determinar las respuestas que, de forma realista, deben darse desde el Derecho.

En efecto, estamos cada vez más acompañados por este tipo de tecnologías que se encuentran en una fase de especial desarrollo, y que desencadenarán una importante transformación económica y social a corto y medio plazo que se ha llegado a identificar con la cuarta revolución indus-

(1) Las Leyes de la Robótica fueron enunciadas por Isaac Asimov en su relato *Círculo Vicioso* (*Runaround*) en 1943 y se mencionan en una de las primeras iniciativas legales en esta materia, como es la Resolución del Parlamento Europeo de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL)) (en adelante, Resolución PE).

trial (2). Se trata de un sector en auge no solo por solo por su creciente importancia económica, ya que se encuentra un fuerte crecimiento anual con el que se prevé que alcance los 38.800 millones de dólares en 2025 (3), sino por tratarse de un sector estratégico ya que permite la transformación de otros sectores (transportes, sanidad, educación) y el posicionamiento a nivel internacional.

En segundo lugar, los planteamientos visionarios en torno a la IA y la robótica producen una deformación de la realidad ya que se formulan en términos extremos, partiendo de la existencia de unos dispositivos actualmente inéditos a los que se atribuye unas características idénticas a las humanas, e incluso unas capacidades superiores. Sin intención de entrar ahora en el debate sobre si esa capacidad creadora podrá ser alcanzada alguna vez por el hombre, lo que no cabe duda es que por ahora, y en un futuro próximo, la IA seguirá siendo programación y no podrá alcanzar capacidades metacognitivas que le permitan una reflexión introspectiva sobre su propia existencia y, en definitiva, disfrutar del libre albedrío.

Por esto conviene no caer en ensoñaciones y atender a la realidad para diseñar una regulación ajustada y eficaz que responda a los verdaderos problemas que plantean en su estado actual, y no entretenernos en diseñar una normativa ideal para unos entes que todavía no existen, ni andar preocupándonos por si los androides sueñan o no con leyes eléctricas (4).

Una tercera advertencia sobre estos planteamientos visionarios en torno a la IA y la robótica es que conducen a una desvinculación de la realidad, de modo que al tratarse con unos avances todavía inexistentes, resulta imposible, no ya someterlos al marco jurídico vigente sino reconducirlos a principios generales, por lo que se acaba acudiendo a Leyes de la ciencia ficción.

Conviene recordar que nos encontramos ante innovaciones tecnológicas con características que, por ahora, son ordinarias y que se ajustan en su mayoría a la normativa actualmente en vigor, si bien es cierto que presentan ciertas características que requieren una adaptación o un replan-

(2) Sobre el impacto de estos avances puede consultarse el conocido informe del McKinsey Global Institute, *Disruptive technologies: Advances that will transform life, business, and the global economy,* 2013. Otro estudio de referencia sobre su impacto en la economía mundial es el elaborado por Klaus Schwab, *La cuarta revolución industrial*, World Economic Forum-Debate, Madrid, 2016.

(3) Según el Dictamen de iniciativa del Comité Económico y Social Europeo (en adelante, Dictamen CESE) sobre la *Inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital), la producción, el consumo, el empleo y la sociedad* (2017/C 288/01), apartados 1.1 y 2.5.

(4) Parafraseando el título de la novela de Philip Dick, *¿Sueñan los androides con ovejas eléctricas?* de 1968, que inspiró la película *Blade Runner* de Ridley Scott y en la que precisamente un cazador de androides se planteaba problemas éticos ante la imposibilidad de distinguir lo artificial de lo natural.

teamiento de algunas cuestiones que, de hecho, ya se están debatiendo en algunas instancias como es el caso de la Unión Europea.

Una vez hechas estas advertencias es posible entender con mayor claridad el propósito de este trabajo, que no es otro que ofrecer un análisis realista y pragmático de la IA para identificar los retos verdaderamente cruciales que debe afrontar el Derecho y las alternativas existen para garantizar que la IA pueda desarrollarse y ofrecer todo su potencial de forma respetuosa con la condición humana y con la vida en sociedad.

2. ¿QUÉ ES LA INTELIGENCIA ARTIFICIAL?

2.1 **Una breve referencia a la evolución de la inteligencia artificial**

Uno de los principales problemas que presentan los avances tecnológicos es la dificultad de utilizar una terminología común que los defina y que permita abordar con claridad su análisis desde las distintas disciplinas del conocimiento, entre otras desde el Derecho. Esto es precisamente lo que ocurre con la Inteligencia Artificial (IA) que puede definirse como una rama de la informática que estudia y desarrolla sistemas capaces de realizar tareas propias de la inteligencia humana, en particular, comportarse de manera autónoma (5).

Sin pretensión de hacer ahora un recorrido por toda su evolución, si conviene recordar que se trata de un avance tecnológico que es relativamente reciente y que ha experimentado su mayor desarrollo en la última década. En efecto, el origen de la IA se remonta a mediados del siglo pasado con la aparición en 1952, de la mano de Arthur Samuel, del primer programa de ordenador capaz de aprender a jugar a la damas mejorando en cada partida y del término IA acuñado en la conferencia de Darthmouth de 1956 por Martin Minsky.

Desde estos inicios la evolución de la IA ha sido irregular a lo largo de las décadas sucesivas, si bien su avance se ha acelerado a partir de año 2006 cuando surge el «*deep learning*» (aprendizaje profundo) término utilizado por Geoffrey Hinton para la aplicación de nuevas arquitecturas de redes neuronales profundas con mayor capacidad de aprendizaje, a lo que se

(5) El DRAE recoge, sorprendentemente, la definición de IA como «*disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico*». De forma muy similar, en el informe del McKinsey Global Institute (2018), *An executive guide to IA*, se define como «*la capacidad de una máquina para desarrollar funciones cognitivas que se asocian a la mente humana, como percibir, razonar, aprender, interactuar con el medio, resolver problemas e, incluso, desarrollar su creatividad*». El Dictamen CESE (apartado 2.1) identifica que «*el objetivo fundamental de la investigación y el desarrollo en materia de IA es la automatización de comportamientos inteligentes como razonar, recabar información, planificar, aprender, comunicar, manipular, observar e incluso crear, soñar y percibir*».

suma el acceso a un creciente volumen de datos tratados de forma masiva (*big data*), gracias una mayor velocidad y capacidad en el procesamiento que se produce en la nube (*cloud computing*), factores todos ellos que convergen para dar lugar a la actual revolución de la IA.

En función de su estado de evolución suele hablarse de una IA débil o estrecha, que es aquella que se dedica a actividades o tareas muy concretas y que no son más que programas informáticos de alto rendimiento, y de una IA fuerte o superinteligencia lo que implica el desarrollo de actividades multitarea o multipropósito de forma similar o superior a la inteligencia humana.

2.2 **El aprendizaje automático *(machine learning)* y el aprendizaje profundo *(deep learning)* como fundamento de la inteligencia artificial**

La IA se basa esencialmente en el aprendizaje automático o *machine learning*, que permite programar sistemas para tomar decisiones y realizar tareas complejas a partir de grandes cantidades de datos sin haber sido programados para ello de forma específica. Este ámbito se encuentra bastante desarrollado en tanto estos sistemas demuestran una gran capacidad para identificar patrones y formular descripciones, predicciones o recomendaciones basadas en algún razonamiento automatizado expresado en un algoritmo (6). Los datos de entrenamiento sirven de base a esos algoritmos para que encuentren patrones, aprendan de ellos y sean capaces de hacer nuevas relaciones, todo ello sin recibir unas instrucciones específicas de forma explícita.

Los principales tipos de *machine learning* se dividen en aprendizaje supervisado (*supervised learning*), en el que los algoritmos usan datos y respuestas humanas para aprender la relación de cierta información con un determinado resultado (se utiliza para fijar precios de venta de productos o servicios, identificar enfermedades en función de los datos de diagnóstico, determinar la demanda de un producto o servicios, etc.); aprendizaje no supervisado (*unsupervised learning*), en el que un algoritmo explora los datos sin que se le exija un resultado específico (se utiliza, por ejemplo, para segmentar cliente y optimizar campañas publicitarias, recomendar películas, libros o música a los usuarios); y aprendizaje reforzado (*reinforced learning*), en el que un algoritmo aprende una

(6) En el Informe del McKinsey Global Institute (2018), *An executive guide to IA* se distinguen distintos tipos de análisis del *machine learning* en función de su nivel de complejidad que van, desde los análisis descriptivos (que a partir de un análisis describen lo que ocurre), los análisis predictivos (que anticipan a lo que ocurrirá, a partir de un sistema esencialmente probabilístico) y los análisis prescriptivos (que ofrece recomendaciones sobre como actuar para alcanzar determinados objetivos).

tarea simple tratando de maximizar la recompensa que recibe por sus decisiones (se emplea, entre otros usos, para el manejo de carteras de inversión, la conducción de vehículos autónomos, sistemas de almacenamiento robotizado, controlar la generación de electricidad en ciclos de demanda variables).

La manifestación más avanzada del *machine learning* lo constituye el aprendizaje profundo o *deep learning*, que permite procesar datos de un mayor rango de fuentes de información, con una menor intervención humana, y ofrece unos resultados más ajustados, aunque necesita una mayor cantidad de datos. Se basa en redes neuronales que están formadas por capas de programas de cálculo interconectados que pueden asumir enormes cantidades de datos y procesarlas en las distintas capas que aprenden funciones cada vez más complejas de los datos en cada capa. Las redes neuronales pueden procesar los datos, aprender que dicho procesamiento es correcto, y utilizar lo que ha aprendido para procesar nuevos datos, por ejemplo, aprende como es un objeto y es capaz de reconocerlo en distintos contextos.

Los tipos de *deep learning* se dividen en dos grandes modelos, uno basado en redes neuronales convolucionales (*convolutional neural network*) en el que una red neuronal multicapa con una arquitectura especialmente diseñada para extraer funciones cada vez más complejas para alcanzar un resultado, como es el caso de clasificación de imágenes, diagnósticos médicos a partir de los datos de escáner, detectar productos defectuosos de la línea de producción. El otro modelo es de redes neuronales recurrentes (*recurrent neural network*) en el que las redes neuronales multicapa pueden almacenar información en nodos, lo que le permite aprender las secuencias de datos y almacenarlos para trabajar en tareas desestructuradas como el reconocimiento de voz o de escritura manual, por lo que se utilizan para los asistentes de voz (*chatbots*), traducción automática, generar pies de fotos de imágenes o identificar probabilidades de fraudes financieros.

2.3 **Distinción de la robótica basada en inteligencia artificial**

Conviene distinguir la IA de la robótica, aunque se trata de fenómenos que se encuentran estrechamente relacionados. En efecto, los robots son dispositivos mecánicos dirigidos por circuitos electrónicos o programas informáticos que se caracterizan por su capacidad para desarrollar actuaciones físicas, es decir, integran la dimensión lógica con el efecto físico, y aunque suelen reducirse a los androides (aquellos con forma humana), pueden tener cualquier otra apariencia (zoomórficos o sin forma definida) o finalidad (industrial, médica, militar, etc.). Sin embargo, ni los robots tienen que tener necesariamente IA (como es el caso de brazos robóticos industriales

de cadenas de montaje), ni tampoco la IA se manifiesta exclusivamente en robots (como es el caso de los *chatbots* o asistentes de voz). Es cierto que la evolución tecnológica apunta a que se podrán generar nuevos modelos de robots que no solo replicarán cada vez mejor las formas y movimientos humanos (7) sino, y lo más importante, que adoptarán formas cada vez más sofisticadas de IA que les permitirán mayores niveles de autonomía.

En el caso de los robots, el nivel de autonomía puede llegar a ser mayor gracias a que puede interactuar con el entorno recibiendo cada vez más y mejor información a través de sensores complejos y a que puede modificar dicho entorno mediante su propia acción. Sin duda los robots multiplican las consecuencias que pueden derivarse del uso de la IA en la medida que están diseñados para desarrollar actuaciones físicas. En este sentido, no cabe pensar en solamente en robots androides que interactúan con humanos sino que también entran dentro de esta categoría dispositivos móviles más o menos sencillos (desde los aspiradores robóticos a los coches autónomos) o estáticos (como los sistemas de control de instalaciones –de energía, de agua, etc.–), que interactúan con el ámbito físico y que se han denominado de forma genérica como «sistemas ciberfísicos» (*Cyber-Physical Systems*, CPS) (8).

3. ¿CÓMO REGULAR LA INTELIGENCIA ARTIFICIAL?

3.1 **La estrategia para la regulación de la inteligencia artificial**

El espectacular desarrollo de los sistemas de IA en los últimos años ha generado una enorme expectación sobre esta cuestión que ha derivado en constantes noticias y numerosos estudios desde todas las disciplinas, entre las que no destaca precisamente el ámbito jurídico (9). La razón de este vacío es que ni existían normas específicas en esta materia ni tampoco se habían planteado iniciativas al respecto ya que ha sido precisamente ahora cuando los avances técnicos en este ámbito han dado lugar al inicio de un debate cada vez más serio y complejo en torno a la regulación de

(7) Basta con consultar cualquiera de los vídeos disponibles de los prototipos de la empresa *Boston Dynamics*.

(8) «*Ethical Aspects of Cyber-Physical Systems*» (*Scientific Foresight study)*, de junio de 2016 (PE 563.501) elaborado para el STOA (Parlamento Europeo) que se caracterizan por interactuar con el medio físico.

(9) Salvo contadas excepciones como el reciente libro dirigido por Moisés Barrio Andrés (2018), *Derecho de los robots*, Wolters Kluwer, y también el de Rafael de Asis Roig (2014), Una *mirada a la robótica desde los derechos humanos*, Dykinson, Madrid. En EE.UU. la literatura es algo más abundante con trabajos como los de Jack Balkin (2015) «The Path of Robotics Law», *California Law Review*, núm. 6; Ryan Calo (2017), «Artificial Intelligence Policy: A Primer and Roadmap», University of Washington - School of Law: Mattew Scherer (2016), «Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies», Harvard Journal of Law & Technology, vol. 29, n.º 2; y Harry Surden (2014), «Machine Learning and Law», *Washington Law Review*, vol. 89, n.º 1, entre otros.

la IA, con la finalidad de adoptar algún tipo de estrategia para su regulación (o más correctamente, su ordenación).

El desarrollo de cualquier estrategia para regular la IA debe tener en cuenta algunas de sus características principales que necesariamente condicionarán su diseño. En primer lugar debe tenerse en cuenta la dificultad inmediata que plantea el desconocimiento en cuanto a su potencial alcance en tanto se trata de una tecnología en pleno desarrollo. No cabe duda de que el potencial disruptivo de la IA implicará profundos cambios, favoreciendo el crecimiento económico y la mejora de la competitividad, una actividad más respetuosa con el medio ambiente, una mayor seguridad en el trabajo, una mejor sanidad, educación y justicia y una sociedad más segura. Sin embargo, se desconoce igualmente el verdadero alcance que puede llegar a tener tanto desde una perspectiva técnica como, por supuesto, económica y social, por lo que las iniciativas que se han desarrollado hasta ahora recomiendan aumentar y profundizar el conocimiento sobre la IA en todos los niveles para poder reconocer, definir y controlar las disrupciones en su desarrollo a fin de poder regularlas adecuadamente y a su debido tiempo (10).

Una segunda característica es que la IA no se está desarrollando en la actualidad al margen de toda normativa, sino que la IA constituye una innovación informática más que aún no ha merecido un tratamiento jurídico específico. Por lo tanto, y para evitar planteamientos adánicos, debe recordarse que la IA ya cuenta con un marco jurídico de referencia constituido por las normas internacionales, europeas y nacionales que le resulten de aplicación, en cuestiones como los derechos humanos, la protección de datos personales, la propiedad industrial e intelectual, la normalización técnica, etc. No obstante es también cierto que este marco jurídico resulta cada vez más insuficiente, por lo que cuando se proceda a regular la IA se irán adoptando normas específicas que irán sustituyendo o completando a las actuales.

En tercer lugar debe recordarse que la IA es un avance técnico en el ámbito de la informática con unos contornos poco definidos y constante cambio que, además, constituye un medio para desarrollar determinadas actividades de forma automatizada (negociar, traducir, conducir, vigilar), por lo que resultaría absurdo establecer un marco jurídico unitario con el que se pretenda regular de forma estable y completa la IA, al igual que no se ha hecho ni con la informática en general, ni con determinados avances dentro de las TICs como, por ejemplo, Internet. Se pueden regular aspectos concretos de estos avances que pueden ser conflictivos (los nombres

(10) Sobre las implicaciones de la IA *vid.* el Dictamen de iniciativa del Comité Económico y Social Europeo (CESE) *Inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital), la producción, el consumo, el empleo y la sociedad* (2017/C 288/01).

de dominio) o las actividades finales con que se utilizan (la prestación de servicios por Internet), pero resultaría inútil una ley integral en esta materia, por lo que se optará por una regulación a partir de la modificación y adaptación de la existente (11).

Por último es necesario hacer mención al carácter transnacional de la IA, ya que se trata de una innovación que se desarrolla principalmente a nivel internacional por grandes multinacionales y que se pone a disposición, en distintas versiones y con distintas condiciones, a usuarios de todo el mundo. Asimismo el uso de la IA puede proyectarse en cualquier actividad, tanto en el ámbito público como privado, por lo que se generalizará su uso y sus consecuencias impactarán en todos los Estados y en sus ciudadanos. Por esta razón parece conveniente optar por impulsar marcos jurídicos de carácter supranacional, uniforme y universal para la IA, de conformidad con los valores comunes y los derechos fundamentales reconocidos a nivel internacional (12).

3.2 **Las iniciativas existentes sobre regulación de la inteligencia artificial**

Las iniciativas que se han dado hasta ahora en cuanto a la regulación de la IA han tenido una finalidad esencialmente prospectiva con la que se pretende identificar la magnitud y características de los cambios que pueden producirse como consecuencia del desarrollo de la IA y la robótica, y, asimismo, las directrices de las medidas que tenga que adoptarse para garantizar su desarrollado y una incorporación seguras de estas nuevas tecnologías.

Estas iniciativas se materializan, en la mayoría de los casos, en la constitución de grupos de trabajo compuestos por expertos de distintas disciplinas que elaboran informes en los que se contienen recomendaciones para el desarrollo de las políticas públicas en este ámbito (13). Además de los grupos de trabajo, también se están adoptando resoluciones por parte de algunas de las instituciones responsables de las políticas públicas en las que se empiezan a fijarse posiciones para la regulación de la IA y la robótica, aunque todavía con carácter no vinculante.

---

(11) Este es la opción a que apunta el informe del STOA «*Ethical Aspects of Cyber-Physical Systems*» (*Scientific Foresight study)*, de junio de 2016 (PE 563.501) en el que se ofrece una relación de normativa europea que se verá afectada por los avances en IA y robótica y, dentro de seis áreas definidas, se identifica un total de treinta y nueve directivas, reglamentos, declaraciones y comunicaciones más la Carta de Derechos Fundamentales de la UE.

(12) Dictamen CESE (apartado 1.4 y 3.35).

(13) En el caso de España, el 14 de noviembre de 2017 se constituyó el Grupo de Sabios que abordarán las implicaciones sociales, jurídicas y éticas de la utilización de la IA y el Big Data en el sector privado, la Administración Pública y la sociedad en general, cuyas conclusiones se recogerán en un Libro Blanco publicado a mediados de 2018.

La instancia que ha prestado una mayor atención a estas cuestiones ha sido la Unión Europea, y, en particular, el Parlamento Europeo cuya Unidad de Prospectiva Científica (STOA) viene elaborando informes (14) sobre IA y robótica, algunos de los cuales sirvieron de base para la adopción por el Pleno de la Resolución de 16 de febrero de 2017, con *recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica* (2015/2103(INL)) que ha sido seguida por una Consulta Pública sobre «El futuro de la robótica y de la inteligencia artificial», cuya conclusiones se fijaron a finales de 2017 (15).

También el Comité Económico y Social Europeo se ha posiciona sobre esta cuestión a través de la elaboración de un Dictamen de iniciativa sobre la *Inteligencia artificial: las consecuencias de la inteligencia artificial para el mercado único (digital), la producción, el consumo, el empleo y la sociedad* (2017/C 288/01) (16) y se propone abrir un debate a partir del mismo con todos los representantes de la sociedad.

Por su parte, el Consejo Europeo ha animado a las instituciones a seguir con sus iniciativas en este ámbito de la IA que ha situado de forma prioritaria en todas sus conclusiones desde la reunión ordinario de octubre de 2017, como una de los principales cuestiones de la Europa Digital (17).

Limitación de la UE para intervenir sobre la IA con carácter global y, en particular, por lo que se refiere a su utilización por parte de los poderes públicos. Esta es la razón de que la Resolución de 16 de febrero de 2017 se limite a cuestiones de responsabilidad civil, propiedad intelectual y contratación, e incidentalmente, a los aspectos éticos de las nuevas tecnologías.

---

(14) En concreto se trata del estudio sobre los aspectos éticos de los sistemas ciberfísicos «*Ethical Aspects of Cyber-Physical Systems*» (*Scientific Foresight study)*, de junio de 2016 (PE 563.501) elaborado para el STOA (*Science and Technology Options Assessment*, que forma parte del Parlamento Europeo) por la Unidad de Prospectiva Científica (*Scientific Foresight Unit*) dependiente de la Dirección General de Servicios de Investigaciones Parlamentarias (EPRS). La EPRS ha elaborado más recientemente otro informe sobre coches autónomos que acompaña a la Resolución de 16 de febrero de 2017 «*A common EU approach to liability rules and insurance for connected and autonomous vehicles*» (*European Added Value Assessment*), de febrero de 2018 (PE 615.635) y otro sobre las amenazas de la IA «*Should we fear artificial intelligence?*», de marzo de 2018 (PE 614.547)

(15) Los resultados de la Consulta Pública sobre «El futuro de la robótica y de la inteligencia artificial» que estuvo abierta d el 8 de febrero de 2017 al 31 de mayo de 2017 pueden consultarse: http://www.europarl.europa.eu/committees/es/juri/robotics.html?tab=Resultados

(16) *DOUE*, de 31 de agosto de 2017 (C 288/1)

(17) En efecto, a partir de la reunión del 17 de octubre de 2017 en todas las conclusiones de las reuniones del Consejo Europeo se hace mención expresa a la cuestión de la inteligencia artificial y a la necesidad de abordarla. De hecho se celebrará una reunión informal de los Jefes de Estado y de gobierno en Sofía en el mes de mayo de 2018 para tratar específicamente esta cuestión y otras de la Europa Digital.

4. RETOS Y PROPUESTAS A LA REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL (I): LOS PROBLEMAS COMUNES EN CUANTO INNOVACIÓN TECNOLÓGICA

En los apartados siguientes se ofrecerá un análisis de los retos que presenta la regulación de la IA y de las posibles alternativas que pueden seguirse para hacer frente a los mismos a partir de las propuestas contenidas en las iniciativas que han surgido en el seno de la Unión Europea, junto a otras de elaboración propia.

Los retos que presenta la IA son muy numerosos y variados, tanto en su situación actual como en el desarrollo que habrá de experimentar a corto y medio plazo. Todos estos retos pueden clasificarse distinguiendo entre aquellos retos que son comunes a todas las innovaciones tecnológicas y que pueden verse potenciados en el caso de la IA (y que se tratan en este apartado), y aquellos otros que son específicos de la IA por razón de la singularidad de sus características (y que se tratan en el siguiente apartado).

4.1 **Las transformaciones socio-económicas: en particular el impacto sobre el mercado de trabajo**

Al igual que los anteriores avances tecnológicos que se han producido en el ámbito de las TICs, la combinación de la IA y la robótica dará lugar a una profunda transformación socio-económica, en particular en el mercado de trabajo.

Si bien se trata de un fenómeno ya conocido es plausible que se manifieste con algunas particularidades. En primer lugar la intensidad del impacto sobre el mercado de trabajo, ya que se calcula que el 45% de los trabajo que se desarrollan por humanos en la actualidad podría ser automatizada con las tecnologías existentes. También el alcance de dicho impacto ya que si bien, hasta ahora, la transformación solamente alcanzaba a trabajos físico poco cualificados, ahora se prevé que la mayor parte del impacto recaiga en trabajos de gestión y administración, aunque sean los que impliquen actividades menos complejas y más repetitivas (18).

Las opiniones acerca de las consecuencias del impacto de la IA y la robótica sobre el mercado de trabajo son muy variadas, y van desde quienes consideran que se traducirá en un mantenimiento o crecimiento del empleo, tal y como ha ocurrido con las innovaciones precedentes, gracias a la mayor eficiencia y productividad que permitirá un desplazamiento

(18) Para el año 2020, 5 millones de puestos de trabajo se perderán sólo en favor de la inteligencia artificial y la robótica, según el *World Economic Forum*. Dos tercios de esas pérdidas se producirán en los sectores administrativos y oficinas con trabajadores de clase media global.

hacia nuevas actividades más flexibles y creativas (19); a aquellos otros que opinan que el alcance será menor ya que se automatizarán, no tanto puestos de trabajo multitarea que ahora resultan inasumibles para la IA sino funciones concretas, y dará lugar a la aparición de nuevos puestos de trabajo para tareas pequeñas y mal remuneradas para un grupo creciente de trabajadores flexibles (20).

Asimismo, parece fuera de toda duda, que esta transformación afectará igualmente a los sistemas de protección social (Seguridad Social) y a los servicios públicos (educación y sanidad) que se basan en unos niveles de cotización y en la recaudación de un volumen de impuestos que se van a ver alterados por las transformaciones que se vayan a producir en la disponibilidad de trabajos y en los salarios.

Por esto se propone llevar a cabo un seguimiento detallado del impacto sobre el mercado de trabajo y los mecanismos de redistribución como son los sistemas de protección social y los servicios públicos, para identificar posibles soluciones entre las que se encuentran la creación de un impuesto para las IA, un reparto de los dividendos que generan o que la propiedad de los sistemas de IA se comparta entre empleados y empleadores, sin que estas medidas se conviertan en un obstáculo para su desarrollo (21).

4.2 **La seguridad como requisito para su funcionamiento**

La IA debe responder a unos estándares mínimos de seguridad que le permitan funcionar correctamente y sin producir daños a los usuarios o destinatarios de su actuación (22), al igual que el resto de los sistemas informáticos, aunque esta exigencia puede verse más comprometida por razón de sus singulares características.

Por lo que respecta a la seguridad interna, es un elemento común a todos los sistemas que deben funcionar de forma correcta para lo que han de estar adecuadamente diseñado. Asimismo ese funcionamiento debe ser estable y resistente frente a alteraciones imprevistas en las condiciones de desarrollo, ya sean fortuitas o provocadas, por ejemplo, a través de un ciberataque. En el caso de la IA estas exigencias son más difíciles de cumplir en la medida que se trata de sistemas especialmente complejos que dependen de muchas variables para su correcto funcionamiento, por

(19) En este sentido se hace referencia al crecimiento continuado del empleo en los últimos doscientos años gracias al desarrollo tecnológico que conlleva una mayor eficiencia y ahorro, no solo en la producción y el comercio, sino también en multitud de ámbitos que van desde la ganadería a los servicios como la educación, el transporte o la sanidad (considerando E de la Resolución PE).

(20) Así se pronuncia en el Dictamen CESE (apartado 3.22).

(21) El CESE se había pronunciado en un Dictamen de 15 de enero de 2016 (DO C 13) sobre la posibilidad de un dividendo digital y el reparto equitativo de dividendos, con el fin de lograr efectos positivos sobre el crecimiento *cfr.* Dictamen CESE (apartado 3.22).

(22) Dictamen CESE *op. cit.* (apartado 3.7)

lo que se mantienen en un equilibrio muy precario que puede verse fácilmente alterado y dar lugar, no ya a una interrupción de su funcionamiento sino a desviaciones que pueden derivar en daños incluso mayores.

En el caso de la seguridad externa, los sistemas de IA plantean unos problemas específicos ya que pueden plantearse dudas en cuanto a las consecuencias de su actividad. En este sentido los algoritmos que generan la capacidad de autoaprendizaje deben responder no solo a las condiciones de funcionamiento normal sino también a circunstancias extraordinarias para evitar que puedan verse superados ante su incapacidad para improvisar. Asimismo debe garantizarse que la totalidad de los posibles resultados de su funcionamiento sean siempre seguros para la sociedad, lo cual introduce el problema del carácter autónomo que se analizará en el siguiente apartado.

Con respecto a la seguridad, deben garantizarse unas condiciones mínimas que deben alcanzar los sistemas de IA para poder funcionar (23). Si bien estos requisitos deben determinarlos conjuntamente los responsables políticos, los especialistas en IA y seguridad, las empresas y las organizaciones de la sociedad civil, se trata de una cuestión muy compleja y conflictiva, sobre todo por lo que respecta a la seguridad externa.

4.3 **Los problemas de privacidad**

La privacidad es otro de los problemas recurrentes que suelen señalarse en el caso de los sistemas de IA ya que los datos son el combustible imprescindible que permite el aprendizaje automático, que evoluciona y mejora con el tratamiento de una mayor cantidad de información.

Esto explica que los sistemas de IA sean receptores de cantidades ingentes de datos, muchos de los cuales son de carácter personal. Incluso, muchos de los dispositivos basados en IA son recolectores masivos de datos personales que se infiltran de manera imperceptible nuestra vida cotidiana (es el caso de los robots aspiradora que mapean hogares, o del Cubo de Amazon permanentemente en escucha). Pero además, los sistemas de IA procesan de manera cada vez más compleja todos estos datos, incluidos los datos personales, y consiguen resultados a menudo impensables a partir de unos datos desagregados y muchas veces anónimos.

Por lo tanto, en todos estos procesos que implican el tratamiento de datos personales, deben respetarse los requisitos fijados en la normativa de protección de los derechos de las personas en relación con el tratamiento de sus datos personales, en concreto en el Reglamento General de Protección de Datos –Reglamento (UE) 2016/679, recientemente en aplicación–. En estos términos, las exigencias que se imponen a los siste-

(23) Dictamen CESE (apartado 3.8)

mas de IA, en cuanto a la protección de datos personales, son comunes a todo tratamiento total o parcialmente automatizado a través de sistemas informáticos, sin que se incluyan medidas específicas al respecto.

Ahora bien, los sistemas de IA plantean retos adicionales gracias a su capacidad de procesamiento de los datos por lo que pueden dar lugar a formas de tratamientos desconocidos hasta ahora, cuyos resultados pueden desbordar las medidas de protección dispuestas en la normativa común, incluso en una tan actualizada como el Reglamento General de Protección de Datos.

En este sentido se identifica la capacidad que tienen los sistemas de IA para influir en las decisiones humanas a través del análisis de grandes cantidades de datos (a menudo personales) en muchos terrenos (desde decisiones comerciales a elecciones políticas). Por eso se propone un seguimiento de para evitar que la aplicación de la IA al tratamiento de los datos personales restrinja la libertad real o percibida de las personas (24), y se proteja de dichas influencias colectivos especialmente vulnerables como es el caso de los niños.

4.4 **La inteligencia artificial como factor competitivo**

La IA se convertirá en uno de los principales elementos competitivos no ya entre empresas, sino entre los distintos países y también a nivel social. Si bien toda innovación tecnológica tiene, en mayor o menor grado este efecto, debe tenerse en cuenta que la relevancia que puede alcanzar la IA para el desarrollo de cualquier actividad humana puede dar lugar a importantes desequilibrios.

Los principales avances en el ámbito de la IA se llevan a cabo esencialmente por cinco grandes empresas tecnológicas (Apple, Microsoft, Google, Facebook y Amazon) que, por ahora, han accedido a llevar a cabo un desarrollo a través de códigos abiertos. Sin embargo, este planteamiento puede cambiar, por lo que los actores políticos internacionales deben procurar que se continúe con el desarrollo de la IA en un entorno abierto.

En todo caso, y en previsión de los sistemas de IA se conviertan en un elemento competitivo y dejen de estar al alcance de todos, se plantean iniciativas para limitar la dependencia de terceros desde el punto de vista tecnológico. Se trata de evitar la dependencia de los particulares, de las empresas y de los propios Estados, a través de iniciativas propias en el desarrollo de la IA como es la creación de una infraestructura de IA europea de fuente abierta (*open source*), que puede servir como ventaja (competitiva) en el mercado mundial mediante el desarrollo y la promoción de «sistemas de IA de responsabilidad europea», provistos de un sistema europeo

(24) Dictamen CESE (apartado 3.15)

de certificación y etiquetado de la IA (25). Asimismo, esta iniciativa debe complementarse con el fomento de la investigación en el ámbito de la IA, tanto en el desarrollo de innovaciones que mejoren la IA y permitan nuevas aplicaciones, como de la investigación sobre el impacto social de la IA.

Pero la IA también puede convertirse en un importante elemento competitivo a nivel social y, a medida que aumente su capacidad y funcionalidades podría dar lugar a graves desequilibrios sociales. La brecha tecnológica se podría profundizar hasta extremos insoportables, provocando una mayor concentración de capacidades y por tanto de riqueza y, en general, de bienestar, en una minoría. Por esta razón, y aunque puede tratarse de un escenario que no llegue a producirse –como no ha ocurrido en términos generales con la informática–, es recomendable prestar atención a la evolución en este sentido (26).

5. RETOS Y PROPUESTAS A LA REGULACIÓN DE LA INTELIGENCIA ARTIFICIAL (II): LOS PROBLEMAS ESPECÍFICOS POR RAZÓN DE LA SINGULARIDAD DE SUS CARACTERÍSTICAS

5.1 **La autonomía de los sistemas de inteligencia artificial**

El carácter autónomo de la IA es su principal característica que la distingue de las innovaciones que se han dado con anterioridad en el ámbito de las TIC. Como se ha podido comprobar, se trata de una autonomía relativa ya que se parte de un diseño concreto que es el que permite adoptar las decisiones y que puede contener mayores o menores limitaciones en función de la modalidad de *machine learning* o de *deep learning*.

En ningún caso se plantea, por ahora, una autonomía absoluta que permita a estos sistema actuar con plena capacidad de autodeterminación y libre albedrío, de forma similar a la mente humana, cuestión con la que ha fantaseado la literatura de ciencia ficción (27). Sin embargo, en la mayoría de IA los sistemas llevan a cabo opciones entre distintas alternativas a partir de unos parámetros, elecciones que no siempre son posibles de prever, lo que genera una autonomía relativa que no se había dado en ninguna de las invenciones precedentes.

---

(25) Dictamen CESE (apartado 1.9)

(26) Como indica el considerando K) de la Resolución PE.

(27) Las reiteradas Leyes de la Robótica de Isaac Asimov se refieren a ese escenario de combinación de la autonomía con posibles daños: «1.ª Un robot no hará daño a un ser humano ni permitirá que, por inacción, este sufra daño; 2.ª Un robot obedecerá las órdenes que reciba de un ser humano, a no ser que las órdenes entren en conflicto con la primera ley; 3.ª Un robot protegerá su propia existencia en la medida en que dicha protección no entre en conflicto con las leyes primera y segunda».

Como ejemplo extremo de este temor basta recordar el superordenador HAL que acaba siendo desconectado en *2001: Una odisea del espacio*, la película dirigida por Stanley Kubrick basada en una novela de Arthur C. Clarke, ambas de 1968.

Este carácter autónomo de los sistema de IA adquiere una especial relevancia por razón de la importancia de las tareas que asumen (desde el manejo de una central eléctrica a la conducción de un vehículo) y la generalización de su utilización (en el caso de los asistentes que terminarán por ser la interfaz imprescindible para todos los dispositivos informáticos), circunstancias que multiplican el alcance y la entidad de los daños que pueden generar.

La combinación de estas dos circunstancias, su autonomía y las consecuencias de su funcionamiento, exigen un planteamiento distinto con respecto al resto de soluciones técnicas existentes. En los sistemas informáticos precedentes, sus actuaciones eran resultado directo del diseño de los fabricantes y programadores en combinación con la acción de sus usuarios. Con la IA, los diseñadores y desarrolladores no predeterminan las decisiones que adopten los sistema de IA –aunque establezcan sus bases– y tampoco los usuarios dominan el resultado su actuación, ya que precisamente se caracterizan por funcionar de manera autónoma.

La autonomía como característica de la IA obliga a plantear, en primer lugar, el problema de su alcance, en concreto, si resultaría admisible un autonomía absoluta, ya sea porque tecnológicamente pudiera alcanzarse o porque simplemente, con las limitaciones que tengan, se dejase actuar a estos sistemas sin supervisión humana. A este respecto se plantea el principio del control humano (*human-in-command*) (28), de manera que las máquinas continúen siendo máquinas y los humanos conserven en todo momento el dominio sobre ellas. En este mismo sentido y frente a las amenazas que pudieran surgir del uso de IA fuerte se plantea la exigencia de un botón para desactivar o reiniciar (*kill-switch o reset-button*) los sistemas de IA desbocados.

Pero la autonomía de los sistemas de IA, en la medida que implica la adaptación de decisiones que tienen consecuencias reales, plantea también otro problema que es el del respeto a los valores, principios y normas de la sociedad en la que actúan. Es decir, el hecho de que los sistema de IA sean autónomos, no puede ser una excusa para puedan actuar al margen de la normativa que serían aplicable a los humanos en su actuación. Ahora bien, no se puede exigir a los sistemas de IA que cumplan las normas sino que son los diseñadores, desarrolladores y usuarios de estos sistemas de IA los que deben cumplir las normas y garantizar que los sistemas de IA los cumplan (29).

Por esto, para que el funcionamiento los sistemas de IA sea compatibles con los principios de la dignidad humana, la integridad, la libertad, la privacidad, la diversidad cultural y de género y los derechos humanos

(28) Dictamen CESE (apartado 1.6)
(29) Así se indica en el considerando T) de la Resolución PE.

fundamentales, se propone la elaboración de un código deontológico uniforme y universal para el desarrollo, despliegue y utilización de la IA (30).

La cuestión de la autonomía y de la responsabilidad de los sistemas de IA conduce directamente al debate sobre la personalidad jurídica. A este respecto existen posturas encontradas ya que el Parlamento Europeo se ha mostrado favorable a la creación a largo plazo de una personalidad jurídica específica (*e-personality*) para los robots, para facilitar la determinación de responsabilidades en caso de causar daños. Por su parte, el CESE está absolutamente en contra ya que, en su opinión, se socavaría los efectos correctores preventivos de la legislación en materia de responsabilidad, generando un riesgo moral tanto en el desarrollo como en la utilización de la IA en cuanto el riesgo de responsabilidad civil dejaría de recaer sobre el autor por haberse transferido al robot, y sería susceptible de uso y aplicaciones indebidos (31).

5.2 **Los sesgos en el funcionamiento de la inteligencia artificial**

Una de las cuestiones más controvertidas que se imputan a la IA es el problema de los sesgos que están afectando a los modelos predictivos que se aplican y las dificultades para detectarlos y corregirlos. Son numerosos los estudios que denuncia la existencia de sesgos en la IA que pueden incrementar la desigualdad a través de una discriminación encubierta y afectar al principio de igualdad efectiva que debe imperar en un democracia (32).

A este respecto es importante acabar con el mito del carácter neutral y objetivo de la IA en tanto que avance tecnológico basado en postulados científicos que opera con procesos matemáticos cuantitativos desarrollados de forma automática por una máquina, lo que parece desterrar todo tipo de parcialidad y subjetivismo en sus actuaciones. Por el contrario, la IA, precisamente por sus características técnicas, presenta un problema de sesgos que no suele manifestarse en otro tipo de avances informáticos, o al menos no con la intensidad y las consecuencias que se presentan en este ámbito.

El problema de los sesgos tiene un origen tanto exógeno como endógeno a la propia IA. Por lo que se refiere a las causas exógenas estas proceden de las características de los datos de entrenamiento que se utilizan como base para el funcionamiento de la IA. Como se ha indicado, las modalidades más complejas de la IA utilizan volúmenes cada vez mayores de datos, por lo que es importante que estos datos sean de calidad, variados,

(30) Dictamen CESE (apartado 1.7 y 3.6)
(31) Dictamen CESE (apartado 1.12).
(32) Así puede consultarse el trabajo de Virgina Eubanks (2018), *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, St. Martin's Press, New York. También el trabajo de Cathy O'Neil (2016), *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy,* Penguin Randim House, New York.

profundos y ecuánimes para que la IA pueda desarrollarse en condiciones de certeza, seguridad y objetividad (33). Los datos no son un elemento perfecto, objetivo y neutral en si mismo, sino que pueden ser incorrectos y, sobre todo, son manipulables cuando no reflejan una variedad suficiente desde el punto de social y cultural.

Por supuesto, la IA puede operar sobre datos acotados cuando se utilice para fines concretos con respecto a determinados segmentos de la sociedad, pero, de ser así, deberán hacerse explícitas las características de los datos que se utilizan, ya que estos, en cuanto fundamento del funcionamiento de la IA, determinarán sus resultados. Por el contrario, cuando la IA se proyecte de forma indistinta para el conjunto de la sociedad, se deberá garantizar que los datos que se utilizan con correctos y suficientemente variados para evitar sesgos derivados de la parcialidad de los datos.

En cuanto a los factores endógenos de los sesgos se encuentran en el diseño de los algoritmos en que se fundamenta el funcionamiento de la IA ya que, aunque estos permitan desarrollar una actuación de forma autónoma, siempre tienen origen en un primer planteamiento que inevitablemente contiene la impronta de sus diseñadores. La IA no surge por generación espontánea sino que procede de programadores que tienen unas características concretas (raciales, culturales) que inevitablemente condicionan su diseño, en mayor o menor medida (34).

En este sentido sería recomendable llevar a cabo un desarrollo abierto y participativo del desarrollo tecnológico de la IA que no siempre es posible por razones derivadas de la normativa de patentes. Como alternativa se debería garantizar la pluralidad en los equipos que desarrollan la IA, lo cual también puede ser difícil de exigir ya que supondría condicionar en exceso la política de organización empresarial que, por cierto, no se hace en otros supuestos similares. En todo caso, y al igual que ocurre con los datos, sería importante, en la medida de lo posible, que se pudiera identificar las características de dichos equipos y de las soluciones que se incorporan en el funcionamiento de la IA para, al menos, estar advertidos de la posible existencia de sesgos en su funcionamiento.

5.3 **La opacidad de los sistemas de inteligencia artificial**

Como se ha podido comprobar uno de los elementos esenciales frente a los retos que plantea la IA es la transparencia y el acceso a sus condiciones de funcionamiento que son, precisamente, los instrumentos que permi-

(33) Dictamen CESE (apartado 3.5)

(34) El desarrollo de la IA se está produciendo hasta ahora en un entorno homogéneo compuesto principalmente por varones jóvenes blancos, lo que deja una impronta cultural y de género, ya que los sistemas de IA aprenden de los datos de formación, tal y como se indica en el Dictamen CESE (apartado 3.5)

ten el control de su funcionamiento sin obstaculizar su desarrollo. En efecto, para identificar problemas de seguridad, la existencia de sesgos, etc. es imprescindible la transparencia e inteligibilidad de los sistemas de IA y, asimismo, la posibilidad de acceso y verificación de los mismos, ya que de otro modo pueden quedar ocultos y resultar indetectables tanto para sus creadores como para los usuarios, sin que fuese posible remediarlos.

La transparencia y la inteligibilidad de los procesos en se basan los sistemas de IA es una condición de partida que concierne, en primer lugar, a sus diseñadores y desarrolladores. En efecto, aunque pueda resultar extraño, los sistemas de IA en su proceso de aprendizaje pueden derivar en el manejo de unos códigos que sean incomprensibles, incluso, para sus propios creadores y que solamente entendibles para las propias máquinas (35). Por lo tanto resulta imprescindible que los sistemas de IA sean siempre transparentes y comprensibles de modo que sea posible acceder en todo momento a sus procesos y descifrarlos, sin que puedan dejarse que los sistemas se conviertan en una caja negra que funcione al margen de toda supervisión, lo que conecta con la cuestión del principio del control humano (*human-in-command)* que se ha analizado anteriormente.

Pero además del carácter transparente y comprensible del funcionamiento de los sistemas de IA, se plantea el necesidad de que sea posible el acceso y verificación de estos procesos para ejercer un control externo que permita velar por su adecuado funcionamiento. En este sentido, se propone la utilización de un sistema de normalización para la verificación, validación y control de los sistemas de IA, basado en un amplio espectro de normas en materia de seguridad, transparencia, inteligibilidad, rendición de cuentas y valores éticos (36). Asimismo se propone el reconocimiento de un derecho de acceso y verificación de los sistemas de IA por parte de los usuarios para que estos ejerzan un mayor control de los procesos de toma de decisiones automatizados y basados en algoritmos (37).

La justificación de este acceso y verificación a los sistemas de IA se basa en la creciente incidencia que estos tienen para la vida de las personas, tanto en el ámbito público (por ejemplo, sistemas policiales basados en IA), como privado (concesión de créditos o seguros). Sin embargo, la transparencia y el acceso a los sistemas de IA no es una cuestión tan sencilla, como tampoco lo es en la actualidad el acceso a las razones últimas de determinadas decisiones tanto en el ámbito público (el acceso a deter-

(35) Es el caso de un sistema de IA desarrollado en *Georgia Tech* que era capaz de aprender y desarrollar nuevas tácticas de negociación y llegó a elaborar su propio idioma a partir de una corrupción del inglés que era mucho más eficiente para sus propósitos pero incomprensible para cualquiera, incluidos sus programadores. *Cfr.* «Facebook apaga una inteligencia artificial que había inventado su propio idioma», *El Mundo*, 28 de julio de 2017.

(36) Dictamen CESE (apartado 1.8)

(37) Como indica el considerando Q) de l a la Resolución PE.

minadas decisiones policiales puede quedar limitada por razón de orden público) como privado (los motivos por los que se deniega un crédito o un seguro quedan a menudo ocultos tras la autonomía de la voluntad).

En todo caso debe tenerse en cuenta que el acceso y la verificación puede quedar frustrada por la complejidad de los sistemas de IA. Por esta razón es necesario llevar a cabo una formación generalizada en materia de IA, en particular en aquellas áreas donde los sistemas de IA puedan presentar mayores riesgos. En todo caso, será igualmente necesaria la asistencia de expertos independientes que sean capaces de verificar el funcionamiento adecuado de los sistemas de IA.

5.4 **La sustitución de la intervención humana**

Otro de los problemas específicos que plantea de forma específica la IA es el peligro de expulsión de las capacidades humanas que quedan excluidas de los procesos. La capacidad de aprender permite sustituir la intervención humana en cada vez más tareas, ya sean del ámbito laboral o profesional o del desarrollo de la vida personal. La IA y los robots no solo trabajan para nosotros sino que se traducen, seleccionan productos y conducen por nosotros.

Este fenómeno, que podría considerarse como algo positivo y deseable, sin embargo puede derivar en un empobrecimiento y una marginación de lo humano que, por el contrario, podría aprovechar las funcionalidades de la IA y de la robótica para potenciar sus capacidades y no para sustituirlas. Este planteamiento es el que subyace en la idea de complementariedad, para no centrarse solo en lo que puede hacer la IA, sino también en lo que pueden hacer las personas (creatividad, empatía, colaboración) tratando de que humanos y máquinas puedan trabajar mejor juntos (38).

Se trata de fomentar sistemas «complementarios» de IA en el ámbito del trabajo, para que personas y máquinas trabajen juntos y se fortalezcan mutuamente. Esto se consigue fomentando el aprendizaje sobre IA y la colaboración en su diseño para que se pueda comprender y aprovechar mejor la IA y el trabajador conserve suficiente autonomía y control (*human-in-command*) y mantenga la satisfacción en su trabajo.

Este planteamiento es extrapolable más allá del ámbito laboral, al uso complementario de la IA y no como sustitutivo, bajo la forma de inteligencia aumentada. Se trata de conseguir una interacción persona-máquina, de modo que la IA sirva para complementar y mejorar la actuación humana y no que los humanos simplemente deleguen sus actividades al funcionamiento de la IA.

(38) Dictamen CESE (apartado 1.11, 3.24 y 3.25)

Para esto es necesario una educación generalizada en el uso de los sistemas de IA y su manejo desde una edad temprana, con especial hincapié en los aspectos relacionados con la ética y la privacidad, para todos podamos aprovechar al máximo las capacidades de la IA sin perder las nuestras, conservando en todo momento nuestra autonomía y control sobre las máquinas (39).

6. ALGUNAS REFLEXIONES SOBRE LA UTILIZACIÓN DE LA INTELIGENCIA ARTIFICIAL POR PARTE DE LOS PODERES PÚBLICOS

Por último, conviene llamar la atención sobre la especial transcendencia que puede llegar a tener la AI cuando se incorpora a las actividades propias de los Estados, ya que implica el ejercicio de poder (público), lo que potencia su alcance y puede derivar en una grave amenaza para las personas y para la sociedad.

En el *ámbito militar,* la AI genera una especial inquietud por las implicaciones que puede tener sobre los derechos fundamentales de las personas y, en particular por su integridad. La eficacia de los avances tecnológicos en este ámbito ha quedado demostrada con el uso de los drones armados que vendrán acompañados en breve por dispositivos similares de desplazamiento por tierra o agua. Ahora bien, la cuestión no es solo el uso de robots que, en última instancia siguen estando operados por humanos aunque desvinculados del peligro, sino del uso de dispositivos que puede actuar de manera autónoma. Es lo que se ha dado en llamar técnicamente «sistemas armamentísticos autónomos letales» (más dramáticamente, *killer robots*) que están movilizando a la comunidad internacional para garantizar que respeten los derechos humanos y del Derecho internacional humanitario (40). En este sentido Naciones Unidas ha adoptado una resolución, y a nivel europeo, Euronest también se ha pronunciado (41).

En el *sector financiero* la IA está dando lugar a un cambio revolucionario con el fenómeno denominado Fintech, al que contribuyen otras innovaciones que se incorporan de forma interrelacionada como el big data y el blockchain. En concreto la IA está sirviendo para extraer patrones significativos a partir de datos sobre mercados, socios, empleados y cliente e interpretarlos con fines concretos como la definición de productos y la segmentación de clientes, aunque también para garantizar el cumplimiento de la normativa y la gestión de riesgos y detección de fraudes. Lo que no cabe

(39) Dictamen CESE (apartado 3.27)

(40) Este preocupación puede contemplarse en el llamamiento de Human Rights Watch, o la carta presentada en la *International Joint Conference on Artificial Intelligence* (IJCIA) celebrada en Melbourne en agosto de 2017.

(41) Resolución de la Asamblea Parlamentaria Euronest sobre los sistemas armamentísticos autónomos letales (2018/C 99/02) (DOUE de 15 de marzo de 2018, C 99/3).

duda es que, en un sector caracterizado precisamente por el desarrollo de un enorme número de transacciones expresadas en cifras, la influencia de la IA será un creciente dominio hasta convertirse en un elemento estructural esencial, del mismo modo que ahora lo son los elementos informáticos. Además se trata de un fenómeno que no se limita a los bancos y aseguradora, sino los propios organismos reguladores y supervisores están recurriendo a sistemas de IA para mejorar la supervisión financiera. Con respecto a este proceso, la Comisión de Estabilidad Financiera se muestra cautelosa señalando que deben sopesarse las ventajas e inconveniente en función de que se cuente con un mayor experiencia y se disponga de más datos (42). En concreto se han identificado un conjunto de ventajas ya que la IA ayudará al sector financiero a reducir costes, mejorar su rentabilidad y ampliar la gama de opciones de sus clientes a la vez que se garantiza mayor seguridad gracias a la mejora en el cumplimiento normativo o la detección del fraude y el lavado de dinero; aunque también señala riesgos para la estabilidad financiera derivados de las dificultades para regular, interpretar y auditar los métodos de IA, a lo que se suma una mayor interdependencia entre las entidades que hagan uso de esta tecnología y la dependencia del sector de empresas tecnológicas que escapan al control de los reguladores.

Por último está el problema de los sesgos que incorpora la IA y que puede tener graves consecuencias cuando se proyecta en el ejercicio de las funciones públicas. Así se han identificado experiencias en las que la utilización de IA para el desarrollo de programas sociales en los EEUU ha estigmatizado a determinados segmentos de la población (afroamericana, sin recursos) a la hora de identificar, por ejemplo, posibles supuestos de maltrato infantil (43). Esto ha dado lugar a cuestionar el alcance de la impronta que tienen los programadores sobre la IA que pueden llevar a perpetuar o amplificar determinados prejuicios. Esto resulta relevante en supuestos en los que se utiliza la IA pudiera utilizarse para identificar las posibilidades de reincidencia de un condenado, tal y como ocurre en los EE. UU. en los que se utilizan este tipo de instrumentos como instrumento complementario para la adopción de decisiones en su política penitenciaria (44).

Cuando estos algoritmos sean utilizados efectivamente por la administración, la transparencia y la rendición de cuentas deberá ser extrema para evitar la discriminación a través de sesgos basados en raza, género, religión o la más común, pobreza.

---

(42) Financial Stability Board (2017), *Artificial intelligence and machine learning in financial services: Market developments and financial stability implications*, 1 de noviembre de 2017.

(43) Virgina Eubanks (2018), *Automating Inequality, op. cit.*

(44) Como se refleja en el artículo «Are programs better than people at predicting reoffending?», *The Economist*, 17 de enero de 2018, que llega a la conclusión de que, a día de hoy, la capacidad de identificar a reincidentes sobre la base de unas variables limitadas (edad, sexo, condena actual y antecedentes penales) es igual entre un programa de IA (COMPAS) y personas sin formación especializada.

CAPÍTULO 9

EL DERECHO DIGITAL A PARTICIPAR EN LOS ASUNTOS PÚBLICOS: REDES SOCIALES Y OTROS CANALES DE EXPRESIÓN

EDUARDO GAMERO CASADO
Catedrático de Derecho Administrativo
Universidad Pablo de Olavide, de Sevilla

1. INTRODUCCIÓN

Las redes de telecomunicación representan un interesante canal para potenciar la participación de la ciudadanía en los asuntos públicos. Cabe articular diferentes plataformas o canales mediante los que se facilite el ejercicio de la democracia directa y se conceda a la ciudadanía la posibilidad de pronunciarse sobre asuntos públicos o de colaborar en el desempeño de las funciones públicas. En particular, el uso de las redes sociales supone una realidad amplísimamente implantada en la sociedad contemporánea, que se presta a los más variados fines y que interesa al Derecho desde muy diversas perspectivas (1).

(1) Véase un enfoque transversal del tema en RALLO LOMBARTE, A. y MARTÍNEZ MARTÍNEZ, R. (Coords.): *Derecho y redes sociales*, Civitas Thomson Reuters, Cizur Menor, 2010.

En este trabajo se pretende explorar el rendimiento de las iniciativas que han tenido lugar hasta la fecha para potenciar la participación ciudadana por medios electrónicos y especialmente mediante las redes sociales. No se aborda el estudio específico del voto electrónico en procesos electorales propiamente dichos, por tratarse de una materia en la que existe mayor acervo y cuyas coordenadas también se encuentran mejor perfiladas en la actualidad (2).

Partimos de la conveniencia de estimular la participación por medios electrónicos como refuerzo de la democracia y del llamado Gobierno abierto (3). Pero al mismo tiempo, deseamos advertir de los peligros que encierran estos medios, que pueden conducir a una distorsión del juego de las mayorías y, por consiguiente, a un debilitamiento de la democracia, en lugar de a su fortalecimiento.

2. LA ARTICULACIÓN ACTUAL DE LA PARTICIPACIÓN CIUDADANA A TRAVÉS DE LAS REDES SOCIALES

En la actualidad existen numerosas iniciativas de las Administraciones públicas para promover la participación de la ciudadanía en los asuntos públicos. Los cauces por los que canalizar esta participación son muy variados; Deligiaouri destaca (4): a) Comunicación por correo-e; b) Participación en blogs políticos; c) Consulta de páginas web de contenido político, como las que mantienen los partidos y organizaciones políticas (si bien no-

(2) Para conocer estudios específicos sobre esa cuestión pueden consultarse los trabajos que se incluyen en Cotino Hueso, L. (coord.): *Democracia, participación y voto a través de las nuevas tecnologías*, Comares, Granada, 2007; Barrat Esteve, J. y Fernández Riverira, R.M. (coords.): *Derecho de sufragio y participación ciudadana a través de las nuevas tecnologías*, Civitas Thomson Reuters, Cizur Menor, 2011; Bermejo Latre, J.L. y Castel Gayán, S. (eds.): *Transparencia, participación ciudadana y administración pública en el siglo* xxi, monografía XIV de la *Revista Aragonesa de Administración Pública*, Instituto Aragonés de Administración Pública, Zaragoza, 2013; y Barrat, J. (Coord.): *El voto electrónico y sus dimensiones jurídicas: entre la ingenua complacencia y el rechazo precipitado*, monográfico de la *Revista General de Derecho Público Comparado*, n.º 13, 2013. La situación (jurídica) de la cuestión no ha variado significativamente desde que fue analizada en estas obras.

(3) Aparte de las aportaciones sobre la materia contenidas en las obras citadas en la nota anterior, pueden verse también Ramos Vielba, I. y Campos Domínguez, E. (eds.): *Democracia en 3D: Democracia digital deliberativa*, Edhasa, Barcelona, 2012; Deligiaouri, A.: «A critical appraisal of forms, features, factors and variables of democratic e-participation with a focus on social media», *Revista D'Internet, Dret i Politica*, n.º 2, 2015, pp. 50 y ss.; así como la tesis doctoral de Vela Navarro-Rubio, R.: *El parlamento abierto. La influencia de la tecnología en la evolución parlamentaria*, 2015 (publicada con fecha de 2017 en el repositorio electrónico de la Universidad Complutense de Madrid), especialmente pp. 166 y ss., dedicadas a la aplicación del «gobierno electrónico» a las Administraciones públicas; Karakiza, M.: «The impact of Social Media in the Public Sector», *Procedia. Social and Behavioral Sciences*, n.º 175, 2015, pp. 384 y ss.; Aguirre Sala, J.F.: «Nuevos alcances de la participación ciudadana a través de las redes sociales», *Culturales*, Época II, vol. I, n.º 2, 2013, pp. 119 y ss.; Garrán Díaz, J.: «Ciudadanía y participación por medios electrónicos. Un future incierto», *Cuadernos de Derecho Local*, n.º 46, 2018, pp. 357 y ss.; y Martínez Alfaro, M.: «E-participación. Nuevas formas de entender la participación ciudadana en el ámbito de las políticas públicas y en el Sistema democrático», 2016 (accessible en http://www.fes-sociologia.com/files/congress/12/papers/3313.pdf).

(4) Véase Deligiaouri, A.: «A critical appraisal…», *op. cit.*, pp. 54 y ss.

sotros pensamos que la mera consulta de webs no constituye participación propiamente dicha); d) Participación en discusiones políticas en línea; e) Participación en consultas (informales) en línea; f) Participación en referéndums en línea; g) Presentación de peticiones electrónicas (procesos colectivos de recopilación de firmas para adhesión a una concreta causa).

En cuanto al caso específico de las redes sociales y asimilados existen cada vez más iniciativas, especialmente en las entidades locales (5). Tenemos, por un lado, el recurso a aplicaciones y medios disponibles con carácter generalizado para los usuarios de las TICs, y que no han sido, por tanto, diseñados *ad hoc* para soportar estos procesos. Esta apuesta es positiva en la medida que los usuarios se encuentran familiarizados con el entorno y no requieren nuevos procesos de alta o autenticación. En contrapartida, ofrecen escasas funcionalidades y muy pocas garantías, como hemos de ver en el apartado siguiente.

En el entorno de las redes sociales es el destacado caso de Facebook, que se puede utilizar por las instituciones públicas para recabar la opinión de los usuarios acerca de cuestiones relacionadas con el funcionamiento de los servicios públicos; la participación puede tener lugar mediante publicaciones en un muro que se difunden o comparten por conocidos, a través de comentarios y respuestas o simples *likes* (icono del pulgar arriba o abajo) a las publicaciones que se realicen por la entidad, o mediante la creación de grupos y eventos específicos creados desde la propia herramienta.

En el mismo ámbito se encuentra Twitter, que puede emplearse institucionalmente como cauce para recibir sugerencias y quejas: por ejemplo, solicitar la reparación de un desperfecto en la vía pública. Esta red social también admite la posibilidad de realizar encuestas o consultas, y el uso de *hashtags* permite que se susciten debates en torno a temas concretos.

La plataforma Change.org se encuentra específicamente orientada a la articulación de iniciativas ante los poderes públicos amparadas en adhesiones de los usuarios. Se configura como una herramienta de petición de firmas para apoyar causas de finalidad cívica. El promotor es, por tanto, un ciudadano, pero la finalidad primordial es lograr una actuación de los poderes públicos en una materia concreta.

---

(5) Sobre esta particular cuestión así como las iniciativas articuladas para la participación política en este ámbito *vid.* especialmente Pagán Martínez, M., y Almonacid Lamelas, V. «Gobierno abierto: ejercicio del derecho de acceso a la información y participación 2.0. Cuando la firma no es necesaria», *El Consultor de los Ayuntamientos*, n.º 5-2015, pp. 592 y ss.; Turro, P.: «Las redes sociales como espacio de participación ciudadana», 17/03/2017 https://www.iebschool.com/blog/participacion-ciudadana-en-redes-sociales/; y Aguirre Sala, J.F.: «Nuevos alcances…», *op. cit.*, pp. 119 y ss. Por lo que particularmente respecta a las iniciativas aglutinadas bajo la etiqueta de *Smart cities* véase en especial Cantó López, T.: «Administración pública y participación activa del ciudadano en la gestión de la ciudad inteligente», en Piñar Mañas, J.L. (Dir.): *«Smart cities». Derecho y técnica para una ciudad más habitable*, Dykinson, Madrid, 2017, pp. 33 y ss.

Por último, la amplia implantación de WhatsApp está llevando también a articular canales de participación ciudadana basados en esta aplicación. Es utilizado por algunas entidades públicas como canal directo de comunicación con la ciudadanía, si bien no permite diseñar procesos transparentes de participación ciudadana mediante la presentación de opiniones públicas o mecanismos de voto.

Pero existen, por otra parte, plataformas institucionales específicas para articular los procesos de participación ciudadana, especialmente en las entidades locales. Destaca el caso de «Decide Madrid» (https://decide.madrid.es), una ambiciosa plataforma que aglutina los siguientes servicios, para cuyo uso es preciso registrarse previamente:

a) Debates. Son foros sobre temas de discusión planteados directamente por los ciudadanos. Las opiniones pueden valorarse **con** *likes* **y** *unlikes* (acuerdo o desacuerdo).

b) Propuestas. Es un cauce de presentación de iniciativas por parte de los vecinos sobre materias de competencia municipal. La particularidad de esta utilidad es que si una propuesta alcanza al menos el apoyo del 1% de los vecinos con derecho a voto (27.662 apoyos de personas mayores de 16 años empadronadas en Madrid), necesariamente habrán de someterse a votación (apartado siguiente), cuyo resultado se considera vinculante.

c) Votaciones. Esta sección se activa cada vez que una propuesta supera el 1% de apoyos del censo, o bien cuando el Ayuntamiento plantea de oficio un tema para que los vecinos se pronuncien. Pueden votar las personas empadronadas mayores de 16 años, y los resultados son vinculantes para el gobierno municipal.

d) Procesos: En esta sección la ciudadanía puede participar en la elaboración y modificación de normativa de la ciudad de Madrid y dar su opinión sobre políticas municipales.

En la misma tónica cabe situar la plataforma «Decide Sevilla» (https://www.sevilla.org/DecideSevilla/), puesta en marcha por el Ayuntamiento de esta ciudad para articular tres tipos de actuaciones: consultas (votaciones), opiniones y propuestas. El uso de cualquiera de estos servicios exige alta previa como usuario. En los dos últimos casos se obtiene una contraseña de acceso que permite participar en todos los temas que se vayan planteando o formular cuantas solicitudes se tengan a bien. En el caso de las consultas, se obtienen además unas claves mediante las que se puede ejercer el derecho al voto (desde cada teléfono se pueden solicitar tres claves, para tres personas distintas, con sus correspondientes DNIs). Las actuaciones que se pueden implementar mediante «Decide Sevilla» son las siguientes:

a) Consultas. Se trata de votaciones sobre cuestiones relativas a la ciudad. Exige el alta previa como usuario, si bien desde cada teléfono móvil se pueden solicitar hasta tres altas distintas.

b) ¿Y tú que opinas? Es un espacio en el que los ciudadanos pueden aportar opiniones sobre diferentes temas o iniciativas municipales, en un tono informal: la accesibilidad en el espacio público, los diferentes planes de actuación que se pretendan implementar, nuevos reglamentos y ordenanzas locales, etc. No incorpora procesos de votación, limitándose a facilitar la participación en los asuntos públicos mediante la expresión de simples opiniones.

c) Haz tu propuesta. Es un canal de presentación de solicitudes, en ejercicio del derecho constitucional de petición, sobre cualquier cuestión que los vecinos consideren de interés.

Ante todas estas iniciativas es oportuno recordar la advertencia realizada por el Defensor del Pueblo Andaluz en relación con el régimen jurídico aplicable a las iniciativas de participación ciudadana por medios electrónicos, puntualizando que, para su plena adecuación a Derecho (y despliegue de los oportunos efectos jurídicos), deben canalizarse por los medios establecidos en la legislación vigente: las Leyes 30/1992 y 11/2007, cuando se pronunció esta Institución; y las Leyes 39/2015 y 40/2015 en la actualidad, por lo que, de no reunir el canal (la red social) los requisitos legales, la iniciativa no da lugar a la incoación de un procedimiento administrativo (6). Al mismo tiempo, el Defensor del Pueblo Andaluz resalta que las Administraciones públicas están siempre sometidas a Derecho, y cuando articulan estos canales de participación deben regular expresamente su funcionamiento, para que los ciudadanos tengan claras las disposiciones que se les aplicarán y el régimen que se seguirá en los procesos que se desarrollen mediante el correspondiente canal.

3. LA DISTORSIÓN DE LAS MAYORÍAS EN LAS REDES SOCIALES

Aunque, tal y como ya se ha dicho, inicialmente se abrazó con entusiasmo la participación de la ciudadanía en los asuntos públicos por medio de las TICS, siempre han existido voces que han advertido la necesidad de precaverse frente a ciertos aspectos o elementos disfuncionales presentes

(6) Véase el Informe del Defensor del Pueblo Andaluz correspondiente a 2012, pp. 69 y ss., donde expone el caso de un Ayuntamiento que había articulado un cauce de consulta y participación ciudadana a través de Facebook. Un vecino planteó por ese medio una solicitud de mejora de las instalaciones deportivas, que consideró indebidamente respondida, perseverando en sus quejas, lo que condujo a que el administrador le excluyera del foro. El Defensor del Pueblo Andaluz señala, por una parte, que la petición presentada por el ciudadano no se canalizó por los medios previstos en la legislación administrativa, por lo que no merece el calificativo de solicitud propiamente dicha, y por consiguiente no se le deben aplicar las exigencias predicables de los procedimientos administrativos en sentido estricto (y las correlativas exigencias aplicables a su resolución).

en el uso de estos canales. Un reciente inventario de problemas y factores que influyen decisivamente en la participación por estos medios ha sido formulado por Deligiaouri, quien identifica esencialmente los siguientes (7): 1) La edad: el interés y participación políticos se incrementan con la edad; 2) Educación: a mayor nivel formativo, mayor participación; 3) Los «cinco grandes rasgos» de la personalidad: extraversión, afabilidad, diligencia, estabilidad emocional y receptividad; estos rasgos influyen especialmente en la decisión de intervenir o no en los debates y votaciones, sobre todo si no son anónimos; 4) Socialización política: individuos con antecedentes de debate y discusión política en la familia, la escuela u otras organizaciones, muestran un mayor grado de participación en estos procesos; 5) La brecha digital, que sigue afectando sensiblemente a la participación por medios electrónicos; dentro de este factor se incluye el análisis del nivel económico y la disponibilidad de acceso a redes. Por su parte, la misma autora identifica una serie de factores institucionales (no personales de los individuos) que influyen en el nivel de participación: 1) El papel del administrador en la gestión del debate: cuando puede suprimir opiniones o mensajes, se produce un descenso de la participación; 2) La funcionalidad del medio o plataforma es crucial para estimular la participación, en particular cuando permite intervenir por diferentes vías (texto, fotos, hipervínculos…); según la autora (y la literatura científica que cita), ello puede explicar el éxito de Facebook; 3) La cantidad de información disponible para documentarse sobre el debate: paradójicamente, cuando es mucha, también disuade de intervenir.

De entre todos estos factores, y por lo que particularmente respecta a la participación mediante las redes sociales, hace ya tiempo que se viene advirtiendo la distorsión que supone aceptar acríticamente los resultados o posiciones aparentemente mayoritarias de los procesos participativos por medios electrónicos y en especial de los canalizados mediante las redes sociales. Por ejemplo, Cotino señala lo siguiente (8):

> «hay que alertar del peligro de la supra o sobre representación de sectores más allá de su importancia real. No debe descuidarse el particular perfil de los usuarios de las nuevas tecnologías, así como la probablemente especial

(7) *Vid.* Deligiaouri, A.: «A critical appraisal…», *op. cit.*, pp. 56 y ss. La autora sustenta sus posiciones con bibliografía específica relativa a cada uno de los factores de influencia analizados.

(8) *Cfr.* Cotino Hueso, L.: «Tratamiento jurídico y normativo de la democracia, participación y transparencia electrónicas: presente y perspectivas», en Barrat i Esteve, J. y Fernández Riveira, R.M. (coords.): *Derecho de Sufragio y Participación ciudadana a través de las Nuevas Tecnologías*, Civitas-Instituto de Derecho Parlamentario Universidad Complutense, Cizur Menor (Navarra), 2011, pp. 217 y ss. El autor, que viene sosteniendo esta posición desde 2003 en diferentes trabajos, cita en apoyo de su tesis, además de los Informes periódicos de la Fundación Telefónica sobre el uso de la red, el trabajo de Previte, J.; Hearn, G. y Dann, S.: «Profiling Internet Users' Participation in Social Change Agendas: An Application of Q-Methodology», Faculty of Business, Queensland University of Technology, disponible en http://arxiv.org/abs/cs/0109058 (última visita: 29 de febrero de 2015).

> idiosincrasia del participante a través de las nuevas tecnologías, puesto que es más que posible que en modo alguno reproduzca transversalmente el perfil del cuerpo social. En este punto, no está de más recordar el fenómeno de los *frikis* de Internet o *geeks,* usuales participantes de la web 2.0. Como se ha dicho, puede considerarse que hay unos de diez millones de participantes y generadores de contenidos en España, por ello, me permito alertar de que en la evolución de las fórmulas de democracia y participación electrónicos no se ha de caer en el error de dotar de sobre representación o particular legitimación a los participantes por medio de las TICs. Además, no ha de perderse de vista que en todo proceso participativo, el perfil más activo de los participantes suele corresponder con las posiciones más polarizadas y dotar a su participación de especial significación puede suponer infravalorar las posiciones mayoritarias y más moderadas.»

Tal y como advierte la doctrina más autorizada, no existen instrumentos fiables para elaborar predicciones o interpretaciones derivadas de las opiniones vertidas en las redes sociales (9), y cuando se han analizado los resultados electorales, no se corresponden con las predicciones que cabría deducir de lo expresado en ellas (10). Lo cual no significa que se deba rechazar a las tecnologías de la información en general y a las redes sociales en particular como instrumentos de opinión y de participación ciudadana: no se trata, necesariamente, de una mayoría silenciosa, pero sí es obvio que existe un *silencio mayoritario* –el porcentaje de ciudadanos que no intervienen en los debates rebasa ampliamente al que lo hace–, y de lo que se trata es de saber interpretar ese silencio, o dicho a la inversa, de articular instrumentos de medida que permitan averiguar hasta qué punto la opinión expresada en las redes sociales es reflejo fiel de la mayoría social.

De hecho, la influencia en la red (y de la red) es una nueva fuente de poder que recorta correlativamente la autoridad del Gobierno. Los procesos masivos de mensajes reenviados *(retwitts* y similares) que crean tendencia *(trending topics)* condicionan indudablemente la acción del Gobierno (11).

---

(9) *Vid.* Schoen, H. y otros: (2013) «The power of prediction with social media», *Internet Research*, Vol. 23, n.º 5, 2013, pp. 528 y ss.; tal y como advierten los autores: «Better understanding the predictive power and limitations of social media is therefore of utmost importance, in order to be successful and avoid false expectations, misinformation or unintended consequences. Today, current methods and techniques are far from being well understood, and it is mostly unclear to what extent or under what conditions the different methods for prediction can be applied to social media».

(10) Como elocuente ejemplo, *vid.* Gayo Avello, D.; Metaxas, P.T. y Mustafaraj, E.: «Limits of Electoral Predictions Using Twitter», Actas de la Fifth International AAAI Conference on Weblogs and Social Media, accessible en http://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/view/2862 (última visita: 28 de febrero de 2015). Los autores demuestran que el resultado de las elecciones al Congreso de los Estados Unidos de 2010 no se correspondieron con lo que cabía predecir del análisis de los datos de Twitter.

(11) Al respecto, puede verse Fernández Torres, M.J. y Paniagua Rojano, F.J.: «El poder de las redes sociales en la política y en los movimientos sociales», en Cotarelo García, R. y Crespo Martínez, I. (coords.): *La comunicación política y las nuevas tecnologías*, Los Libros de la Catarata, Madrid, 2012, pp. 130 y ss.

Pero carecen, sin embargo, de legitimidad democrática, no sólo porque quienes los promueven no han sido elegidos en sufragios universales, libres, directos y secretos, sino también porque quienes les siguen no son necesariamente grupos representativos de las mayorías reales, y sobre todo, porque se han desarrollado herramientas tecnológicas mediante las que se manipulan los debates y se influye decisivamente en los resultados: por un lado, los algoritmos que las propias plataformas desarrollan para orientar los debates, haciendo prevalecer unas opiniones sobre otras, influyendo de manera opaca en los sucesivos posicionamientos; y por otro, prácticas maliciosas de terceros, que irrumpen en los debates artificialmente y manipulan las aparentes mayorías, como sucede con el empleo de *trolls* u ordenadores y cuentas *zombis,* que replican cientos o miles de veces una opinión o información intoxicada mediante la cual se pervierte todo el debate.

Aunque estas circunstancias se intuían hace ya años, actualmente las críticas se han agudizado, a raíz de diferentes sucesos que han puesto claramente de manifiesto las manipulaciones a que se presta la opinión pública en las redes sociales como consecuencia de prácticas maliciosas, siendo recurrentes los ejemplos de *fake news* y la interferencia de diferentes actores, como el Gobierno ruso, en procesos electorales de todo el mundo (la elección de Donal Trump, el *Brexit,* la consulta sobre la independencia de Cataluña, etc.) (12).

Por lo que se refiere a los cauces electrónicos institucionales de participación ciudadana, la crítica generalizada ha sido su escaso éxito, al no lograr niveles significativos de votantes. Así, la consulta realizada por «Decide Madrid» para la remodelación de la Plaza de España, solo logró la participación de 26.686 vecinos, esto es, un 1% de los madrileños con derecho a voto (2,6 millones). En el caso de «Decide Sevilla» los datos de la única consulta que se ha realizado son un poco mejores, pero en todo caso descorazonadores: de los 588.000 ciudadanos que podían participar (vecinos mayores de 16 años), sólo lo hicieron 40.659, es decir, un 6,91%. En este caso se da además la paradoja de que, si bien la mayoría de votantes (25.133 personas, esto es, el 61,8% de los votos emitidos) lo hizo a favor de modificar el calendario de la Feria de Abril, en el barrio donde se asienta el Real de esta fiesta la participación fue más alta que la media (11,54%), pero el resultado de la votación negativo (63% de votos en contra), lo cual representa una nueva manifestación de las contradicciones que venimos resaltando, pues quienes se ven más directamente afectados

(12) Véanse, entre otros, Tucker, J.A.; Theocharis, Y.; Roberts, M. y Barberá, P.: «From Liberation to Turmoil: Social Media and Democracy», *Journal of Democracy,* n.º 28-4, 2017, pp. 46 y ss.; Chakrabarti, S.: «Hard Questions: What Effect Does Social Media Have on Democracy?», 22/01/2018 (https://newsroom.fb.com/news/2018/01/effect-social-media-democracy/); y Vromen, A.: «Is Social Media Good or Bad for Democracy?», publicado en el «Newsroom» de Facebook el 25/01/2018 (https://newsroom.fb.com/news/2018/01/vromen-democracy/).

por la medida, no son quienes ven satisfecha su voluntad, y ello, a pesar de haber participado más numerosamente en la consulta.

4. CONSECUENCIAS: ¿CÓMO ARTICULAR LA PARTICIPACIÓN CIUDADANA EN LOS ASUNTOS PÚBLICOS A TRAVÉS DE LAS REDES SOCIALES?

La primera medida a reclamar para la implementación de medios de participación ciudadana en los asuntos públicos a través de las redes sociales es la previa regulación normativa de todos los aspectos relativos a la puesta en marcha de la iniciativa, servicios implementados, régimen de altas de los usuarios, régimen y funciones del administrador del sistema, procedimiento a seguir a lo largo del proceso participativo, y eficacia jurídica que alcanzará su resultado. A pesar de la aparente obviedad que supone la necesidad de disponer de normas jurídicas que regulen todo esto, se trata de una exigencia escasamente percibida por los actores que se vienen ocupando de la materia (13), siendo así, en cualquier caso, que existen ya precedentes de disposiciones que regulan la participación ciudadana y aluden de alguna manera a los canales electrónicos, aunque todavía con muy escasa intensidad en comparación con la implantación real que tienen estas iniciativas.

No se trata de aprobar una mera guía o protocolo de actuación, o de adoptar un mero acuerdo (político) de implementación de un sistema: a mi juicio, puesto que está en juego el ejercicio de las competencias atribuidas a la Administración, la articulación de todos estos canales de participación requiere de una norma que previamente establezca su marco jurídico. Habida cuenta que los principales promotores de estos cauces de participación son las entidades locales, entiendo que se debería dictar una Ordenanza reguladora de la participación ciudadana por medios electrónicos.

Por lo reciente de su aprobación, conviene referirse a la Ley 7/2017, de 27 de diciembre, de participación ciudadana de Andalucía (LPCA), aunque se encuentre actualmente en *vacatio legis* (entrará en vigor el 05/01/2019, a los 12 meses de su publicación en el *BOJA).* Su Título VI lleva por rúbrica «Sistema público de participación digital». En particular, conviene reproducir su artículo 65, que dispone:

> Artículo 65. *Sistema público de participación digital.*
>
> 1. La Administración de la Junta de Andalucía creará un sistema público de participación digital para la puesta en marcha de los procesos contenidos en esta ley.

(13) Es excepción Cotino Hueso, L.: «Derecho y *Gobierno abierto…*», *op. cit.*, pp. 65 y ss., quien insiste en la necesidad de regular formalmente la participación de la ciudadanía por medios electrónicos.

2. El centro directivo competente en materia de dirección, impulso y gestión de la política digital en lo concerniente a las nuevas tecnologías aplicadas al gobierno abierto asumirá las funciones, con carácter transversal para la Administración de la Junta de Andalucía, de dirección técnica y desarrollo de las plataformas de participación ciudadana basadas en el uso de las tecnologías de la información y la comunicación (TIC) necesarias para la materialización del derecho a la participación ciudadana, en el marco de lo establecido en la presente ley.

3. Dicho sistema contará con el desarrollo de una plataforma de participación, en software libre, provista de herramientas y funcionalidades que cubran las necesidades informativas de deliberación, de voto y de seguimiento de las iniciativas a las que dé soporte.

4. El método de autenticación garantizará que cada persona usuaria registrada corresponda efectivamente con algunos de los sujetos previstos en el artículo 6, asegurando el cumplimiento de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

5. El portal de la Junta de Andalucía será el punto de acceso general a las plataformas web de participación ciudadana.

6. El centro directivo proponente del proceso participativo asumirá la gestión del propio proceso en cualquiera de las plataformas de participación desarrolladas de acuerdo con lo establecido en el presente artículo.

7. La Administración de la Junta de Andalucía facilitará el acceso al sistema público de participación digital en edificios y dependencias públicas, contando con unidades móviles a fin de acercar a toda la ciudadanía en igualdad de condiciones el uso de estos instrumentos de participación.

Es interesante que la plataforma se suministre por la Administración autonómica, no ya solo por razones de eficiencia del gasto, sino también para preservar las garantías que este tipo de herramientas deben reunir.

La Ley no sólo es de aplicación a la Administración de la Junta de Andalucía y sus entidades instrumentales, sino también a la Administración local andaluza (art. 3). Define los siguientes procesos de participación ciudadana (art. 12), todos ellos necesariamente en el ámbito propio de cada Administración promotora: a) Deliberación participativa; b) Participación ciudadana en la elaboración de presupuestos; c) Participación ciudadana mediante consultas populares; d) Participación ciudadana en la proposición de políticas públicas y elaboración de normas; y e) Participación ciudadana en el seguimiento y evaluación de las políticas públicas y de la prestación de los servicios públicos. Los procesos de participación se podrán desarrollar sobre los siguientes asuntos o materias, siempre que sus planteamientos no sean contrarios al ordenamiento jurídico (art. 13): a) Proposición, adopción, seguimiento y evaluación de las políticas públicas con singular impacto o relevancia; b) La elaboración de instrumentos de planificación para la determinación de políticas; c) La priorización sobre aspectos puntuales del gasto; d) La elaboración de leyes y reglamen-

tos; y e) La prestación, seguimiento y evaluación de los servicios públicos. Así, la deliberación participativa del artículo 12.a) puede tener lugar en las materias del artículo 13.a) y b); las consultas populares se pueden articular para recabar la opinión de la ciudadanía sobre cualquier asunto de la competencia propia de la Administración (con excepción del referéndum), y pueden implementar mediante los instrumentos establecidos por el artículo 26 (14). Se regula, asimismo, la iniciativa ciudadana como proceso de participación para la proposición de políticas y normas (arts. 27 y ss.), así como la participación en el seguimiento de las políticas públicas (arts. 1 y ss.), y las consultas participativas autonómicas y locales (arts. 33 y ss.), que se realizan mediante votación.

El régimen no es lo suficientemente prolijo para despejar muchas de las dudas que suscita la implementación de la participación por medios electrónicos, pero desde luego representa un importante punto de partida, y tampoco resulta razonable que una disposición de rango legal descienda a detalles que le confieran un alcance más adecuadamente reglamentario.

Dentro de los aspectos que la normativa reguladora de los procesos participativos debe contemplar, conviene destacar algunos puntos críticos.

En primer lugar, es necesario implantar algún medio de identificación, para a) Evitar que participen en el procedimiento robots o perfiles *zombies;* b) Evitar que una misma persona vote varias veces. Este tipo de restricciones tiene efectos disuasorios y reduce la participación, pero resulta imprescindible implantarlas en razón del carácter sensible del derecho que se ejerce y del impacto de un ejercicio sobre las políticas públicas, siendo preciso preservar el carácter democrático de las consecuencias a que conduzca el proceso participativo.

De otro lado, atendiendo a la *brecha digital,* para evitar la distorsión de mayorías, el canal electrónico debería ser complementario del presencial, especialmente en procesos que consistan en la votación de propues-

(14) Concretamente, los siguientes:

a) Encuestas: se realizan mediante técnicas demoscópicas adecuadas a la naturaleza o características del asunto, con el objeto de conocer la opinión de la ciudadanía.

b) Audiencias públicas: en el ámbito de esta ley, son un instrumento de consulta en el que, mediante un procedimiento oral y público, las Administraciones públicas posibilitan a las personas, entidades, organizaciones y agentes sociales relacionados o directamente afectados por una política pública ser escuchados antes de adoptar una decisión sobre el asunto que les afecta.

c) Foros de participación: son espacios de debate, creados por iniciativa de la Administración pública, que tienen por objeto debatir y reflexionar sobre los efectos de una política pública, así como elaborar análisis valorativos de los efectos reales de dichas políticas en la ciudadanía.

d) Paneles ciudadanos: son espacios de información que se crean por la Administración pública con carácter temporal y que tienen por finalidad responder a las consultas planteadas por esta sobre cualquier asunto de interés público y, en especial, sobre las expectativas de futuro de la ciudadanía.

e) Jurados ciudadanos: son grupos creados por la Administración pública que tienen como finalidad analizar los efectos de una determinada acción, proyecto o programa llevado a cabo por la misma.

f) Las consultas participativas, reguladas en el capítulo VII de la Ley.

tas, articulándose canales para el ejercicio presencial del voto, aunque sea durante un segmento temporal más reducido que el del voto electrónico. En ese sentido cabe destacar lo establecido en el artículo 65.7 de la LPCA, anteriormente transcrito.

Tenemos, por otra parte, el problema de la representatividad de los resultados alcanzados. Una primera medida que se presenta para lograr que el resultado de las consultas sea representativo es fijar un porcentaje mínimo de participación o de votos. Sin embargo, los niveles de movilización que estos procesos muestran hasta hoy son tan bajos, que esa medida no supondría en la práctica solución alguna, pues conduciría más bien a celebrar procesos sistemáticamente frustrados por los reducidos resultados de participación, siendo así, además, que cuando las iniciativas tengan mayoría a favor, su victoria supondrá siempre un factor de presión sobre la entidad promotora a pesar de que no quede avalado que esa mayoría formal responda a la real.

Más pertinente parece introducir en el proceso elementos que permitan extrapolar los resultados obtenidos al conjunto de la población. Más atrás (§ 3) hemos indicado los factores que influyen en la participación por medios electrónicos: edad, nivel económico, grado educativo, etc. Las plataformas destinadas a articular procesos participativos podrían recabar estos datos de los usuarios con ocasión del alta, a fin de poder analizar después los resultados para verificar que la muestra de votantes es representativa del conjunto electoral, pudiendo validar o extrapolar los resultados o bien no reconocerlos como suficientemente representativos. Ahora bien, a medida que se incrementa el número de datos que los ciudadanos deben suministrar para participar en plataformas o redes, se reduce el número de usuarios dispuestos a inscribirse, lo cual introduce un nuevo factor de distorsión.

Por último, parece deseable que las Administraciones públicas implementen sus propias plataformas de participación ciudadana para evitar los riesgos a que expone el uso de las redes sociales genéricas. En el caso de la LPCA, parece descartarse el uso de las redes sociales una vez el texto entre en vigor, fecha en la que se supone que estará disponible el sistema público de participación digital establecido en su artículo 65. Cuando se trate de entidades que carezcan de esta o análoga cobertura, lo deseable es dictar al menos una disposición de carácter reglamentario, y en su defecto, elaborar y publicar de manera fácilmente accesible una guía o protocolo (como sugería en su Informe el Defensor del Pueblo Andaluz), en el que se establezcan claramente todos los aspectos mencionados en el primer párrafo de este apartado, para que todos los usuarios (y los terceros) conozcan las condiciones y efectos de la actuación (pública) que se está llevando a cabo por esos medios.

CAPÍTULO 10

TRIBUTACIÓN EN UN MUNDO DIGITAL: LIMITACIONES, OPORTUNIDADES Y MODELOS POSIBLES

Marta Villar Ezcurra
Catedrática de Derecho Financiero y Tributario
Universidad San Pablo-CEU

1. INTRODUCCIÓN

Los desafíos que el mundo digital del siglo xxi plantea a la tributación y a la configuración de los sistemas nacionales de ingresos y gastos públicos, han sido objeto de atención por parte de organismos in-

ternacionales, especialmente, por la OCDE (1), la ONU (2) y la UE (3). En estos y otros foros (4) se han promovido las acciones necesarias para afrontar los problemas más urgentes y se ha puesto de manifiesto, una vez más, la necesidad de coordinar las políticas fiscales a nivel global.

En un escenario global, los problemas tradicionales asociados al fraude y a la competencia fiscal dañina (5) se han visto desbordados por fenómenos nuevos, que ponen de manifiesto la insuficiencia de los esquemas tradicionales de fiscalidad internacional y, precisamente, muchos de ellos están relacionados con el auge de la economía digital, que viene, en el terreno de las finanzas públicas y de la justicia tributaria, a agravar la situación de partida (6).

La economía digital pone en cuestión principios clásicos de la fiscalidad internacional, asentados en el principio de territorialidad y en la presunción de que la obtención de beneficios se realiza mediante una localización física (7),

---

(1) El encuentro de junio de 2016, de Ministros procedentes de 43 países de la OCDE, en Cancún, constituyó un hito en la toma de conciencia de la necesidad de promover acciones coordinadas y de incluir la transformación digital en las agendas políticas públicas, *Vid.* «*Declaración de Cancún*», sobre economía digital: Innovación, crecimiento y prosperidad social (anexo 1.A2) en: OECD, Digital Economy Outlook, 2017, OECD publishing, París, 2017. http://dz.doi.org/10.1787/9789264276284-en, pero la preocupación por la tributación de la economía digital es constatable en trabajos previos, *vid.* OCDE, *La fiscalidad del comercio electrónico: Implantación del marco tributario de la Conferencia de Ottawa*, OECD publishing, París, 2001. El Internet de las cosas, la analítica *big data*, la tecnología descentralizada *blockchain* son, junto otros, componentes clave del nuevo ecosistema digital.

(2) *Vid.* ONU, Li, J., *Protecting the Tax Base in the Digital Economy, Papers* on Selected Topics in protecting the Tax Base of Developing Countries, Paper n. 9, Junio, 2014; *The taxation of fees for technical, managerial and consultancy services in the digital economy with respect to art 21A of the 2017 UN Model*, Ginebra, 17-20 de octubre de 2017.

(3) *Vid.* Comunicación de la Comisión, «Una iniciativa europea en el sector del comercio electrónico» (COM (1997) 157 final, Bruselas, 18 de abril de 1997.

(4) La Organización Mundial de Comercio (OMC) cuenta con un Programa de trabajo sobre el comercio electrónico (WT/L/274), adoptado el 15 de septiembre de 1998, que parte del compromiso de los Estados miembros de no imponer derechos de aduana a las transacciones electrónicas. Este Programa se ha reafirmado en ulteriores Declaraciones y Decisiones Ministeriales. *Vid.* Declaración adoptada en la Segunda Conferencia Ministerial, el 20 de mayo de 1998 en Ginebra (WT/MIN(98)/DEC/2), Consejo General OCM de 30 de noviembre de 2017 (WT/GT/W/739) y Comunicación de los EEUU al Programa de trabajo con vistas a la Quinta Conferencia Ministerial de Cancún (WT/GC/W/493/REv.1).

(5) Sobre los efectos de la economía digital en la competencia fiscal local en EEUU *vid.* Agrawal, D. R., «The Internet as a Tax Haven? The Effect of the Internet on Tax Competition», 21 de septiembre de 2013, última revisión de 17 de febrero de 2017, localizable en: http:/ssrn.com/abstract=2328479.

(6) La expresión «economía digital» se utiliza del pasado siglo. Aunque es difícil de definir, hay consenso en que comprende diversos tipos de actividades, como las tiendas de aplicaciones, la publicidad en línea, la computación en la nube, los servicios de pago en línea, las plataformas participativas en red, la negociación de alta frecuencia, y el comercio electrónico. *Vid.* OCDE, *Addressing the Tax Challenges on the Digital Economy,* Action 1-2015, Final Report, OECD/G20 Base Erosion and Profit Shifting Project, OCDE, Paris, párrafo 116 y siguientes.

(7) Para más información, *vid.* el completo estudio de Collin, P. y Colin, N., *Task Force on Taxation of the Digital Economy*, que presentaron como Informe para cuatro Ministerios franceses, en enero de 2013. El Informe de 188 páginas es de acceso público y puede localizarse en: https://www.hldataprotection.com/files/2013/06/Taxation_Digital_Economy.pdf.

en el concepto de «establecimiento permanente» (8), como elemento clave para atribuir la potestad de gravar al Estado de la fuente, y en el principio de neutralidad (9).

Hoy en día, es posible –y es una realidad indiscutible y generalizada– que los negocios y actividades se desarrollen, y creen valor añadido, sin la mediación de una presencia física en una determinada jurisdicción. Las tecnologías digitales han posibilitado también la denominada «economía colaborativa» (10) y han transformado radicalmente los modelos de actividad empresarial (11), muy conscientes de la volatilidad de los nuevos estándares de negocio pluridimensionales (12).

Por ello, cuestiones como el nexo (13), las reglas de atribución de beneficios, el tratamiento fiscal de los activos intangibles (14) y los precios de transferencia, o la calificación de determinadas rentas y operaciones (15) en un entorno digital (16), se convierten en cuestiones clave a la

---

(8) Para un estudio doctrinal sobre la reformulación del concepto de establecimiento permanente, *vid.* Hongler, P. y Pistone, P., *Blueprints for a New PE Nexus to Tax Business Income in the Era of the Digital Economy Income in the Era of Digital Economy*, WU International Taxation Research Paper Series No. 2015 – 15 Working paper 20 January 2015.

(9) Como principio general, los sistemas tributarios deben minimizar discriminaciones y perseguir la neutralidad y equidad en los sectores económicos, cualquiera que sea la elección de oferta y demanda. En la revisión de los principios de la fiscalidad internacional, las instituciones de la UE han subrayado la importancia del principio de neutralidad fiscal (*vid.* Consejo de la UE, Outcome of proceedings, 5 de diciembre de 2017, (15445/17, FISC 346 ECOFIN 1092), apartado 15, p. 4).

(10) Se trata de «modelos de negocio en los que se facilitan actividades mediante plataformas colaborativas que crean un mercado abierto para el uso temporal de mercancías o servicios ofrecidos, a menudo por particulares». Desde el punto de vista tributario, la economía colaborativa plantea problemas relacionados con el cumplimiento de las obligaciones tributarias por la dificultad de identificar a contribuyentes e ingresos imponibles. *Vid.* Comunicación de la Comisión Europea *Una Agenda Europea para la economía colaborativa*, Bruselas, 2 de junio de 2016 (COM (2016) 256 final, pp. 3 y 15 y siguientes.

(11) *Vid.* Ayres, R. U., Williams, E., «The digital economy, Where do we stand?», *Technological Forecasting and Social Change*, vol. 71, Issue 4, May 2004, pp. 315-339 y Zimmermann, H-D., «Understanding the Digital Economy: Challenges for New Business Models», 2000 (https://ssrn.com/abstract=2566095 or http://dx.doi.org/10.2139/ssrn.2566095).

(12) *Vid.* OECD, *Addressing the Tax Challenges of the Digital Economy*, Action 1, 2015. Final Report, OCDE/G20 Base Erosion and Profit Shifting Project, OCDE, París, párrafos 151 y ss.

(13) Sobre este tema, en la doctrina, *Vid.* Moreno González, S., «Los desafíos fiscales de la economía digital en y después del Plan BEPS. Especial referencia al problema del nexo» en: *Tendencias y Desafíos de la Economía Digital*, Thomson Reuters Aranzadi, 2017, pp. 97-137, así como Hongler, P. y Pistone, P., *Blueprints for a New PE Nexus to Tax Business Income in the Era of the Digital Economy*, White Papers IBFD, 2015, pp. 10 y 14.

(14) La desmaterialización en la economía digital no significa que todo sea digital o virtual. Las personas siguen siendo importantes como productores y sobre todo, como consumidores, que son la fuente del *big data*. De otra parte, el suministro físico de bienes es parte importante del *e-commerce*.

(15) Un ejemplo de estas dificultades para calificar las rentas y operaciones en relación a la tributación de los pagos por servicios técnicos puede encontrarse en: Committee of Experts on International Cooperation in Tax Matters, Ginebra, 17-20 de octubre de 2017. *Tax consequences of the digitalized economy. The taxation of fees for technical, managerial and consultancy services in the digital economy with respect to art 12.ª of the 2017 UN Model* (E/C.18/2017/CRP.23).

(16) Los efectos del «soft» capital, incluyen la hibridación de mercancías y servicios, y pueden ser relevantes para las políticas que incentivan inversiones, como por ejemplo, las deducciones fiscales a la I+D+i, las reglas de contabilización de la depreciación acelerada o las ayudas a las inversiones extranjeras directas, y, en general, para todas aquellas medidas que fomentan inversiones tradicionalmente concebidas para bienes tangibles y capitales físicos con base en una jurisdicción, no para intangibles o inversiones que forman parte de un servicio que puede comprarse desde el extranjero.

hora de plantear correctamente los problemas tributarios, para poder proponer alternativas o modelos nuevos –transitorios o definitivos– que lleven a los convenientes ajustes normativos (17).

Sin embargo, las características y oportunidades del mundo digital no solo requieren reajustar los esquemas de la tributación directa, sino que también plantean problemas relacionados con la imposición indirecta, especialmente en el ámbito del impuesto sobre el valor añadido. Este impuesto desde hace tiempo ha incorporado motorizadamente reformas normativas acordes a la realidad del comercio electrónico (18), que incluyen medidas de registro y control, aunque el tiempo ha evidenciado su insuficiencia para garantizar el fundamental principio de neutralidad, que es su esencia.

Finalmente, no puede dejar de advertirse que los procedimientos de aplicación de los tributos también se han visto favorecidos por el crecimiento y generalización de las nuevas tecnologías, que, de un lado han facilitado las relaciones jurídico-tributarias Administración-contribuyente, pero, de otra parte, han puesto en entredicho los derechos a la protección de datos y a la privacidad de los obligados tributarios. En efecto, en el plano procedimental, las nuevas tecnologías han permitido a las Administraciones tributarias ser más eficaces en su función de verificar y controlar el cumplimiento de obligaciones tributarias, y han facilitado el acceso de los particulares a la información tributaria requerida para la correcta gestión de los tributos, pero no siempre la regulación jurídica o la puesta en práctica de los procedimientos de aplicación de los tributos permiten garantizar los derechos de los contribuyentes. En particular, estos problemas se plantean en los intercambios automáticos de información entre Administraciones tributarias, posibilitados por las directivas y reglamentos de la UE y los Convenios de Doble Imposición (CDI), existiendo singularidades respecto a los problemas generales como los derivados de

(17) *Vid.* sobre estas y otras cuestiones la relación de estudios publicados en el libro dirigido por Moreno González, S., *Tendencias y Desafíos de la Economía Digital*, cit. y así como el trabajo de Telecom advisory services, LLC, *The impact of taxation on the digital economy*, publicado en la colección Regulatory and Market Environment, 2016 y presentado en el ITU Regional Economic and Financial Forum of Telecommunications/ITC for Africa, Abidjan, Côte d´Ivoire, el 19 de enero de 2016.

(18) No existe una definición consensuada y universalmente aceptada de lo que es el comercio electrónico. Han abordado esta cuestión tanto la OCDE como la ONU a través de UNCITRAL/CNUDMI, la OMC y la UE. En una acepción amplia, el comercio electrónico se caracteriza por la existencia de una transacción comercial y su desarrollo a través de medios electrónicos de datos, que, como operación económica, constituye un contrato a distancia (entre ausentes) con inexistencia de interacción física entre las partes, sobre productos digitales o tangibles. La Comisión Europea ha propuesto medidas para mejorar el entorno del IVA para el comercio electrónico en la UE con objeto de facilitar a los consumidores y a las empresas, en particular a las empresas emergentes y a las pymes, la compra y la venta de bienes y servicios en línea, mediante la creación de una «ventanilla única», esto es, un portal para los pagos del IVA en línea en toda la UE. *Vid.* el documento de la Comisión Europea, *Modernising VAT for e-commerce: Question and Answer*, *Brussels*, *5 December 2017*, localizable en: europa.eu/rapid/press-reease_MEMO-16-3746_en.htm.

la insuficiencia del derecho de audiencia, así como de las garantías de seguridad y privacidad de los datos en un entorno digital (19).

Este es, en apretada síntesis, el contexto tributario internacional en el que la economía digital se inserta, y desde el cual este trabajo se plantea, con el objeto de abordar cuáles son los límites, oportunidades y modelos posibles para la tributación en un mundo digital.

2. ACCIONES INTERNACIONALES PARA EL ESTABLECIMIENTO DE UN NUEVO ORDEN INTERNACIONAL EN TORNO A LA ECONOMÍA DIGITAL

En la actual economía digital se diluyen las fronteras geográficas y se hace más compleja la atribución de actividades y rentas a una determinada jurisdicción fiscal. Las plataformas digitales ostentan el monopolio de las redes ante los problemas de coordinación de los usuarios y conectan diferentes actores, siendo las estrategias de fijación de precios independientes de las posibilidades de las plataformas. Empresas multinacionales como Amazon, Microsoft, Google, Apple o Facebook han transformado y siguen transformando los modelos de negocio. Estas compañías obtienen más que significativos beneficios con una fiscalidad reducida, sobre la base de estructuras de planificación fiscal, que se han considerado «agresivas», y a lo que se ha reaccionado con acciones diversas y con un nuevo arsenal normativo unilateral o concertado. Entre estas acciones, ha destacado la aplicación por parte de la Comisión Europea del régimen de ayudas de Estado incompatibles con el mercado interior (20).

En los últimos años, los organismos internacionales han centrado sus esfuerzos en poner freno a las estrategias de planificación fiscal agresiva de determinadas empresas multinacionales, que incluyen, específicamente, acciones relacionadas con el mundo digital. Aunque mucho se ha logrado ya, hasta la fecha, no se ha conseguido el necesario consenso global ni en el ámbito de la OCDE ni de la UE [pese al Plan BEPS (21) y sus Ac-

(19) Con la expansión del uso de las TIC, empresas y ciudadanos se enfrentan a mayores riesgos de seguridad y privacidad de sus datos, fraude online y los asociados al crecimiento del comercio electrónico, lo que requiere de estrategias y normas apropiadas para incorporar medidas preventivas y correctivas (seguridad digital), así como códigos de buenas prácticas. Respecto del derecho a la protección de los datos personales conviene citar el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, así como con la Directiva 95/46/CE del Parlamento Europeo y del Consejo.

(20) *Vid.* Artículo 107 del Tratado de Funcionamiento de la Unión Europea (TFUE) y las Decisiones de la Comisión Europea al respecto, entre otras, la de 4 de octubre de 2017, para el caso *Amazon,* en la que se declara la existencia de una ayuda de Estado por parte de Luxemburgo en la aplicación del *tax ruling* de 6 de noviembre de 2003.

(21) *Base Erosion and Profit Shifting.* Impulsado por la OCDE y el G-20, este Plan de acción publicado en 2013, pone énfasis como primera acción (Acción 1) en cómo abordar los desafíos de la economía digital, planteamiento que se desarrolla en un extenso informe publicado en el año 2014, cuyas conclusiones aparecen recogidas en un informe final de octubre de 2015.

ciones (22)], para solventar los problemas detectados, por lo que los países están adoptando medidas unilaterales para defender su recaudación [como el impuesto inglés sobre los «beneficios desviados», al que se ha sumado Australia, a finales de 2015, estableciendo una cláusula antiabuso, o la conocida como «tasa google» francesa, declarada inconstitucional (23)], que en ocasiones provocan fenómenos de doble imposición o doble no imposición (24) y que han recibido, sobre todo desde un punto de vista político, importantes críticas. Por esta razón, una vez identificados los rasgos de la economía digital (25) como paso previo a la determinación de sus efectos tributarios, recientemente, las instituciones de la UE han llamado a una acción global y a una estrategia europea sobre la base de abordar a corto y medio plazo los temas más urgentes (26).

Todas las instituciones de la UE y otros organismos internacionales coinciden en reconocer que el mayor desafío de todos es la reforma y la adaptación del marco fiscal internacional a la economía digital. En efecto, las bases sobre las que se asienta la fiscalidad internacional se diseñaron a principios del siglo XX y se plasman en reglas obsoletas que casan mal con las actuales actividades comerciales, hoy en día globalizadas y digitalizadas.

Un principio básico de la tributación societaria es que los beneficios han de gravarse donde se crea el valor añadido. Sin embargo, en un mundo

(22) OCDE/G20, *Addressing the Challenges of the Digital Economy, Action 1 – 2015 Final Report*. La acción 1 de BEPS ha identificado como rasgos característicos los siguientes: la movilidad de activos intangibles, usuarios y funciones comerciales, el uso masivo y utilidad de los datos para mejorar productos y servicios, los efectos de red, la utilización de modelos de negocios pluridimensionales, la tendencia hacia el monopolio u oligopolio en determinados modelos de negocio y su volatilidad.

(23) El *Diverted Profits Tax* se introdujo en Reino Unido por la *Finance Act* de abril de 2015, para gravar al 25% los beneficios de las compañías multilaterales que desvían desde el Reino Unido sus beneficios hacia territorios de baja tributación, con dos presupuestos imponibles: la realización de operaciones sin sustancia económica y la práctica que evita la existencia de establecimiento permanente. *Vid.* Rodríguez Márquez, J., «El impuesto sobre beneficios desviados (*Diverted Profits Tax*)», en Moreno González, S., *Tendencias y Desafíos Fiscales*, cit., pp. 487-516.

(24) Conviene destacar lo que se conoce como «asimetría híbrida», que se refiere a la situación existente entre el contribuyente de un Estado miembro y una empresa asociada de otro Estado miembro, o bien un mecanismo estructurado entre participantes de distintos Estados miembros, cuando el siguiente resultado es atribuible a diferencias en la calificación jurídica de un instrumento o entidad financieros: a) una deducción del mismo pago, o de los mismos gastos o pérdidas, tanto en el Estado en el que se origine el pago, se generen los gastos o se hayan sufrido las pérdidas, como en otro Estado («doble deducción»), o b) una deducción de un pago en el Estado en el que tiene su origen el pago sin la correspondiente inclusión a efectos fiscales de dicho pago en el otro Estado («deducción sin inclusión»).

(25) Son ocho los «vectores de la transformación digital» identificados por la OCDE, incluidas las economías de escala o la importancia de las fuentes de valor intangibles, que pueden generar nuevos datos (servicios) o activos híbridos de bienes y servicios. Para mayor desarrollo del tema, *vid. OECD Digital Economy Outlook 2017*, *cit.* en nota 1, p. 26.

(26) *Vid.* Conclusiones del Consejo UE, de 5 de diciembre de 2017 al Documento de 27 de noviembre de 2017, «Responding to the challenges of taxation of profits of the digital economy», así como la Comunicación de la Comisión de 21 de septiembre de 2017 «A Fair and Efficient Tax System in the European Union for the Digital Single Market» (COM (2017) 547 final y 15445/17) así como la Propuesta de Directiva del Consejo por la que se establecen normas relativas a la fiscalidad de las empresas con una presencia digital significativa (Bruselas, 21.3.2018, COM (2018) 147 final).

digital, no siempre resulta claro cuál es el valor añadido, ni cómo debe éste medirse o dónde se ha generado. Por ello, las políticas tributarias actuales se enfrentan principalmente a dos grandes retos que, además, han de abordarse conjuntamente y que pasamos a comentar a continuación.

El primer gran reto es la cuestión del «nexo», esto es, la determinación del criterio que termine el lugar donde se ha de tributar y la protección del derecho a gravar por parte del país donde el negocio permite prestar servicios digitales con poca o nula presencia física, pese a tener presencia comercial. El segundo gran reto, es la cuestión de qué es lo que ha de gravarse, cuestión ligada al concepto de «valor añadido», que exige fijar la atribución de beneficios en modelos de negocio digitales, basados en bienes intangibles (27), datos (28) y transmisión de conocimiento.

Es evidente que este desafío solo puede ser abordado con soluciones multilaterales e internacionales, y que las medidas unilaterales de algunos países están provocando, a la vez, distorsiones y un indeseado efecto dominó. Sin embargo, las organizaciones internacionales solo han promovido acciones de coordinación de políticas fiscales y no está en sus manos la decisión final, puesto que la soberanía fiscal sigue residiendo en los distintos países. La Comisión Europea se ha esforzado en instar a los Estados miembros de la UE a promover una postura común y coordinada, de cara a conseguir un mayor impacto en los trabajos que se están emprendiendo a nivel global.

La coordinación de políticas tributarias –se argumenta– podría traducirse en buenos resultados, beneficiosos para todos, como la estabilización de las bases imponibles o mayores garantías de una sana competencia fiscal, así como en la proliferación de empresas que operan en el mercado interior. En definitiva, las instituciones comunitarias están promoviendo las acciones precisas que puedan asegurar una tributación efectiva de los beneficios generados en su territorio y una justa redistribución entre el país de la fuente y el de la residencia, pero si bien deja claras las alternativas, no se decanta por una u otra solución.

(27) El desarrollo y la explotación de activos intangibles es una característica clave en la economía digital y a medida que el negocio evoluciona, la importancia de los intangibles crece, concentrándose el valor de los mismos. Los derechos de los intangibles pueden ser fácilmente transferidos entre empresas vinculadas.

(28) El gran activo de muchas multinacionales hoy, es convenir las ingentes cantidades de datos en información con valor económico y es que los algoritmos se han convertido en el secreto del éxito de muchas grandes compañías, y se habla ya del negocio de los algoritmos y el llamado *big data*. En la economía digital, el conocimiento y la información (el dato) es considerado el principal factor de producción, por detrás de los más importantes factores de producción de una sociedad industrializada: trabajo, capital y tierra. Otra característica importante de la economía digital es la digitalización de las actividades económicas centrales, incluyendo producción, distribución y consumo de bienes y servicios. La digitalización, a fin de cuestas es un conductor del crecimiento económico.

En el contexto de la ONU, el Comité de Expertos para la cooperación internacional en cuestiones tributarias, ha trabajado especialmente desde el año 2008 (29) en las cuestiones relacionadas con la tributación de los beneficios derivados de «servicios técnicos» en el Modelo de Convenio de para prevenir la Doble Imposición (MCDI). Concretamente, se ha planteado la introducción de un nuevo precepto en el MCDI de 2017 (el art. 12A), que contemple específicamente la tributación de los pagos por servicios técnicos, ante las dudas que se plantean sobre su calificación, y ante la dificultad de distinguir los cánones derivados de la transmisión de know-how, de los pagos por servicios de consultoría o asistencia técnica. Si nos atenemos a los Comentarios a los Modelos de Convenio de Doble Imposición de la OCDE y de la ONU, pueden resultar claros los criterios para distinguir estos conceptos, pero lo cierto es que, desde una perspectiva práctica, no hay apenas diferencias entre «asistencia técnica» y «servicio técnico», en sentido estricto (30).

Esta Propuesta de la ONU, tiene la ventaja de evitar la necesidad de computar el tiempo de presencia en el territorio de un determinado negocio. Consiste en permitir una retención fiscal en origen sobre el importe bruto de los pagos por los servicios realizados a un tipo de gravamen que se negociaría entre los dos Estados contratantes del CDI. Esta solución de aplicar el criterio de la retención fiscal en origen, se comparte favorablemente por otros organismos internacionales, como la OCDE y la Unión Europea, y se destaca la ventaja de que con ella se evita la difícil tarea de definir de manera uniforme lo que es «economía digital», el nexo «digital» y/o las «transacciones relacionadas». Además de lo anterior, permite conseguir recaudación fiscal por las operaciones sobre bienes y servicios. Los trabajos en el seno de la ONU plantean otras alternativas a la introducción del nuevo artículo 12A en los CDI, como por ejemplo la de reducir los 183 días de presencia en el territorio para determinadas clases de renta.

Por su parte, la OCDE (31) y el G20, han adoptado en los últimos años un gran protagonismo en el escenario de la fiscalidad internacional y han centrado toda su atención en el conocido como «Plan BEPS» (*Base Erosion and Pofit Shifting*), para luchar contra las estrategias de planificación fiscal agresiva tendentes a minimizar la carga fiscal separando de forma artificial los beneficios empresariales de las empresas que los ge-

(29) ONU, Committee of Experts on International Cooperation in Tax Matters, Secretariat Note-*Recent Work of the Committee on Tax Treatment of Services*, E/C.18/2013/CRP.17 (2013), pp. 2-3.

(30) *Vid.* Valta, M., *Article 12, in Klaus Vogel on Double Taxation Conventions*, para 180, en: E. Reimer & A. Rust eds., 4th edition, Kluwer 2015.

(31) La OCDE ha analizado la evolución, oportunidades y retos de la economía digital en *OECD Digital Economy Outlook 2017*, cit. en nota 1.

neran. El Plan BEPS comprende 15 Acciones, de las cuales, justamente la primera (acción 1 BEPS) se refiere a los desafíos fiscales de la economía digital.

En el ámbito de la imposición directa, el Informe Final de la Acción 1 BEPS, del año 2015, identifica como riesgos que son consecuencia de la estructura de cadena de valor de las empresas digitales los siguientes: la eliminación o reducción de la tributación en la jurisdicción de la fuente; el evitar la retención fiscal de salida en el Estado de la fuente; la eliminación reducción de tributación en el Estado o Estados intermedios; o la eliminación o reducción de tributación en el Estado de residencia de la matriz última (32). En todo caso, la Acción 1 BEPS, deja claro que el problema de la economía digital no son las empresas digitales distintas de las tradicionales, sino que está en determinados modelos de negocio, por lo que no se puede abordar el problema atacando solo a determinadas empresas, sino que el análisis es más complejo. Entre las dificultades específicas, destaca el Informe la cuestión del nexo, el valor de los datos desconectados de la base territorial y el tema de cómo se calcula éste o la caracterización de las distintas rentas percibidas. Sin embargo, y pese a las bondades de las Propuestas y el detenido análisis de los Informes, la Acción 1 BEPS no se pronuncia sobre cómo superar los problemas de seguridad jurídica, sobreimposición o adecuación a los principios clásicos de la fiscalidad internacional, puesto que se orienta a la eliminación de los problemas que se traducen en pérdida recaudatoria para los Estados.

Por lo que se refiere a los impuestos al consumo, son dos los riesgos identificados relacionados con la economía digital: de un lado, los que se refieren a la provisión digital remota de servicios e intangibles a empresarios exentos de IVA, y, por otra parte, los relativos a la provisión digital remota de servicios a empresas multilocalizadas.

Mientras que las soluciones a los problemas de imposición directa se confían al éxito del resto de las acciones BEPS, las medidas propuestas en el ámbito de la imposición indirecta, se orientan a atribuir el derecho de gravar a la jurisdicción donde el cliente esté establecido, debiendo éste autoliquidar el IVA correspondiente a los bienes entregados y a los servicios prestados a distancia por proveedores situados en el extranjero conforme a la normativa aplicable en la jurisdicción de la empresa cliente. La Acción 1 BEPS también considera retos impor-

(32) El Grupo de Expertos sobre Fiscalidad de la Economía Digital (GEFDE) de la OCDE, define el concepto de «actividades digitales totalmente desmaterializadas» en los siguientes términos: «*las empresas que precisan de unos mínimos elementos físicos en el Estado de la fuente para poder realizar sus actividades principales, con independencia de que esos elementos físicos (oficinas, edificios o personal, entre otros) se hallen o no en el Estado de la fuente para realizar actividades secundarias*».

tantes la fijación del nexo o criterio de sujeción, el tratamiento fiscal de los datos y la calificación de las rentas fruto de los nuevos modelos de negocio basados en productos como la computación en nube o impresión en 3D.

Por su parte, las instituciones de la Unión Europea, han adoptado diversas iniciativas, en la misma línea que las de la OCDE y los países del G20, destacando la Directiva 2016/1164, de 12 de julio de 2016, por la que se establecen normas contra las prácticas de elusión fiscal que inciden directamente en el funcionamiento del mercado interior, conocida como Directiva antiabuso tributario («ATAD») (33).

La economía digital es un problema global, pero las reformas fiscales en los EEUU parecen más un pulso a las políticas europeas que un alineamiento necesario para una solución común. En cuanto a los países en vías de desarrollo, sus propios problemas no comunes a los de los países desarrollados, les hace desplegar sus propias medidas, como someter a tributación los pagos por servicios y royalties (34).

3. LA CRISIS DEL CONCEPTO DE ESTABLECIMIENTO PERMANENTE Y LA POLÉMICA CUESTIÓN DEL NEXO EN LA ERA DIGITAL

La principal dificultad que el mundo digital plantea a la tributación internacional reside en la configuración del criterio de sujeción que permite a una concreta jurisdicción gravar un determinado hecho, actividad u operación. Caracterizar, delimitar y calificar jurídicamente las transacciones digitales y los pagos que se realizan como contraprestación resulta fundamental para justificar la posible tributación de las rentas generadas en el país de la fuente, como también lo es la necesidad de adaptar el concepto clásico de establecimiento permanente (que se utiliza tanto en los Convenios de Doble Imposición como en las normativas unilaterales) o introducir un nexo alternativo de sujeción.

Para entender correctamente el problema, hay que partir de que el concepto «establecimiento permanente» data del siglo XIX. Se introdujo por primera vez en Alemania, donde el término «*stehendes Gewerbe*» se tradujo como «transacción con base fija de negocio» (35). Fue incorpora-

(33) DOL 193/1, de 19 de julio de 2016. La Directiva se hace eco de las prioridades políticas actuales en materia de fiscalidad internacional, y en la necesidad de garantizar el pago del impuesto allí donde se generen los beneficios y el valor. *Vid.* considerandos 1 a 3 de la Directiva.

(34) *Vid.* Li, J., *Protecting the tax base in the digital economy*, cit., p. 44. Son dos los grupos de países que dominan el «*top 10*» digital: los países del Norte de Europa (Finlandia, Suecia, Noruega y Dinamarca) y los «tigres asiáticos» (Singapur, Taiwán, República de Corea, Hong Kong).

(35) *Vid.* Skaar, A., *Permanent Establishment – Erosion of a Tax Treaty Principle*, Wolters Kluwer, 1991, p. 72 y bibliografía allí citada.

do posteriormente a la normativa no tributaria hasta que se codificó en la Ley tributaria prusiana de 1891 con la actual acepción. Desde entonces, se ha reconocido su transcendencia para poder repartir la tributación de los beneficios entre el Estado de la residencia y el de la fuente, pues, como pronto se puso de manifiesto, sin este concepto es extremadamente difícil la tributación en la fuente (36).

La redefinición del concepto «establecimiento permanente» (37) y/o la configuración de un nexo alternativo se hace necesaria, en primer lugar, porque la economía digital permite que no sea necesaria la presencia física de bienes ni personas en el Estado de la fuente para que se pueda desarrollar un negocio o una actividad comercial, que reporte beneficios. Sin esa presencia física, no hay registros ni control de las actividades realizadas por una empresa no residente, y por ello, es de extraordinaria importancia el intercambio de información financiera entre las Administraciones tributarias del Estado de la fuente y de la residencia, para que las rentas no queden libres de control y gravamen. Por esta razón, mediante una desviación del concepto tradicional de establecimiento permanente en la economía digital, el Estado de la fuente puede ejercitar su derecho a gravar los beneficios obtenidos en su territorio, pues la mera existencia de una cuenta bancaria en un Estado no constituye establecimiento permanente. Estas desviaciones al concepto tradicional pueden encontrarse en los artículos 10, 11, 12, 16 y 17 de los MCDI de la OCDE y de la ONU, y en consecuencia, se permite al Estado de la fuente practicar una retención fiscal sobre el importe bruto de las cantidades distribuidas como dividendos, intereses y cánones por parte de uno de los Estados contratantes.

La posibilidad de crear un nuevo concepto –el establecimiento permanente virtual– es la opción que mejor se adaptaría a los esquemas de la fiscalidad internacional ya existentes, puesto que únicamente consistiría en atribuir el carácter de establecimiento permanente a determinadas entidades que tienen una presencia relevante en el mercado de un Estado a través de las herramientas tecnológicas y sistemas de comunicaciones que sirven de soporte al comercio digital. Para delimitar la existencia de

(36) Así se reconoce en la Liga de Naciones, London and Mexico Model Tax Conventions - Comentare and Text, C.88. M.88.1946. II. A, 1946, p. 13.

(37) Revisar o reinterpretar los criterios definitorios del establecimiento permanente constituye un primer paso para abordar los problemas BEPS de erosión de bases imponibles y los problemas de las bases «cibernéticas», debido a los avances de las tecnologías digitales. En el caso del artículo 5.4 del Modelo de CDI, el sentido de las excepciones está ligado al hecho de que las actividades desarrolladas por una base fija de negocio en el Estado donde está el mercado son de naturaleza preparatoria o auxiliar. Si estas excepciones se aplican a la economía digital, los criterios fallan. Otra posibilidad es revisar el artículo 5.3 del Modelo de la ONU, reduciendo el periodo de tiempo requerido para que exista un establecimiento permanente, respecto a la construcción, montaje, instalación o servicios de supervisión y consultoría. Los actuales 6 meses o 183 días pueden reducirse significativamente como consecuencia de la desmaterialización que puede reducir el tiempo de presencia física requerida, especialmente en aquellos casos en los que una parte del proyecto se desarrolla en el país del proveedor del servicio o en un tercer Estado.

un establecimiento permanente de estas características, se ha propuesto tomar como referencia la realización de un volumen determinado de transacciones y la disponibilidad de determinados elementos tecnológicos, como dominios locales, plataformas web, sistemas de pago electrónicos, un número de usuarios determinado en el Estado, un volumen de tráfico de datos relevante, o la celebración de contratos *on line* que represente un cierto nivel de actividad.

Esta alternativa es la que contempla para el ámbito de la UE la Propuesta de Directiva de armonización de la base imponible común del Impuesto sobre Sociedades (BIC), de 2016 (38). En ella, el concepto de establecimiento permanente se define, siguiendo fielmente la definición «postBEPS» recomendada en el Modelo de Convenio Tributario de la OCDE. Al contrario de lo que sucedía en la propuesta de Directiva de armonización de la base imponible consolidada común del Impuesto sobre Sociedades (BICCIS) 2011 (39), la definición revisada solo se aplica a los establecimientos permanentes situados en la UE y pertenecientes a un contribuyente residente a efectos fiscales en la Unión. Se trata, con ello, de garantizar que todos los contribuyentes afectados compartan una noción común y de descartar la posibilidad de desajustes debidos a definiciones divergentes. No se ha considerado esencial proponer una definición común de los establecimientos permanentes situados en un tercer país, o en la Unión, pero pertenecientes a un contribuyente residente a efectos fiscales en un tercer país. De este modo, la dimensión relativa a los terceros países, se deja a los Convenios fiscales bilaterales y a la legislación nacional (40).

Respecto de la cuestión del nexo, pueden distinguirse tres modelos de negocio en la economía digital (41): el modelo de comercio electrónico, consistente en la venta de bienes tangibles a través de una plataforma de Internet; el modelo de comercio electrónico digital y de servicios en la nube, en el que los productos se transmiten directamente a través de medios telemáticos; y, el modelo pluridimensional, en el que existen varios

(38) Propuesta de Directiva del Consejo, relativa a una base imponible común consolidada, de 25 de octubre de 2016. COM (2016) 685 final. Esta Propuesta constituye la «primera fase» (base imponible común del impuesto sobre sociedades (BIC), de un planteamiento gradual hacia un sistema de imposición de las sociedades a escala de la UE y establece normas comunes en relación con el Impuesto sobre Sociedades para computar la base imponible de las sociedades y los establecimientos permanentes en la Unión. La segunda fase se plasma en la propuesta de base imponible común consolidada (BICC) del Impuesto sobre Sociedades (COM (2016) 683 final).

(39) Propuesta de Directiva relativa a una base imponible consolidada común del impuesto sobre sobre sociedades (BICIS), Bruselas, 16 de marzo de 2011, C7-0092/11 (COM (2011) 121 final).

(40) *Vid.* Propuesta BIC, *cit.*, p. 10

(41) *Vid.* Nocete Correa, F. J., «Comercio electrónico e imposición directa: un análisis post-BEPS», en: Moreno González, S., *Tendencias y Desafíos de la Economía Digital*, Thomson Reuters Aranzadi, 2017, pp. 143-176. Cita en esta distinción el trabajo de Hemmerlarth, A. y Wilcox, E., «AOA, BEPS, E-Commerce – "Permanent Establishment" in Flux», en Jochum, H. *et al.* (dir.), *Practical Problems in European and International Tax Law*, IBFD, Ámsterdam, 2016, p. 126.

niveles de actividad, la que permite el acceso y uso gratuito de servicios digitales a cambio de determinados datos personales que son usados, y la que dirige a su comercialización con fines publicitarios o de otro tipo.

En el primer modelo, se puede llegar a constatar la existencia de un nexo con el Estado donde se generan los beneficios derivados de la venta de bienes tangibles, aunque ello exija reconfigurar determinadas actividades o elementos tradicionalmente considerados como auxiliares o accesorios, como constitutivos de una presencia física suficiente como para justificar su sometimiento a gravamen por el Estado de la fuente, mientras que en los otros dos, no existe ninguna conexión física con el Estado de residencia de los clientes o con el Estado donde éstos han adquirido o utilizado los bienes y servicios.

El Informe final de la Acción 1 BEPS plantea tres opciones para resolver el problema del criterio de sujeción: introducir un nuevo nexo basado en la presencia económica significativa (42); someter las transacciones digitales a una retención en la fuente; y adoptar un gravamen de equiparación, que garantice un tratamiento fiscal análogo a proveedores residentes y no residentes (43).

Por parte de la doctrina, hay defensores y detractores de cada una de las opciones que se han puesto encima de la mesa, y algunos proponen reformas radicales de la bases de la fiscalidad internacional. Así, por ejemplo, Devereux y De la Feria, defienden un modelo de impuesto sobre sociedades que considere el beneficio global en el lugar de las ventas y que se acerque al principio de tributación en destino, al estilo del IVA (44).

Finalmente, debe destacarse la importancia de las decisiones jurisdiccionales, y en particular la Sentencia del Tribunal Supremo de EE.UU., dictada el 21 de junio de 2018, en el caso *South Dakota v. Wayfair, Inc., et al.* pues permite a los gobiernos estatales exigir impuestos a las ventas *on line* realizadas en su territorio, pese a la ausencia de presencia física del vendedor. El Tribunal se separa en esta decisión del precedente sobre la

(42) Este concepto jurídico indeterminado puede generar conflictos interpretativos «El artículo 4 de la Propuesta de Directiva sobre fiscalidad de las empresas con una presencia digital significativa, refiere la "presencia digital significativa" a la actividad consistente total o parcialmente en la prestación de servicios digitales a través de una interfaz digital cuando se cumplen una o varias condiciones como la proporción de los ingresos totales obtenidos en ese periodo impositivo y resultante de la prestación de los servicios digitales a usuarios situados en dicho Estado miembro durante el mismo periodo impositivo sea superior a 7 000 000 euros o el número de usuarios de uno o más de los servicios digitales que estén situados en ese Estado miembro en dicho periodo impositivo sea superior a 100 000» (COM (2018) 147 final).

(43) El gravamen de equiparación, compensación o *equalisation levy* ha sido introducido por algunos países como, por ejemplo, la India, en el año 2016, exclusivamente sobre servicios de publicidad. Esta medida se plantea a nivel internacional como temporal y autónoma del ámbito de aplicación de los convenios bilaterales para evitar la doble imposición.

(44) *Vid.* Devereux, M. y De la Feria, R., *Designing and implementing a destination-based corporate tax*, Oxford University Centre for Business Taxation, Working paper series, Mayo 2014, pp. 1 y 8 y siguientes.

aplicación de la cláusula de comercio interestatal e interpreta que el nexo sustancial de tributación no depende del criterio de la presencia física (45).

4. EL COMERCIO ELECTRÓNICO Y LA IMPOSICIÓN INDIRECTA

El comercio electrónico, *e-commerce* o *Internet-commerce* es quizás, el modelo de negocio mejor conocido. La OCDE lo define como la compra o venta de bienes o servicios, realizado mediante redes informáticas con métodos específicamente diseñados con el proposito de recibir o localizar compras. El *e-commerce* puede ser utilizado bien para facilitar la compra de bienes o servicios que se entregarán por cauces tradicionales (*offline e-commerce*) o por cauces *on-line* (*online e-commerce*). Dependiendo de las partes que intervengan en las operaciones, se distinguen operaciones *business-to-business* (B2B), *business-to-consumer* (B2C) y *business-to-government* (B2G), pero más del 90% de las mismas es B2B (46). Las operaciones *consumer-to-consumer* (C2C) están haciéndose cada vez más comunes. En este caso, el negocio está en el papel de la intermediación, mediante plataformas o aplicaciones que publican la información o facilitan las operaciones, como es el caso de eBay (47).

El fenómeno del comercio electrónico y la preocupación por sus efectos en la tributación se planteó en la década de los noventa del pasado siglo XX. Ya por aquel entonces para la Comisión Europea «*bajo la denominación de comercio electrónico se incluye tanto el comercio electrónico indirecto (pedido electrónico de bienes tangibles) como el directo (entrega en línea de bienes intangibles)*» (48). La dualidad de tipos de comercio electrónico depende de la naturaleza física o intangible de los productos objeto de intercambio, y no del proceso en sí.

En el ámbito de la UE, el desarrollo del comercio electrónico ha cambiado las condiciones de competencia fiscal entre los países que aplican distintos tipos de gravamen en el IVA, en la medida en que abarata los costes de las operaciones transfronterizas y permite a las plataformas evitar el impuesto, lo que refuerza la competencia entre países cuando se aplica la tributación en origen.

A efectos de la tributación por el IVA, las operaciones gravadas son «entregas de bienes» o «prestaciones de servicios». El concepto de entrega de bienes se define como la «*transmisión del poder de disposición sobre un*

(45) *Vid.* CHRISTENSON, E., HADJILOGIOU, S., y BRUNO, M., «An Introduction to the Complexities of Taxing Cross-Border Transfers of Digital Goods and Services», *The Florida Bar Journal,* February 2018, pp. 56-62.

(46) WTO *E-commerce in Developing countries. Report*, OECD Discussion Draft, apartado 62.

(47) Nuevas formas de *social e-commerce social* o *F-commerce* se posibilitan por las redes sociales como Facebook, Twitter, Linkedin o Instagram o por medio del teléfono móvil y tabletas.

(48) *Vid.* Comunicación de la Comisión Europea, de 17 de junio de 1998 «Comercio electrónico y fiscalidad indirecta» (COM (1998) 374 final).

bien corporal con las facultades atribuidas a sus propietarios» (49), de tal manera que el requisito de la corporalidad del bien objeto de la operación sujeta a IVA, implica la consideración de las operaciones de comercio electrónico directo (*on line*) como prestaciones de servicios.

Esta consideración tributaria está en línea con la posición de la OCDE al respecto, y ha sido internacionalmente aceptada. La tributación de las operaciones de comercio electrónico *on line* ha sido una de las que han experimentado mayores cambios normativos, si bien la Directiva IVA no ha introducido una definición de «servicios prestados por vía electrónica», a diferencia de lo que ha ocurrido con el concepto de «servicios de telecomunicación» (50). El Reglamento 282/2011, aclara que «*abarcarán los servicios prestados a través de internet o de una red electrónica que, por su naturaleza, estén básicamente automatizados y requieran una intervención humana mínima y que no tengan viabilidad al margen de la tecnología de la información*» (51).

De acuerdo con el principio de tributación en destino, que es el que rige actualmente al haberse abandonado la idea de instaurar el régimen definitivo de imposición en origen, los servicios prestados han de tributar en el Estado miembro donde se consumen, tanto si la transacción se efectúa con otro sujeto pasivo (B2B: *business to business*) como si se realiza con un consumidor final (B2C: *business to consumers*) (52). Existen dos regímenes especiales que pretenden facilitar el cumplimiento de las obligaciones formales exclusivamente en un Estado miembro, uno para los sujetos establecidos en el territorio UE de aplicación del IVA y otro, para los no establecidos, pero en ambos casos, se exige la identificación del operador. El sistema funciona a modo de ventanilla única: se recibe la declaración y el pago por todas las transacciones en los países de la UE, y se reparte la recaudación entre los Estados miembros de consumo en función de las operaciones que se han realizado en su territorio. Por el contrario, las operaciones de comercio electrónico indirectas (*off line*), serán consideradas como entregas de bienes, si bien podrán quedar sujetas al régimen establecido para ventas a distancias, adquisiciones intracomunitarias o importaciones.

El 5 de diciembre de 2017, el Consejo de la UE ha adoptado nuevas normas para facilitar a las empresas en línea el cumplimiento de las obligaciones del IVA. Se trata de la Directiva de noviembre de 2017 relativa a

(49) Artículo 14 de la Directiva 2006/112/CE, de 28 de noviembre de 2006, relativa al sistema común del impuesto sobre el valor añadido de la Unión Europea (Directiva IVA).

(50) Artículo 24 de la Directiva IVA 2006/112/CE, citada.

(51) Artículo 7 del Reglamento 282/2011, citado.

(52) Un mayor desarrollo de este tema puede encontrarse en Macarro Osuna, J. M., «El IVA en el comercio electrónico como punto de partida de un nuevo paradigma de las ventas a distancia en la Unión Europea», en Moreno González, S., *Tendencias y Desafíos Fiscales*, *cit.*, pp. 177-209.

las obligaciones en materia de IVA para la prestación de servicios y la venta de bienes a distancia (53), del Reglamento relativo a disposiciones de aplicación del sistema común del IVA y del Reglamento relativo a la cooperación administrativa y la lucha contra el fraude (54).

Fuera del ámbito de la UE, las operaciones de tráfico internacional de mercancías contratadas a través de fórmulas de comercio digital, se concretan en importaciones de bienes que son objeto de transporte desde países no comunitarios, y en prestaciones que tienen por objeto bienes intangibles, cuya cesión de uso o de otros derechos, se materializa, fundamentalmente, a través de las redes digitales de transmisión de datos.

5. LOS PROCEDIMIENTOS TRIBUTARIOS Y EL CONTRIBUYENTE EN LA ERA DIGITAL

Es sabido que la información constituye la base de las actuaciones administrativas de inspección y verificación del cumplimiento de las obligaciones tributarias. Pues bien, la era digital dificulta el acceso de las Administraciones tributarias a los datos necesarios para desarrollar sus funciones. En particular, las restricciones legales relativas a la protección de datos y las impuestas para los intercambios de información entre Administraciones de distintos países, se traduce en diferencias significativas respecto de la información tributaria disponible dentro del ámbito del comercio tradicional (55).

Los derechos y garantías del contribuyente a la protección de sus datos y respecto de su derecho de audiencia, se proyectan en los distintos procedimientos de aplicación de los tributos de una manera específica, cuando se trata, de operaciones realizadas en el marco del comercio digital. Así, por ejemplo, el principio del tratamiento leal y lícito de la información implica que los interesados deben estar, en todo momento, en condiciones de conocer la existencia de los tratamientos de datos, así como de contar con información sobre las características de su obtención y posterior tratamiento. De otra parte, los principios de finalidad y proporcionalidad exigen que, única y exclusivamente, se recojan y manipulen los datos estrictamente pertinentes, adecuados y nece-

(53) Directiva modificativa de la Directiva 2006/112/CE y Directiva 2009/132/CE (Brussels, 28 November 2017 (FISC 256, ECOFIN 922 UD 257).

(54) Los Estados miembros dispondrán hasta el 31 de diciembre de 2018 y el 31 de diciembre de 2020 para incorporar las disposiciones correspondientes de la Directiva a su ordenamiento jurídico nacional. El Reglamento sobre cooperación administrativa será de aplicación a partir del 1 de enero de 2021.

(55) Sobre el acceso a los datos personales en poder de la Administración tributaria, *vid.* El trabajo de Olivares Olivares, B. D., publicado en la *Revista de Contabilidad y Tributación* núm. 419, febrero 2018, pp. 83-124.

sarios para llevar a cabo fines determinados, explícitos y legítimos, sin que puedan ser tratados posteriormente de forma incompatible con dichos fines (56). Finalmente, el principio de legitimidad del tratamiento de datos personales, exige contar con el consentimiento del afectado, lo que implica que la transparencia sea, en palabras de la Comisión «condición fundamental e indispensable para permitir a las personas efectuar un control sobre sus propios datos y para garantizar la protección efectiva de los datos personales» (57). En igual sentido, el Reglamento 2016/679, afirma que «el responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento legal y transparente, habida cuenta de las circunstancias y del contexto especifico en que se traten los datos personales» (58).

Tanto el Tribunal de Justicia de la UE como el Tribunal Constitucional español se han pronunciado sobre la cuestión del necesario equilibrio entre la libre circulación de los datos personales y la tutela del derecho a la intimidad (59) y de sus pronunciamientos de deduce la necesidad de establecer procedimientos coordinados de intercambio de información entre Estados miembros (60).

La adecuada regulación del derecho a la protección de datos no es el único problema que se plantea en el contexto digitalizado, sino especialmente, el hecho de que el nivel de protección no está suficientemente armonizado a nivel europeo. Si bien es cierto que existen directivas y reglamentos comunitarios que favorecen la cooperación entre Administraciones tributarias de los distintos Estados miembros de la UE e incluyen fórmulas de intercambio automático de información, la reglamentación no garantiza un nivel uniforme y elevado de protección de datos de carácter personal. La libre circulación de datos en el seno de la UE plantea, además, problemas específicos en el actual contexto del mundo global y digitalizado, en orden a garantizar la eficacia de los intercambios de datos entre Administraciones tributarias de los distintos Estados miembros.

---

(56) *Vid.* Moreno González, S., «El intercambio de información tributaria y la protección de datos personales en la Unión Europea. Reflexiones al hilo de los últimos progresos normativos y jurisprudenciales», *Quincena Fiscal* núm. 12/2016, p. 44.

(57) *Vid.* Comunicación de la Comisión «Un enfoque global de la protección de los datos personales en la Unión Europea, de 4 de noviembre de 2010, COM (2010), 699 final, p. 6.

(58) Considerando 60, del Reglamento 2016/679.

(59) Entre otras, pueden citarse la STJUE de 6 de noviembre de 2003, asunto *Lindqvist*, C-101/01 o las SSTC 142/1993 y 202/1999.

(60) *Vid.* Baker, P. y Pistone, P., «BEPS Action 16: The Taxpayers' Right to an Effective Legal Remedy under European Law in Cross-Border Situation», *Tax Review* núm. 5-6/2016 y Sánchez López, E, «La posición del contribuyente en el intercambio automático de información entre administraciones tributarias», en Moreno González, S., *Tendencias y Desafíos de la Economía Digital*, cit., pp. 697-732.

6. CONCLUSIONES

El sector de la economía digital aporta beneficios indiscutibles a la economía, pero también está produciendo distorsiones importantes en los mercados y las finanzas públicas, como las que se derivan de la ausencia de gravamen donde se crea valor añadido y del hecho de que el sector digital tribute a un 9%, mientras que el resto de las actividades tributan a un tipo aproximado efectivo de un del 23 % (61).

Las bases de la fiscalidad internacional han de revisarse para adaptarse a la realidad actual de un mundo, que, desde hace ya tiempo, se mueve en un contexto global y digitalizado. La economía digital está desafiando la capacidad de las Haciendas públicas para gravar transacciones comerciales y beneficios empresariales, ante la emergencia de plataformas gigantes en internet, capaces de transformar sectores tan importantes como el comercio o la publicidad y capaces también de utilizar precios de transferencia, que se traducen en pérdidas de recaudación de tributos.

Gracias al impulso de las principales organizaciones internacionales y a la adopción de instrumentos *soft law*, que promueven soluciones multilaterales, se está consiguiendo cambiar las reglas de juego y los cánones del marco de referencia para asentar un modelo nuevo, que sirva a los problemas que plantea la economía digital.

Los problemas de ahora y los de siempre –exacerbados por las posibilidades tecnológicas y del desarrollo digital (62)–, requieren promover acciones distintas. Para el ámbito de la imposición societaria, se necesita redefinir, ampliar o reinterpretar el concepto de «establecimiento permanente» o crear uno nuevo como el de «establecimiento permanente digital», será preciso cambiar el nexo de tributación y prosperarán las propuestas reformistas, innovadoras o quizás mixtas. En lo que respecta a la imposición indirecta, cabe esperar aún más malabarismos al objeto de que ninguna operación económica que caiga en el ámbito del IVA quede sin tributar, y probablemente se acercarán estructuralmente poco a poco impuestos directos e indirectos.

No sabemos qué modelo primará, pero de lo que no hay duda es que el debate en las políticas públicas no es ya la justicia tributaria sino cómo hacer que se pague «la parte efectiva y justa de impuestos» (63) en un escenario global, que a fin de cuentas, busca evitar la «inmunidad fiscal».

---

(61) De ahí las propuestas de la Comisión Europea relativas a la tributación justa. *Vid.* Declaraciones del Comisario Pierre Moscovici: *Keynote speech by Commissioner Moscovici at the «Masters of Digital 2018» event*, localizable en: http://europa.eu/rapid/press-release_SPEECH-18-981_en.htm.

(62) La economía digital puede exacerbar los problemas de BEPS, pero los temas BEPS no son exclusivos de las empresas digitales.

(63) El Consejo Europeo de Tallin, celebrado el 29 de Septiembre de 2017, adoptó sus Conclusiones el 19 de Octubre de 2017 (doc. EUCO 14/17), en las que subrayó la necesidad de un

Aunque permanecen las tensiones y diferencias de enfoques, que son del todo lógicas y propias de jurisdicciones con planteamientos muy diversos en la forma de abordar las soluciones del modelo de tributación de la era digital, se están realizando esfuerzos de coordinación política y reformas normativas, que técnicamente hacen que el Derecho siga en su función de adaptarse a una realidad social siempre nueva, y que a menudo le desborda.

efectivo y justo sistema de tributación para la era digital, remarcó la importancia de asegurar que todas las empresas paguen su parte justa de impuestos y de garantizar un marco legal alineado con los trabajos actualmente emprendidos por la OCDE, a la vez que invitó al Consejo a continuar examinando la Comunicación de la Comisión para presentar una propuesta a principios de 2018.

III

PRIVACIDAD EN UN MUNDO DIGITAL

CAPÍTULO 11

INTELIGENCIA ARTIFICIAL, DERECHO Y DERECHOS FUNDAMENTALES

RICARD MARTÍNEZ MARTÍNEZ
Director de la Cátedra de Privacidad y Transformación Digital Microsoft
Universitat de Valencia (1)

En los últimos años, las tecnologías de la información han integrado en su seno un conjunto de desarrollos que han sido esenciales para alumbrar la llamada transformación digital o Cuarta Revolución Industrial (2). Entre estas tecnologías la inteligencia artificial probablemente es una de las que mayor recorrido histórico posee y, de algún modo, una de las que más ha inspirado el imaginario colectivo. De hecho, las primeras reflexiones de

(1) El presente trabajo se enriquece y contribuye al debate en sendos proyectos de investigación sobre la reforma del sistema europeo de protección de datos financiados por el Ministerio de Economía y Competitividad (DER2012- 34764) y por la Universitat Jaume I (P1-2012-12).

(2) SCHWAB señala el carácter revolucionario de un periodo en el que «Los cambios son tan profundos que, desde la perspectiva de la historia humana, nunca ha habido una época de mayor promesa o potencial peligro». De ahí que afirme la necesidad de un esfuerzo colectivo para «asegurarnos que gire alrededor del empoderamiento y los seres humanos, en lugar de que sea divisoria y deshumanizante». SCHWAB, KLAUS. *La cuarta revolución industrial.* Barcelona, Debate. 2016, pp. 15 y 16.

carácter científico y tecnológico en relación con la inteligencia artificial, se sitúan en sendas conferencias celebradas en los Ángeles en 1955 (3) y Darmouth en 1956 (4).

De algún modo, la inteligencia artificial no podía ser más que una consecuencia lógica del modelo computacional. ¿Será capaz una máquina de emular el funcionamiento del cerebro humano? En este sentido, el análisis de la lógica interna del funcionamiento de la informática se ha comparado con las redes neuronales y, a la vez, el modelo informático ha sido utilizado por la neurociencia dando lugar al concepto de neurociencia computacional.

El territorio de la inteligencia artificial (IA) es un espacio abierto a la utopía. Podría conducirnos a un modelo de sociedad sin precedentes en el que nuestro mundo pudiera funcionar gracias a inteligencias calificadas de algún modo como superiores que nos liberasen del trabajo repetitivo, que gestionasen el tráfico, redujesen la contaminación o eliminasen la enfermedad (5). Pero también, de todo lo contrario, de un futuro distópico. Se trata de escenarios en los cuales una inteligencia artificial toma decisiones contra los intereses y derechos de seres humanos. Podemos identificar en ambos casos, un conjunto de prejuicios subyacentes que inspiran sin duda gran parte del pensamiento jurídico y sociológico en relación con la IA. De este modo, presumimos que una inteligencia sintética con una capacidad computacional ilimitada será superior a cualquier inteligencia humana. Y si esto fuera así, esa inteligencia debería entender muy rápidamente que su superioridad implicaría asumir la responsabilidad de regir los destinos de una especie inferior. O lo que es peor, considerar que

(3) Para entender qué es la Inteligencia Artificial y su historia: López de Mántaras Badía, Ramón y Messeguer González, Pedro. *Inteligencia Artificial*. Madrid, Catarata-CSIC, 2017.

(4) La Conferencia de Darmouth de 1956 fue organizada por John McCarthy, padre del término «inteligencia artificial», junto con Marvin Minsky, Claude Shannon y Nathaniel Rochester, de una reunión que tuvo lugar en Dartmouth College (New Hampshire, EEUU). Véase, Mccarthy, John, Minsky, Marvin, Rochester, Nathaniel y Shannon Claude. «A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence». Disponible el 09/04/2018 en http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html.

En todo caso, se atribuye al matemático Alan Turing, una primera formulación de esta idea. Turing, Alan. «Computing machinery and intelligence» en *Behalf of MIND (Journal of the Mind Association)*, vol. LIX, n.º 236, pp. 433-60, 1950. Disponible el 09/04/2018 en http://web.cs.ucla.edu/~rosen/161/turing_paper.html.

(5) Este optimismo ha conducido en su extremo a las tesis transhumanistas, al sueño de una inmortalidad basada en un modelo de medicina celular regenerativa o a la posibilidad de transferir la mente humana a un programa informático, como sucede, por ejemplo, en la película Trascendence. En este sentido, Ray Kurzwell ha definido un momento de transformación radical en 2045, al que denomina la Singularidad, en el que por primera vez una inteligencia sintética superará la humana. Kurzwell, RAY. *The Singularity Is Near: When Humans Transcend Biology*. Penguin, New York, 2005. Pero no sólo esto, en su opinión, mente humana y máquina se podrán integrar a través del Cloud dando lugar a una nueva superinteligencia.

Véase Grace, Katja, *et alii*. « When Will AI Exceed Human Performance? Evidence from AI Experts», Oxford, Future of Humanity Institute Disponible el 09/04/2018 en https://arxiv.org/pdf/1705.08807.pdf

la acción antrópica es un peligro para el planeta (6) y es necesario extinguir, sojuzgar o controlar a los propios humanos (7).

El pensamiento distópico no es sólo patrimonio de la literatura o el cine. Elon Musk ha considerado los riesgos que la Inteligencia Artificial plantea, por ejemplo, para el futuro de la economía y financia la iniciativa OpenAI para promover una inteligencia artificial segura cuyos beneficios se distribuyan a toda la sociedad (8). Y Stephen Hawking llegó a afirmar que la inteligencia artificial podría significar el fin de la raza humana (9).

Desde este punto de vista, el análisis de los aspectos jurídicos relacionados con inteligencia artificial se enfrenta a una primera dificultad. En el imaginario colectivo, lejos de apreciar las oportunidades que pueden derivar del desarrollo y utilización de la inteligencia artificial, la sociedad percibe antes los riesgos que las oportunidades. Sin embargo, desde el Derecho debemos aproximarnos al fenómeno de un modo más matizado. Si caemos en la trampa de demonizar la tecnología desde una óptica puramente preventiva corremos el riesgo de paralizar el avance del conocimiento y las ventajas que pueda proporcionar a nuestra sociedad. Pero no podemos ni ignorar ni obviar los riesgos. Debemos operar desde la realidad proponiendo reglas que, sin paralizar la innovación, la disciplinen y alineen con el ineludible deber de salvaguardar a toda costa la dignidad del ser humano y garantizar el pleno respeto de los derechos fundamentales.

---

(6) Ceballos, Gerardo *et alii*. «Biological annihilation via the ongoing sixth mass extinction signaled by vertebrate population losses and declines», en *Proceedings of the National Academy of Sciences of the Unitated states of America PNAS*, July 25, 2017. 114 (30) E6089-E6096. Disponible el 09/04/2017 en https://doi.org/10.1073/pnas.1704949114. Earth's sixth mass extinction

(7) La lista de películas, o libros que nos presentan un futuro distópico en el que las inteligencias artificiales se revelan o dominan al hombre es amplia. Baste con citar a HAL 9000 en 2001 Una odisea del espacio, o las saga Matrix. Pero seguramente es la frase final de John Connor en Terminator 3 la que mejor ejemplifique esta percepción temerosa de la Inteligencia Artificial:

«Todo era sofware, y ciberespacio. No había núcleo del sistema. No se podía desconectar. El ataque empezó a las 18:18, tal como él había dicho. El Día del Juicio, el día que la raza humana quedó prácticamente destruida por las armas que había fabricado para protegerse. Debí darme cuenta de que nuestro destino nunca fue evitar el Día del Juicio. Era simplemente sobrevivir a él. Juntos. El Terminator lo sabía. Intentó decírnoslo, pero yo no quise escucharle. Puede que el futuro ya esté escrito. No lo sé. Solo se lo que el Terminator me enseñó. Nunca dejes de luchar. Y nunca lo haré. La batalla no ha hecho mas que empezar».

Más cercanas a la realidad, son las ficciones como la serie televisiva «Person of Interest» que presentan inteligencias artificiales ordenadas a asistir el trabajo policial identificando riesgos o a manipular y controlar la realidad en una sociedad permanentemente vigilada por el Estado.

(8) Véase https://openai.com/press/elon-musk/.

(9) En *ABC* tecnología, http://www.abc.es/tecnologia/informatica-software/20141202/abci-stephen-hawking-peligros-inteligencia-201412021837.html.

Sobre los riesgos de esta tecnología véase Bostrom, NICK. *Superintelligence: Paths, Dangers, Strategies*. Oxford University Press, 2014.

1. UNA APROXIMACIÓN JURÍDICA BASADA EN LOS HECHOS

Aproximarse a la inteligencia artificial, desde el punto de vista de un experto en protección de datos, y por extensión en el Derecho de Internet (10), ofrece una cierta ventaja competitiva. En el ámbito de las tecnologías de la información no existen soluciones teóricas de despacho y cualquier aproximación que desconozca la realidad está condenada al fracaso. Lo que obliga a conocer con detalle la realidad técnica, social e incluso económica, subyacente a los fenómenos a los que aplicamos la norma. No es posible reflexionar sobre el impacto jurídico y las necesidades normativas derivadas del desarrollo de la inteligencia artificial sin una breve descripción de las tecnologías que la han hecho posible.

Desde el punto de vista de sus objetivos la inteligencia artificial perseguiría, actuar y razonar como las personas y hacerlo racionalmente. Para ello, debe distinguirse entre una inteligencia artificial fuerte, que tendría todas las capacidades de la mente humana, y otra débil o de propósitos específicos (11). Todos los esfuerzos dirigidos en la primera línea han fracasado sistemáticamente por varias razones. La primera es de índole material, ya que se carecía de capacidad de almacenamiento y computación para desarrollar una máquina de esta naturaleza. La segunda, reside en que para razonar como una persona se requiere de dos características que han identificado perfectamente los neurocientíficos: la empatía, la capacidad para ponerse en el lugar de otro (12), y en segundo lugar un aprendizaje emocional (13) que al menos hasta hoy no ha sido posible para una máquina. Por ello, la mayor parte de desarrollos vinculados a la inteligencia artificial que han culminado sus objetivos con éxito se centran en propósitos específicos como jugar al ajedrez. De hecho, es precisamente este modelo de inteligencia artificial en el que está produciendo muchos y muy positivos resultados en muy distintas áreas a los que después nos referiremos.

La confluencia de distintas tecnologías en los últimos años hace posible un desarrollo intenso de la inteligencia artificial. La primera de ellas es el *Cloud* o computación en la nube. Este modelo de computación distribuida ha permitido incrementar de modo sustancial la capacidad de almacenar información y la velocidad o la rapidez en su proceso. Por tanto, disponemos de tecnologías que facilitan el análisis masivo de información caracterizadas por «*las 3V del Big data*»: velocidad, variedad y volumen. Esta tecnología permite analizar un volumen masivo de datos, con una

(10) Barrio Andrés, Moisés. «Del Derecho de Internet al Derecho de los Robots en Barrio Andrés Moisés (Coord.). *El Derecho de los Robots*. Madrid, Wolters Kluwers, 2018, pp. 65 a 68.

(11) López de Mántaras Badía, Ramón y Messeguer González, Pedro. *Inteligencia Artificial*, *op. cit.*, pp. 8 y 11 a 13.

(12) Rizzolatti, Giacomo *et alii*. «Neuronas espejo», en *Investigación y Ciencia* Enero 2007-n.º 364

(13) Damasio, Antonio. *El error de Descartes*. Barcelona, Ed. Destino, 2011.

enorme velocidad en la recogida y procesado de la información y al mismo tiempo puede afrontar el análisis de una gran variedad de datos. Adicionalmente se unen por algunos teóricos dos V adicionales, la correspondiente a la posibilidad de crear valor en el en el uso de estas tecnologías, y en segundo lugar la llamada veracidad. Es decir, la capacidad de obtener información verídica y útil para la toma de decisiones, aunque evidentemente esta última V es más bien discutible (14).

A ella se unen las llamadas herramientas de *Machine Learning, q*ue permiten que las máquinas analicen grandes volúmenes de datos a partir de determinados algoritmos de programación. Algunos de ellos supervisados, es decir con reglas de aprendizaje predefinidas de modo que se ha programado tanto el *input* como el esperable *output*. Pero también los hay no supervisados en los que el programa se diseña para que analice conjuntos de datos e identifique patrones. Y modelos en los cuales la evolución en el análisis y autodesarrollo del programa dependerá de las confirmaciones, premios o incentivos que se asignen a los resultados que va mostrando a lo largo del proceso (15).

Y esto implica que, por primera vez en la historia de la humanidad, un programa informático es capaz de evolucionar a partir de las correlaciones que encuentra en un conjunto de datos. Y esto en ocasiones puede suponer un funcionamiento de caja negra que dificulta evaluar las razones por las que la programación llega a unas u otras conclusiones. Una vez desarrollamos estas capacidades, el paso siguiente resulta bastante previsible, disponemos de los datos, disponemos de la capacidad de analizarlos, y disponemos de software que puede establecer correlaciones y determinar consecuencias para las mismas. Tenemos la capacidad de diseñar herramientas que tomen decisiones a partir de los datos, y con ello, de expandir las posibilidades de la inteligencia artificial a un enorme abanico de supuestos.

Llegados a este punto, debe advertirse al lector, que en este trabajo no nos ocuparemos de la llamada robótica (16) y su evolución de la mano de las tecnologías de la información. Hemos pasado de robots autómatas diseñados para un propósito concreto, al diseño de robots inteligentes, e incluso antropomórficos o que cumplan funciones propias de agentes

(14) Para un análisis muy comprensible véase Mayer-Schönberger, Viktor y Cukier, Kenneth. *Big Data*. Madrid, Turner, 2013.

(15) Caballero, Rafael y Martín, Enrique. *Las bases de Big Data*. Madrid, Catarata, 2015. Véanse ejemplos en el blog divulgativo de Phillips sobre innovación «Machine Learning: Inteligencia Artificial aplicada al diagnóstico médico». Disponible en http://www.comparteinnovacion.philips.es/innovacion-en-healthtech/articulos/machine-learning-inteligencia-artificial-aplicada-al-diagnostico-medico. Y en BBVA «Las cinco tribus del "machine learning"». Disponible en https://www.bbva.com/es/las-cinco-tribus-del-machine-learning/

(16) Como bien señala Moisés Barrio se trata de un ámbito que posee perfiles propios. Barrio Andrés, Moisés. «Del Derecho de Internet al Derecho…, pp. 73 a 78.

como las mascotas. Estas máquinas, necesitan disponer de herramientas de inteligencia artificial para adquirir la capacidad de tomar decisiones en el ámbito funcional para el que han sido diseñadas. En este sentido, la computación en la nube, multiplica las capacidades de las unidades físicas para permitir el análisis de datos. Por otra parte, es precisamente esta capacidad, el impacto de inteligencia artificial en la robótica, la que permite concebir lo que podemos definir como robots incorpóreos que desarrollan actividades al servicio del ser humano, pero sin estar dotados de corporeidad. El ejemplo paradigmático son los asistentes vocales (17).

Este escenario puede ganar en complejidad en los próximos años debido sin duda al desarrollo de los nuevos modelos computacionales basados en la computación cuántica (18).

2. EL IMPACTO ECONÓMICO Y SOCIAL DE LA INTELIGENCIA ARTIFICIAL

En el epígrafe anterior describimos el conjunto de tecnologías que permitían alcanzar o sentar las bases que hacen posible el diseño de procesos de toma de decisiones automatizadas por una máquina de acuerdo con las inferencias y correlaciones obtenidas. En este sentido el impacto de la analítica, está siendo fundamental para muchas áreas de la vida social y económica. De algún modo, se instala un nuevo paradigma, en el que la celeridad del proceso de decisión es fundamental, de modo que supera con mucho las capacidades de un ser humano. Por otra parte, aparecen nuevas posibilidades de investigación científica y tecnológica hasta ahora inalcanzables. De algún modo encontramos atajos en el paradigma científico al incorporar un modelo que parte del establecimiento de patrones, basado más en la correlación que en la causalidad, y que puede trabajar sobre un universo amplísimo de datos.

En este sentido podemos identificar diversos sectores en los que el análisis masivo de datos ha permitido la implantación de herramientas de inteligencia artificial o la favorecerá en un futuro inmediato (19):

(17) Satya Nadella, CEO de Microsoft ofrece una completa reflexión sobre los desarrollos en Inteligencia Artificial de la compañía y pronostica una mejora significativa en 10 años que permitirá un incremento sustancial en la capacidad de ver y entender de la IA. No obstante, «la próxima frontera es la comprensión del lenguaje natural, la interacción entre ordenadores y seres humanos». Nadella, Satya. *Pulsa actualizar*. Madrid, Harper Collins, 2017, p. 145.

(18) Satya Nadella indica que para alcanzar este objetivo son necesarios tres avances significativos a nivel científico y de ingeniería para hacer posible la computación cuántica. El primero, ser capaces de construir lo que se define como cubit topológico. A partir de ello se especulará sobre si la computación cuántica efectivamente fijará las condiciones para el diseño de una inteligencia artificial de propósito general. Nadella, Satya. *Pulsa actualizar*, *op. cit.*, pp. 155 a 159.

(19) Mc Kinsey señala esta tecnología como un reto empresarial y macroeconómico estratégico: «The application of AI and the automation of activities can enable productivity growth and other benefits not just for businesses, but also for entire economies. (…) At a macroeconomic level, based on our scenario modeling, we estimate automation alone could raise productivity

— Marketing y *profiling*

El modelo de negocio de las redes sociales y de los buscadores en internet, constituye el paradigma sobre cómo pueden funcionar sistemas basados en el análisis masivo de datos personales que alimentan procesos decisionales automatizados. Se trata de algo tan sencillo como ofrecer una navegación personalizada al usuario, de asegurar que el cliente en un entorno de comercio electrónico alcance con facilidad aquellos productos que busca o que necesita (20) y de que la publicidad que se ofrece sea adecuada al perfil del consumidor (21). Esto proporciona un conocimiento profundo de los clientes, y en consecuencia un alto grado de fidelización, y a la vez, la gestión de inmensos volúmenes de datos al servicio de la venta de publicidad, entre otros posibles modelos de negocio.

— Medicina

En este sector se ha abierto un campo de investigación basado en el análisis de datos retrospectivos (22) que introduce cambios y oportunidades antes prácticamente inexistentes. En primer lugar, la investigación clínica de carácter retrospectivo podría acceder a un enorme volumen de datos digitalizados por los sistemas de salud. Así, a diferencia de los ensayos clínicos generalmente confinados a universo limitado de pacientes caracterizados por padecer una patología, es posible superar un enfoque limitado por un modelo en el que analizar todas las interacciones posibles. El siguiente avance cualitativo vendrá definido por el diseño de programas de inteligencia artificial capaces de ofrecer modelos diagnósticos que funcionen como apoyo a la decisión final del facultativo.

---

growth on a global basis by 0.8 to 1.4 percent annually. In short, businesses and the economy need the productivity boost from automation».

Véase Mc Kinsey. «What's Now and Next in Analytics, AI, Aad Automation». Briefing Note. May 2017, p. 6. Disponible el 11/04/2018 en https://www.mckinsey.com/global-themes/digital-disruption/whats-now-and-next-in-analytics-ai-and-automation.

(20) «Hay que dar siempre prioridad al cliente, aunque ello requiera tomar una decisión que reduzca los ingresos. Se trata de una estrategia ganadora a largo plazo. Aunque el futuro parezca estar aún a años luz. Solo pensar en la idea puede acercar un poco más rápidamente ese futuro. Tus competidores te odiarán por ello, pero los clientes quedarán impresionados, o como mínimo les harás reir». Brandt L., Richard. *Un click. Jeff Bezos y el auge de* amazon.com. Barcelona, Gestión 2000, p. 28.

(21) Algo tan sencillo como editar un anuncio en Internet exige una compleja batalla en la que en milésimas de segundo distintas inteligencias artificiales verifican el patrón de conducta del usuario, definen si se corresponde con su «*target*» y pujan en una subasta en tiempo real. Y no solo es un negocio para agentes como Google y Facebook, parece ser un espacio de mercado abierto a la innovación de nuevas empresas. Véase Kaplan, Jerry. *Abstenerse humanos*. TEELL, 2016, pp. 43 a 48.

(22) Véase mi trabajo Martínez Martínez Ricard. «Big data, investigación en salud y protección de datos personales: ¿Un falso debate?» en *Revista Valenciana d'Estudis Autonòmics*, N.º 62, 2017, pp. 235-280, Disponible el 11/04/2018 en http://bit.ly/2EDdjig.

— Confiabilidad del cliente en entornos bancarios y aseguradores

Con toda probabilidad se incrementarán los procesos de decisión basados en herramientas de inteligencia artificial cuando se requiera el análisis de las condiciones de confiabilidad de una persona para la toma de una decisión. Este tipo de análisis resulta particularmente relevante en el denominado *scoring* bancario y en el análisis de riesgos actuariales en la contratación de un seguro. Se trata de superar el estricto marco del análisis basado en la morosidad, nivel de renta o de ingresos, o en las declaraciones sobre el estado de salud de una persona que contrata un seguro de vida. En un futuro inmediato se buscaría un mercado del crédito bastante más riguroso que aquél que nos condujo a la crisis de las hipotecas basura, y una adaptación de los servicios bancarios basados en las condiciones reales y capacidades del cliente. Por otra parte, en el sector asegurador, se ofrecerán seguros altamente personalizados basados en el pago por consumo reduciendo, por ejemplo, el coste de los seguros vinculados a los vehículos e individualizando en tiempo real la cuota de cada conductor de un mismo coche.

— Analítica de recursos humanos

En este campo, ya existen procesos de selección de personal automatizados en los que las máquinas obtienen inferencias a partir de test de personalidad. La inteligencia artificial podría jugar un papel determinante en la analítica del desempeño del puesto de trabajo orientada por ejemplo a auxiliar al trabajador en la toma de decisiones que faciliten la economía, la eficiencia, y la seguridad en el trabajo.

— Asistentes virtuales y negocios que requieren de análisis semántico y lingüístico

Un sector en el que la evolución de la inteligencia artificial está resultando acelerada es el de los servicios que requieren el uso del lenguaje humano y la asistencia y apoyo a personas. Los asistentes virtuales telefónicos, o los servicios de traducción automática son la mejor muestra. Pero este sólo es el principio. Debemos imaginar un mundo con recepciones de hotel automatizadas, con guías turísticos virtuales que interactuarán con el usuario de modo dinámico, con aplicaciones médicas que conversarán con el paciente, o con «conversadores» que nos hagan compañía.

La lista no se agota aquí, las posibilidades para el despliegue de la inteligencia artificial en la gestión contable, en la administración electrónica, en la gestión del tráfico o la conducción automática son muy amplias, y en algunos casos ya se están ensayando. Con toda seguridad, la inteli-

gencia artificial acabará sustituyendo al ser humano en todos aquellos procesos que sean «robotizables», esto es que puedan ejecutarse mediante rutinas automatizables a partir de un conjunto de variables susceptibles de ser analizadas por un algoritmo decisional.

En sentido positivo, la inteligencia artificial apunta un escenario de liberación del ser humano respecto de trabajos rutinarios susceptibles de ser prestados por máquinas y nuevas oportunidades de actividad, negocio y especialización (23).

3. EL ANÁLISIS DE RIESGOS, UN ELEMENTO ESENCIAL PARA LA PROSPECTIVA JURÍDICA

En el anterior epígrafe hemos enumerado un conjunto de usos de la inteligencia artificial de carácter positivo. Sin embargo, una de las funciones esenciales del Derecho consiste precisamente en la adopción de políticas preventivas que permitan asegurar que el despliegue de la tecnología no produzca efectos adversos. Precisamente por ello, es esencial incorporar al diseño jurídico las metodologías de análisis de riesgos que caracterizan el diseño e implementación de cualquier herramienta informática.

En este sentido, es esencial considerar las metodologías de diseño basado en el cumplimiento normativo incorporadas a nuestro Ordenamiento jurídico de la mano del Reglamento (UE) 2016/679 que regula la protección de datos desde el diseño y por defecto y la evaluación de impacto. Corresponde al desarrollo informático el ineludible deber de incorporar la ley al código de programación (24). Pero también resulta esencial realizar la operación inversa. Esto es, incorporar metodologías de análisis provenientes de otras áreas al desarrollo de la actividad normativa.

---

(23) Satya Nadella apunta, citando un estudio de Standford, que la IA atravesará una fase de transición pero sus resultados a largo plazo generarán nuevas oportunidades para la humanidad. Nadella, Satya. *Puls a actualizar. Op. cit.*, p. 193. Stanford University. «One Hundred Year Study on Artificial Intelligence (AI100),» Stanford University, disponible el 11/04/2018 en https://ai100.stanford.edu.

McKinsey indica cómo: « But our analysis shows that humans will still be needed in the workforce. So even while technologies replace some jobs, they are creating new work in industries that most of us cannot even imagine, as well as new ways to generate income and match talent to jobs. One third of new jobs created in the United States in the past 25 years were types that did not previously exist, or barely existed, in areas including IT development, hardware manufacturing, app creation, and IT systems management. The growing role of big data in the economy and business will create a significant need for statisticians and data analysts, for example; we estimate a shortfall of up to 250,000 data scientists in the United States in a decade». Mc Kinsey. «What's Now and Next..., *op. cit.*, p. 10.

(24) Se trata, rememorando a Lessig, de insertar el Derecho en el código, en el diseño de los procesos, las aplicaciones y los negocios. Lessig Lawrence: *El código y otras leyes del ciberespacio*. Madrid, Taurus, 2001. Lessig Lawrence. *Code version 2.0*. New York, Basic Books. Perseus Books Group. Disponible en http://pdf.codev2.cc/Lessig-Codev2.pdf. Traducción al castellano disponible el 21/05/2017 en http://www.articaonline.com/wp-content/uploads/2011/07/El-c%C3%B3digo-2.0-Lawrence-Lessig.pdf.

En este sentido, para regular una nueva tecnología es esencial entender su significado y funcionamiento, y conocer el riesgo que plantea. Las metodologías más usuales tratan de establecer el nivel de riesgo que puede soportar un sistema. Para ello, identifican las vulnerabilidades, esto es los eventos adversos que se pudieran producir, y ponderan la probabilidad de que se materialicen en relación con el impacto o daño que podrían causar. Esta ponderación permite determinar el riesgo real derivado de una determinada tecnología (25). Establecido el riesgo, resulta necesario verificar si existen medidas para gestionarlo. Una vez establecidas éstas, sabremos si podemos eliminar el riesgo, mitigarlo, y si éste es o no asumible. El resultado final permitirá conocer la naturaleza del riesgo residual, esto es del riesgo que permanece si implantamos medidas preventivas o reactivas.

Los objetivos y extensión de este trabajo no permiten desarrollar un análisis de riesgos de carácter general respecto de la inteligencia artificial. No obstante, si se toman como referencia los ejemplos que anteriormente planteamos podríamos identificar algunas situaciones de riesgo que pueden presentar.

— En el ámbito de la medicina la mala calidad de los datos puede afectar el adecuado funcionamiento de un algoritmo. Por otra parte, la propia naturaleza de la tecnología sin duda afectará a la supervisión humana ya que se pondrá al médico ante la decisión de seguir o no una recomendación asumiendo la correspondiente responsabilidad.

— En el ámbito del marketing y la fidelización no sólo pueden producirse errores en la clasificación o categorización de un cliente. El mayor de los riesgos es lo que podría definirse como la inducción de preferencias. Si como se afirma desde el neuromarketing (26) toda compra en inicio es emocional, se podría inducir el consumo de modo artificial. Y esto resultaría particularmente grave en el caso de los menores y en el de las personas cuyas capacidades cognitivas se encuentren funcionalmente limitadas. ¿Podrá un ludópata evitar el impacto de un muro en una red social en el que sólo se habla de apuestas deportivas?

— En el *scoring* bancario o en el ámbito de los seguros, los riesgos más severos son los que se refieren a la posible discriminación de personas.

(25) AEPD.« Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD», Disponible el 11/04/2018 en http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/index-ides-idphp.php

(26) El impacto de las emociones en los procesos decisionales, antes referido, y su traslación al mundo del marketing es un área de investigación emergente y también fuente de innumerables publicaciones de *coaching* empresarial. Véase. VV. AA. *Tu cerebro lo es todo. ¿Sabes cómo y por qué decides?* Barcelona, Plataforma editorial, 2012 y Braidot, Néstor. *Neuromarketing. ¿por qué tus clientes se acuestan con otro si dicen que les gustas tú?* Barcelona, Planeta, 2011.

Con carácter general los expertos identifican tres tipos de riesgos para los derechos que pueden derivar de las aplicaciones de la inteligencia artificial:

A. **El sesgo en el funcionamiento**

En una conocida obra se denomina a los algoritmos que alimentan *machine learning* e inteligencia artificial como «armas de destrucción matemática». A lo largo de su análisis se muestra cómo las decisiones tomadas con el soporte de herramientas de IA pueden producir efectos perniciosos. Por ejemplo, programas de prevención del delito y auxilio a la actividad policial que causan incrementos significativos en la frecuencia con la que se para y registra a personas, afectando sobre todo a minorías. O también, procesos de selección de personal que laminan la diferencia y restan toda oportunidad a personas con diversidad funcional (27).

Ese sesgo puede deberse a muy distintos factores. En unas ocasiones la calidad de los datos que se toman como marco de análisis, en otras las preconcepciones del programador. En algunos casos, son las propias elecciones de sus usuarios las que incorporan el sesgo al insertar datos cuando el sistema debe retroalimentarse con nueva información.

Más preocupante resulta este anormal funcionamiento cuando es intencional, cuando el resultado perverso es exactamente el que se espera obtener. Usualmente, se acusa al marco normativo europeo de limitar la innovación. Pero no es menos cierto que ha surgido un modelo de negocio orientado a la eficiencia que tiende a confundir ésta con la obtención de un resultado económico positivo. Lo que «nos importa» es ganar nuestro primer millón de dólares (28). Nos da igual si nuestra maravillosa aplicación incrementa el número de menores ludópatas que realizan apuestas deportivas, o el de adictos a videojuegos o compras, si discrimina a mujeres y personas con discapacidad en proceso de selección, o si expulsa del mercado del crédito a personas que en condiciones normales lo recibirían.

---

(27) Su conclusión es contundente y planteada desde el inicio: «The math-powered applications powering the data economy were based on choices made by fallible humans beings. Some of these choices were no doubt made with the best intentions. Nevertheless, many of these models encoded human prejudice, misunderstanding, and bias into the software systems that increasingly managed our lives. Like gods, this mathematical models were opaque, their workings invisible to all but the highest priests in their domain: mathematicians and computer scientists. Their verdicts, when even wrong or harmful, were beyond dispute or appeal. And they tended to punish the poor and the oppressed in our society, while making the rich richer». O'Neil, Cathy. *Weapons of Math Destruction*. New York, Crown, 2016, p. 3.

(28) Las inteligencias artificiales se diseñan para la satisfacción de objetivos específicos. No entienden de emociones, pánico o dolor. Así que puede ocurrir que un programa de contratación bursátil de alta frecuencia, vea la oportunidad de ganar unos dólares, aunque pueda desatar un pánico precursor de una crisis global. Y esto no es un ejemplo, sucedió el día 6 de mayo de 2010, con una caída de 1.000 puntos en el Índice Dow Jones entre las 14:42 y las 14:47. Véase Kaplan, Jerry. *Abstenerse humanos*, *op. cit.*, pp. 41 y ss.

Y, al final del camino siempre se podrá afirmar que el individuo en una economía abierta es libre de decidir y debe asumir su responsabilidad si no se informó y no fue consciente de las consecuencias.

Desde el Derecho no podemos someter la innovación a un corsé que la asfixie. Pero tampoco podemos renunciar a un modelo democrático que pone en su centro la dignidad y la libre autodeterminación de las personas. Desde este punto de partida, no todo vale, no todo es posible, no todo es admisible. Existen reglas, algunas muy antiguas y la más elemental fue formulada por Ulpiano entre los siglos II y III: «*alterum non laedere*». Aunque probablemente el lector *millenial* esté más familiarizado con el más moderno *don't be evil* (29).

B. **La sacralización o la impenetrabilidad del algoritmo**

Quienes desarrollan algoritmos y los aplican son, sin duda, los modernos demiurgos. El matemático es el lenguaje infalible de la ciencia y parece no admitir cuestionamiento. Por otra parte, quienes los desarrollan y aplican persiguen resultados objetivos desligados de toda intervención humana. Y, sin embargo, el sesgo o el error existen y pueden causar daños.

Por otro lado, en muchos de los procesos de *machine learning* basados en el autoaprendizaje la programación se diseña para que la máquina reprograme sus procesos. En este nivel de *Deep Learning*, el sistema funciona como una caja negra (30). Conocemos los datos que se facilitan o a los que se accede, los objetivos de programación y los resultados esperables. Pero cuando estos se producen podrían escapar a nuestro control ya que desconocemos la lógica interna (31).

C. **El impacto en la economía**

La sustitución del hombre por procesos automatizados y/o gestionados por máquinas que integran la IA podría suponer la desaparición de muchos puestos de trabajo. En muchos sentidos esta posibilidad puede

(29) En este sentido, señala Stefano Rodotà: «Quando la relazione tra i poteri pubblici e privati e le persone viene basata su di un ininterotto «data mining», sulla raccolta senza limiti di qualsiasi informazioni che la riguardi, e affidata poi all'algoritmo, le persone sono trasformate in astrazioni, la costruzione della loro identità viene sottratta alla loro consapevolezza. Tutto questo incide sui diritti fondamentali, mette in discussione la libera costruziione della personalità e l'autodeterminzaione, imponnedo cosí di chiedersi se e come la società dell'algoritmo possa essere democrática». Rodotà, Stefano. *Il mondo nella rete. Quali i diritti, quali i vincoli*. 6.ª ed. Roma, Laterza, 2018.

(30) Véase, Knight, Will. «El secreto más oscuro de la inteligencia artificial: ¿por qué hace lo que hace?», en *MIT Technology Review*. Disponible el 11/09/2018 en https://www.technologyreview.es/s/7692/el-secreto-mas-oscuro-de-la-inteligencia-artificial-por-que-hace-lo-que-hace.

(31) Un ejemplo lo encontramos en esta noticia: «Facebook apaga una inteligencia artificial que había inventado su propio idioma», Diario *El Mundo*, 28/07/2017. Disponible en http://www.elmundo.es/tecnologia/2017/07/28/5979e60646163f5f688b4664.html.

contribuir a eliminar multitud de oficios altamente peligrosos e incluso insalubres. En otros ámbitos, la confluencia de las tecnologías de la transformación digital puede hacer innecesarios, por ejemplo, todos los puestos relacionados con la conducción de vehículos, o con tareas cuyas variables sean muy limitadas como el mantenimiento y la limpieza de la vía pública o la reposición y cobro de productos en supermercados. La asistencia telefónica humana podría limitarse a supuestos muy específicos, y la asistencia virtual puede alcanzar incluso a las recepciones de los hoteles (32). Cada uno de estos ejemplos nos conecta con tareas que no requieren necesariamente un alto grado de formación, aunque también podría afectar a tareas de nivel intermedio como la gestión económica y administrativa. Por otra parte, aparecerán nuevos nichos de empleo ya que se estima una alta demanda de personas altamente cualificadas en el ámbito de la ingeniería, las matemáticas o el análisis especializado de datos.

Las especulaciones sobre un cambio de modelo económico han abandonado el territorio de la profecía y forman parte de la visión estratégica de las más reputadas empresas y *think tanks* internacionales (33). Así, si en el último lustro se calculaba el impacto de Big Data desde el punto de vista del ahorro de costes, hoy el impacto de IA comienza a replantear el modelo económico global y la necesidad de considerar propuestas como las de la renta básica universal tan denostadas en el pasado reciente (34).

---

(32) Así McKinsey recomienda a los gobiernos: « Rethinking income support and safety nets: If automation (full or partial) does result in a significant reduction in employment and/or greater pressure on wages, some ideas such as universal basic income, conditional transfers, and adapted social safety nets may need to be considered and tested». Mc Kinsey. «What's Now and Next..., *op. cit.*, p. 12.

Martin Ford afirma que en este contexto los empresarios no desean contratar más trabajadores y «la tentación ahorradora de trabajo humano será irresistible». Y apuesta por diseñar nuevos incentivos para el mercado y un ingreso básico garantizado. Ford, Martin. *El ascenso de los robots*. La amenaza de un futuro sin empleo. Ciudad de México, Paidós, 2016, pp. 359 a 365.

(33) McKinsey señala: «Activities that are more easily automatable include physical activities in highly predictable and structured environments, as well as data collection and data processing (Exhibit 5). These activities account for 51percent of wages in the US economy and exist across the entire spectrum of sectors, though they are more prevalent in sectors such as accommodation and food service, manufacturing, transportation and warehousing, and retail trade (Exhibit 6). (…) However, we find that about 30 percent of the activities in 60 percent of all occupations could be automated (Exhibit 8). This means that many workers will work alongside rapidly evolving machines, which will require worker skills also to evolve. This rapid evolution in the nature of work will affect everyone from welders to landscape gardeners, mortgage brokers—and CEOs; we estimate about 25 percent of CEOs' time is currently spent on activities that machines could do, such as analyzing reports and data to inform decisions». Mc Kinsey. «What's Now and Next..., *op. cit.*, p. 8.

(34) En este sentido Satya Nadella afirma que uno de los valores que deben inspirar el crecimiento y desarrollo de IA es el de democratizar el acceso a esta tecnología. Se coincide con esta apreciación. El escenario de desigualdad entre personas, entre empresas, y la profundización de la desigualdad entre países podría llegar a ser aterrador. Nadella, Satya. *Pulsa actualizar*, *op. cit.*, p. 146.

D. **Los riesgos para las libertades**

El reciente affaire Cambridge Analytica ha puesto de manifiesto el impacto del uso de algoritmos con la finalidad de manipular el discurso y alterar el debate público. No es ocioso recordar que en el contexto de los Ordenamientos constitucionales occidentales la jurisprudencia clásica ha afirmado el valor prevalente del derecho a la información y la libertad de expresión cuando se trata de garantizar la formación de una opinión pública libre en una sociedad democrática. Del mismo modo, la jurisprudencia norteamericana sobre internet nos permitió otear una sociedad más libre, en la que por primera vez se empoderaba a la ciudadanía que podía ejercer su libertad de expresión de un modo radicalmente nuevo que merecía ser protegido (35).

Y sin embargo, la analítica de datos en redes sociales y la aplicación de la IA a la personalización de estos entornos permite una manipulación de las preferencias que carece de precedentes (36). La operación es sencilla, a la par que sofisticada. Por ejemplo, para obtener el voto en un proceso electoral, se trata de lograr que los sujetos convencidos operen como un altavoz y que los indecisos sólo puedan ver o leer en sus redes aquellos argumentos que finalmente les convenzan. Y para ello no existen límites, se contratará publicidad altamente personalizada, se generarán miles de perfiles falsos que mantendrán un debate ficticio, se difundirán falsas noticias o verdades a medias para crear una realidad propia de la posverdad (37).

Por otra parte, muchas voces alertan sobre una nueva sociedad de la vigilancia. Es la sociedad que ofrece medios sociales sin precedentes pero

---

(35) «From the publishers' point of view, it constitutes a vast platform from which to address and hear from a world wide audience of millions of readers, viewers, researchers, and buyers. Any person or organization with a computer connected to the Internet can «publish» information. Publishers include government agencies, educational institutions, commercial entities, advocacy groups, and individuals. Publishers may either make their material available to the entire pool of Internet users, or confine access to a selected group, such as those willing to pay for the privilege. «No single organization controls any membership in the Web, nor is there any centralized point from which individual Web sites or services can be blocked from the Web.» (…)

The record demonstrates that the growth of the Internet has been and continues to be phenomenal. As a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it. The interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship».

Supreme Court of the United States, No. 96-511, Janet Reno, Attorney General of the United States, Et Al., Appellants V. American Civil Liberties Union Et Al. On appeal from the United States District Court For the Eastern District of Pennsylvania [June 26, 1997]. Disponible 11/04/2018 en https://www.law.cornell.edu/supct/html/96-511. ZO.html.

(36) Véase, Pariser, Eli. *El filtro burbuja. Cómo la red decide lo que leemos y lo que pensamos*. Barcelona, Taurus, 2017.

(37) Y esta realidad nos debería hacer reflexionar sobre el sentido del derecho a la información en internet. Véase Pauner Chulvi, Cristina. «La libertad de expresión e información como límite al derecho de protección de datos: la excepción periodística», en *Teoría y realidad constitucional*, N.º 36, 2015, pp. 377-398.

que explota la información cosificando al consumidor. Es la sociedad que ofrece las herramientas que dinamizan los movimientos sociales alternativos y a la vez permite un control sin precedentes de éstos, cuando no explota comercialmente los datos que se generan en páginas «solidarias» (38). Se trata de una sociedad vigilada donde el panóptico digital no sólo pertenece al Estado, sino a corporaciones multinacionales, e incluso a pequeños productores de aplicaciones móviles a los cuales regalamos inconscientemente nuestros datos más valiosos a cambio de servicios banales, o en la que ponemos en riesgo a nuestros menores comprando muñecas dotadas de inteligencia artificial (39).

4. ABORDAR LA INTELIGENCIA ARTIFICIAL DESDE EL DERECHO

Cuando se trata de considerar la tecnología es un lugar común el afirmar que no se pueden poner puertas al campo. El legislador, como en la paradoja de Aquiles y la tortuga, siempre se encontrará a mitad de camino de su meta. Los tiempos de la tecnología son mucho más rápidos, que los tiempos del legislador que nunca podrá regular este ámbito si se centra en un enfoque basado en regular cada manifestación tecnológica. Pero renunciar por completo a la regulación de una materia tan particularmente sensible como la inteligencia artificial resulta sencillamente imposible.

Por otra parte, se afirma que en la Unión Europea el regulador opera como una significativa barrera para la innovación tecnológica. Desde este punto de vista, un modelo abierto como el norteamericano facilita la generación de ecosistemas favorables a la innovación y explica la razón por la que el desarrollo de las tecnologías de la información se produce en Estados Unidos. Es posible, que tanto la lentitud de legislador como la superproducción normativa, deban reorientarse evitando rigideces y estimulando la investigación. Pero no es menos cierto, que apostar por la desregulación podría ser una decisión no exenta de peligros. Esencialmente, porque la experiencia demuestra que en los últimos decenios el desarrollo tecnológico persigue como objetivo esencial maximizar el beneficio con independencia del daño que se pudiera causar. En el ámbito

(38) El negocio del *data broking* ha sido abordado en profundidad por la Federal Trade Commission. El título de su informe lo dice todo. VV. AA. *Data Brokers. A Call for Transparency and Accountability*. FTC, 2014. Disponible el 11/04/2018 en https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

(39) Martínez Martínez, Ricard. «Juguetes conectados» en *Bez Diario* 05/01/2016. Disponible el 11/04/2018 en https://www.bez.es/45098303/Juguetes-conectados.html.

de la inteligencia artificial, contamos con ejemplos más que significativos (40).

Afirmar que el Derecho no puede abordar de ninguna manera tecnología es tan falso como atribuir a la acción normativa un efecto paralizante. Los hechos demuestran que las normas son necesarias, y la visión de una tecnología neutral resulta sencillamente idílica. La tecnología ni tiene porqué ser neutral, ni tiene porqué perseguir las mejores condiciones para el desarrollo del ser humano. Este es precisamente el objetivo que debería perseguir el Derecho.

En nuestros días, puede afirmarse que la formulación más acabada y reciente para abordar el fenómeno de la Inteligencia Artificial es el Reglamento (UE) 2016/679 (41). Esta norma nos propone ciertas estrategias muy relevantes para aproximarnos al fenómeno:

---

(40) Ya se ha señalado hasta qué punto los sistemas automatizados de intermediación en el mercado bursátil causan crisis. Y de todos resulta ya tristemente conocido el caso Cambridge Analytica. Véase, «Five things we learned from Mark Zuckerberg's Facebook hearing», The Guardian, Disponible el 12/04/2017 en https://www.theguardian.com/technology/2018/apr/11/mark-zuckerbergs-facebook-hearing-five-things-we-learned

Byung-Chul Han, se refiere al «capitalismo de la emoción: «Las emociones, en cuanto *inclinaciones*, representan el fundamento energético, incluso sensible de la acción. Están reguladas por el sistema límbico, que también es la sede de los impulsos. Constituyen un nivel prerreflexivo, semiinconsciente, corporalmente instintivo de la acción, del que no se es consciente de forma expresa. La psicopolítica neoliberal se apodera de la emoción p*ara influir en las acciones a este nivel prerreflexivo*. Por medio de la emoción llega hasta lo profundo del individuo. Así la emoción representa un medio muy eficiente para el control piscopolítico del individuo». El modo de obtener la información, de poner en funcionamiento el Big Brother se basa en la amabilidad y usabilidad del *Smartphone*. Han, Byung-Chul. *Psicopolítica*. Barcelona, Herder, 2014, pp.61, 74 y 75.

David Lyon, en su conversación con Zygmunt Bauman concluye que «Bauman ha demostrado una y otra vez cómo el consumo está en simbiosis con la producción de las divisiones sociales. Lo paradójico aquí reside en que, mientras el consumismo implica la placentera seducción de los consumidores, esta seducción es el resultado de la vigilancia sistemática a gran escala». Bauman, Zygmunt y Lyon, David. Vigilancia liquida. Barcelona, Austral, 2013, p. 15.

(41) Esta óptica ha sido adoptada por la Comisión Nacional para la Informática y las Libertades francesa que apunta en gran medida conclusiones coincidentes con muchas de las obras citadas en este trabajo:

«Le prestige et la confiance accordés à des machines jugées souvent infaillibles et «neutres» ne risquent-ils pas de générer la tentation de se décharger sur les machines de la fatigue d'exercer des responsabilités, de juger, de prendre des décisions (…)

Les algorithmes et l'intelligence artificielle peuvent susciter des biais, des discriminations, voire des formes d'exclusion. (…)

L'écosystème numérique tel qu'il s'est construit avec le Web, mais également plus anciennement les echniques actuarielles, ont fortement exploité les potentialités des algorithmes en termes de personnalisation.(…)

Le choix du type de données alimentant un modèle algorithmique, leur quantité suffisante ou insuffisante, l'existence de biais dans les jeux de données servant à entraîner les algorithmes d'apprentissage constituent un enjeu majeur.(…)

L'autonomie croissante des machines ainsi que l'émergence de formes d'hybridation entre humains et machines (hybridation au plan d'une action assistée par des recommandations algorithmiques, mais aussi prochainement au plan physique) questionnent l'idée d'une spécificité humaine irréductible. Faut-il et est-il possible de parler au sens propre d' «éthique des algorithmes»?» CNIL. *Comment permettre à l'homme de garder la main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*. Diciembre 2017. Disponible el 11/04/2018 en https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf.

1. **La privacidad basada en el diseño**

Este principio implica un enfoque determinante. Antes de iniciar cualquier proceso de IA, sus responsables deben considerar los riesgos que derivarán del uso de datos para los derechos fundamentales.

2. **El principio de minimización y los principios relacionados con el tratamiento**

Cuando un proceso requiera de datos personales ineludiblemente deberá utilizar exclusivamente que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados, la llamada «minimización de datos»). El resultado práctico de la privacidad basada en el diseño sumada a la minimización condicionará la licitud de las acciones, el volumen de datos a tratar y las finalidades de dichos tratamientos.

Habida cuenta del carácter instrumental del derecho fundamental a la protección de datos, estos principios operarán como garantía del conjunto de las libertades al limitar las condiciones del tratamiento y sus resultados.

3. **El principio de transparencia**

El artículo 13.2.f) RGPD obliga a ofrecer al interesado una información significativa sobre la lógica aplicada, así como respecto la importancia y las consecuencias previstas de un tratamiento cuando implica la adopción de decisiones automatizadas de las que deriven efectos jurídicos o le afecten significativamente de modo similar. Por tanto, la norma permite dotar de transparencia a los algoritmos empleados por la Inteligencia Artificial en este tipo de situaciones (42).

4. **Evaluación del daño y notificación de violaciones de seguridad: *«non laedere»***

En protección de datos, ciertos tratamientos exigen desplegar una evaluación de impacto relativa a la protección de datos (43) ordenada precisamente a identificar situaciones de alto riesgo para los derechos y

(42) Véase https://algorithmwatch.org/en/the-adm-manifesto/.

(43) De nuevo los que impliquen «evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar». El Grupo de Trabajo del artículo 29 plantea una interpretación extensiva de estos conceptos que podría alcanzar sin duda a los modelos de IA que funcionen con datos personales.

libertades de las personas físicas. Estas situaciones, cuando derivan de un incidente de seguridad obligan a notificarlo a los interesados.

El regulador subraya por tanto el carácter central de un principio milenario: no podemos hacer daño a las personas.

A partir del ejemplo, del Reglamento (UE) 2016/679 no parece descabellado afirmar que existen marcos normativos que pueden contribuir a la garantía de los derechos de las personas en relación con los usos de la Inteligencia Artificial. Por tanto, no parece necesario diseñar un nuevo derecho fundamental digital específico. Sin embargo, la IA no se desplegará únicamente sobre información personal, puede operar sobre cualquier contexto, afectar a cualquier sector de la vida social y económica e incidir sobre casi cualquier ámbito físico o virtual desde la producción de bienes y servicios a la gestión del tráfico, de las *Smart Cities* al medio ambiente.

Ello implica sin duda requerir una acción urgente de los poderes públicos que podrá ser o no materialmente regulatoria (44). Sobre lo que no cabe ninguna duda, es sobre la urgente necesidad, de definir ciertos pilares básicos que deberían orientar las políticas públicas y la normativa en materia de Inteligencia Artificial (45):

— Situar la dignidad del ser humano y la garantía de los derechos fundamentales como límite infranqueable para el desarrollo de la tecnología.

— Asegurar la responsabilidad de las personas y entidades que desarrollen algoritmos de IA. No pueden compartirse las reiteradas, y por otra parte agotadoras reflexiones, que pretenden establecer un *tertium genus* en la personalidad jurídica de la inteligencia artificial y los robots. Estos ingenios existen porque alguien los concibió, porque alguien los diseñó y programó, y porque alguien decidió usarlos para un determinado propósito.

— Garantizar modelos de desarrollo basados en datos legítimamente obtenidos, con procesos orientados a verificar su calidad, y con claros deberes de verificar las consecuencias del uso de la IA en condiciones de ensayo previo. El análisis de riesgos y el análisis de impacto no pueden sino ser un principio normativo de cumplimiento ineludible.

— Asegurar el principio de transparencia de los algoritmos que deben ser auditables. Este principio deberá conciliarse sin duda con la protección de la innovación científica e industrial y la propiedad intelectual, lo

(44) El Parlamento Europeo ha instado a que se inicie una reflexión en este sentido: «Informe de 27 de enero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica [2015/2103(INL)]. Disponible el 11/04/2018 en http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0005+0+DOC+XML+V0//ES.

(45) Véase, Barcelona Declaration for the Proper Development and Usage of Artificial Intelligence in Europe. Disponible el 11/04/2018 en https://www.iiia.csic.es/barcelonadeclaration/.

que podría exigir la atribución de competencias de fiscalización a autoridades independientes.

— Obligar a la trazabilidad de los sistemas cuando se pongan en juego valores fundamentales como la salud de las personas, la discriminación o la vigilancia policial. En este tipo de usos deberá poder identificarse el proceso de decisión, las personas implicadas y las consecuencias que se deriven.

— Ordenar la nulidad de cualquier decisión con consecuencias jurídicas y materiales, y particularmente de las pruebas incriminatorias, cuando vulneren estos principios básicos.

— Situar la garantía de la autodeterminación individual, de la libertad de las personas y de los colectivos en los que se integran como un límite absolutamente intangible.

Con toda seguridad, se han ofrecido al lector ideas ciertamente básicas en las que deberá profundizarse. Desgraciada, o afortunadamente, la mente humana es limitada, no puede alcanzar todas las posibilidades y correlaciones. Afortunadamente, algo tan limitado, humano, poco tecnológico –y «habermasiano»–, como el debate democrático a la búsqueda de un consenso racional sea una de esas cosas que requerirían de una inteligencia general, emocional y empática de la que las máquinas carecen.

Y este debate no puede ser únicamente nacional. Debe ser internacional y plantearse desde un enfoque en positivo. Resulta fundamental definir un marco transnacional para la inteligencia artificial, e incluso para un marco global, que bajo la filosofía de una «Convención Digital de Ginebra», dote de seguridad jurídica. Y es esencial un enfoque centrado en el ser humano que borde el uso de la información, de los datos para el bien común de la humanidad.

CAPÍTULO 12

EXPECTATIVAS DE PRIVACIDAD, TUTELA DE LA INTIMIDAD Y PROTECCIÓN DE DATOS

JUAN ANTONIO HERNÁNDEZ CORCHETE
Universidad de Vigo

1. LA PRIVACIDAD COMO ESPACIO DE AUTONOMÍA PERSONAL EN LA SOCIEDAD DIGITAL.
2. LAS REGLAS DE TRATAMIENTO DE LA INFORMACIÓN PERSONAL SON GARANTÍA O INSTRUMENTO DE PRIVACIDAD.
3. EL ALCANCE DE LA GARANTÍA DE PRIVACIDAD: ENTRE SU CONDICIÓN DE DECISIÓN POLÍTICA, LA COHESIÓN INTERNA EN LA UE Y EL MERCADO INTEGRADO DE LA SOCIEDAD DIGITAL GLOBAL.
   - 3.1 Decisión política.
   - 3.2 Cohesión económica y social en la UE.
   - 3.3 El mercado integrado de la sociedad digital global.
4. LÍMITES DE LA PRIVACIDAD. EN ESPECIAL LA NECESARIA INTERVENCIÓN LEGISLATIVA.
5. TÉCNICAS DE TUTELA DE LA PRIVACIDAD. APUNTES.
   - 5.1 A vueltas con el consentimiento.
   - 5.2 Mero cumplimiento *vs.* análisis de riesgo: consecuencias.
   - 5.3 La patrimonialización de los datos personales no es garantía de privacidad.
   - 5.4 La reacción sancionadora, con especial consideración al RGPD.

1. LA PRIVACIDAD COMO ESPACIO DE AUTONOMÍA PERSONAL EN LA SOCIEDAD DIGITAL

La sociedad digital y los nuevos desarrollos tecnológicos y organizativos que ha traído consigo presentan innumerables ventajas, tanto para la iniciativa privada y el bienestar económico general de los ciudadanos, como también para la más eficaz consecución de los fines estrictamente públicos. Este proceso, que no ha hecho más que comenzar, seguirá reportando nuevos beneficios, que serán mayores en la medida que se acierte a crear un entorno favorable, también en lo relativo a la regulación jurídica de este sector de actividad (1).

Las exigencias de privacidad (2), y de un modo específico la regulación positiva del tratamiento de la información personal, impiden que el manejo de dicha información pueda abordarse de cualquier forma, vedando ciertos usos y requiriendo en cualquier caso adoptar cautelas y cumplir principios, todo lo cual se configura como una gravosa carga que ha de levantarse para que sea posible el tratamiento de datos personales que está en la base del servicio digital de que se trate. Surge entonces una pregunta clave: ¿Tiene sentido una reglamentación que pone en riesgo una serie de ventajas tan importante?

La respuesta depende, obviamente, de qué beneficios se busquen con la regulación y, en última instancia, de si los mismos han de prevalecer sobre el gravamen que supone para la innovación tecnológica y el surgimiento y consolidación de nuevas aplicaciones digitales. Las reglas de tratamiento de datos personales, consideradas simplemente como técnica regulatoria que ordena este sector de actividad, no justificarían consecuencias tan inconvenientes para la extensión y refuerzo de la innovación tecnológica en el ámbito digital. Mayor peso en la ponderación adquieren estas reglas cuando se aprecia que mediante ellas se tiende a garantizar el control que cada sujeto realiza sobre una emanación de la persona sobre la que es predicable una cierta pretensión patrimonial. No obstante, en la medida que el sujeto implica en estos casos una posición patrimonial, no es difícil argumentar que las reglas de tratamiento de datos personales

(1) Acerca de la función del Derecho (y sus límites) respecto de las nuevas realidades que derivan de la innovación tecnológica, *cfr.* Piñar Mañas, J. L.: Derecho e innovación tecnológica, Discurso leído en la festividad de San Raimundo de Peñafort el 8 de febrero de 2018, CEU Ediciones, 2018.

(2) «Este trabajo opta por el término de privacidad para enfatizar que se trata de algo radicalmente distinto de lo tradicionalmente entendido por intimidad. Hay autores que se refieren a estas mismas cuestiones bajo el concepto de intimidad, pero atribuyéndole este alcance completamente nuevo, con lo que se trataría más que nada de una diferencia terminológica que no debe inducir a confusión. *Vid.* en este sentido el extraordinario estudio de Ollero Tassara, A.: *De la protección de la intimidad al poder de control sobre los datos personales*, Real Academia de Ciencias Morales y Políticas, 2008, en especial pp. 137 a 167; y también López Ortega, J.J., "Intimidad informática y derecho penal", en *Derecho a la intimidad y nuevas tecnologías*, Cuadernos de Derecho Judicial 2004 (IX), pp. 131-132».

deberían ceder frente a los muy notables intereses generales que hemos indicado que reviste la expansión y asentamiento de la sociedad digital. Y tampoco sería tarea extraordinariamente ardua mantener que los sujetos cuya posición patrimonial quedaría sacrificada obtienen multitud de compensaciones a cambio, ya sea en forma de servicios que reciben individualmente, ya sea en forma de bienes públicos que no serían igualmente posibles (o directamente no serían posibles) sin las ventajas asociadas a la sociedad digital.

Cambia por completo el juicio de ponderación cuando se aprecia que los sistemas actuales de tecnologías de la información y con más razón los que son de esperar en un futuro muy cercano, al admitir el análisis masivo y a un coste inapreciable de los datos de carácter personal que se puedan recoger o que se obtengan mediante alguna cesión legal, suministran a quienes los operan una información acerca del sujeto titular que es tremendamente significativa, lo que a su vez les coloca en situación de condicionar las decisiones de dicho sujeto, haciendo ilusa su autonomía personal para organizar y desarrollar su proyecto vital. Esta capacidad de influencia no se configura en la actualidad como un futurible, sino que es una realidad que ya se está practicando (3). A este esquema responden los servicios en línea que se prestan gratuitamente debido a que su modelo de negocio consiste en elaborar, mediante la combinación de sus datos personales generados con el uso de la aplicación, perfiles de los usuarios al objeto de dirigirles publicidad orientada, siendo la comercialización de esa publicidad la fuente de ingresos empresariales. La conclusión es necesariamente que, siendo posible obtener información significativa de un usuario con el fin de comunicarle publicidad que sea de su interés o de prestarle otro servicio de análisis que le beneficie, es igualmente factible hacerlo con propósitos que, prescindiendo absolutamente de su interés, se orienten a condicionar sus decisiones para ventaja exclusiva de un tercero (i.e. elecciones y consultas refrendarias, juego, seguros, acceso al empleo y carrera, etc.).

La autonomía personal, comprendida como espacio de libre decisión del sujeto, es un atributo esencial del individuo que se conecta directamente con su dignidad como persona. En nuestro ordenamiento jurídico el libre desarrollo de la personalidad aparece ligado directamente a la dignidad de la persona en el artículo 10.1 CE, donde se califica a ambos de «fundamento del orden político y de la paz social», si bien es cierto que, en materia de derechos, el Tribunal Constitucional reconduce el valor jurídico de dichas previsiones constitucionales a los derechos y libertades

(3) Hay autores que lo ven como un proceso imparable y recomiendan como única solución introducir confusión con comportamientos digitales simulados. *Cfr*. Brunton, F y Nissenbaum, H.: *Obfuscation: a user's guide for privacy and protest*, The MIT Press, 2015.

explícitamente enunciados en su articulado. Este enfoque restrictivo, que no es el de otros ordenamientos de nuestro entorno ni el del sistema del Convenio de Roma (4), se está demostrando inconveniente y necesitado de superación, sobre todo en relación a nuevas realidades conectadas con los bienes de la personalidad como la que estamos exponiendo.

La autonomía personal así entendida se ha reputado vulnerada cuando los poderes públicos han interferido en ella de un modo coercitivo, sea mediante la prohibición de ciertas opciones (limitar la libertad de procreación en virtud de esterilizaciones de incapaces, STC 215/1994, FJ 4), sea a través de la imposición de algunas otras (asociar forzosamente ciertas consecuencias a las uniones de hecho, STC 93/2013, FJ 8). Pero es susceptible de resultar afectada no solo de manera coercitiva, sino también por medio de condicionantes que, principalmente sin la conciencia del sujeto, alcancen a manipular sus decisiones, guiándolas sin su voluntad efectiva en determinadas direcciones. Los tratamientos de datos personales ligados al desarrollo de la sociedad digital pueden, por suministrar información significativa de la persona y porque lo hacen sin que ésta repare en esta realidad ni en que se usa para influirle, producir esta incidencia manipulativa y consecuentemente pueden mermar o incluso anular la privacidad del sujeto entendida como espacio de libre decisión o, dicho con otras palabras, de autonomía personal (5).

No faltan voces autorizadas que han negado rotundamente que la privacidad tenga algún juego como límite a los servicios digitales que implican el tratamiento de datos personales. Se ha sostenido, por un lado, que la privacidad es un valor que no interesa al sujeto titular de los datos, como lo acreditaría la facilidad con la que consienten que sus datos sean recogidos, tratados y cedidos en los términos que se anuncian en el aviso de privacidad. Esta consideración lo único que revela es la distancia que hay entre admitir que los datos propios sean objeto de ciertos tratamiento y aceptar que el producto de ese manejo alcance a constreñir su ámbito de autonomía personal. Esto último, aun en la hipótesis que sea derivación natural de los usos y cesiones consentidas, no queda razonablemente comprendido en el consentimiento, pues es un resultado que el sujeto titular de los datos no se representa al tiempo de prestarlo.

(4) El TCFA alude con normalidad en materia de derechos a la dignidad y al libre desarrollo de la personalidad (arts. 1 y 2.1 GG), recientemente Decisión de 10 de octubre de 2017 (1 BvR2019/16). Véanse, respecto del Convenio de Roma, las SSTEDH de 25 de marzo de 1992 (caso «B» c. Francia), de 11 de julio de 2002 (casos «I» y Christina Goodwin c. Reino Unido) y de 8 de enero de 2009 (caso Schlumpf c. Suiza).

(5) *Cfr.* Bernal, P: *Internet Privacy Rights*, Cambridge University Press, 2014, que en la p. 2 afirma que «the key reason that privacy has become important is that privacy matters to people, at least in part, because people cares about their autonomy». Para una exposición de esta concepción de la privacidad, véase Solove, D.: «Conceptualising Privacy», *California Law Review*, 2002, pp. 1116 a 1118.

Se argumenta igualmente que la privacidad es un valor del todo incompatible con la sociedad digital, debiendo adaptarse la persona al nuevo entorno, orientándose a aprovechar las virtualidades que ofrece al tiempo que se pierden otras situaciones ventajosas. En el fondo de este criterio está la idea de que la falta de privacidad no es una merma grave para quien no tiene nada que ocultar (6). Este planteamiento halla un déficit grave al dejar de apreciar que la información significativa de la persona que es apta para limitar su autonomía deriva principalmente de la consideración masiva de aspectos minúsculos e insignificantes de la actividad del sujeto. No es el carácter íntimo o el componente negativo de los datos personales manejados lo que suministra esa imagen significativa, sino la combinación de un sin número de insignificantes vicisitudes, con lo que no parece verosímil que las personas en general admitan que la sociedad digital conlleve esa pérdida (7). Baste como ejemplo el historial crediticio de un individuo, en el que lo relevante, más que las eventuales referencias negativas a la no realización de pagos debidos, es la información sobre el conjunto de pagos que ha hecho satisfactoriamente (8).

En fin, la privacidad entendida como espacio de autonomía personal es un bien jurídico que debe ser protegido también en la sociedad digital, aun cuando su respeto pueda exigir una regulación del tratamiento de datos personales que condicione de alguna manera la innovación tecnológica y en última instancia el desarrollo de la sociedad digital. Sin embargo, como más adelante se expondrá, la tutela de este bien jurídico no necesariamente requiere renunciar a ciertos tratamientos, bastando con someterlos a garantías adecuadas y suficientes.

2. LAS REGLAS DE TRATAMIENTO DE LA INFORMACIÓN PERSONAL SON GARANTÍA O INSTRUMENTO DE PRIVACIDAD

Otra polémica relevante en la doctrina especializada gira en torno a si la privacidad es un valor en sí mismo o, por el contrario, es instrumental de otros bienes jurídicos. Muy probablemente, o al menos a mí me lo parece, está divergencia doctrinal va ligada estrechamente a una situación de equivocidad terminológica. Afirman que la privacidad es instrumental aquellos autores que reconocen en ella el control que a la persona se le debe garantizar sobre la información que le concierne, sosteniendo que así entendida está al servicio de la libre decisión del sujeto sobre cómo desarrollar su personalidad. Naturalmente, aquellos otros autores que ven

(6) *Cfr.* Brin, D: *The Transparent Society*, Addison Wesley, 1998.

(7) *Cfr.* Solove, D., «I´ve got nothing to hide' and other misunderstandings of privacy», *San Diego Law Review*, num. 44, 2007, pp. 745 y ss.

(8) Acerca del potencial revelador de estos datos, *Cfr.* Cuena Casas, M: «Intercambio de información positiva de solvencia y funcionamiento del mercado de crédito», *InDret*, núm. 3, 2017.

en la privacidad precisamente este ámbito de libre decisión del sujeto le atribuyen carácter final y no instrumental (9).

Centrándome en esta segunda concepción, que es la que he defendido en el apartado anterior, es importante resaltar que lo que el tratamiento incondicionado de datos personales pone en riesgo no es la capacidad para realizar una u otra concreta opción vital. Si así fuera la ponderación con otros bienes jurídicos dependería de qué tipo de opción se tratase y lo que acabaría protegiéndose no sería propiamente la capacidad de decisión sino los intereses del sujeto en ese preciso ámbito material. Por este motivo cabe insistir en que lo que verdaderamente se compromete es la autonomía personal en su integridad. Primero porque ésta no es susceptible de fragmentación, como acredita que resulta absolutamente imposible predecir a priori sobre qué decisión o decisiones recaerá el condicionamiento derivado del manejo masivo de datos personales. Segundo, porque lo que caracteriza al hombre como persona es precisamente la capacidad genérica de decisión libre y no meramente la garantía de decidir libremente aspectos concretos, situación esta última que puede conllevar una protección específica y adicional conectada con el sustrato material de la decisión concreta.

Las que sí se conforman como garantía o instrumento de la privacidad en el sentido que se viene apuntando son las reglas y principios que rigen el tratamiento de la información personal. Este carácter instrumental es el que determina que deba verse en ellas mucho más que una simple técnica regulatoria, pues son en realidad preceptos que están informados por su función de garantizar un bien jurídico del máximo calibre como es el espacio de libre decisión que connota la autonomía de la persona. Ahora bien, debe observarse igualmente que la afectación de la autonomía personal que la regulación del tratamiento de datos personales pretende evitar es un riesgo notablemente abstracto. No siempre el incumplimiento de alguna de estas previsiones normativas coadyuvará de un modo relevante a que se produzca una vulneración de la autonomía personal, y además en los casos en que así ocurra será una condición necesaria pero en ningún caso suficiente, dado que la afectación de aquélla se producirá por un cúmulo de acciones y no por una sola.

Este carácter abstracto o remoto del riesgo de quiebra de la autonomía personal debe tenerse muy presente al definir y también al aplicar la normativa de protección de datos de carácter personal. Y cabe defender como principio esencial de este planteamiento que, desde la perspectiva de la protección de la autonomía personal, que es la relevante cuando se aborda la protección de datos como derecho fundamental, lo importante no es un enfoque estrictamente reglamentista, que ponga el acento en la reali-

(9) Sobre las distintas concepciones de la privacidad en relación a su consideración como bien instrumental o valor intrínseco, *Cfr*: Solove (2002), *op. cit.*, p. 1145.

zación de uno o varios trámites previstos en la ley, sino una visión de conjunto, que verifique hasta qué punto un tratamiento de datos de carácter personal arriesga que la autonomía personal resulte afectada.

En este sentido procede reconocer que el enfoque de responsabilidad proactiva que caracteriza el RGPD (véase en especial su artículo 24), según el cual al responsable del tratamiento se le exige una valoración general del riesgo que el mismo conlleva, se acerca más a este planteamiento que pone el énfasis más en el derecho fundamental del ciudadano que en el mero cumplimiento de una reglamentación técnica por el responsable del tratamiento. Este nuevo enfoque requiere para su más correcto funcionamiento de algunas opciones regulatorias complementarias. Destaca entre ellas que el incumplimiento de determinadas previsiones concretas de la normativa de protección de datos no necesariamente conlleve la imposición de sanciones, debiendo valorarse y justificarse cuándo la adopción de otras medidas correctoras no se considera como medida adecuada y suficiente. Es cierto, no cabe ninguna duda, que este planteamiento, que resalta la virtualidad de los derechos en detrimento del mero cumplimiento reglamentista, presenta el inconveniente de la incertidumbre en la aplicación de las normas, que exigirá como contrapeso que tanto las Administraciones como los Tribunales motiven con un mayor grado de detalle las razones que les llevan a optar por una u otra solución aplicativa. En esta misma línea merece un juicio positivo que en el RGPD se termine con la separación existente en la Directiva 95/46/CE entre el procedimiento de tutela y el procedimiento sancionador. Existirá un solo procedimiento en que se examinará el cumplimiento de la normativa de protección de datos y se ponderará si conviene una reacción sancionadora o simplemente medidas de tutela de la posición jurídica del titular de los datos personales.

3. EL ALCANCE DE LA GARANTÍA DE PRIVACIDAD: ENTRE SU CONDICIÓN DE DECISIÓN POLÍTICA, LA COHESIÓN INTERNA EN LA UE Y EL MERCADO INTEGRADO DE LA SOCIEDAD DIGITAL GLOBAL

3.1 **Decisión política**

La privacidad como espacio de libre decisión de la persona es un bien jurídico básico en cualquier Estado de Derecho, pero depende de cada ordenamiento jurídico la forma en que se garantiza. No es solo que los principios y reglas que caractericen el tratamiento de la información personal se organicen de uno u otro modo configurando sistemas diferentes de protección, sino que también resultan legítimas las distinciones en el grado mismo que revista la protección. Al fin y al cabo disponer una tutela más o menos intensa de la privacidad es una opción de carácter relacio-

nal, dado que implica correlativamente dar mayor o menor intensidad a la protección del resto de situaciones jurídicas que entran en conflicto. Se trata, en definitiva, de una decisión política que delimita el alcance de derechos individuales (que afectan a la esencia del individuo) y no de una opción regulatoria en la que prevalezca un componente técnico. La consecuencia inmediata es que el alcance de la garantía de la privacidad es una decisión cualificada de la representación política que, con absoluta normalidad, puede cambiar de una sociedad a otra (10). El poder público, sin embargo, no puede obviar al definir este alcance el carácter integrado del entorno digital, así como las pretensiones de unidad económica y cohesión social que gobiernan la Unión Europea.

3.2 **Cohesión económica y social en la UE**

Comenzando por esto último, el tratamiento de datos de carácter personal, aparte de incidir en los derechos individuales de los titulares, ha de ser objeto de atención como elemento productivo, en la medida que cada vez son más las iniciativas empresariales, y en general los proyectos que surgen en la sociedad con propósitos diversos, que tienen como ingrediente imprescindible el manejo de datos personales. Desde esta perspectiva, que considera la información personal como un recurso productivo más, la Unión Europea necesita garantizar su flujo transfronterizo dentro de los Estados Miembros y a este objeto eliminar las barreras que lo puedan obstaculizar, entre ellas la diversidad regulatoria. La Directiva 95/46/CE, aprobada en un tiempo en que las competencias de la Unión Europea eran mayormente de carácter económico, se apoyó en esta condición de recurso productivo de los datos personales para aproximar las regulaciones nacionales de esta materia. El nuevo RGPD, aunque en este momento las competencias de la Unión Europea superan con mucho los aspectos económicos y el Derecho Primario incluye una declaración de derechos fundamentales que proclama el derecho fundamental a la protección de datos de carácter personal en su artículo 8, vuelve a justificarse principalmente por la necesidad de fomentar el flujo transfronterizo de los datos personales. Lo que justifica en realidad el RGPD es que se ha alcanzado el convencimiento de que el grado de unidad económica y cohesión social que se desea entre los Estados de la Unión Europea requiere no solo reducir las diferencias regulatorias relativas al tratamiento de los da-

(10) Murray, A.: «Conceptualising the Post-Regulatory (Cyber)state» en R. Brownsword y K. Yeung (Eds.): *Regulating Technologies*, Hart, 2008, p. 297, sostiene que los poderes públicos no pueden aspirar a regular el ciberespacio, cuyas reglas se fijan a nivel supranacional y de un modo conjunto por los actores privados intervinientes. A mi juicio, aun reconociendo que la sociedad digital tiene un importante potencial de autorregulación, no es admisible que el poder público haga dejación de su responsabilidad de decidir los elementos esenciales de la organización social.

tos personales mediante la aproximación de legislaciones nacionales, sino uniformar las mismas salvo contadas excepciones, para lo que se necesita una norma europea en forma de Reglamento y no de Directiva.

Como se viene desarrollando en este trabajo, las reglas y principios que rigen el tratamiento de la información personal se orientan a la protección de la privacidad. No es posible, por tanto, uniformar el tratamiento de datos personales como recurso económico sin proceder al mismo tiempo a delimitar el alcance de la garantía de la privacidad. Son dos caras inescindibles de la misma realidad. En cuanto a esta segunda perspectiva cabe avanzar la siguiente valoración. Algunos tribunales constitucionales europeos, aunque sea con matices, ya han sentado que los derechos fundamentales integran la identidad nacional que informa en última instancia sus Constituciones, por lo que afirman su jurisdicción para el caso de que la protección dispensada en la legislación europea no se considere adecuada. En este contexto resulta más apropiado un planteamiento que deje un cierto margen a los Estados miembros para definir cuál es el régimen de cautelas conforme al que un determinado tratamiento de datos personales se repute compatible con las exigencias de privacidad, de tal modo que se admite que sean los legisladores de los Estados miembros quienes ponderen los bienes jurídicos en presencia, prefiriendo un cierto equilibrio entre ellos u otro. Este enfoque era el de la Directiva 95/46/CE y también el del RGPD en lo que hace a los tratamientos que vienen justificados por fines de interés general [véanse los apartados c) y e) del art. 6.1 en conexión con los arts. 6.2 y 6.3]. Por el contrario, el RGPD parece abandonar esa aproximación por lo que se refiere a los tratamientos de datos personales ligados a actividades de interés privado, pues su artículo 6.1.f) los admite incluso sin el consentimiento del titular de los datos, con tal que sean «necesarios para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero» y «siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado», no permitiendo, o al menos a ello apunta su silencio por contraste con los artículos 6.2 y 6.3, que los Estados miembros intermedien en la determinación de qué intereses privados son legítimos y prevalentes ni en la precisión de qué régimen de cautelas en el tratamiento les confiere esa condición.

Se aprecia, por tanto, que la ponderación entre la privacidad y otros bienes jurídicos, estableciendo en qué condiciones ciertos tratamientos son admisibles por sacrificar la privacidad de un modo proporcionado, se remite al legislador nacional cuando los fines del tratamiento son de interés general y, a la inversa, no se permite esta intervención nacional cuando el tratamiento persigue intereses privados que deban reputarse legítimos y prevalentes. Sin olvidar que a los Estados miembros debe reservárseles un

amplio margen en la selección de los fines públicos que persiguen y en qué medida la privacidad del sujeto debe ceder para hacerlos posibles, parece que esa diferencia obedece también a que al segundo tipo de tratamientos responderán los que se realizan característicamente en el contexto de las actividades económicas privadas, ámbito en el que se pretende llevar la uniformidad regulatoria a su grado máximo para facilitar la cohesión económica y social dentro de la Unión Europea. En conclusión, el legislador europeo sacrifica en relación a esta categoría de tratamientos la intervención de los legisladores nacionales en la definición del alcance de la garantía de privacidad en función de que las reglas de juego aparezcan determinadas de un modo completamente uniforme y que ello facilite la actuación transfronteriza de las empresas, la mayor competencia entre ellas y en general las ventajas del mercado interior. El objetivo es claro y producirá beneficios relevantes. Habrá que ver, no obstante, si los legisladores nacionales aguantan la tentación de intervenir a falta de legislaciones europeas de carácter sectorial. Esto, sin embargo, ya es materia del epígrafe 4.

3.3 **El mercado integrado de la sociedad digital global**

El carácter inmediato del entorno digital se resiste a las fronteras nacionales. El usuario accede de forma instantánea a un servicio digital que se le ofrece desde cualquier ubicación en el mundo, aunque sea muy lejana, aunque esté en otro país y allí la regulación del tratamiento de datos personales sea otra muy diferente. De igual manera, la información generada a partir del tratamiento de datos personales se inserta como recurso económico en un mercado global que destaca por su carácter completamente integrado (11). Siempre aporta complejidad la sujeción a diferentes normativas de las relaciones jurídicas de componente transfronterizo, pero en las circunstancias descritas en que opera el entorno digital la distorsión se hace más patente. Por todo ello, no cabe la menor duda que cualquier aproximación de legislaciones en este ámbito material favorece el avance de la sociedad digital y el desarrollo de las nuevas tecnologías que lo hacen posible, siendo por tanto la solución regulatoria más eficiente. Ahora bien, el hecho de que resulte conveniente una regulación homogénea no quita para que los Estados, privilegiando unos bienes jurídicos en conflicto frente a otros, mantengan disciplinas distintas, circunstancia que por otro lado es la que se corresponde con la realidad, como salta a la

(11) Una defensa del flujo internacional de datos personales como un asunto estrictamente de mercado en M. Byrne Sedgewick: «Transborder Data Privacy as Trade», *California Law Review*, 2017, pp. 1513 y ss.

vista con solo apreciar el contraste entre el sistema europeo y el que rige en los Estados Unidos de América (12).

El entorno digital es así propicio para relaciones jurídicas que comprenden actividades que se realizan en distintos países, cada uno con su propia normativa, o incluso que no es fácil precisar dónde se realizan. Para referirse a la aplicabilidad de una determinada regulación normativa sobre tratamiento de datos personales a una actividad que se realiza materialmente en otro país o que no se sabe dónde se realiza su utiliza convencionalmente la expresión «eficacia extraterritorial». En estos casos, sin embargo, esa terminología induce peligrosamente a error. No se trata de proyectar la normativa de un país más allá de su territorio, sino de precisar en qué territorio se sitúa el «centro de gravedad» (13) de una relación jurídica y aplicar a toda ella la regulación de ese territorio. Consiste, por tanto, en fijar que el criterio que debe usarse para conectar una relación jurídica de componente transfronterizo con un territorio u otro y, consecuentemente, determinar su régimen jurídico con arreglo a la normativa de ese territorio. Claro está que este planteamiento deriva, como premisa de razonamiento, de que las distintas actividades implicadas en dichas situaciones jurídicas no tienen entidad por separado sino solamente se justifican en el conjunto de esas relaciones. Un tratamiento de datos personales, al menos desde el punto de vista de las reglas y principios que debe cumplir como garantía de privacidad, no tiene más virtualidad que la incidencia en los derechos individuales del titular de la información personal, por lo que, en definitiva, el principio de territorialidad de aplicación de las normas debe tener en cuenta el país donde con regularidad ejerce sus derechos individuales (14).

Este criterio plantea el grave inconveniente de que quien incluya en un tratamiento datos personales de varios sujetos tendrá que ajustarse a varias regulaciones jurídicas, pero la solución contraria no resulta satisfactoria ya que acaba por anular el irrenunciable margen de decisión política que corresponde a cada Estado sobre el alcance de la garantía de la privacidad de las personas. Obviamente resulta recomendable que los Estados voluntariamente aproximen el alcance de esa garantía de privacidad con el fin de evitar ese resultado perjudicial, pero a falta de ello es forzoso reco-

(12) STJUE de 6 de octubre de 2015 (Asunto C-362/14), por el que se declaró inválida la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, sobre la adecuación de la protección conferida por los principios de puerto seguro.

(13) Véase el uso de esta expresión por el Abogado General Cruz Villalón en sus conclusiones en el asunto que dio lugar a la STJUE eDate Advertising y Martínez (C509/09 y C161/10), puntos 32 y 55.

(14) Este es el criterio que se ha consolidado en la jurisprudencia del TJUE, pues las SSTJUE Google Spain (C-131/12) y Schrems (C-362/14) admiten que los tratamientos de datos personales que Google y Facebook hacen en Estados Unidos están sujetos a la regulación europea cuando se trate de datos recogidos en el contexto de actividades realizadas en países europeos. Y también es el acogido en el arrtículo 3 del nuevo RGPD. Sobre ello, *Cfr.* Ripol Carulla, S.: «Aplicación territorial del Reglamento», en Piñar Mañas, J. L., *Reglamento General de Protección de Datos*, Reus, 2016, 77 ss.

nocer que la normativa aplicable a los tratamientos de datos personales es la que viene determinada por el sujeto titular de los mismos, a pesar de las contrariedades que pueda producir para las empresas y en última instancia para la innovación tecnológica y el desarrollo de la sociedad digital.

Distinto de la norma que rige estas relaciones jurídicas es el criterio que ha determinar la competencia jurisdiccional. El foro competente admite varias soluciones, pero sea cual sea el competente deberá aplicar la norma sustantiva que derive del criterio más arriba expuesto, aunque sea una regulación extraña al territorio donde se asienta el tribunal actuante. De otro lado, deberán preverse sistemas que aporten seguridad de que los fallos tengan una adecuada ejecución, particularmente cuando el responsable del tratamiento carezca de una presencia suficiente en el territorio donde radique el «centro de gravedad» de la relación jurídica.

4. LÍMITES DE LA PRIVACIDAD. EN ESPECIAL LA NECESARIA INTERVENCIÓN LEGISLATIVA

La privacidad de la persona vista como espacio de decisión autónoma, por mucho que sea un bien jurídico de importancia cualificada, ha de convivir con otros bienes e intereses jurídicos también relevantes. Para la realización de éstos puede admitirse la licitud del tratamiento de datos personales con ciertas finalidades, si bien que, para ajustar proporcionadamente el sacrificio de la privacidad del titular de los mismos, cabe someter ese tratamiento a un conjunto de condicionantes que constituye su régimen jurídico. Determinar qué finalidades justifican que sea lícito un tratamiento de datos personales, así como definir los condicionantes y límites que hacen en cada caso que el tratamiento no constituya más que un sacrificio proporcionado de la privacidad del sujeto, es una tarea que, al entrañar una ponderación abierta entre derechos individuales y otros intereses jurídicos relevantes en una sociedad democrática, debe ser abordada, a menos en sus aspectos centrales, por el legislador. El TEDH (y reflejamente el TC) viene exigiendo a las medidas de injerencia en un derecho fundamental lo que se ha venido a denominar «calidad de ley», que supone que la injerencia esté recogida en ley formal, la cual prevea como mínimo en qué circunstancias y bajo qué condiciones se habilitan tales medidas (15).

(15) *Cfr.* STEDH de 30 de julio de 1998, Caso Valenzuela, & 46. Por su parte, la STC 70/2009, resolviendo acerca del uso de la historia clínica en un expediente de jubilación por incapacidad, afirma que «la injerencia en la misma exige de un modo inexcusable una previsión legal que "ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención", [que] ha de poseer lo que en otras ocasiones hemos denominado cierta "calidad de ley" (SSTC 49/1999, de 5 de abril, FJ 5; 169/2001, de 16 de julio, FJ 6; 184/2003, de 23 de octubre, FJ 2)».

El sistema dispuesto por el RGPD es a priori conforme con este planteamiento en lo que hace a los tratamientos de información personal motivados por fines de interés público, pues remite la determinación de cuáles sean éstos y de las condiciones del tratamiento a los Estados miembros, debiendo éstos proceder a regular mediante ley formal los aspectos que exijan sus Derechos nacionales. También sería compatible con este concreto requisito de que el régimen de interferencia proceda del legislador que las condiciones exigibles a los tratamientos orientados a determinados fines públicos fueran fijadas directamente por el legislador comunitario. Un ejemplo de ello sería la Directiva 2006/24/CE, en materia de conservación de datos generados o tratados con motivo de la prestación se servicios de comunicaciones electrónicas de acceso público, que fue declarada inválida en la STJUE Digital Rights (C-293/12 y C-594/12), pero no por falta de rango en la injerencia sino precisamente por insuficiente detalle en la determinación legal de los presupuestos de la intervención que el legislador europeo habilitaba.

Es perfectamente admisible, por otra parte, que haya intereses privados que, prevaleciendo en determinadas circunstancias sobre las pretensiones de privacidad del titular de los datos personales, justifiquen el tratamiento de los mismos incluso faltando su consentimiento. Esto es en el fondo lo que dispone el arrtículo 6.1.f) RGPD, al prever que un interés privado legítimo y prevalente es título habilitante por sí (sin necesidad de consentimiento del titular) de tratamientos de datos personales.

A diferencia de lo que ocurre con los tratamientos motivados por finalidades públicas, el RGPD no remite al legislador nacional la determinación de cuáles sean estos intereses y de qué condicionantes han de incorporarse en cada ámbito sectorial al tratamiento para que el sacrificio de la privacidad del titular de los datos sea proporcionado. Y ese silencio, como se argumentó en el epígrafe 3.2 y resulta coherente con la configuración del Reglamento como fuente normativa directamente aplicable, debe entenderse como una proscripción del complemento normativo por el legislador nacional, salvo cuando éste sea expresamente requerido. Esta circunstancia conlleva, en el contexto que ahora nos ocupa, que no sea el legislador quien, luego de ponderar en qué medida procede el sacrificio de la privacidad de los titulares de los datos, disponga los presupuestos y las condiciones de los tratamientos que se admitan como lícitos. Una regulación tan genérica como la del artículo 6.1.a) RGPD deja enteramente para el momento aplicativo la selección de los intereses privados que justifican un tratamiento y la precisión de los términos y condiciones dentro de los cuáles se reputa lícito. Serán las autoridades administrativas de control y luego los tribunales de justicia, con el Tribunal de Luxemburgo como última instancia, quienes realicen caso por caso esta tarea, y la harán con

completa libertad porque su decisión no resulta constreñida y ni siquiera guiada por criterios normativamente preestablecidos.

Ello merece algunas valoraciones. La más importante es que no será el legislador el que decida las notas esenciales de la ponderación entre derechos, por lo que esa decisión carecerá de la legitimación democrática que subyace bajo el principio de «calidad de ley». Vale la pena añadir que una cosa es que el TJUE emane de vez en cuando sentencias de contenido constitucional, a veces controlando la ponderación de derechos y bienes jurídicos que haya realizado el legislador y otras avanzado criterios respecto de situaciones concretas que se le plantean mediante cuestiones prejudiciales de interpretación, y otra muy distinta es que acabe confiándosele la labor del legislador de delimitar el contenido y alcance de los derechos.

La otra valoración, de carácter más pragmático, es que parece que este sistema combinará las desventajas de la incertidumbre y la inseguridad jurídica con las ventajas del enfoque a posteriori y de caso concreto. Lo primero porque los operadores tendrán que arriesgarse a realizar tratamientos en la esperanza que los aplicadores del Derecho resuelvan que el interés legítimo que invocan para realizar el tratamiento y los términos en que lo hacen determinan su condición de prevalente, incertidumbre que, aun siendo inevitable en toda situación de innovación tecnológica, no será favorable al desarrollo de nuevos servicios digitales. Por contrapartida, el enfoque a posteriori y de caso concreto posibilitará que el régimen jurídico sea adapte mejor a cada tipo de tratamiento.

Con todo, sería aconsejable que, no siendo en principio aceptable la intervención del legislador nacional, sea el legislador europeo (y no unas directrices sin la necesaria legitimación democrática) el que, mediante normas especiales *ratione materiae*, estableciese el régimen jurídico en que son lícitos los tratamientos que se funden en aquellos intereses legítimos más comunes, en especial aquellos con base en los cuales se realiza una actividad económica ya consolidada. Valga como ejemplo los tratamientos necesarios para elaborar sistemas de información crediticia, actividad económica consolidada que, a falta de una regulación legal, se seguirá realizando y, a diferencia de la situación anterior, sin que quede claro en qué términos debe abordarse el tratamiento para que la injerencia en los derechos de los titulares de los datos sea proporcionada (16).

(16) Tan conveniente es la fijación legal de este régimen jurídico que el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal –BOCG (Congreso de los Diputados) de 24 de noviembre de 2017–, a pesar de que parece que el artículo 6.1.f) RGPD lo excluiría, procede a preverlo en su artículo 20.

5. TÉCNICAS DE TUTELA DE LA PRIVACIDAD. APUNTES

5.1 **A vueltas con el consentimiento**

El consentimiento es quizá la base legal que se usa más comúnmente como justificación de un tratamiento de datos personales. Y nunca ha estado exento de polémica. De hecho, en un intento de incrementar las garantías de privacidad, una de las novedades del RGPD es, y con ello se profundiza en la diferencia con el sistema americano, endurecer las condiciones que ha de revestir el consentimiento, que debe constar en forma afirmativa y de un modo separado cuando las finalidades sean distintas. Tengo dudas de que este régimen vaya a suponer una mejora sustancial como tal garantía. La reflexión acerca de su función ha de continuar.

Por un lado, no puede obviarse que el consentimiento tiene la virtualidad de conectar al titular de los datos con el responsable del tratamiento, de tal modo que éste puede encontrar un incentivo empresarial en demostrarle a aquél que en el manejo que hace de sus datos privilegia la seguridad de los mismos y que no sean utilizados ulteriormente para vulnerar su espacio de libre decisión en que consiste su privacidad. En este sentido pueden hallar largo recorrido las exigencias de transparencia elevadas en el RGPD a principio que debe informar el tratamiento de datos de carácter personal. Este principio de transparencia, que no deja de presentar la desventaja de incrementar los costes económicos del responsable del tratamiento, tiene la extraordinaria valencia de resultar apto para establecer una relación de confianza con el titular de los datos personales, sin la cual va a ser cada vez más difícil desarrollar actividades empresariales que requieran el tratamiento de datos personales (17).

Sin embargo, el consentimiento presenta serias deficiencias (18) para configurarse como una garantía definitiva de privacidad. Está demostrado que el usuario de un servicio digital encuentra mayor desincentivo cuando se condiciona su prestación a una pequeña contraprestación económica que cuando se sujeta al consentimiento sobre el tratamiento de los datos personales que genere con el uso del servicio. En realidad, este consentimiento se presta de un modo automático sin leer siquiera los concretos tratamientos que se consienten. No hay, ni probablemente podría haber, tanto por su cantidad como por su complejidad, una verdadera conciencia de los tratamientos que se consienten. En contra, cabría argumentar que

(17) Véase Hernández Corchete, J. A., «Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos», en Piñar, J. L., *Reglamento General de Protección de Datos*, Reus, 2016, 205 ss.

(18) *Cfr.* Solove, D.: «Privacy self-management and the consent dilemma», *Harvard Law Review*, núm. 126, 2013, pp. 1880 y ss.

la aceptación del tratamiento de datos personales es la contraprestación de un servicio digital que de otro modo no se ofrecería.

Se suscita, conforme a los argumentos indicados, un difícil dilema acerca de la eficacia del consentimiento en el plano de cada tratamiento individualmente considerado. Pero es que, a la hora de considerar una eventual vulneración de la privacidad, el plano relevante no es el de cada tratamiento individualizado sino el del resultado derivado de una acumulación de tratamientos y desde esta óptica es aún más claro que el consentimiento del titular de los datos personales, al no conocer los tratamientos futuros a que se someterán sus datos, no puede expresar una ponderación de parte del titular de los mismos que prefiera las ventajas del tratamiento a los perjuicios para su privacidad. La circunstancia de haber consentido genéricamente esos futuros tratamientos o de que fueran legales por obedecer a fines compatibles no suponen un obstáculo a este razonamiento, pues en todo caso el titular de los datos no pudo ponderar sus consecuencias al tiempo de consentir.

Cabe dar todavía un paso más. Aun cuando se admitiese que el consentimiento ampara también los tratamientos posteriores mencionados lo que en ningún caso cubre es que arrojen como resultado una invasión relevante de la privacidad como espacio de autonomía de la persona (i.e. cesión de datos de Facebook a Cambridge Analytica). Este planteamiento puede apoyarse en que el titular de los datos consiente precisamente los tratamientos de que se trate y en ningún caso determinados resultados derivados de esos tratamientos (expectativa de privacidad que implícitamente delimita el alcance del consentimiento), pero también en que el sujeto carece de entera disposición sobre la privacidad inherente a su personalidad o, incluso, en que la privacidad de la persona sirve a intereses sociales que justifican que se impongan límites legales externos a su disponibilidad (19). No es una novedad que el Derecho imponga límites a la virtualidad del consentimiento en atención a la mejor realización de ciertos bienes jurídicos. La cuestión por resolver es qué límites específicos se manifiestan en el entorno digital, en particular como medio de proteger la privacidad de la persona.

5.2 **Mero cumplimiento *vs.* análisis de riesgo: consecuencias**

La tutela de la privacidad en el entorno digital requiere distinguir el plano del tratamiento de datos personales de aquel otro de los eventuales resultados dañosos para la privacidad de sus titulares. Cualquier trata-

(19) *Cfr.* Cohen, J.: «What Privacy is for», *Harvard Law Review*, núm. 126. 2013, pp 1918 y ss; y también Richards, M.: *«The Dangers of Surveillance»*, *Harvard Law Review*, núm. 126. 2013, pp. 1945 y ss.

miento de datos personales, y en mayor medida la acumulación de tratamientos, entrañan un riesgo de invadir de un modo sustancial la privacidad de las personas, que puede ser mitigado más no anulado sometiendo ese tratamiento a reglas precisas y a principios generales. De ahí que la protección de la privacidad en una situación de innovación tecnológica como la presente debe adoptar, en lugar de una forma estática de mero cumplimiento normativo, en enfoque dinámico que analice los riesgos y reaccione instrumentando las cautelas oportunas.

El responsable del tratamiento, al conocer en profundidad sus peculiaridades y su funcionalidad, estando en su mano hacer las correcciones pertinentes, es quien está en mejor posición de realizar este análisis de riesgos, por lo que imponerle esta obligación formal no resulta en absoluto una carga desproporcionada. Este análisis de riesgo necesita revestir al menos carácter sustantivo, no siendo bastante con rellenar formalmente las cuestiones previstas en un formulario genérico, y continuado, en el sentido de que esta tarea no se satisface enteramente con un estudio previo al tratamiento sino que es necesario que se prolongue y actualice mientras el tratamiento continúe.

Este enfoque activo impuesto al responsable del tratamiento, indudablemente más exigente que el mero cumplimiento formulario de un conjunto cerrado de requisitos, es el apropiado para la tutela de la privacidad en el entorno incierto y en constante evolución tecnológica como el digital. El RGPD acierta plenamente al optar por él, pero una cosa es que el responsable del tratamiento soporte esta carga formal y otra muy distinta que cualquier riesgo que se concrete en daño para la privacidad del titular de los datos le sea imputable desde un punto de vista jurídico. Hay que avanzar en la construcción de un sistema más ponderado de reparto de las responsabilidades (20) derivadas del tratamiento de datos personales que tenga en cuenta que esta actividad de riesgo beneficia no solo al responsable del tratamiento sino también a quienes reciben los servicios generados y de un modo más mediato, mas igualmente cierto, a la sociedad en general.

5.3 **La patrimonialización de los datos personales no es garantía de privacidad**

La información que se genera a partir del tratamiento de datos personales tiene un valor económico notable (y creciente) por su potencialidad como medio productivo. Coherentemente con ello cada vez los operado-

(20) Veáse sobre esta ponderación de responsabilidades, De Hert, P. y Stefanatou, D.: «The accountability culture in its european union dress», en A. Rallo y R. García (Eds), Hacia un nuevo derecho europeo de protección de datos, Tirant Lo Blanch, 2015, pp 389 y ss.

res invierten más recursos en su elaboración y, como es lógico, pretenden mejores y más adecuadas técnicas jurídicas para proteger ese interés económico. Esta es la razón de la proliferación de estudios que profundizan en las posibilidades que el derecho de propiedad en sus diversas formas puede dispensar para este recurso económico (21).

Cabe preguntarse hasta qué punto el derecho de propiedad no solo protege eficazmente a los operadores que generan información a partir de datos personales sino también al titular de los datos personales. Esta cuestión es lo que, al fin y al cabo, se pone encima de la mesa por quienes esgrimen que el usuario de servicios digitales que son gratuitos los paga con el consentimiento a que los datos personales que generan al usarlos sean tratados (y en consecuencia explotados económicamente) a voluntad del prestador.

A mi juicio, es innegable que la persona tiene un cierto de derecho de disposición sobre sus datos personales, que le autoriza para ceder su explotación en los términos que considere adecuado. Esta circunstancia, que en el fondo es una fórmula de patrimonializar los datos personales, es lo que explica el modelo de negocio indicado *ut supra* y también lo que justifica que si un operador maneja unos datos personales sin consentimiento haya de entregar al titular una compensación económica. Y este planteamiento también exigirá plantearse cuándo los tratamientos que se realizan en virtud de bases legales distintas al consentimiento no conllevan una indemnización independiente porque ya obtiene el titular un beneficio de otro tipo que opera como compensación.

Ahora bien, debe quedar claro que esta relación patrimonial entre la persona y sus datos personales no es en absoluto una garantía de privacidad. Hay que insistir que la persona respecto de sus datos personales detenta varios intereses jurídicos. Que uno de ellos pueda gestionarse con arreglo a criterios de relación patrimonial que se caracteriza por su entera disponibilidad no quiere decir que este mecanismo de protección absorba el resto, sobre todo aquellos que tienen una virtualidad diferente. Es por ello que el consentimiento a un tratamiento de datos personales a cambio de utilizar un servicio digital no blinda por completo la posición del responsable del tratamiento. Este habrá adquirido el derecho a hacer suyos los beneficios económicos derivados del tratamiento de los datos personales, pero deberá hacerlo sin afectar a la privacidad del titular de los datos y en todo caso cumpliendo las reglas y principios previstos en el ordenamiento jurídico como garantía de este interés jurídico.

(21) *Cfr. Legal study on ownership and access to data. A study prepared for the European Commission*, SMART number 2016/0085; y también *Building the European Data Economy, Data Ownership*, White Paper, 1 January 2017, Bird & Bird.

5.4 **La reacción sancionadora, con especial consideración al RGPD**

La reacción sancionadora es un elemento regulatorio esencial que debe resultar acorde con el resto de decisiones estratégicas que determinan el alcance de la garantía de privacidad. En tal sentido el sistema del RGPD merece atención desde dos puntos de vista.

En el RGPD, y ello se aprecia desde la fuente normativa escogida, resalta la opción por uniformar al máximo la garantía de privacidad a que se someten los tratamientos de datos personales con el fin de, sin merma para los derechos individuales, contribuir a la creación de un mercado único digital. Este objetivo resulta imposible si la reacción sancionadora no participa de esta uniformidad y por ello, frente al planteamiento de la Directiva 95/46/CE que la remitía a la voluntad de los legisladores nacionales permitiendo así que alguno de ellos no estableciese ninguna, el RGPD prevé una normativa común a todos los Estados miembros y directamente aplicable prácticamente en su totalidad, que se caracteriza por que el incumplimiento de las obligaciones del responsable o encargado del tratamiento podrán dar lugar (si el aplicador considera que se dan las condiciones para ello) a la imposición de multas administrativas conforme al régimen que se establece principalmente en su artículo 83 y al que se volverá más adelante.

El legislador nacional ve reducido su margen de decisión a dos extremos. Por un lado, si las multas administrativas son ajenas al ordenamiento jurídico de un Estado miembro podrán ser sustituidas por un sistema equivalente de multas impuestas por órganos judiciales (apartado 9). Por otro, el ejercicio de esta potestad sancionadora «estará sujeto a garantías procesales adecuadas de conformidad con el Derecho de la Unión y de los Estados miembros» (apartado 8), margen de decisión en cuanto a la fijación de garantías procesales que halla un límite en el carácter efectivo y disuasorio que el apartado 1 de este artículo 83 predica del sistema de multas administrativas.

La fijación de plazos de prescripción de infracciones y sanciones, a pesar de ser un elemento apto para generar profundas diferencias, se confía a los Estados miembros a través de esta remisión relativa a la previsión de garantías procesales. Es cierto que la STC 63/2005 aprecia que la prescripción responde a una perspectiva axiológica que la inserta como una dimensión del principio de legalidad y conforme a ello este instituto sería más que una simple garantía procesal alcanzando cierto contenido sustantivo. Sin embargo, en Derecho alemán y francés preva-

lecen los planteamientos que justifican la prescripción en consideraciones procesales (22).

Debe insistirse, no obstante, que el margen del legislador nacional es limitado como lo exige el objetivo de uniformar la regulación en esta materia y al mismo tiempo la exigencia de que el sistema de multas administrativas sea efectivo y disuasorio, requisito que se deriva con naturalidad de la existencia misma del sistema (23) pero que además se explicita en el artículo 83.1 RGPD. De este modo, una legislación nacional que estableciese un plazo de prescripción tan corto que impidiera en la práctica la virtualidad del sistema de multas administrativas sería contraria al artículo 83.1 RGPD y en general al propio sistema de garantía de la privacidad que instituye el RGPD.

El otro eje del RGPD es que, atendiendo a que la sociedad digital se desenvuelve en un entorno tecnológico que además está en innovación constante, abandona el modelo de mero cumplimiento y opta por articular la garantía de privacidad conforme a un enfoque responsable en torno al análisis continuo de los riesgos. Coherentemente con ello, el RGPD no contiene más que una definición muy abierta de las circunstancias en que cabe acordar una multa administrativa. No es solo que la norma no gradúa la gravedad de las infracciones, salvo de un modo extraordinariamente indirecto que luego se dirá. Es además que no hay una verdadera tipificación de infracciones distinta de las obligaciones cuyo incumplimiento puede ser objeto de multa, a lo que debe añadirse que el alcance de dichas obligaciones tiene algo de incierto dado el modo en que se configura el principio de responsabilidad en el apartado 1 del artículo 24 RGPD (24).

---

(22) *Cfr.* Pedreira González, F.: *La prescripción de los delitos y de las faltas*, pp. 136 y ss., señala que un fundamento de la naturaleza procesal de la prescripción es la teoría de las dificultades probatorias, que dice que «está muy extendida en el ámbito de la doctrina alemana». Dice también que «al margen de su transcendencia histórica, esta fundamentación ha sido manejada por numerosos autores, hasta el punto de que quizá constituye el argumento más frecuentemente invocado», con cita de autores alemanes, franceses e italianos (también en relación a la teoría del castigo a la negligencia del Ministerio Público).

(23) *Cfr.* STJUE Taricco (C-42/17) en la que confirma esencialmente el criterio que había sostenido en su Sentencia Taricco de 2015 (C-105/14). Este criterio consiste en que el plazo de prescripción de las penas por infracciones de la normativa de IVA, que corresponde establecer a los Estados Miembros, será contrario al Derecho Europeo si es tal que determina que las penas no sean efectivas y disuasorias. La materia IVA se asemeja a la de Protección de Datos Personales en el intenso interés comunitario que revisten, por lo que tal criterio pudiera ser extensible a este ámbito.

Adviértase que una cosa que la duración de un plazo de prescripción no desvirtúe la regulación sustantiva que el sistema sancionador garantiza y otra distinta, que sí puede conectarse con garantías constitucionales nacionales de carácter esencial, es la aplicación retroactiva desfavorable de un plazo de prescripción.

(24) Téngase en cuenta la STC 104/2009, en la que se resalta, en relación a la predeterminación normativa de las infracciones en materia de instalaciones nucleares y radioactivas, que también se ligan al mero incumplimiento de obligaciones, que no hay vulneración del artículo 25 CE porque se trata de «normas de contenido predominantemente técnico que disciplinan la actividad de las empresas del sector y que deben ser perfectamente conocidas por éstas». En mi opinión, sin embargo, no es una situación asimilable.

En el modelo del RGPD se reduce al mínimo la parte de la decisión sancionadora que deriva directamente de la norma y ese espacio que se resta a la configuración normativa acrece al margen de apreciación del aplicador. Será éste el que resuelva (a) si se ha producido incumplimiento de una de tales obligaciones, para lo cual deberá precisar previamente el alcance de la obligación en el caso concreto; (b) si producido el incumplimiento procede o no la reacción sancionadora, pues no hay una vinculación automática entre incumplimiento e infracción; y en este último caso (c) cuál será la cuantía de la multa administrativa, lo que encierra una valoración de la gravedad de la infracción y de individualización de la sanción. Y en la adopción de estas decisiones no está vinculada más que por una serie de once criterios genéricos que condicionan de un modo general todas estas decisiones.

Esta regulación presenta la virtud de confiar al aplicador un mayor margen de apreciación que le permite modular la reacción sancionadora según las circunstancias del caso, lo que se corresponde con el enfoque regulatorio basado en la evaluación de los riesgos que cada tratamiento singular presenta en cada momento. Sin embargo, también conlleva desventajas, pues la reducción de la predeterminación normativa al enunciado general de once criterios genéricos que vinculan de un modo global la reacción sancionadora disminuye la previsibilidad de ésta y también la participación de los representantes públicos en la fijación de los rasgos esenciales de la reacción sancionadora. Habrá que reflexionar, de un lado, si esta merma de la dimensión formal y material del principio de legalidad deja intacto o no su contenido esencial (o si se prefiere si resulta proporcionado) y, de otro, si cabe desarrollar otras garantías en el nivel aplicativo que de algún modo contribuyan a que el principio de legalidad no quede desvirtuado.

Este análisis de la conformidad del sistema del RGPD con el principio de legalidad va a ser un nuevo escenario para observar la relación de colaboración juez nacional-TJUE. Serán los jueces nacionales (o quizá las autoridades de control) las que pueden suscitar la decisión del TJUE sobre la conformidad del RGPD con los principios del Derecho comunitario y en particular de la CDFUE, pero la decisión del TJUE habrá de tener presente que, tratándose de derechos fundamentales de las personas, los tribunales constitucionales pueden amagar con considerar que una cierta interpretación del TJUE desconoce sus identidades nacionales (25).

(25) Véase los términos en que la *Corte Costituzionale* planteó la cuestión prejudicial en el asunto Taricco (C- 42/2017) y el análisis que de ello hace el Abogado General en sus conclusiones. *Cfr.* en la doctrina, DE LA QUADRA JANINI, T., «El papel del Tribunal Constitucional y de los tribunales ordinarios en un contexto de tutela multinivel de los derechos fundamentales», en *El Cronista*, núm. 52, pp. 34 y ss.

La merma en la predeterminación normativa también afecta, aunque con menor intensidad, a la definición de las sanciones. El RGPD se ciñe (a) a prever que la sanción será multa administrativa; (b) a fijar que su cuantía oscilará, sin tramos intermedios, entre 0 € y millones de euros; y (c) a vincular la fijación de la cuantía a los once criterios genéricos a que el artículo 83.2 RGPD remite globalmente la reacción sancionadora. La STC 175/2012, apartándose de su doctrina anterior acerca de las exigencias de la dimensión material del principio de legalidad, admitió que una tipificación similar de sanciones en materia de defensa de la competencia no contrariaba el artículo 25 CE.

Otro ámbito abierto a la reflexión deriva de la habilitación al CEPD para, en ejercicio de su función de garantizar «la aplicación coherente del presente Reglamento», «formular directrices para las autoridades de control relativas… a la fijación de multas administrativas» [art. 70.1.k)] (26). Todo son preguntas sobre la virtualidad jurídica de estos instrumentos en un ámbito tan especial como el sancionador. ¿Es una norma? ¿Qué es si no? Si no es una norma el aplicador podrá separarse de tales criterios, pero comúnmente los seguirá por su propia voluntad. ¿Qué ocurrirá cuando el operador ajuste a estos criterios sus comportamientos y el aplicador se separe puntualmente de ellos?

Sí parece haber certidumbre en que esta merma en la previsibilidad de la reacción sancionadora y de su gravedad no puede ser resuelta contemplando en la ley nacional una tipificación más concreta de infracciones y sanciones, así como una gradación de las mismas en leves, graves y muy graves. Con ello se rompería la uniformidad de la garantía de privacidad prevista en el RGPD y se iría en contra de la vocación de esta norma de ser aplicada directamente y sin desarrollos nacionales salvo donde se prevén expresamente.

(26) El Grupo del artículo 29 adoptó el 3 de octubre de 2017 su WP 253 titulado *Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679*.

CAPÍTULO 13

DERECHO AL OLVIDO Y CONSTRUCCIÓN DE UNA MEMORIA COLECTIVA

María Álvarez Caro
Abogada (BBVA)

1. REFLEXIONES CONCEPTUALES Y JURÍDICAS EN TORNO AL DERECHO AL OLVIDO

1.1 El acceso a la información en el siglo xxi y el rol de los motores de búsqueda

Internet y las nuevas tecnologías han supuesto un punto de inflexión en muchos órdenes y ámbitos. Entre otros, en el modo en el que accedemos a la información y en la fácil disponibilidad de datos e información sobre las personas. Ello ha supuesto que hace unos años, desde distintos ámbitos,

entre otros, desde el jurídico, se reflexionase sobre la privacidad y sobre cómo debe ser ésta considerada y protegida en el siglo XXI, así como sobre la adecuación o posible obsolescencia del marco regulatorio vigente.

En un amplio abanico de cambios sociales incentivados por la innovación tecnológica, destaca la conversión de la frágil memoria humana en una potente y poderosa memoria digital, con el posible impacto en los derechos fundamentales de las personas. La accesibilidad universal a casi contenido sobre las personas está en la base de la reflexión sobre la necesidad de introducir algún límite a la infinita capacidad de memoria de la Red (1). No cabe duda de que avances como los motores de búsqueda o redes sociales cumplen, en cierto modo, una función de amplificador o altavoz, a la vez que desempeñan un rol fundamental como herramientas clave para el acceso a la información. El TJUE puso de manifiesto que la inclusión de información en una lista de resultados de un motor de búsqueda «puede constituir una injerencia mayor en el derecho fundamental al respeto de la vida privada del interesado que la publicación por el editor de una página web» (2).

El tratamiento de datos personales efectuado por el gestor de un motor de búsqueda, ofreciendo una lista de resultados a partir de la búsqueda realizada con el nombre de una persona física, puede afectar significativamente a los derechos fundamentales de respeto de la vida privada y de protección de datos personales, toda vez que dicho tratamiento permite a cualquier internauta obtener mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet, que afecta potencialmente a una multitud de aspectos de su vida privada, y puede establecer un perfil más o menos detallado de la persona de que se trate (3).

Por tanto, «el actual desarrollo de las tecnologías de la información, hace posible recoger y almacenar, sin límite de espacio, infinidad de datos sobre un mismo individuo, realizar un auténtico catálogo de informaciones personales sobre él y, además, interrelacionar todos los datos existentes sobre una misma persona, con independencia de que se encuentren en archivos distintos, relativos a diferentes etapas de sus vidas o que éstos hayan sido recogidos incluso en lugares lejanos. Se puede acumular, sin límite, la información y recabarla en cuestión de segundos con independencia de la distancia a la que se encuentre» (4).

---

(1) Solove, D.: *The future of reputation. Gossip, rumor and privacy on the Internet*, New Haven, Yale University Press, 2007, pp. 1-18. https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2081&context=faculty_publications

(2) Apartados 86 y 87 de la sentencia del TJUE (2014, C-131/12) de 13 de mayo, Mario Costeja y AEPD v. Google Inc. y Google Spain.

(3) Sentencia de la Audiencia Nacional 107/2015, de 17 de febrero, FJ 10 (AN, 2015/107).

(4) Garriga Domínguez, Ana: *Tratamiento de datos personales y derechos fundamentales*, Madrid, Dykinson, 2009, p. 24.

Tal y como destacó el Abogado General en sus conclusiones en el caso Mario Costeja y AEPD v. Google Inc. y Google Spain, en la época actual cualquier contenido es susceptible de ser puesto a disposición de terceros a gran escala, de forma instantánea y permanente. Por ello, señala el Abogado General «ha de establecerse un equilibrio entre diversos derechos fundamentales, como la libertad de expresión, el derecho a la información y la libertad de empresa, por un lado, y la protección de datos de carácter personal y la privacidad de los particulares, por otro» (5).

Internet tiene el inconveniente de la ausencia de un catálogo donde se recoja la situación exacta de toda la información publicada, debido a la imposibilidad de abarcar la totalidad de la Red. Por ello, buscar directamente en las páginas web se convierte en una estrategia poco adecuada, a menos que se sepa con certeza dónde se sitúa la información deseada (6). Los motores de búsqueda surgen como herramientas de ayuda para buscar información en la web, en respuesta a la dificultad de mantener un catálogo con toda la información que contiene la Red (7), debido fundamentalmente a la volatilidad de ésta dado su volumen (8).

Los motores de búsqueda en Internet tienen tres componentes básicos: por un lado, una araña o robot (*crawler* en su denominación en inglés), que es el programa informático que rastrea por la web leyendo las páginas; por otro un programa que añade las páginas leídas a una base de datos o catálogo; y en tercer lugar, un programa que permite al usuario, a través de la utilización de palabras clave, realizar la búsqueda (9). Ello se efectúa mediante un proceso de comparación y aproximación entre las páginas de sus bases de datos y las palabras clave, para posteriormente devolverle al usuario los resultados (10).

En definitiva, un motor de búsqueda es un prestador de servicios de la sociedad de la información (11) y de localización de contenido en Inter-

(5) Conclusiones del Abogado General Niilo Jääskinen, en el caso Mario Coesteja y AEPD contra Google Spain y Google Inc., de 25 junio de 2013, punto 2.

(6) White, Marilyn y Livonen, Mirja: «Questions as a factor in Web search strategy», *Information Processing & Management*, Vol. 37, 2000, pp. 721 a 740.

(7) Wukovitz, Laura: «Using Internet search engines and library catalogues to locate toxicology information», *Toxicology*, vol. 157, 2001, pp.121 a 139.

(8) Salmerón, José Luis *et alii*: «Localización de la información en motores de búsqueda en Internet: análisis de la efectividad», *Economía Industrial*, n.º 346, Universidad Pablo de Olavide de Sevilla, 2002, p.173.

(9) Fischer, Ingrid et alii: «The role for web search engines», *The CPA Journal*, enero, vol. 70, n.º 1, 2000, p. 43.

(10) Clarke, Charles et alii: «Relevance ranking for one to three term queries», *Information Processing & Management*, vol. 37, 2000, pp. 291 y ss.

(11) La definición de servicio de la sociedad de la información se encuentra en el apartado 2 del artículo 1 de la Directiva 98/34/CE, de 22 de junio, en su redacción modificada por la Directiva 98/48/CE, de 20 de julio, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas Diario Oficial n.º L 217 de 05/08/1998, pp. 18-26. Se considera servicio de la sociedad de la información «todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios». A su vez, el anexo de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio

net, que permite a los individuos acceder, de manera cómoda y sencilla, a una gran cantidad de información sobre una infinita variedad de temas. Según el derecho de la UE, un servicio de la sociedad de la información es «todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios» (12). Con base en el considerando 18 de la Directiva 2000/31/CE, de 8 de junio, sobre Comercio Electrónico, no necesariamente debe existir un pago del destinatario del servicio, siempre que el servicio constituya una actividad de naturaleza económica para el prestador.

Los motores de búsqueda desempeñan un rol de proveedor de contenidos, que consiste en hallar información publicada o subida a la Red por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas, según un orden de preferencia determinado. No cabe duda de que cumplen una función esencial en el acceso a la información y al conocimiento, han contribuido notoriamente a la democratización del acceso a la información, así como a la innovación y al progreso.

Desde el plano del derecho a la protección de datos de carácter personal, sin embargo, los motores de búsqueda permiten ensamblar informaciones reducidas y elaborar un perfil bastante completo de las personas físicas. En el caso de que, a través de un motor de búsqueda, se dé información inexacta o desactualizada, se podría poner en riesgo el prestigio, reputación o estima social de una persona. «A todo ello se une el *chilling effect* o desincentivo de ciertas búsquedas en una especie de autocensura, cuando el individuo es consciente de que el sistema registra las búsquedas efectuadas desde cada dirección IP» (13).

En relación a la actividad de los motores de búsqueda, el TJUE, en sentencia TJUE 2014, C-131/12, de 13 de mayo, Caso Mario Costeja y AEPD c. Google Inc. y Google Spain, destacó que dicha actividad, como proveedor de contenido, en la medida en que encuentra información publicada o puesta en Internet por terceros, la indexa de forma automática, la almacena temporalmente y, por último, la pone a disposición de los in-

---

Electrónico destaca al respecto que se trata de «todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios».

(12) Artículo 1.2 de la Directiva 98/48/CE de 20 de julio, del Parlamento Europeo y del Consejo, que modifica la Directiva 98/34/CE, de 22 de junio, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas Diario Oficial n.º L 217 de 05/08/1998, pp. 18-26.

(13) Tene, Omer: «What Google knows: Privacy and Internet search engines?», *Utah Law Review*, Vol. 2008, n.º 4, pp. 1457-1464.

ternautas según un orden de preferencia determinado, implica un tratamiento de datos personales, del cual Google es responsable (14).

La reflexión en torno al derecho al olvido surge, por tanto, en el momento del auge de los motores de búsqueda como herramientas de acceso y localización de contenidos. De hecho, el primer fallo judicial que contempló este derecho como aquel que permite a las personas físicas dirigirse directamente a un motor de búsqueda para que éste elimine de la lista de resultados determinada información, ciñó el derecho al olvido al contexto de los motores de búsqueda con campo de acción universal en Internet. No obstante, el Reglamento 2016/679, de 27 de abril, General de Protección de Datos, recoge el derecho al olvido en su artículo 17 en un sentido amplio, englobando a todo responsable del tratamiento de cualquier naturaleza, sea bien un motor de búsqueda o un prestador de servicios de la sociedad de la información de cualquier otra índole o, en general, cualquier responsable del tratamiento. Por tanto, en dicho Reglamento, se podría afirmar que el derecho al olvido es la actualización y adaptación al entorno digital de los clásicos derechos de cancelación u oposición.

1.2 **La memoria individual y colectiva, el recuerdo y el olvido**

La memoria humana cumple un rol fundamental en el aprendizaje humano y conocimiento del entorno. Sin embargo, hay una diferencia fundamental entre la memoria humana y la de las máquinas, que es que la primera olvida (15). Las máquinas o computadoras pueden continuar almacenando recuerdos mientras se les agregue más capacidad de memoria, la información está ordenada y no se pierde salvo que sea dañada de alguna manera. En cambio, la memoria humana a veces falla, pierde información y, en ocasiones, recuerda de manera incorrecta.

Frente a la memoria individual, capaz de recordar e interpretar acontecimientos pasados, se encuentra la memoria colectiva, «dirigida a reforzar sentimientos de pertenencia sociales, a mantener la cohesión de los grupos y las instituciones que componen una sociedad» (16). En la segunda década del pasado siglo, Maurice Hallbwachs fundó la noción de memoria social o colectiva, que alude a los recuerdos del conjunto de la sociedad (17). Hoy en día, en la construcción de esa memoria colectiva, las nuevas tecnologías desempeñan un rol clave al ser herramientas esencia-

(14) Apartado 60 de la sentencia TJUE, 2014, C-131/12, caso Mario Costeja y AEPD v. Google Inc. y Google Spain.

(15) Baddeley, Alan: *Human memory: theory and practice*, Psychology Press, Reino Unido, 2002, p. 5.

(16) Pollack, Michael: *Memoria, olvido, silencio: la producción social de identidades frente a situaciones límite*, Ediciones Al Margen-La Plata, 2006, p. 25.

(17) Halbwachs, Maurice: *La memoria colectiva*, Zaragoza, Prensas Universitarias de Zaragoza, 2004.

les para acceder a la información y a la comunicación. En la medida en que servicios de la sociedad de la información como las redes sociales o buscadores tienen una función amplificadora o actúan a modo de altavoz y se han convertido en herramientas clave para la búsqueda de información y para la libertad de expresión contribuyen notoriamente a la construcción de la memoria colectiva.

Mayer-Schönberger, uno de los máximos referentes y principales defensores del derecho al olvido, insiste en que con la ayuda de la tecnología y la difusión «olvidar se ha convertido en la excepción a la regla por defecto, que no es otra que el recuerdo» (18). En este sentido, el jurista austríaco destaca que con la capacidad del recuerdo somos capaces de comparar, aprender y experimentar el tiempo como un cambio e igualmente importante es la habilidad para olvidar, desempeñando un rol muy relevante en la función humana, en la toma de decisiones, al permitir la generalización y abstracción y no quedar anclado en las experiencias individuales (19). Para este experto, de algún modo, el recuerdo digital nos amenaza como individuos y como sociedad, en lo relativo a nuestra capacidad para aprender, razonar y actuar en el tiempo, así como también nos expone a la 'potencialmente devastadora' sobrerreacción humana ante nuestro pasado (20).

Ligado a la reflexión precedente, estaría el derecho al libre desarrollo de la personalidad y dignidad de la persona, recogido en el artículo 10 de la Constitución Española, de 29 de diciembre de 1978 (21), que podría verse obstaculizado en el caso de que datos personales o informaciones referentes a las personas físicas permaneciesen accesibles *sine die*, a golpe de *clic*.

1.3 **Definición y derecho al olvido como derecho fundamental**

El derecho al olvido podría ser definido como un interés jurídicamente protegido de los ciudadanos que consiste en lograr efectivamente que sus datos personales, en un entorno digital, sean cancelados o no sean accesibles por el público. En cierto modo, podríamos afirmar que es «una forma poética de referirse principalmente al derecho de cancelación y, eventualmente también al de oposición, en el marco del derecho fundamental de la protección de datos» (22). Si un ciudadano ve cómo datos publicados

(18) Mayer-Schönberger, Viktor: *Delete: the virtue of forgetting in the digital age*, Princeton University Press, 2009, p. 49.
(19) Mayer-Schönberger, *op.cit*, p. 12.
(20) *Ibidem*.
(21) El artículo 10 de la Constitución Española señala: «La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social».
(22) Simón Castellano, Pere: *El reconocimiento del derecho al olvido digital en España y en la UE*, Barcelona, Bosch, pp. 97 y ss.

lícitamente en el pasado, podrían perjudicarle objetivamente en la actualidad y a estos datos se puede acceder en Internet, tendría un derecho, con limitaciones, de oponerse, a que tales datos continúen a disposición de terceros que quieran conocerlos (23).

Tras una primera aproximación al concepto de derecho al olvido, se ve claramente la contradicción entre derechos y principios generales del ordenamiento jurídico. De un lado está el derecho a la intimidad, secuencia del derecho a la dignidad de la persona, y específicamente de la protección frente a la informática. De otro, se encuentra el principio de transparencia y los derechos de información, además de otros derechos o intereses que pueden entrar en juego como la libertad de empresa, libertad de expresión o el necesario impulso de la innovación y el desarrollo tecnológico.

El derecho al olvido deriva del derecho a la protección de datos de carácter personal, que a su vez deriva del derecho a la intimidad. Por tanto, gozaría de la condición de derecho fundamental. Es más, podríamos decir que es la manifestación del derecho a la protección de datos –cancelación u oposición– en el entorno de Internet. Así, cabe destacar que «el derecho a la protección de datos personales tiene, (…), un objeto más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el artículo 18.1 CE, sino a la esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inseparablemente unidos al respeto de la dignidad personal, como el derecho al honor, y al pleno ejercicio de los derechos de la persona. El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado» (24).

Como suele ser habitual en el ámbito de los derechos fundamentales, el derecho al olvido podría entrar en colisión con otros derechos y, por tanto, en ningún caso nos movemos en el terreno de los derechos absolutos. En el ámbito de los derechos fundamentales se han venido identificando colisiones entre intereses o derechos. Así, destacan el conflicto entre seguridad y libertad, entre la intimidad y el derecho de defensa y la investigación penal o «la colusión entre el derecho a expresarnos o incluso exhibirnos y el derecho a arrepentirnos» (25). Hay que buscar un justo equilibrio entre

(23) Álvarez Caro, María: *Derecho al olvido en Internet: El nuevo paradigma de la privacidad en la Era digital*, Madrid, Editorial Reus, 2015, p. 71.

(24) SSTC 292/2000, de 30 de noviembre (RTC 2000, 292); Sentencia de la Audiencia Nacional 107/2015, de 17 de febrero, FJ 9.º

(25) Llaneza, Paloma: «Derechos fundamentales e Internet», *Revista Telos Cuadernos de Comunicación e Innovación*, Fundación Telefónica, 2010, n.º 85, p. 1.

el interés legítimo de los internautas en tener acceso a la información en una búsqueda que verse sobre el nombre de una persona y los derechos fundamentales de la misma y pueda resultar que, por razones concretas, como el papel desempeñado por el interesado en la vida pública, la injerencia en sus derechos fundamentales está justificada por el interés preponderante del público en tener acceso a la información de que se trate (26).

Como derecho fundamental que deriva del derecho a la protección de datos de carácter personal, el derecho al olvido no es absoluto, siendo necesario un ejercicio de ponderación o *balancing test,* para resolver los conflictos que pueda plantear con otros derechos a su vez fundamentales. Así, el Tribunal Constitucional destaca que «el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los poderes públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución» (27).

En los últimos años se han expandido servicios como las redes sociales o prestadores de servicios de la información en general, a la vez que se ahondaba en el debate sobre la necesidad de unos límites y de dotar al ciudadano de mecanismos de garantía de sus derechos, principalmente cuando se trata de informaciones no difundidas ni reveladas por ellos (28).

El hecho de que el derecho al olvido esté ligado al 'arrepentimiento' o al derecho al borrado, nos puede llevar a la conclusión de que el derecho al olvido parte de la premisa de veracidad de los datos. Si una injuria o calumnia implica el insulto, descalificación o imputación falsa de un delito, el ejercicio del derecho al olvido iría referido al derecho a eliminar datos de la Red que el interesado considere que le perjudican aunque esos datos se ajusten a la realidad pasada. Por tanto, podría definirse como el derecho a equivocarse o a que una equivocación pasada no marque y determine la vida de un individuo que, por definición, no es otra cosa que un proceso evolutivo, una secuencia de aciertos y errores, siempre en proceso de conformación, de cambio y de evolución constante. «La existencia humana es la manifestación más acusada del devenir, porque el hombre no está hecho, sino que se hace a sí mismo, y no puede suspender su autocreación ni un instante» (29).

---

(26) Ver apartados 81, 93 y 97 de la sentencia del TJUE (2014, C-131/12) de 13 de mayo, Caso Mario Costeja y AEPD v. Google Inc. y Google Spain.

(27) SSTC 39/2016, de 3 de marzo (RTC 2016, 39), recordando lo ya establecido en la SSTC 292/2000, de 30 de noviembre (RTC 2000, 292).

(28) Rallo, Artemi: «El derecho al olvido y su protección», *Revista Telos Cuadernos de Comunicación e innovación*, Fundación Telefónica, octubre-diciembre, 2010, pp. 1 a 5.

(29) Fernández de la Mora, Gonzalo: *La envidia igualitaria*, Barcelona, Editorial Áltera, 2012, p. 252.

Las críticas en torno a la idea del derecho al olvido también fueron abundantes. Entre los argumentos utilizados por los detractores o los no partidarios del derecho al olvido, además de la libertad de expresión e información, están los referentes al falseamiento de la historia. A este respecto, algunos cuestionan hasta qué punto la noción del respeto a la privacidad puede extenderse al ocultamiento de información a petición de parte interesada en que no se conozcan hechos o acontecimientos, simplemente por no convenir a sus actuales intereses (30).

2. EL DERECHO AL OLVIDO EN EL CONTEXTO DE LOS MOTORES DE BÚSQUEDA EN INTERNET

2.1 **Caso Mario Costeja y AEPD v. Google Inc. y Google Spain**

El fallo judicial que sentó las bases para resolver los conflictos sobre derecho al olvido en el contexto de los buscadores de Internet tuvo lugar en mayo de 2014, en la sentencia del TJUE en el caso Mario Costeja y AEPD contra Google Inc y Google Spain. La sentencia contempla un derecho al olvido lleno de matices y condicionantes de alcance general y particular. El fallo judicial resuelve un caso concreto, con unas características determinadas, e insiste en su argumentación en que habrá que ir resolviendo, caso por caso, para ver en cada caso si prima más el derecho al acceso a la información o, por el contrario, la privacidad del sujeto. Precisamente por tratarse de una solución para un supuesto concreto, el fallo deja abiertas cuestiones que se plantean en torno al derecho al olvido para las que el fallo citado no da una solución.

La sentencia tiene su origen en una cuestión prejudicial planteada por la Audiencia Nacional al TJUE por dudas interpretativas en relación con la Directiva 95/46/CE, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. El TJUE en su argumentación deja claro que la actividad de un motor de búsqueda proveedor de contenido, en la medida en que encuentra información publicada o puesta en Internet por terceros, la indexa de forma automática, la almacena temporalmente y, por último, la pone a disposición de los internautas según un orden de preferencia determinado, realiza un tratamiento de datos de carácter personal con su servicio de búsqueda en el sentido del artículo 2, letra b) de la citada Directiva (31).

(30) Ver el artículo de opinión, publicado en el *ABC*, el 28 de abril de 2012, por Milagros del Corral, bajo el título de *Derecho al olvido en la era de Internet*. http://sevilla.abc.es/historico-opinion/index.asp?ff=20120428&idn=1502726688681.

(31) El artículo 2, letra b), de la Directiva destaca que el tratamiento de datos personales es: «cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales, como la recogida, registro, organización, conservación,

Tanto para el Abogado General, Niilo Jääskinen, como para el TJUE el hecho de que el buscador no edite o transforme el contenido sino que lo indexe, como un mensajero, intermediario o transmisor, no impide la existencia de un tratamiento de datos personales conforme a la citada Directiva 95/46/CE. Sin embargo, hay un punto clave de divergencia entre la sentencia y las conclusiones del Abogado General, que es precisamente el hecho de que Google no diferencia entre datos personales y datos no personales, que unido al hecho de que se trate de un proceso automático basado en un algoritmo y sin intervención humana, no siendo Google consciente de la existencia de datos personales en sus resultados de búsqueda lleva, en parte, al Abogado General a considerar que Google no es responsable del tratamiento de datos personales que realiza. Así, en opinión del Abogado General el hecho de que la labor como buscador en Internet sea una labor intermediaria, debe tener un reflejo en la atribución de responsabilidad. Pese a ello, el TJUE consideró que en la medida en que el gestor del motor de búsqueda determina los fines y los medios del tratamiento es responsable del mismo. Además, consideró que «dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda en cuestión sea económicamente rentable y, dado que este motor es, al mismo tiempo, el medio que permite realizar las mencionadas actividades, […]» (32), hay que considerar que «se realiza el tratamiento de datos personales en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en el territorio de un Estado miembro, cuando el gestor de un motor de búsqueda crea en un Estado miembro una sucursal o filial, cuyo objetivo es promocionar y vender espacios publicitarios propuestos por el mencionado motor, como es el caso de Google Spain, y que dirige, además su actividad, a los habitantes de ese Estado miembro» (33). Y, por todo ello, el TJUE considera que el buscador debe cumplir con la normativa europea de protección de datos y que es responsable del tratamiento de datos personales que efectúa a través de su servicio de búsquedas, cada vez que un usuario realiza una petición de búsqueda.

A su vez, el TJUE apunta que «las actividades del gestor del motor de búsqueda y las de su establecimiento situado en el Estado miembro de que se trate están indisociablemente ligadas, dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda en cuestión sea económicamente rentable» (34)· El buscador no sólo facilita el acceso a los contenidos alojados en las páginas web

---

elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción».

(32) Apartado 60 de la sentencia TJUE 2014, C-131/12, de 13 de mayo de 2014.

(33) *Ibidem*.

(34) Apartado 56 de la sentencia TJUE 2'14, C-131/12, de 13 de mayo de 2014.

indexadas, sino que también aprovecha esta actividad para incluir publicidad asociada a los patrones de búsqueda introducidos por los internautas, contratada, a cambio de un precio, por las empresas que desean utilizar esta herramienta para ofrecer sus bienes o servicios a éstos.

La analizada sentencia del TJUE pone de relieve, a su vez, que un tratamiento de datos personales inicialmente lícito puede devenir con el tiempo en contrario a la normativa de protección de datos. A este respecto, señala que «incluso un tratamiento inicialmente lícito de datos exactos, puede devenir con el tiempo, incompatible con dicha Directiva cuando estos datos ya no sean necesarios en relación con los fines para los que se recogieron o trataron. Este es el caso, en particular, cuando son inadecuados, no pertinentes o ya no pertinentes o son excesivos en relación con estos fines y el tiempo transcurrido» (35).

La sentencia del TJUE apunta literalmente que, en efecto, respecto al hecho de que los editores web dispongan de protocolos «*no archive*», «*no index*» o códigos de exclusión (36), ésta circunstancia no modifica el hecho de que el gestor determina los fines y los medios de este tratamiento. Sin embargo, desde el momento en que el buscador desempeña un rol intermediario, no edita contenido y se trata de un proceso automatizado que no distingue entre datos personales y no personales, y en aras de una mayor eficacia y logro del fin pretendido, la inclusión de protocolos de no indexación por el editor web hubiese sido, sin duda, una solución, al menos, a considerar.

A su vez, el TJUE deja claro que el derecho del titular de los datos afectado está por encima del interés económico del gestor del motor de búsqueda, y en general, aunque hay que ver caso por caso, también se halla por encima del derecho del internauta al acceso a la información. La sentencia destaca, sin embargo, que «en la medida en que la supresión de vínculos de la lista de resultados podría en función de la información de que se trate, tener repercusiones en el interés legítimo de los internautas potencialmente interesados en tener acceso a la información en cuestión, es preciso buscar en situaciones como las del litigio, un justo equilibrio» (37). Para dicha ponderación de intereses en conflicto, la sentencia facilita el criterio de la relevancia en la vida pública del afectado y el criterio de si la información es o no de interés público. Sin duda, crite-

(35) Apartado 93 de la sentencia TJUE 2014, C-131/12, de 13 de mayo de 2014.

(36) Los códigos de exclusión, conocidos también como protocolos *robot.txt* son herramientas para evitar que ciertos programas informáticos que analizan sitios web agreguen información. Son herramientas de uso frecuente por los motores de búsqueda, para categorizar archivos de los sitios web y utilizados también por los editores web (*webmasters*) para corregir o filtrar el código fuente. El protocolo de exclusión *robot.txt* hace referencia a una serie de estándares web que regulan el comportamiento de los robots o arañas y la indexación de los motores de búsqueda.

(37) Apartado 81 de la sentencia TJUE 2014, C-131/12, de 13 de mayo de 2014.

rios que dan pie a cierta interpretación, donde la casuística puede ser variada y compleja.

2.2 **Alcance territorial de la eliminación de resultados de búsqueda**

El alcance territorial de la eliminación de resultados de búsqueda es un punto de gran relevancia que, no obstante, la sentencia del TJUE 2014, C-131/12, de 13 de mayo, pasa por alto sin precisar el alcance geográfico o a qué versiones del buscador debe aplicar. Ha habido mucha reflexión sobre si la decisión de eliminación de resultados de búsqueda del motor de búsqueda debe limitarse sólo a los dominios europeos o, por el contrario, extenderse globalmente a todos los dominios. Al respecto el Grupo de Trabajo del Artículo 29 (WP 29 en adelante) destaca que una interpretación adecuada de la sentencia del TJUE 2014, C-131/12, de 13 de mayo, es aquella que permite la protección efectiva de los sujetos titulares de los datos, una protección contra la diseminación y accesibilidad universal a información personal que posibilitan los motores de búsqueda en Internet cuando la búsqueda se realiza en base al nombre de una persona. Asimismo, el WP29 destaca que las soluciones concretas pueden variar en función de la estructura y diseño específico de cada motor de búsqueda, pero siempre se debe ofrecer una solución que permita dicha protección efectiva del individuo sin sortear la normativa comunitaria de protección de datos. A este respecto, el WP29 destaca que «limitar la desindexación a los dominios europeos bajo el pretexto de que los usuarios suelen acceder a la información en buscadores a través de sus dominios nacionales no puede ser considerado suficiente para garantizar satisfactoriamente los derechos de los titulares de los datos de acuerdo con la sentencia» (38).

Sin embargo, el informe del grupo de expertos independiente de Google destacó al respecto que se produce una protección de los derechos de los usuarios si, por regla general, la eliminación de resultados de búsqueda se limita a los dominios europeos. Al respecto señala dicho grupo de expertos que, según fuentes de la propia compañía, el 95 % de las peticiones de búsquedas que se producen en la UE proceden de versiones locales del buscador y, además, es práctica habitual que a los usuarios que utilizan en la UE el dominio «.com» se les redirija de manera automática a una versión local. Además, considera el grupo de expertos independiente de Google que el alcance geográfico de la eliminación de resultados de búsqueda es un asunto de soberanía territorial y podría entrar en conflic-

(38) Punto 20 de las *Guidelines* del WP29 «*Guidelines on the implementation of the Court of Justice of the European Union judgement on 'Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzalez, C-131/12*», de 26 de noviembre de 2014.

to con otros derechos protegidos fuera de las fronteras de la UE relacionados con el acceso a la información, aunque pueda suponer mayor protección de los derechos de los usuarios en la UE (39).

El TJUE deberá pronunciarse sobre el alcance territorial de la deliminación de resultados de búsqueda por los motores de búsqueda. En una cuestión prejudicial planteada el pasado 19 de julio de 2017 a la Corte de Luxemburgo por el Consejo de Estado francés (C-507/17) (40), se pregunta sobre el alcance geográfico de la eliminación de resultados de búsqueda. Las tres cuestiones que se plantean son: 1) si se debe llevar a cabo la eliminación de resultados de búsqueda en todas las versiones del motor de búsqueda, de modo que los enlaces cuestionados no aparezcan en la lista de resultados del buscador, con independencia del lugar donde se realice la búsqueda e incluso si ésta se realiza desde fuera del ámbito territorial de la UE; 2) si la respuesta a la pregunta anterior es negativa, ¿debe la eliminación de resultados de búsqueda aplicarse en toda la UE o sólo en el ámbito del Estado desde el cual el ciudadano ha ejercido el derecho al olvido; 3) si el buscador está obligado a emplear el geobloqueo para suprimir los enlaces en las búsquedas que se efectúen desde direcciones IP localizadas en el país de quien solicitó la retirada –o incluso desde direcciones IP de cualquier país de la UE– con independencia de cuál sea la versión del buscador que se consulte.

La respuesta del TJUE a la cuestión del alcance de la eliminación de resultados de búsqueda es uno de los retos pendientes. Sin embargo, cabe señalar que la universalización del derecho al olvido o su aplicación extraterritorial plantea, *a priori*, conflictos, ya que implicaría la extralimitación del derecho comunitario y podría considerarse contraria al derecho internacional. No obstante, cabe destacar que ya contamos con un precedente que reconoce el alcance global de la eliminación de resultados de búsqueda, si bien fuera de las fronteras de la UE. Al respecto, en junio de 2017 el Tribunal Supremo de Canadá avaló el alance global de la eliminación de resultados de búsqueda, amparándose en el alcance global de Internet y la ausencia de fronteras en el mismo (41).

(39) Ver el Informe del Grupo de expertos independiente de Google sobre derecho al olvido, de 6 de febrero de 2015, punto 5.4, p.18. El citado informe destaca (literal en inglés): «*In considering whether to apply a delisting to versions of search targeted at users outside of Europe, including globally, we acknowledge that doing so may ensure more absolute protection of a data subject's rights. However it is the conclusion of the majority that there are competing interests that outweigh the additional protection afforded to the data subject […]. These considerations are bolstered by the legal principle of proportionality and extraterritoriality in application of European Law*».

(40) http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC

(41) Sentencia del Tribunal Supremo de Canadá, Google Inc. v. Equustek Solutions Inc., 2017. https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do.

3. DERECHO AL OLVIDO EN EL MARCO DEL REGLAMENTO 2016/679, DE 27 DE ABRIL, GENERAL DE PROTECCIÓN DE DATOS

El Reglamento 2016/679, de 27 de abril, General de Protección de Datos recoge el derecho a la supresión o al olvido en el artículo 17, ligado al concepto de supresión o cancelación. Por tanto, el Reglamento se desvía del encuadre del derecho al olvido realizado por la sentencia del TJUE 2014, C-131/12, de 13 de mayo, donde se configuraba como el derecho a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona. Es decir, el Reglamento no se centra en la eliminación de contenido de una lista de resultados sino en la cancelación o supresión de contenido en sentido más amplio. Es más, algún autor considera que la redacción del artículo 17 del Reglamento es un tanto ambigua (42), donde no aparecen mencionados explícitamente los buscadores.

Con respecto a la naturaleza y configuración del derecho al olvido en el Reglamento, mayoritariamente la doctrina parece decantarse por considerar que se trata de la manifestación de derechos existentes en el nuevo entorno de Internet. Así para algunos autores, el derecho al olvido «supone una concreción del derecho de oposición y cancelación en un caso concreto como es el tratamiento de los datos en Internet (43). Ya con anterioridad a la aprobación del Reglamento, parte de la doctrina había destacado que «podría mantenerse que se ha otorgado un nuevo nombre a derechos ya conocidos como son los de oposición y cancelación, si bien este nuevo nombre se emplearía para una aplicación particular de los mismos» (44).

El considerando 65 del Reglamento apunta que «los interesados deben tener derecho a que se rectifiquen los datos personales que les conciernen y un derecho al olvido si la retención de tales datos infringe el Derecho de la UE, o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener Derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente regla-

(42) López Calvo, José: «Derecho al olvido. Génesis y nacimiento de un nuevo derecho en la era de Internet», *Diario La Ley*, n.º 7, sección Ciberderecho, Editorial Wolters Kluwer, 23 de mayo de 2017.

(43) López García, M.: «Derecho a la información y derecho al olvido en Internet», *La Ley Unión Europea*, n.º 17, julio 2014, p. 49.

(44) Pazos Castro, Ricardo: «El mal llamado derecho al olvido en la era de Internet», *Boletín del Ministerio de Justicia*, núm. 2183, noviembre 2015, año LXIX, p. 40.

mento». «Este derecho es pertinente, en particular, si el interesado dio el consentimiento siendo un niño, no siendo plenamente consciente de los riesgos que implicaba el tratamiento. Sin embargo, la retención ulterior de datos debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público, o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público o en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones».

En el artículo 17 del Reglamento se estructura el derecho al olvido en tres bloques. Así, en el apartado primero se hace referencia al derecho de los interesados a obtener del responsable del tratamiento, sin dilación indebida, la supresión de los datos personales inexactos que le conciernan. El responsable del tratamiento estará obligado a la supresión de los datos cuando se den una serie de circunstancias a las que hace referencia dicho apartado primero del artículo 17 (45). En el segundo apartado, se establece la obligación del responsable de tratamiento de notificar la solicitud del interesado al resto de responsables que estén tratando dichos datos, con el fin de que tomen las medidas oportunas. Finalmente en el apartado tercero (46) se establecen una serie de excepciones o limitaciones al derecho a la supresión o al olvido (47).

---

(45) El apartado primero del artículo 17 del Reglamento recoge dichas circunstancias, señalando que se dan cuando: «a) Los datos personales ya no son necesarios en relación con los fines para los que fueron recabados o tratados de otro modo; b) el interesado retire el consentimiento en el que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2), letra a), y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2; d) los datos personales hayan sido tratados ilícitamente; e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.»

(46) El artículo 17.3 del Reglamento destaca: «Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario: a) para el ejercicio de la libertad de expresión e información; b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la UE o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3; d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o; e) para la información, el ejercicio o la defensa de reclamaciones».

(47) Álvarez Caro, María: «El derecho a la supresión o al olvido», *Reglamento General de Protección de Datos: hacia un nuevo modelo europeo de privacidad* (Dir: Piñar Mañas, José Luis), Editorial Reus, 2016, p. 246.

Con respecto a la obligación del responsable del tratamiento de informar a los responsables que estén tratando los datos personales de la solicitud de supresión del interesado (48), el considerando 66 del Reglamento destaca que «a fin de reforzar el derecho al olvido en el entorno en línea, el derecho de supresión debe ampliarse de tal forma que el responsable de tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables de tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando datos personales». De la lectura de este considerando y de lo dispuesto en el artículo 17.2 del Reglamento, se puede estimar que si bien hay algunos autores que han venido considerando que el derecho al olvido debe pivotar sobre el derecho de oposición ejercido sobre los motores de búsqueda como responsables de sus propios tratamientos, el Reglamento construye el derecho al olvido en Internet sobre las obligaciones del responsable principal o del responsable en origen que ha hecho públicos los datos (49).

Aunque no se recoja en la literalidad del artículo 17, se podría interpretar que para cumplir con la obligación de tomar medidas razonables, teniendo en cuenta la tecnología y medidas técnicas, con el fin de informar a otros responsables que estén tratando datos, cabría entender que la utilización de protocolos de exclusión, cuando sea posible, es un mecanismo válido para cumplir con dicha obligación. Al respecto, ha habido varios pronunciamientos que avalan la utilización de dichos protocolos de no indexación (50).

4. RETOS EN TORNO AL DERECHO AL OLVIDO

Pese a contar con una sentencia *leading case* sobre la materia (sentencia del TJUE, 2014, C-131/12, de 13 de mayo, caso Mario Costeja y AEPD v. Google Inc. y Google Spain) y con el artículo 17 del Reglamento

(48) El artículo 17.2 del Reglamento señala al respecto: «Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos».

(49) Troncoso Reigada, Antonio: «Las redes sociales a la luz de la Propuesta de Reglamento General de Protección de Datos Personales», *Revista de Internet, Derecho y Política*, Universitat Oberta de Catalunya, número16, junio 2013, p. 33.

(50) Ver las conclusiones del Abogado General, Niilo Jääskinen, de 25 de junio de 2013, en el caso Mario Costeja y AEPD, v. Google Inc. y Google Spain. Ver asimismo la STS, de 15 de octubre de 2015 (RJ 2015/4417).

2016/679, de 27 de abril, General de Protección de Datos, además de con la normativa en tramitación que adaptará la legislación española al reglamento europeo, hay algunos aspectos sobre los que aún existen dudas en relación con el derecho al olvido.

Al margen de dudas sobre algunos aspectos procedimentales y, además del mencionado asunto sobre el alcance geográfico de la eliminación de resultados de búsqueda, el Consejo de Estado francés preguntó recientemente al TJUE, a través de una cuestión prejudicial (C-136/17) (51) sobre el alcance del derecho al olvido en su aplicación práctica. En concreto ha preguntado sobre la posibilidad de que los motores de búsqueda puedan ser compelidos a bloquear todo resultado de búsqueda que remita a *websites* que contengan datos personales de carácter sensible, de manera automática y, por tanto, sin necesidad de realizar el juicio de valor que la propia Corte de Luxemburgo estableció en la sentencia de mayo de 2014. Es decir, se pregunta al TJUE si la existencia de datos sensibles en las páginas web de la lista de resultados de una búsqueda debe prevalecer en todo caso frente al interés público de la información.

No resulta difícil imaginarse situaciones donde, pese a la existencia de datos sensibles en una información como, por ejemplo, la afiliación política o ideología, sin embargo, la información resulte de gran interés público para la ciudadanía, como son los casos de corrupción protagonizados por políticos. Pretender, por tanto, un bloqueo automático sin entrar a ponderar los derechos e intereses en conflicto resulta, además de poco coherente con la propia sentencia del TJUE 2014, C-131/12, de 13 mayo, poco respetuoso con el derecho al acceso a la información en una sociedad democrática avanzada. Habrá que esperar el fallo del TJUE en ese asunto y ver cómo queda configurado el alcance del derecho al olvido en dicha aplicación práctica.

Finalmente, y no menos importante, otra de las cuestiones que supone todo un reto es la relacionada con la tecnología *blockchain*. Dicha tecnología es la que subyace en la moneda virtual *Bitcoin*. En esencia, el *blockchain* es una tecnología en la que, mediante protocolos P2P y técnicas criptográficas, se crea un registro, una base de datos distribuida y descentralizada, cuyos datos son inmutables. La tecnología *blockchain* tiene un gran potencial para transformar los procesos de negocio y, en particular, los servicios financieros o las relaciones contractuales a través de los denominados contratos inteligentes (*Smart contracts*).

Precisamente es la característica de inmutabilidad del *blockchain* la que da pie al debate sobre su compatibilidad con la normativa de protección de datos, en concreto, con el derecho al olvido, cancelación o supre-

(51) http://english.conseil-etat.fr/Activities/Press-releases/Right-to-be-delisted.

sión. Para solucionar el conflicto, la legislación podría limitar el alcance del derecho al olvido en los sistemas *blockchain*, de modo que bastase con la inaccesibilidad al dato y no fuese necesario suprimir. También, otra posible solución pasaría por el desarrollo de un *blockchain* editable, donde ya la característica de inmutabilidad no esté presente y alguno o varios administradores puedan cambiar bloques de información sin afectar a la totalidad de la cadena.

Por su parte, el WP29 recientemente ha anunciado, en su última reunión plenaria del 6 y 7 de febrero de 2018 (52), que trabajará en la actualización de las *Guidelines* y criterios en relación con el derecho al olvido.

(52) http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614823.

CAPÍTULO 14

INTERNET DE LAS COSAS

JAVIER PUYOL MONTERO
Abogado. Magistrado en excedencia. Consultor TIC's.
Director de Puyol-Abogados & Partners

1. INTRODUCCIÓN

En el análisis de Internet de las Cosas ha de partirse del hecho acaecido hace más de 150 años, cuando Internet no era siquiera un sueño, el visionario Julio Verne imaginó algo similar a la gran red que hoy condiciona nuestro día a día. El escritor francés incluyó en París en el siglo XX (1863), su obra perdida, la idea de un telégrafo mundial que funcionaba como una gran red de telecomunicaciones. Existen otras imágenes, ya que Verne no fue el único que fantaseó con algo parecido a la actual Internet. En el relato de 1898 «*From the London Times of 1904*», Mark Twain definía el telectroscopio como «un dispositivo que, conectado al teléfono, daba acceso a una gran red global de información compartida que incluía audio y vídeo». Nikola Tesla en 1909, Paul Otlet (padre de la documentación) en 1934, H. G. Wells en 1937 *(World brain)* y Jorge Luis Borges en 1939 (La biblioteca total) aventuraron ideas muy cercanas a la telefonía móvil, la *World Wide Web* e incluso la Wikipedia. En 1968, ya con más pistas, Arthur C. Clark y Stanley Kubrick imaginaron el iPad y los diarios digitales en 2001: «Una odisea del espacio»; y en 1985, Orson Scott Card volvió a insistir en la idea de las tabletas y adelantó con mucha exactitud los foros de Internet en «El juego de Ender». Finalmente, cuando Internet vio la luz, muchas de estas profecías se cumplieron y otras fueron incluso más allá. En los últimos veinte años –en los que se ha vivido la gran explosión de este prodigioso invento–, Internet ha avanzado de revolución en revolución: el correo electrónico, los buscadores, la mensajería instantánea, los blogs, el boom del vídeo, el comercio electrónico, las redes sociales, el salto a los dispositivos móviles, la economía colaborativa... (1), hasta convertirse en lo que hoy es, y sin lugar a dudas, será el día de mañana.

Hoy en día, Internet de las Cosas («*IoT*») consiste en que los objetos tengan conexión a Internet en cualquier momento y lugar. En un sentido más técnico, consiste en la integración de sensores y dispositivos en objetos cotidianos que quedan conectados a Internet a través de redes fijas e inalámbricas (2). Y que el Grupo de Trabajo creado por del artículo 29 de

(1) *Cfr.:* APARICIO, DANIEL G. «El futuro de Internet: conexión para todos y en todas partes, desde la ropa hasta la nevera». 20 Minutos. 17 de mayo de 2015. http://www.20minutos.es/noticia/2457696/0/dia-de-internet/futuro-de-la-red/internet-de-las-cosas/#xtor=AD-15&xts=467263

(2) Internet de las Cosas será la estructura más compleja que la humanidad haya creado jamás. En una generación, es probable que exista un billón de nodos que midan cualquier cosa que se pueda medir sobre la faz de la Tierra y con la información extraída de esos datos controlaremos todos los aspectos del mundo que hemos construido. Internet de las Cosas va a afectar a toda nuestra vida, con grandes repercusiones sociales, económicas y sobre la privacidad. Por lo tanto, más vale que sea construida de forma inclusiva, ya que, de lo contrario, el temor puede superar sus beneficios. Una de las características más importantes de esta nueva revolución de la tecnología es que su control esta fuera del ámbito de las grandes compañías que monopolizan el mundo de las comunicaciones, o al menos el «coto» no está cerrado para que, de manera aislada e individual, aficionados, estudiantes, universidades y cualquier persona pueda intervenir con sus aportaciones en una «comunidad tecnológica «*Open Source*» (de contenido abierto)». *Cfr.:* RUIZ GUTIERREZ, JOSÉ MANUEL. «Arduino e

la Directiva 95/46/CE los ha definido como la «infraestructura en la que miles de millones de sensores embebidos en dispositivos comunes de todos los días –«cosas», o cosas vinculadas a otros objetos o individuos– diseñados para registrar, procesar, almacenar y transferir datos y que están asociados con identificadores únicos para interactuar con otros dispositivos o sistemas que utilizan las capacidades de red». Además, Internet de las cosas generalmente implica el tratamiento de los datos que se refieren a personas físicas identificadas o identificables, y por tanto se califican como datos personales en el sentido del artículo 2 de la citada Directiva 95/46/CE de Protección de Datos de la Unión Europea, y los apartados 1.º y 2.º del artículo 1 del Reglamento (UE) 2016/679 del Parlamento y del Consejo de 27 de abril de 2016, General de Protección de datos de la Unión Europea (3).

El término «*IoT*» va mucho más allá, y engloba objetos comunes que hasta ahora no disponían de conectividad. Con esta evolución, algunos elementos como neveras, hornos, lavadoras, coches, relojes, televisores y un largo etcétera disponen ya de conexión a Internet. La conectividad de estos elementos permite, entre otras muchas cosas, controlar el objeto de forma remota a través de otro dispositivo o una aplicación a través de Internet. Hasta ahora Internet era una herramienta de trabajo, de consulta de información y de comunicación. Mediante esta nueva forma de interacción, hacemos que Internet sea una parte necesaria en las tareas comunes y cotidianas de la vida. La tendencia es que siga evolucionando y aumentando exponencialmente (4) como lógica consecuencia de la creación de nuevos modelos de negocio, productos y compañías con actividades nuevas y completamente diferentes a las que conocemos en la actualidad.

El internet de las cosas constituye, por tanto, una gran evolución, que permitirá una mejor calidad de vida para los ciudadanos, ya que este puede recopilar múltiples informaciones que, reunidas entre sí, se pueden convertir en una fuente de información importante y trascendente, proporcionando conocimientos que permitan profundizar en todos los aspectos de la vida económica, social e incluso cultural de cualquier colectivo o

---

'Internet de las Cosas'». Fundación telefónica. 6 de febrero de 2.013. http://encuentro.educared.org/profiles/blogs/arduino-y-el-internet-de-las-cosas

(3) El apartado 1.º, del artículo 1, del Reglamento General de Protección de Datos de la Unión Europea, determina que «*El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos*», mientras que el apartado segundo afirma que «*El presente Reglamento protege los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales*».

(4) En este sentido, *cfr*. «Seguridad en Internet de las cosas. Estado del Arte». Centre Seguretat TIC de la Comunitat Valenciana. Generalitat Valenciana. Fondo Europeo de Desarrollo Regional. Unión Europea.

sociedad (5). En este sentido, hace 20 años Internet se usaba principalmente como herramienta para buscar información. En los últimos 10 años se ha construido una nueva forma de uso de Internet donde todos se ha convertido en social, transaccional, y móvil. Si el número de cosas conectadas a Internet sobrepasó en el año 2008 el número de habitantes del planeta, se estima que habrá 50.000 millones de dispositivos conectados en el año 2020, siendo en la práctica incalculable las cifras de negocio que ello puede generar teniendo en cuenta la mayor productividad, el ahorro de costes, y los nuevos mercados que se van a generar para las empresas (6). Obviamente si el consumo de Internet de las Cosas aumenta, el gasto y la inversión realizada en este sector también crecen, y además, lo hace de manera considerable.

Los servicios que se corresponden con los mercados profesionales, de consumo y de conectividad han alcanzado un gasto de 256.340 millones de euros en 2017. Si nos referimos al gasto en hardware que han sido utilizado por parte de las empresas, la cifra alcanza los 905.000 millones de euros, mientras que la inversión en aplicaciones dedicadas exclusivamente al consumidor ha sido de 680.750 millones. Gartner estima que en 2020 el gasto en ambos segmentos podría llegar a ser de casi 3.000 millones de euros (7).

En este sentido, se puede afirmar que estamos presenciando el prólogo de la historia de los productos inteligentes conectados a internet, y aún quedan muchos retos por resolver, de los cuales hemos aportado algunas pinceladas: seguridad y privacidad, el consumo energético y las necesidades de mantenimiento, nuevos modelos de relación producto-persona que se derivan de las relaciones producto-usuario-fabricante o de nuevos modelos de negocio adaptados a su dualidad.

Un escenario que, según señala Taravilla (8), supondrá que miles de objetos se unan a la red en un breve plazo y participen en una nueva y tupida malla de interconexiones e información. Se estima que ya son más de 2.000 millones las personas que se conectan a Internet (9), y que habrá

(5) Por ejemplo, en el ámbito de la salud, permitirá detectar enfermedades que algunas veces no se pueden identificar fácilmente, entonces por medio de micro-chips en las personas se detectará cualquier anomalía y esta información será enviada por medio de diferentes dispositivos a la persona que está encargada del cuidado del paciente y esta podrá tener un mejor seguimiento y control del paciente.

(6) Pastor, Javier, y Everlet, Alvaro. «Introducción al Internet de las Cosas. Construyendo un proyecto de IoT». Universidad Rey Juan Carlos. Noviembre 2013.

(7) *Cfr.:* Ferrer Caballero, Carolina. «8.400 millones de dispositivos estarán conectados a internet a finales de 2017». Blogthinkbig.com. https://blogthinkbig.com/8-400-millones-de-dispositivos-estaran-conectados-a-internet-a-finales-de-2017

(8) *Cfr.:* Taravilla Herrera, Javier. «El futuro de la red. Internet de las cosas». Junio de 2013. http://www.academia.edu/6399803/El_futuro_de_la_red_Internet_de_las_cosas

(9) *Cfr.:* http://www.internetworldstats.com/stats.htm

que sumar a esta cifra unos 15.000 millones de objetos conectados (10). Así, bajo el concepto de «Internet de las cosas» se encuentra la idea primordial de que los objetos que nos rodean, sean electrodomésticos, vehículos, ropa, latas de refresco o el propio banco de la calle se convierten en ciudadanos de primera clase en internet, como productores y consumidores de información, generada por ellos mismos, por las personas o por otros sistemas (11).

Los beneficios que subyacen de Internet de las Cosas son amplios y muy diversos, pero para hacerlos realidad el Internet de los objetos se enfrenta a importantes retos. Tanto las personas como los objetos van a poder conectarse y participar en la red casi en cualquier momento y lugar. En caso de cumplirse las previsiones, nos encontramos a las puertas de un nuevo modo de interacción en el mundo físico, inspirado en la idea de ubicuidad y facilitado por el desarrollo de las tecnologías de la información y la industria electrónica. Se crearía una malla de conexiones en el planeta que establecería una especie de «sistema nervioso mundial», donde la aldea global (12) alcanzará a los objetos cotidianos. Pero, aunque este horizonte se instale con fuerza en los programas de los centros de investigación, empresas y estados, ni el nombre ni la idea son tan nuevos (13). En concreto, dicha denominación es atribuida a Kevin Aston, cofundador y director del Auto-ID Center del MIT (14), que en 1999 utilizó esta expresión para llamar la atención de los directivos de la em-

---

(10) *Cfr.:* http://www2.alcatel-lucent.com/knowledge-center/public_files/Internet-of-Things.pdf

(11) *Cfr.:* Vazquez, Juan Ignacio. «C@mbio. Horizontes y desafíos de Internet de las cosas». BBVA. http://bbvaopenmind.com. Dicho autor, señala que el estilo de vida digital que nos impregna continuamente permite que los objetos conectados a internet superen la barrera de aceptación ante lo nuevo, ante el cambio, que quizá es el mayor de los obstáculos que establecemos los seres humanos, y se integren poco a poco en la cotidianidad. Al usar servicios de internet diariamente (prensa digital, redes sociales o comercio electrónico) es mucho más sencillo aceptar que algunos objetos de nuestro entorno van a participar también de este ecosistema, con el propósito de hacer nuestra vida más fácil y cómoda.

(12) Termino que se debe a Marshall McLuhan y que hizo famoso tras la aparición en sus obras tituladas:» La Galaxia Gutenberg: la génesis del hombre tipográfico». Círculo de Lectores, Barcelona, 1988; y en «Comprender los medios de comunicación: las extensiones del ser humano». Editorial Paidos, Barcelona, 1996.

(13) Según Neil Gershenfeld, investigador del Instituto Tecnológico de Massachusetts (MIT), quien publicó en 1999 el libro Cuando las cosas empiecen a pensar, «*la expresión de Internet 0 (cero) nace del proyecto Media House, que se llevó a cabo en Barcelona. Se levantó una estructura con la idea de una vivienda programable basada en microchips, que son servidores web, y sensores que controlan la energía y pueden comunicarse de muy distintas maneras. El nombre de Internet 0 procede del empleo de una comunicación lenta para hacer más fácil su implementación*». En el artículo de referencia, dice la autora: «*El Internet de las Cosas permitirá conectar computadoras, personas y cosas en todas las combinaciones. No importará si es de día, de noche o si los objetos están en movimiento, ni tampoco si estamos en un edificio, en un avión, en el metro o al aire libre. En otras palabras, dispondríamos de capacidades ilimitadas de comunicación*». Se calcula que este tipo de comunicaciones ocupa ya un 12% del tráfico de la Red. *Cfr.:* Puchet, Clara y Bolaños, Sirio. «Conexión Total: El Internet de las Cosas». Mayo de 2013.

(14) La red de laboratorios Auto-Id es un grupo de investigación centrado en el desarrollo de etiquetas RFID y sensores, con centros en varios países. http://www.autoidlabs.org/

presa Project & Gamble, que intentaba hacerles ver que la inclusión de etiquetas RFID (15) en sus cadenas de suministros, sumado a las posibilidades de la Internet de entonces, podría acarrear importantes beneficios para su empresa (16), y a tales efectos, realizaba investigaciones en el campo de la identificación por radiofrecuencia en red (RFID) y las tecnologías de sensores emergentes. Los laboratorios de investigación estaban conformados por siete universidades ubicadas en cuatro continentes, seleccionadas por Auto-ID Center para diseñar la arquitectura de Internet de las cosas. Y la idea inspiradora fue la mencionada «ubicuidad». Un concepto aparecido en la obra de Philip K. Dick Ubik (17) y que en 1991 Mark Weiser, director científico del Centro de Investigación de Xerox en Palo Alto, materializó en el término de «computación ubicua» o «*ubicomp*». Una expresión utilizada desde 1988 en los ambientes de investigación y que saltó a la luz pública con su artículo «*The Computer for the Twenty-First Century*» (18). Para Weiser, los ordenadores personales deberían ser sustituidos por dispositivos invisibles encajados en los objetos diarios, pues eran elementos demasiado enredados que suponían demasiado tiempo y atención por parte de los usuarios. Los ordenadores requerían una atención casi exclusiva de estos y les distraían de otras tareas. La computación ubicua se definió entonces como el intento de integrar la informática en el entorno personal a través de variados dispositivos con el objetivo de ayudar en el desarrollo de las tareas diarias. El concepto también es conocido como «*calm technology, persuasive computing, things that think o everyware*». Pues bien; esta ubicuidad tecnológica, pensada para el entorno doméstico y personal, aspira en la actualidad a expandirse al ámbito de la industria, servicios, consumo o medio ambiente, de la mano de la rápida evolución de la electrónica y las redes, bajo este nombre de «Internet de las cosas». Debe tenerse presente que los seres humanos evolucionan porque se comunican. Por ejemplo, después de haber descubierto el fuego y de haberlo compartido,

(15) «Radio Frecuency Identification», Wikipedia. RFID (siglas de *Radio Frequency Identification*, en español identificación por radiofrecuencia) es un sistema de almacenamiento y recuperación de datos remoto que usa dispositivos denominados etiquetas, tarjetas, transpondedores o tags RFID. El propósito fundamental de la tecnología RFID es transmitir la identidad de un objeto (similar a un número de serie único) mediante ondas de radio. Las tecnologías RFID se agrupan dentro de las denominadas Auto ID («*automatic identification*», o «identificación automática»). Las etiquetas RFID (RFID Tag, en inglés) son unos dispositivos pequeños, similares a una pegatina, que pueden ser adheridas o incorporadas a un producto, un animal o una persona. Contienen antenas para permitirles recibir y responder a peticiones por radiofrecuencia desde un emisor-receptor RFID. Las etiquetas pasivas no necesitan alimentación eléctrica interna, mientras que las activas sí lo requieren. Una de las ventajas del uso de radiofrecuencia (en lugar, por ejemplo, de infrarrojos) es que no se requiere visión directa entre emisor y receptor. *Cfr.:* http://es.wikipedia.org/wiki/RFID

(16) *Cfr.:* Aston, K. «That 'Internet of the Things' Things», RFID Journal, 1999: http://www.rfidjournal.com/article/print/4986

(17) Dick, Philip K. «Desgraciadamente ha muerto». La Factoría de Ideas, Madrid, 2005.

(18) *Cfr.:* Weiser, M. «The Computer for The twenty-First Century», 1991.http://web.media.mit.edu/~anjchang/ti01/weiser-sciam91-ubicomp.pdf

ya no hacía falta redescubrirlo: solo había que comunicarlo. Un ejemplo más moderno sería el descubrimiento de la estructura helicoidal del ADN, moléculas que transportan información genética de una generación a la siguiente. Una vez que el artículo de James Watson y Francis Crick apareció en una publicación científica en abril de 1953, las disciplinas de la medicina y la genética pudieron tomar esta información y avanzar desde allí a pasos agigantados (19). Este principio de compartir información y aprovechar los descubrimientos se puede comprender mejor si se analiza la manera en que los seres humanos procesan los datos desde la base hasta la cúspide, las capas de la pirámide incluyen datos, información, conocimiento y sabiduría. Los datos representan la materia prima que se procesa para obtener información. Los datos individuales por sí mismos no son muy útiles, pero en grandes volúmenes permiten identificar hábitos, tendencias y patrones. Esta y otras fuentes de información se unen para conformar el conocimiento. En su sentido más básico, el conocimiento es la información de la que alguien es consciente. Luego, la sabiduría nace de la combinación de conocimiento y experiencia. En tanto que el conocimiento cambia con el tiempo, la sabiduría es atemporal, y todo comienza con la adquisición de datos. También resulta importante destacar que existe una correlación directa entre la entrada (datos) y la salida (sabiduría). Cuántos más datos se generan, más conocimiento y sabiduría pueden obtener las personas. Internet de las cosas aumenta drásticamente la cantidad de datos que están disponibles para que los procesemos. Este aumento, combinado con la capacidad de Internet de comunicar estos datos, hará posible que las personas avancen aún más.

Actualmente, Internet de las cosas está compuesto por una colección dispersa de redes diferentes y con distintos fines. A medida que Internet de las cosas evoluciona, estas redes y muchas otras estarán conectadas con la incorporación de capacidades de seguridad, análisis y administración (20). Esta inclusión permitirá que Internet de las cosas sea una herramienta aún más poderosa, y que adquiera una gran importancia, porque se trata de la primera evolución real de Internet (un salto que conducirá a aplicaciones revolucionarias con el potencial de mejorar drásticamente la manera en que las personas viven, aprenden, trabajan y se entre-

(19) *Cfr.:* «The Discovery of the Molecular Structure of DNA», NobelPrize.org. http://books.google.es/books?hl=es&lr=&id=s_UmoMXRTIYC&oi=fnd&pg=PP1&dq=the+discovery+of+the+molecular+structure+of+dna+-+the+double+helix&ots=XN_gQR1Nh6&sig=yVyedFNcyI7frMX44II9JCrQW0s#v=onepage&q=the%20discovery%20of%20the%20molecular%20structure%20of%20dna%20-%20the%20double%20helix&f=false

(20) Evans, Dave. «Internet de las cosas. Cómo la próxima evolución de Internet lo cambia todo». Cisco. Abril de 2011. http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCoQFjAA&url=http%3A%2F%2Fwww.cisco.com%2Fweb%2FLA%2Fsoluciones%2Fexecutive%2Fassets%2Fpdf%2Finternet-of-things-iot-ibsg.pdf&ei=tiydVKu2GcurUeDKgqAL&usg=AFQjCNHXVdJtOj7bwuOXPN1Zqm1QeLsKhQ&bvm=bv.82001339, d.d24

tienen). Internet de las cosas ya ha logrado que Internet sea sensorial (temperatura, presión, vibración, luz, humedad, estrés), lo que nos permite ser más proactivos y menos reactivos. El hecho de que Internet esté presente al mismo tiempo en todas partes permite que la adopción masiva de esta tecnología sea más factible. Dado su tamaño y su coste, los sensores son fácilmente integrables en hogares, en los entornos de trabajo y toda clase de lugares públicos. De esta manera, como ha quedado dicho, cualquier objeto es susceptible de ser conectado y «manifestarse» en la Red. Además, Internet de las cosas implica que todo objeto puede ser una fuente de datos. Esto está empezando a transformar la forma de hacer negocios, la organización del sector público y el día a día de millones de personas (21).

En la clasificación de las relaciones existentes entre Internet de las Cosas, y el ser humano, debemos tener presente, que muchos aspectos de esta interrelación, tienen una interconexión directa, con los derechos fundamentales de los que es portador la persona, y que afectan a múltiples facetas de su actividad. En este sentido, cabe referirse de manera especial a los siguientes aspectos de dicha relación:

a) **Salud**

En este caso, es preciso hacer expresa referencia principalmente a todo tipo de aplicaciones que monitoricen remotamente la salud del individuo sea por ejemplo el nivel de azúcar, el ritmo cardíaco, etcétera. Esos datos se envían al centro de salud y los responsables sanitarios realizan las actuaciones necesarias según las medidas recibidas del paciente.

b) **Seguridad**

Con relación a este campo, los avances producidos se materializan en cuestiones tales como el control de presencia, el control de accesos, la monitorización de todo tipo de incidencias. El ejemplo típico es la alarma que muchas familias tienen instaladas en sus domicilios.

(21) *Cfr.:* «El Internet de las Cosas». Fundación para la innovación Bankinter. Madrid 2011. http://www.fundacionbankinter.org/es/publications/the-internet-of-things. Las aplicaciones del internet de las cosas que reciben más publicidad suelen estar muy orientadas al consumidor, pero resultan poco escalables a nivel industrial. La pregunta más lógica es si su implementación se extiende a sectores más amplios y si es capaz de redefinir sus procesos para crear eficiencia y valor perdurable. Los sectores de la logística y el transporte han sido de los primeros en sumergirse en el concepto de Internet de las cosas con su adopción de las etiquetas RFID. En 2010, había cerca de 3.000 millones de etiquetas en circulación en el mundo. Sin embargo, solo se trata de los primeros pasos hacia la adopción generalizada de la tecnología en otras industrias. Se tienen que analizar las primeras incursiones de Internet de las Cosas en sectores como el sanitario, el agrícola, la logística o el de suministros, permitiendo conectar todo tipo de máquinas para monitorizar y controlarlos de manera inteligente. También cómo el smartphone se está convirtiendo en los ojos y oídos de las aplicaciones; sensores de movimiento y ubicación nos dicen dónde estamos, lo que estamos viendo y la velocidad a la que nos movemos, en tiempo real.

c) **Vivienda**

Hace referencia al concepto popularmente conocido como «*domótica*» (22), y que se concreta en la existencia de sensores que controlan múltiples aspectos del hogar entre los que están la temperatura, apertura y cierre de puertas y ventanas, suministro de aquellos insumos, que sean necesarios, etcétera.

d) **Cuerpo humano**

En este apartado debe incluirse un concepto anglosajón conocido como «*wearables*» (23), es decir, aquella ropa o instrumentos en contacto con el ser humano y que sirven para mejorar su confort o su salud desde un aspecto no médico. Consecuentemente con ello, en esta categoría se encontrarían los relojes y pulseras que se utilizan para monitorizar el ejercicio físico, la ropa de moda que contiene algunos de estos sensores, las gafas de realidad aumentada o las gafas de sol que no se pierden al estar geo posicionadas. También se incluyen en esta categoría las aplicaciones para teléfono móvil que monitorizan a los deportistas o a aquellos que están siguiendo una dieta, entre otros muchos desarrollos y avances técnicos.

e) **Ciudad**

Las «*Smart cities*» (24) o ciudades conectadas recogen datos de utilidad para la gestión de la ciudad y para el confort del ciudadano, tales

(22) La domótica es un término empleado en el área de la tecnología, para referirse a todo aquello que constituye el dominio y la supervisión de todos los elementos que integran una edificación compuesta por oficinas o sencillamente una vivienda. Es un grupo de tecnologías que se encuentran adaptadas para ejercer el control y sistematización dentro de una vivienda, con la finalidad de poder proporcionar un eficiente uso de la energía, así como aportar seguridad y comodidad; permitiendo de esta manera que exista una comunicación entre el beneficiario y el sistema.

(23) «*Wearable*» hace referencia al conjunto de aparatos y dispositivos electrónicos que se incorporan en alguna parte de nuestro cuerpo interactuando de forma continua con el usuario y con otros dispositivos con la finalidad de realizar alguna función concreta, relojes inteligentes o smartwatchs, zapatillas de deportes con GPS incorporado y pulseras que controlan nuestro estado de salud son ejemplos entre otros muchos de este género tecnológico que se halla poco a poco más presente en nuestras vidas. La palabra wearable posee una raíz inglesa cuya traducción significa «llevable» o «vestible», en el argot tecnológico hace referencia a pequeñas computadoras que van siempre con el usuario. Bajo esta concepción, el PC deja de ser un dispositivo extraño para el usuario que solo lo usaba en un espacio definido pasando a ser un factor que se incorpora e interactúa de forma continua con él, además de acompañarlo a todas y cada una de las partes. La tecnología wearable hace referencia a los productos que incorporan un microprocesador y que usamos a diario formando una parte de nosotros, en esta definición no consideramos wearable a nuestra TV del salón, a la máquina de café de la cocina o bien al e-book que usamos para leer nuestros libros, en tanto que si bien sean dispositivos electrónicos que poseen microprocesadores y los empleamos a diario no forman una parte de nosotros dado a que no son «llevables» o «vestibles» en cambio unas gafas, pulseras, relojes, etc., son productos wearables si le agregamos uno o varios microprocesadores electrónicos. *Cfr.:*«¿Qué es un *wearable*? Los Dispositivos convertibles». http://www.dispositivoswearables.net/

(24) La expresión «ciudad inteligente» es la traducción y adaptación del término en idioma inglés «*Smart City*». Es un concepto emergente, y por tanto sus acepciones en español y en otros

como la ubicación de plazas de aparcamiento libre, gestión de flotas de transporte público o predicción de zonas potencialmente delictivas, entre otras muchas aplicaciones.

f) **Ocio**

Dentro de esta categoría están una gran variedad de situaciones que van desde los videojuegos en red hasta gafas de realidad virtual para interactuar con otras personas.

g) **Industria y agricultura**

Las nuevas posibilidades que se ciernen en ambos campos son inconmensurables. La prueba de la evolución tecnológica, determinará nuevas formas de vivir y de comportarse socialmente. El uso de toda clase de dispositivos, sean estos móviles o no, o el empleo de las redes sociales constituye un claro ejemplo de ello. Hemos pasado de la sociedad de la información a la sociedad del conocimiento, donde todos los ciudadanos tienen la posibilidad de acceder a toda la información que precisen en tiempo real, sobre prácticamente cualquier aspecto o fenómeno de la vida. En este ámbito, los cambios operados en la agricultura y en la manufactura de los alimentos también constituyen hechos muy singulares y relevantes, entre otros muchos a considerar.

Y como ha quedado dicho, la llegada de Internet de las Cosas implicará cambios en nuestra forma de vivir teniendo implicaciones tecnológicas, sociales, económicas y jurídicas. A todos estos retos hay que añadir, dentro de la lógica tutela de los derechos fundamentales, la obligación de garantizar la protección de datos y la privacidad de todas las personas, como un elemento necesario e indispensable para cualquier avance tecnológico que efectivamente se produzca. Por todo ello, se hace procedente determinar los elementos claves para el desarrollo de

---

idiomas, e incluso en el propio idioma inglés, están sujetas a constante revisión. Es también un término actual, que se está utilizando como un concepto de marketing (mercadotecnia) en el ámbito empresarial, en relación a políticas de desarrollo, y en lo concerniente a diversas especialidades y temáticas. La «ciudad inteligente» a veces también llamada «ciudad eficiente» o «ciudad súper-eficiente», se refiere a un tipo de desarrollo urbano basado en la sostenibilidad que es capaz de responder adecuadamente a las necesidades básicas de instituciones, empresas, y de los propios habitantes, tanto en el plano económico, como en los aspectos operativos, sociales y ambientales. El concepto Smart City surge de la evolución de las llamadas Ciudades Digitales, que en el año 2004 nacen en España tras un trabajo que realizó el Ministerio de Industria de este país con la elaboración del primer programa de Ciudades Digitales que se abordaba en el mundo. Ciudades inteligentes, dado su origen natural de las Ciudades Digitales, se basa en el uso intenso de las Tecnologías de la Información y Comunicación (TIC) en prestación de servicios públicos de alta calidad y calidez, seguridad, productividad, competitividad, innovación, emprendimiento, participación, formación y capacitación. *Cfr.:* WIKIPEDIA. Concepto de «*Smart Cities*» o «Ciudad Inteligente». https://es.wikipedia.org/wiki/Ciudad_inteligente

Internet de las Cosas (*«IoT»*), y dentro de ellos, debemos hacer especial hincapié en las diferentes tipologías de dichos elementos (25), fundamentales para el desarrollo de esta nueva tecnología, y que son los siguientes:

a) En primer término, hay que hacer referencia a aquellos elementos técnicos o de mercado. Dichos elementos hacen referencia a factores tan importantes como: (i) la confiabilidad; (ii) la escalabilidad o el crecimiento; (iii) la energía; (iv) la conectividad; (v) el coste; (vi) la capacidad, o (vii) el llamado «*IPv6*» (26).

b) Frente a ellos se alzan aquellos elementos clave que también son fundamentales para el desarrollo de Internet de las cosas, basados en el desarrollo de políticas concretas, especialmente aquellas de naturaleza pública. Estos elementos son: (i) la ubicación de los datos; (ii) el acceso a datos/datos abiertos; (iii) los modelos regulatorios preexistentes; (iv) los derechos de propiedad intelectual; (v) el tráfico transfronterizo; (v) la gobernanza.

c) Como espacio común a ambas categorías anteriores, cabe señalar otros elementos a seguir que también tienen una importancia capital como elementos clave para el desarrollo integral de Internet de las Cosas. Así, entre estos, cabe reconocer como tales: (i) los estándares; (ii) la interoperabilidad; (iii) la seguridad; (iv) la privacidad; (v) las limitaciones de espectro y ancho de banda.

2. RETOS ACTUALMENTE EXISTENTES PARA EL DESARROLLO DE INTERNET DE LAS COSAS *(«IoT»)*

En la actualidad son muchos los retos que condicionan el desarrollo de Internet de las Cosas seguidamente vamos a analizar alguno de ellos (27).

(25) *Cfr.:* Harnessing the Internet Of Things for Global Development. UIT. 2016

(26) *IPv6* es la abreviatura de «versión 6 del protocolo de Internet». IPV6 es el protocolo de Internet de última generación, diseñado para reemplazar al protocolo de Internet actual, IP versión 4. Para comunicarse a través de Internet, las computadoras y otros dispositivos deben tener direcciones de remitente y de destinatario. Estas direcciones numéricas se conocen como «direcciones de protocolo de Internet». A medida que Internet y su cantidad de usuarios crecen exponencialmente, también crece la necesidad de direcciones IP. *IPv6* es un estándar desarrollado por el Grupo de trabajo de ingeniería de Internet (IETF), una organización que desarrolla tecnologías de Internet. Anticipándose a la necesidad de un mayor número de direcciones IP, el IETF creó *IPv6* para satisfacer la demanda del creciente número de usuarios y de dispositivos que acceden a Internet. IPv6 permite que un mayor número de usuarios y de dispositivos se comunique a través de Internet por medio del uso de números más grandes para la creación de direcciones IP. *Cfr.:* Apple. Inc. (US). «¿Qué es *IPv6*?». https://support.apple.com/es-mx/HT202236

(27) Por su interés, debe ser consultado el documento «Internet de las cosas: retos para su desarrollo». Instituto Federal de telecomunicaciones. Estavillo Florez, María Elena. Ciudad de México. 24 de mayo de 2016.

2.1 **La suficiencia de las direcciones IP**

En primer término, debe abordarse el problema suscitado como consecuencia de que los recursos de numeración, a veces no son suficientes, y no se dispone de ellos en la cantidad necesaria. En este sentido, tenemos que tener en cuenta que el número de direcciones IP hoy por hoy es insuficiente a todas luces. Para ello ha de tomarse en consideración la circunstancia de que cada dispositivo necesita disponer de su correspondiente dirección IP, lo que constituye un grave problema, ya que las actualmente existentes, no son suficientes para dar el correspondiente servicio o para cubrir las necesidades de los usuarios a consecuencia de los objetos o dispositivos conectados a Internet. A consecuencia de ello, lo que expertos ponen de manifiesto a los efectos de solventar esta situación, es la necesidad de transitar cuanto antes al sistema llamado «*IPv6*» antes citado, a los efectos de poder dar una solución a este problema con una visión a largo plazo.

Debe tenerse presente que, en este conflicto, en la actualidad se encuentran muchos operadores involucrados, entre los cuales cabe citar los siguientes: (i) los fabricantes de equipos; (ii) los desarrolladores de software; (iii) los operadores de red; (iv) los reguladores; (v) las organizaciones internacionales; (vi) y, por último, las instituciones de estandarización o certificación; y que para la resolución del mismo, no debe perderse de vista que cada uno de los actores tiene distintos intereses y problemáticas relacionadas con la implementación del citado sistema *IPv6*. En este punto, se destaca la importancia de la acción gubernamental a los efectos de poder conciliar los diferentes intereses en conflicto y facilitar la adopción y el tránsito a dicho sistema. No obstante, ello, sea cual sea el sistema técnico que finalmente se adopte a los efectos de propiciar el desarrollo de Internet de las Cosas («*IoT*»), deben implementarse medidas a corto plazo a los efectos de no frenar el desarrollo de esas nuevas tendencias.

2.2 **La armonización de políticas comunes entre los diferentes Estados**

Dicha actuación gubernamental entre países se hace imprescindible en numerosos supuestos, que inciden en el normal desarrollo de Internet de las Cosas. Así, por ejemplo, se pueden citar los siguientes supuestos que a continuación se indican:

a) Cuando el dispositivo se usa continuamente fuera de la cobertura de la red. Lo que de manera generalizada se conoce como «*roaming*».

b) Cuando los datos viajan, se almacenan y procesan en países distintos de aquel donde se ubica el dispositivo en el que se generó la información.

c) Cuando dicha colaboración sea necesaria para facilitar el cambio de proveedor de servicios, a lo largo de la vida útil del dispositivo de que se trate.

Para propiciar está colaboración de la acción intergubernamental pueden existir soluciones tecnológicas orientadas a la interoperabilidad de los diferentes dispositivos y sistemas, que doten a los mismos de una mayor flexibilidad, y que permitan cambiar el perfil de una manera sencilla y fácil.

Del mismo modo, debe establecerse una mayor regulación sobre la ubicación de los datos, y los límites de tráfico transfronterizo, ya que a través de ellos se pueden obstaculizar la capacidad de enviar datos a los servidores basados en la nube, donde se concentren y analicen los datos de dicho tratamiento. Al hilo de ello, debe tenerse en cuenta que, si bien las políticas de datos abiertos se están generalizando, es posible que se generen de manera alternativa otras políticas que regulen: (i) la transmisión; (ii) el almacenamiento; (iii) el procesamiento; (iv) o la distribución de datos recopilados por los sensores correspondientes, orientados a la efectiva protección de los datos de carácter personal.

2.3 **La potenciación de la portabilidad de los datos de carácter personal**

Con relación a dicha portabilidad (28), debe partirse de su reconocimiento en el artículo 20 del Reglamento General de Protección de datos de la Unión Europea donde se ha producido su reconocimiento genérico. No

(28) El artículo 20 del Reglamento General de Protección de Datos, que será aplicable el 25 de mayo de 2018, recoge que los usuarios tienen un nuevo derecho: la portabilidad. Este derecho complementa al derecho de acceso, ya que permite a las personas obtener los datos que han proporcionado a una entidad/empresa/organización (responsable del tratamiento) en un formato estructurado, de uso común y de lectura mecánica. El derecho a la portabilidad también implica que los datos personales de ese usuario podrían transmitirse directamente de una entidad o empresa a otra, sin necesidad de ser entregados al propio usuario, siempre que ello sea técnicamente posible. El Reglamento abre así la posibilidad no sólo de obtener los datos y reutilizarlos, sino también de transmitirlos a otro proveedor de servicios. Por tanto, el ciudadano tendría dos opciones: la descarga de sus datos o la transmisión de los mismos directamente de una entidad a otra. El objetivo, tal y como se recoge en las Directrices sobre el derecho a la portabilidad de datos del Grupo de Autoridades europeas de Protección de Datos, es «aumentar la capacidad de los usuarios de trasladar, copiar o transmitir sus datos personales fácilmente de un entorno informático a otro», facilitando además el cambio de un proveedor de servicios a otro y reforzando la competencia entre servicios. El nuevo derecho a la portabilidad de datos puede ejercerse: (i) cuando el tratamiento de datos se efectúe por medios automatizados; (ii) cuando el tratamiento se base en el consentimiento o en un contrato; (iii) cuando el usuario lo solicita con respecto a los datos que él mismo ha proporcionado a quien los está tratando y que le conciernan, incluidos los datos derivados de su propia actividad. No obstante, no es aplicable: (i) a los datos que el usuario haya facilitado sobre terceras personas; (ii) en el caso de que el usuario haya solicitado la portabilidad de datos que le incumban pero que hayan sido proporcionados al responsable a través de terceros. La Agencia Española de Protección de Datos recomienda a las organizaciones que comiencen a desarrollar medios que contribuyan a responder las solicitudes de portabilidad de los datos, como herramientas de descarga e interfaces de programación de aplicación. *Cfr.* Agencia Española de Protección de Datos. https://www.agpd.es/blog/que-es-el-derecho-a-la-portabilidad-ides-idPhp.php

obstante, ello, el concepto de «portabilidad de datos» debe interpretarse en el sentido de interoperabilidad, que constituye la capacidad de transferir y utilizar datos, y otra información a través de sistemas, aplicaciones o componentes diferentes. Esta interoperabilidad, se caracteriza por tres componentes bien caracterizados, que son los que se citan seguidamente:

a) La necesidad de que la interoperabilidad sea necesaria para aprovechar en todo su potencial, el valor que puede ser generado por Internet de las cosas en sus diversos entornos.

b) En la actualidad existen al menos 115 protocolos diferentes utilizados por dispositivos de todas clases, que tienen la capacidad de ser conectados a la nube

c) Con independencia de lo indicado anteriormente, debe indicarse que es importante que la interoperabilidad se acompañe con las políticas adecuadas de protección de datos personales, y de ahí la trascendencia que tiene la homologación o la estandarización de protocolos a los efectos de que dicha protección se lleve a cabo de manera real y efectiva, de modo que se garantice a los ciudadanos una protección adecuada de su derecho a la privacidad. La necesidad de cooperación entre las diferentes acciones gubernamentales y los operadores interesados en el desarrollo de Internet de las Cosas, se concreta de manera negativa, en el sentido, de que la falta de portabilidad de datos tiene repercusiones importantes en cuestiones tales como:

a') En lo que atañe a la competencia económica: como consecuencia del posible establecimiento de barreras a la competencia, que disminuyan los beneficios esperados como consecuencia de la implementación de la técnica derivada de Internet de las Cosas. A título de ejemplo, se puede citar el hecho de que la información solamente se encuentre disponible para ciertos: (i) dispositivos, (ii) marcas, o (iii) aplicaciones, entre otros elementos a considerar, produciendo como consecuencia final, el hecho de que los datos almacenados o generados en un sistema, ni pueda ser trasladados a otro, ni este otro los pueda procesar o tratar de manera correcta.

b') La falta de un cumplimiento adecuado de los derechos de los usuarios. La imposibilidad de llevar a cabo la portabilidad de los datos de ordinario puede llevar consigo una restricción a la libre elección entre los diferentes sistemas, las aplicaciones o los componentes, toda vez que la elección del usuario quedaría condicionada por las características de los mismos, de modo y manera que no existiría la posibilidad de dar marcha atrás con relación a la elección adoptada, a consecuencia, precisamente, de la incompatibilidad del sistema, aplicación o componente elegido frente a los demás.

2.4 **La necesidad de prestar especial atención a las características de los componentes incluidos en los diferentes dispositivos**

Cada vez más se tiene la conciencia de la importancia que tienen los chips y los sensores para el desarrollo adecuado de Internet de las Cosas. Así, los chips y los sensores son componentes vitales para el desarrollo de esta técnica, y, por ello, resulta muy relevante poner especial atención a los diferentes aspectos que atañen a los mismos. Por ejemplo, a efectos clarificadores, se puede citar algunos aspectos muy relevantes relativos a los chips y a los sensores, que son los siguientes:

a) Se hace imprescindible mejorar su eficacia. A los chips y a los sensores cada vez se le exige que sean capaces de tener un mayor rendimiento con relación a la posibilidad de captar una mayor cantidad de información, procesarla más eficientemente, y obtener resultados cada vez más precisos.

b) Además, es necesario que dichos componentes alarguen su vida útil y ello condicione la seguridad en el uso del hardware, la posibilidad de proceder a actualizar el software, y al mismo tiempo, proporcionar el mantenimiento requerido. En este sentido, no debe pasarse por alto que, en la actualidad, existe un decalaje de precios con relación al coste de dichos sensores, probablemente excesivo, y que cada vez existe un número mayor de dispositivos conectados cuya cifra está en constante alza, lo que ciertamente haría muy complicado proceder a su sustitución.

c) Hoy en día, constituye una exigencia ineludible el hecho de que dichos chips y sensores incorporen de manera ineludible la capacidad de poder ser conectados de a cualquier tipo de tecnología, haciendo referencia específicamente tanto a la conectividad alámbrica como a la de carácter inalámbrica.

2.5 **La necesidad de una mejora técnica, mediante la disminución de los consumos de energía de los dispositivos; y en el desarrollo de las baterías y otros elementos de almacenamiento de la energía**

Debe partirse del hecho incuestionable de que el desarrollo de Internet de las Cosas está condicionado por la disminución del consumo de energía de los dispositivos que se empleen, así como, por el desarrollo de baterías eficientes y más versátiles, a los efectos de garantizar que la conectividad de todos los dispositivos se lleve a cabo de manera permanente y más prolongada en el tiempo. Esta cuestión es sumamente relevante en lo que atañe a la conectividad de carácter inalámbrica. Por ello, debe ponerse especial énfasis en las características que deben reunir a los efectos que nos ocupan, tanto los dispositivos como las baterías para su correcto funcionamiento en lo que respecta a su interconectividad en Internet de las Cosas. En este sentido, hay que tener en cuenta lo siguiente:

a) Debe exigirse que los dispositivos cada día tengan un menor consumo de energía, y al mismo tiempo, que dispongan de baterías que tengan una mayor autonomía de duración en el tiempo. Por tanto, las características que, en este momento deben ser objeto de consideración son las siguientes: (i) la disminución del consumo de energía; y, (ii) que las baterías reduzcan su tamaño, y que simultáneamente, aumenten su eficiencia mediante una prolongación de su duración o vida útil de uso.

b) También es importante poner de manifiesto: (i) la necesidad de que los chips y los sensores varíen su consumo de energía en función de las tareas que realicen o lleven a cabo, y, (ii) el desarrollo de las llamadas «tecnologías de la conectividad», todo ello conducente a una reducción real y efectiva del consumo de energía de todos y cada uno de los dispositivos que se utilicen al efecto.

c) Finalmente, hay que indicar que en determinadas aplicaciones, –cada vez más numerosas–, se prefiere el uso de dispositivos que sean completamente autosuficientes durante su vida útil.

La exigencia de disminución del consumo de energía y la mejora en la operatividad de las baterías necesariamente viene avocada también al empleo de mejores tecnologías de conectividad. Así, debe indicarse que las tecnologías de la conectividad entre las que cabe citar las siguientes: Wi-Fi, Bluetooth, 3G, 4G y 5G, LTE, satelital, cobre, coaxial, fibra, etc. difieren en la cantidad de energía necesaria para que el dispositivo establezca efectivamente la conectividad. Consecuentemente con ello, y de acuerdo con el estado actual de la técnica, se puede afirmar que las tecnologías alámbricas, hoy por hoy, consumen menos energía que las inalámbricas, y que dentro de estas últimas, las tecnologías de naturaleza inalámbrica tipo Bluetooth,4G y satelital tienen un alto consumo de energía, mientras que en la Wi-Fi, dicho consumo es bastante reducido. Finalmente, debe indicarse que en la conectividad inalámbrica, cuando se requiere un mayor ancho de banda, normalmente los dispositivos llevan consigo también un consumo de energía mayor.

2.6 **Se hace necesario potenciar la seguridad de los dispositivos, y por ende, de la información en ellos contenida, así como garantizar la privacidad de los datos de carácter personal que se utilicen, procesen o traten**

Por el concepto de «seguridad de la información» debe entenderse aquel conjunto de reglas, mecanismos y acciones que permiten mantener la confidencialidad, la integridad y la disponibilidad de la información (29). Simultáneamente, también es imprescindible garantizar la

(29) Por los términos confidencialidad integridad disponibilidad debe entenderse los siguientes conceptos:

«privacidad» de la información contenida en el uso de los dispositivos vinculados a Internet de las Cosas. En este caso, la privacidad representa el derecho de la seguridad de la información personal en términos de integridad, confidencialidad, y disponibilidad, a los que se ha hecho referencia anteriormente. Con relación a la seguridad y a la privacidad de la información, debe tenerse presente que Internet de las Cosas representa un mayor flujo de información, con la existencia de un riesgo real de que se produzca una vulneración efectiva de dicha información. Esto representa y conlleva, la necesidad de un mayor esfuerzo a la hora de implementar medidas técnicas y organizativas adecuadas, que garanticen una situación de mayor seguridad, de cara a evitar la producción de ataques, y, por tanto, la vulnerabilidad de la información que sea objeto de dicho tratamiento. Del mismo modo, debe tenerse presente que Internet de las Cosas va llevar consigo una potenciación de los denominados trabajos colaborativos (30), –entendidos como aquellos procesos intencionales de un grupo para alcanzar objetivos específicos, más que herramientas de dar soporte y facilitar este tipo de aportes–, así como la forma de llevar a cabo o de realizar los mismos. Por ello, con arreglo a estas consideraciones cobra una especial importancia la reflexión relativa al hecho de mantener unos adecuados niveles de seguridad y privacidad en este entorno, teniendo sobre todo en cuenta los nuevos principios de auto organización, de *accountability*, y de responsabilidad pro activa que pesa sobre el responsable del tratamiento, y que no solamente tiene que garantizar la seguridad y la privacidad de la información, sino que tiene que demostrar que ha implementado todas aquellas medidas técnicas y organizativas necesarias para garantizar de manera

---

a) «Confidencialidad». La confidencialidad se conoce como una forma de prevenir la divulgación de la información a personas o sistemas que no se encuentran autorizados.

b) «Integridad». Cuando hablamos de integridad en seguridad de la información nos referimos a cómo los datos se mantienen intactos libre de modificaciones o alteraciones por terceros, cuando una violación modifica algo en la base de datos, sea por accidente o intencionado se pierde la integridad y falla el proceso. Por este motivo, se debe proteger la información para que sólo sea modificada por la misma persona, evitando así que se pierda la integridad. Una manera de proteger los datos es cifrando la información mediante un método de autenticidad como una contraseña o mediante huella digital.

c) «Disponibilidad». Es un pilar fundamental de la seguridad de la información, nada hacemos teniendo segura e integra nuestra información, si no va a estar disponible cuando el usuario o sistema necesite realizar una consulta. Para cumplir con la última condición tenemos que tener claro cuál será el flujo de datos que debemos manejar, para conocer donde se debe almacenar dicha información, que tipo de servicio debemos contratar, etc. *Cfr.:* SGSI. «¿Qué es el CIA (Confidencialidad, Integridad, Disponibilidad) en la seguridad de la información?». 6 de julio de 2017. http://www.pmg-ssi.com/2017/07/cia-confidencialidad-integridad-disponibilidad-seguridad-de-la-informacion/

(30) El trabajo colaborativo constituye un proceso en el cual cada individuo aprende más del que aprendería por sí solo, fruto de la interacción de los integrantes del equipo, y, por lo tanto, un trabajo hecho en un grupo de forma colaborativa, tiene un resultado más enriquecedor que el que tendría la suma del trabajo individual de cada miembro. En este sentido, *Cfr.:* Alcalde, Ignasi. «El trabajo colaborativo en entornos virtuales». https://ignasialcalde.es/el-trabajo-colaborativo-en-entornos-virtuales/

adecuada y eficaz, los derechos y libertades fundamentales de las personas afectadas por cada uno de dichos tratamientos.

Sobre esta base, Internet de las Cosas va a aumentar y potenciar el desarrollo de los servicios digitales, y, por tanto, la obtención de una información muy abundante de carácter personal sobre cada usuario o cliente, que se va a constituir como necesaria para proveer al mismo de un servicio altamente especializado y adecuado a sus características. No obstante, está justificación no puede servir de estrategia para vulnerar el derecho a la privacidad de cada persona, al cual tiene pleno y completo derecho. A raíz de ello, cabe preguntarse cómo se puede compaginar la efectiva protección del derecho a la protección de datos de carácter personal, devolviendo cada uno de los ciudadano, tal como exige el Reglamento General de Protección de Datos de la Unión Europea, el empoderamiento y control sobre sus propios datos personales, favoreciendo, al mismo tiempo, el desarrollo de estas nuevas tecnologías, que tantas ventajas y utilidades puede proporcionar a los ciudadanos en particular, y a la Sociedad general.

En este sentido, no se puede perder de vista que, además de las vulnerabilidades actualmente existentes en materia de Tecnologías de la Información y la Comunicación (TIC's), se le tienen que agregar aquellas que son propias de Internet de las Cosas, que se concretan en los siguientes aspectos o circunstancias más características:

a) Constituye un hecho perfectamente constatable que a través de Internet de las Cosas van encontrarse en circulación una mayor cantidad de datos de carácter personal con relación a cualquier persona. Así los datos personales relativos al: (i) patrimonio; (ii) salud; (iii) autenticación; (iv) ubicación física; (v) grabaciones de la actividad por medio de cámaras IP; (vi) sistemas de alarma o hábitos de consumo a través de los dispositivos (deportivas, Smart TV, o cualquier otro objeto susceptible de ser conectado a través de chips o sensores a Internet).

b) Adicionalmente, se debe considerar también la importancia notoria que adquiere el incremento de la automatización en el envío, el procesamiento y el tratamiento de toda clase de datos de carácter personal, siendo posible a su vez, distinguir entre:

b.1) El incremento de información transmitida M2M (31), cuya característica fundamental consiste en el intercambio de datos que no requiere la intervención de las personas en cada evento.

b.2) Aquellos dispositivos y aplicaciones que no podrán funcionar intercambio mínimo de información.

(31) M2M *(«Machine-to-Machine»)* se refiere a la comunicación entre máquinas. Una máquina puede ser un dispositivo electrónico, un robot, un automóvil, un motor industrial, cualquier cosa que no sea una persona. Esa máquina tiene que comunicar por Internet con un servidor.

Todo ello, tiene que traer como lógica consecuencia, la necesidad de proceder a la realización de diferentes análisis y valoraciones:

a) La determinación relativa a qué tipo de información se trata, transmite y almacena en cada caso.

b) La necesidad de concretar si la misma tiene que ser total o parcialmente automatizada, y, por ende, si tiene que procederse a su desagregación como tal información personal.

c) Las medidas de naturaleza técnica y organizativa que se tienen que implementar a los efectos de garantizar la seguridad de la información y de los datos personales, que sean objeto de dicho tratamiento.

d) Y, por último, la determinación de los diferentes perfiles o niveles de acceso que en cada caso sean de aplicación en función, precisamente, del nivel de seguridad que haya que aplicar a los datos que sean objeto de envío y procesamiento.

Otro elemento que tiene que ser valorado, y que es importante tener en consideración, es el relativo a la determinación de los interfaces con que va a contar el usuario a los efectos de garantizar adecuadamente un mayor control acerca de su privacidad.

3. OTRAS CONSIDERACIONES SOBRE INTERNET DE LAS COSAS

En el examen de las circunstancias que rodean a la implementación y el desarrollo de Internet de las Cosas, se deberán abordar otra serie de cuestiones que son sumamente importantes, a los efectos del desarrollo y la generalización en el uso de esta nueva tecnología. Seguidamente vamos a proceder al análisis de alguna de ellas.

3.1 **Las políticas públicas**

Parece conveniente reforzar la dinámica de colaboración entre la actividad pública y la privada. A partir de esta colaboración debe valorarse si el Estado debe ejercer en Internet de las Cosas el mismo rol que ejerce sobre Internet en general, y ello, con independencia la procedencia de fomentar, desarrollar, e incentivar el uso generalizado de Internet. En este sentido, cobra especial importancia la necesidad de proceder a impulsar la conectividad y el acceso, no solamente en centros urbanos sino en todo el territorio de cada Estado, y ello, sobre la base de que Internet de las cosas no constituye un elemento exclusivo del ámbito de las comunicaciones, sino que tiene un carácter transversal a los distintos sectores de la actividad social y económica tales como: (i) la salud; (ii) la educación, (iii) el transporte; (iv) a energía, etc. Por lo que su incidencia no sólo es generalizada, sino que en un futuro muy próximo va a cobrar un papel

sustancial, y de ahí, la necesidad de trabajar coordinadamente en todas y cada una de estas áreas económicas con un amplio impacto social.

3.2 **Los recursos y las infraestructuras**

Cada vez se constata como más necesario actuar el desarrollo de las infraestructuras que las necesidades reales de Internet de las Cosas va a demandar. Por ello, es preciso alinear el cuadro de atribución de frecuencias de manera acorde a lo establecido por la UIT (32), estándares internacionales aplicables al caso. Así, el uso del espectro no sólo tiene que ser eficaz, sino que se necesita una mayor disponibilidad del mismo considerando la posibilidad de que sea compartido por los diferentes operadores de manera más eficiente. Asimismo, parece importante diferenciar el espectro autorizado, de aquel que no lo es, así como promover la instalación y los desarrollos de nuevas infraestructuras, que permitan la generalización del uso de estas nuevas tecnologías.

3.3 **La privacidad y la seguridad**

Aunque ya se ha hecho referencia a estos dos conceptos dentro del contenido de las presente reflexiones urge aprobar y desarrollar la normativa de desarrollo del Reglamento General de Protección de Datos de la Unión Europea, y al mismo tiempo, tomar conciencia de la importancia que tiene la ciberdelincuencia con relación al uso de estas nuevas técnicas, siendo completamente necesario adoptar las medidas apropiadas para luchar contra la misma, mediante la promulgación de aquella normativa adecuada en materia de ciber seguridad, así como a la toma en consideración de aquellas medidas técnicas y organizativas, –entre las que se encuentran la obtención de los recursos suficientes humanos, materiales y de carácter económico–, que permitan luchar eficazmente contra esta nuevo fenómeno de delincuencia organizada.

(32) La UIT –Unión Internacional de Telecomunicaciones– es el organismo especializado de las Naciones Unidas para las Tecnologías de la Información y la Comunicación-TIC, es el encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras.

CAPÍTULO 15

PRIVACIDAD E INTERCAMBIO DE INFORMACIÓN EN EL MUNDO DIGITAL

José Torregrosa Vázquez (1)
Profesor de Derecho Administrativo
Universidad CEU San Pablo

1. CONSIDERACIONES PREVIAS: LA RESPUESTA DE LA ADMINISTRACIÓN PÚBLICA ANTE LA INNOVACIÓN TECNOLÓGICA

El derecho fundamental a la protección de datos de carácter personal ha sufrido, desde muy poco tiempo atrás, un severo «golpe de timón». Un estacazo felizmente practicado por el legislador europeo el 27 de abril de 2016 –fecha en la que aprobó, al fin, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se de-

(1) El presente trabajo se inscribe en el Proyecto de Investigación sobre *Protección de Datos, Seguridad e Innovación: retos en un mundo global tras el Reglamento Europeo de Protección de Datos*, Ref. DER 2016-79819-R, del Programa Estatal I+D+i del Ministerio de Economía, Industria y Competitividad, del que José Luis Piñar Mañas es el investigador principal: www.privacidadyacceso.com.

roga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (2) (RGPD)– para ofrecer una aflorada estampa de uniformidad normativa en materia de protección de datos en el mapa europeo. Y lo forja, de un lado, de manera ortodoxa, partiendo del ya enraizado contenido de este derecho de control y disposición sobre los datos y de los tradicionales principios y fundamentos asentados en la anterior norma europea, la hoy derogada Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Directiva 95/46/CE) (3) y, de otro lado, hiende áreas inéditas –por ejemplo, con la introducción de los flamantes principios desde el diseño o por defecto [art. 25 del RGPD]–, altera el sistema de fuentes en la materia y, lo que es verdaderamente trascendente, alumbra un auténtico salto de perspectiva, que transita «de la gestión de los datos al uso responsable de la información» (4).

Aprobar, en efecto, un Reglamento europeo, de aplicación inmediata, de alcance general y obligatorio en todos sus elementos, desplazando a la ley interna de los Estados miembros –ley, que, a su vez, procedía de la obligada transposición de la ya citada Directiva 95/46/CE– y colocándose en la cúspide de la normativa en materia de protección de datos personales, informa del gran calado de la reforma. No debe sorprender, por tanto, que esta norma, ya en vigor desde mayo de 2016, no sea aplicable y jurídicamente exigible hasta el 25 de mayo de 2018; período que se ofrece, como reza el considerando 171, para «ajustar» los tratamientos de datos al Reglamento, pues de vital importancia será para que Estados miembros, Instituciones Europeas y todas las Administraciones Públicas y empresas puedan adaptarse al mismo. Por no olvidar, por supuesto, la metamorfosis que supone que el derecho fundamental que se desprende del artículo 18.4 de la Constitución (STC 292/2000) y, por tanto, de obligado desarrollo por ley orgánica, se vea regulado por un preponderante acto jurídico europeo, el Reglamento, que se impone a todas las legislaciones nacionales.

Las comunicaciones o cesiones de datos de carácter personal, siendo uno de los tratamientos de datos que más riesgo implica para el derecho de control y disposición de éstos, es una de esas materias cuyo régimen se presenta con un régimen variado según se produzcan en un ámbito u otro. Ya que, si estas comunicaciones de datos se producen entre un Estado miembro y un país tercero que no pertenece a la UE o una organización

(2) DO L 119/1, de 4 de mayo de 2016, pp. 1-88.
(3) DO 281/31, 23 de noviembre de 1995, pp. 31-50.
(4) Piñar Mañas, J. L.: «Introducción. Hacia un nuevo modelo europeo de protección de datos», en Piñar Mañas, J. L., (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016, p. 16.

internacional estaríamos entonces ante una transferencia internacional y, sin embargo, si estas cesiones de datos tienen lugar entre Estados miembros de la UE, a tenor del Reglamento, no se les considera como tal y por tanto no se aplica dicho preciso régimen. Régimen al que remitimos (5) y, por tanto, estas breves líneas justamente lo que pretenden es reflexionar acerca de la relación entre la privacidad y las comunicaciones de datos que se producen en el seno de las Administraciones de los diferentes Estados miembros, actividad extendida y desarrollada que afecta a todos los ciudadanos europeos y que ha permitido la innovación tecnológica en este contexto. Las Administraciones Públicas europeas utilizan en su quehacer diario una cantidad ingente de información de los ciudadanos. En muchas ocasiones –o prácticamente casi en su totalidad– suelen ser datos de carácter personal. Esta utilización de datos personales por el sector público, de suyo, no supone riesgo grave alguno si la finalidad y la utilidad de poseer esos datos sigue los principios asentados ya en el ámbito europeo, esto es, que sea concreta, proporcional y necesaria para el buen funcionamiento de la convivencia en sociedad. Las Administraciones Públicas necesitan, en cierta medida, tratar esos datos para la mejor prestación de servicios y mejorar el bienestar de las personas en el Estado Social y Democrático en el que *vivimos.* Sin embargo, esto no es del todo pacífico, pues, aunque ya se han abandonado las viejas creencias sobre la potencial peligrosidad de que el sector público efectúe tratamientos de datos personales (6), considerándose hoy su gran valedor del derecho de los ciudadanos a la protección de sus datos, en no pocas ocasiones invocando el principio de eficacia de la Administración Pública se debilita la tutela de la protección de datos de carácter personal. Principio de eficacia que encuentra en todo este impulso de la Administración electrónica su piedra angular. La Unión Europea, en este sentido, no ha sido ajena a todo este proceso de desarrollo de la Administración electrónica en relación al derecho de protección de datos. En concreto, el ahora institucionalizado Grupo Europeo de Protección de Datos del Artículo 29 (7), elaboró en 2003 un Documento sobre la Administración electrónica (8) en la que advirtió su

(5) Un actual análisis del actual régimen de las transferencias internacionales, se puede encontrar en Piñar Mañas, J. L.: «Transferencias de datos personales a terceros países u organizaciones internacionales», en Piñar Mañas, J. L., (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016, p. 427-460 y su bibliografía allí citada.

(6) Al respecto, *vid.* Rodotà, S., *Elaboratori elettronici e controllo sociale*, Il Mulino, Bologna, 1973.

(7) El Grupo de Trabajo del Artículo 29 (GT 29), creado por la Directiva 95/46/CE, es un órgano consultivo e independiente integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea. Este Grupo será sustituido por el Comité Europeo de Protección de Datos, como un organismo de la Unión, con igual composición y semejantes funciones (Artículo 68 y siguientes del *GDPR*).

(8) Working Document on E-Government, adoptado el 8 de mayo de 2003 (WP 73), consultable en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/e-government_en.pdf

preocupación sobre las interconexiones de los sistemas de información en la implantación de la Administración electrónica (letra E). Se anotaba en dicho documento, en primer lugar, por expresa prescripción de la autoridad británica, que la implementación de la Administración electrónica «should not operate as a smokescreen hiding a generalised interconnection of public information databases and an increased exchange of personal data between administrations». Esto es, el intercambio de información entre Administraciones no podría suponer, en ningún momento, una «cortina de humo» que ocultara de manera indiscriminada interconexiones de bases de datos personales. Asimismo, se determinaba que si se acogiera de manera absoluta la famosa teoría del derecho a la autodeterminación informativa establecida por el Tribunal Constitucional federal de Alemania limitaría en demasía las posibilidades –sino la prohibición absoluta– de las interconexiones. Por lo que, a nivel jurídico, recomendaba –hay que tener en cuenta que en el 2003 la implantación de la Administración aún se encontraba en sus inicios– la aprobación de Leyes (como ocurría ya en Francia) o el requerimiento del consentimiento al afectado (como en España) que autorizara las interconexiones entre bases de datos. En cualquier caso, y ante las dudas expresadas por la autoridad británica, se señalaba en último lugar que «interconnections are not inevitable to improve the services of the administration». De esta forma, la Unión Europea, como sucede en todo plano jurídico, siempre ha intentado ponderar y buscar el complicado equilibro entre la reducción de cargas burocráticas de los ciudadanos, que se pueden obtener con la innovación tecnológica, y el respecto a la protección de datos en el intercambio de información entre Administraciones Públicas (9).

En puridad, el trasfondo de esta primitiva dicotomía –entre eficacia tecnológica y protección de datos personales– no es en absoluto novedosa; pudiéndose, de hecho, situar el origen de esta cuestión ya en el clásico artículo de Warren, S. D., y Brandeis, L. D., «The Right to Privacy» (10). Supone, eso sí, un desenterramiento de otra vieja polémica, hoy activamente avivada tanto por una expectante exhibición del principio de eficacia de la Administración Pública –frecuentemente invocado, pero no operado– como por una profusa «euforia informatica», a la que se refería

(9) Al respecto, Piñar Mañas aboga por encontrar un equilibrio «entre las interconexiones (y la supuesta mejora que conlleva en los servicios de la Administración) y la protección de los usuarios» («Administración electrónica y protección de datos personales», *op. cit.*, pp. 173-174).

(10) Este famoso artículo se puede encontrar en la revista *Harvard Law Review*, vol. IV, 5, 1890, pp. 193-220. Al respecto, *vid.* Recio Gayo, M., *Protección de datos personales e innovación: ¿(in) compatibles?*, Reus, Madrid, 2016. También, sobre la discusión que ha ocasionado la introducción, cada vez más veloz, de las tecnologías en la Administración Pública y su repercusión para el ciudadano, *cfr.* con el texto de Valero Torrijos, J., «Administración pública, ciudadanos y nuevas tecnologías», *Revista jurídica de la Región de Murcia*, núm. 25, 1998, pp. 13-35.

Buttarelli (11), que está alterando, incluso, los tradicionales principios de protección de datos (12).

2. LA DÓCIL RELACIÓN DEL RGPD CON LAS ADMINISTRACIONES PÚBLICAS

La potente irradiación del RGPD en todo el marco normativo de protección de datos ensombrece por expresa fijación del legislador europeo ante las Administraciones Públicas. Y no porque el RGPD realice una diferenciación de regímenes en función del tratamiento de datos personales que se efectúe por un sujeto público o un privado, que no lo hace, sino por la remisión que realiza en favor de la normativa interna de los Estados miembros.

En efecto, el Reglamento, siguiendo la estela marcada por la Directiva 95/46/CE, no impone obligación alguna de distinción entre ámbito público y ámbito privado, al igual que hiciera el Convenio n.º 108, en el que ni distinguía entre archivos públicos y privados. Muy al contrario de lo que se pudiera pensar, pues muchos Estados miembros sí realizaron esa diferenciación de regímenes jurídicos en la transposición de la Directiva 95/46/CE (como Italia, por ejemplo) ésta no vino motivada por una exigencia de la Directiva, sino que, al respecto, la añeja norma europea, como ahora el Reglamento, se limitan estrictamente a indicar unas condiciones objetivas –y alternativas– que confieren legitimación a las operaciones de datos personales. Esa fue, al final, la opción satisfactoria que fraguó pues una primera propuesta de Directiva sí preveía este régimen diferenciado entre el ámbito público y privado; finalmente suprimido (enmiendas núm. 27, 28 y 29) por las modificaciones introducidas por el Dictamen del Parlamento Europeo (DO C 94, de 13 de abril de 1992, p. 179) debido, en parte, en la dificultad de diferenciar entre «lo público

(11) *(Banche dati e tutela della riservatezza. La privacy nella Società dell´Informazione. (Commento analítico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comuntaria ed internazionale)*, Giuffrè, Milano, 1997, p. 433).

(12) Al respecto, Poullet ha señalado que la implantación de las nuevas tecnologías ha provocado el establecimiento de nuevos principios de protección de datos, como por ejemplo el «de encriptación y anonimato reversible; el de beneficios recíprocos; el de potenciación de las soluciones tecnológicas que favorezcan o no vayan en contra de la privacidad; el del completo control por parte del usuario del equipo terminal; y el principio según el cual los usuarios de determinados sistemas de información se beneficien de la legislación sobre defensa de los consumidores y usuarios» («Hacia nuevos principios de protección de datos en un nuevo entorno TIC», *Revista de Internet, Derecho y Política*, núm. 5, 2007, pp. 3. Recientemente, Buttarelli, y al contrario, considera que no será necesario «reiventar» estos principios, sino «ser digitales»: «we do need to ‹go digital›, to make them more effective in practice in our technology-driven society, and to integrate them with some new principles specifically arising from the digital age» («Prólogo», en Piñar Mañas, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016, pp. 12, nota 2).

y lo privado» de algunos países europeos (13). Ante aquella disyuntiva, la Directiva optó por remitir a los Estados miembros a que concretizaran la licitud en distintos supuestos especiales de tratamiento, que algunos Estados llevaran a cabo en un plano subjetivo, con los sujetos públicos; decisión final que pudo originar, como advertía el ahora institucionalizado Grupo de Trabajo del Artículo 29, denominado Comité Europeo de Protección de Datos, distintas interpretaciones y aplicaciones por parte de los Estados miembros (14). El RGPD, sin embargo, sigue ahora esa misma senda.

El propio Reglamento, como antes se ha avanzado, remite al «Derecho de los Estados miembros para que, en unas puntualizadas «situaciones específicas de tratamiento», detallen y concreticen las condiciones de licitud de una determinada operación de datos personales, bien por el tipo de dato (por ejemplo, datos sensibles) o bien por el tipo de sujeto, como así ocurre con el sector público; reconociendo así un amplio «margen de maniobra» a la normativa interna de los Estados miembros (considerando 10). Se produce de esta forma, una fuerte oquedad que no pasaría inadvertido sino fuera por su prolijo texto; resultando cuanto menos llamativa dicha paradoja: una norma que regula hasta la extenuación en pro de la uniformidad se sacrifica por la especial incidencia de algunos específicos tratamientos de datos personales. Situación que produce, en términos más ilustrativos, «una suerte de «efecto Gruyère», en tanto y en cuanto su tenor [el del Reglamento] se encuentra en múltiples ocasiones jalonado de «vacíos regulatorios» cortésmente cedidos» (15). Vacíos, o remisiones (16), al facultar a los Estados miembros regular aquellos tratamientos de datos personales cuya licitud se sitúe en el cumplimiento de una obligación legal, en el cumplimiento de una

(13) Al respecto, *vid.* Acciai, R., *Privacy e banche dati pubbliche (Il trattamento dei dati personali nelle pubbliche amministrazioni)*, CEDAM, Padova, 2001, p. 45; *cfr.*, Buttareli, G., *Banche dati e tutela della riservatezza. La privacy nella Società dell'Informazione*, *op. cit.*, p. 427, nota 210). *Cfr.*, Heredero Higueras, M., *La directiva comunitaria de protección de los datos de carácter personal (comentario a la directiva del Parlamento Europeo y del Consejo 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos)*, Aranzadi, Cizur Menor,1997.

(14) *Vid.* Dictamen 06/2014 del Grupo de Trabajo sobre Protección de Datos del Artículo 29 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, adoptado el 9 de abril de 2014. 844/14/ES. WP 217, p. 32, nota 51.

(15) García Mexía, P., «La singular naturaleza jurídica del reglamento general de protección de datos de la UE. Sus efectos en el acervo nacional sobre protección de datos», en Piñar Mañas, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, *op. cit.*, p. 26.

(16) Además de las mencionadas en el texto, el Reglamento también envía a los Estados miembros una específica regulación a aquellas «disposiciones relativas a situaciones específicas de tratamiento» (capítulo IX). Concretizadas en el artículo 85 (Tratamiento y libertad de expresión y de información), artículo 86 (Tratamiento y acceso del público a documentos oficiales), artículo 87 (Tratamiento del número nacional de identificación), artículo 88 (Tratamiento en el ámbito laboral), artículo 89 (Garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos), artículo 90 (Obligaciones de secreto) y artículo 91 (Normas vigentes sobre protección de datos de las iglesias y asociaciones religiosas).

misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (considerando 10), alguna de estas, focalizadas en las Administraciones Públicas.

Ahora bien, el Reglamento salva su noble honor, con respecto a las Administraciones Públicas, al limitarles a éstas o, mejor dicho, a los Estados miembros en su específica regulación, que puedan justificar operaciones de datos personales apoyados en los clásicos principios de consentimiento o de interés legítimo. Novedad ostensible, sin duda, que estremece sobre todo a aquellos Estados miembros en los que habían cimentado siempre su concepción de la privacidad en el principio del consentimiento del ciudadano.

3. ESPECIAL ATENCIÓN A LOS PRINCIPIOS DE CONSENTIMIENTO Y DE INTERÉS PÚBLICO

Así, respecto al principio del consentimiento, el considerando 43 del RGPD señala que «[p]ara garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública» y argumenta tal medida al entender que es «improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular». Lo que significa, dicho de otro modo, que el Reglamento convierte en irrelevante el consentimiento del interesado cuando una de las partes sea una Administración Pública; y el motivo esgrimido es que, en efecto, la exigua libertad del interesado en la práctica habitual convertía su beneplácito ya no en un símil contrato de adhesión, donde se puede aceptar o rechazar, sino en la única posibilidad de tolerarlo, en muchas ocasiones si quería el ciudadano iniciar, por ejemplo, cualquier procedimiento. El Reglamento, de esta forma, acoge un insólito sistema para la privacidad europea por el que se exonera a la Administración Pública de solicitar el consentimiento del interesado para el procesamiento de sus datos personales.

Este «polémico» escenario, sin embargo, resulta familiar para algunos Estados miembros como, por ejemplo, la normativa italiana de protección de datos, donde ya se implantó un distinto régimen jurídico para el ámbito público y otro para el ámbito privado; siendo el principio del consentimiento uno de los protagonistas de dicha disparidad (17). Así es, la

(17) Sobre la importancia del principio del consentimiento en el derecho a la protección de datos personales en la normativa italiana, *vid.*, entre otros, Buttarelli, G., *Banche dati e tutela della riservatezza*, *op. cit.*, p. 280-296; Carbone, V., «Il consenso, anzi i consensi, nel trattamento informatico dei dati personali», *Danno e resp,* 1998, pp. 23-30*;* Comandè, G., «Commento agli artt.11-

normativa italiana de protección de datos, el *Decreto Legislativo 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali* (*Codice della Privacy*) en la obligada transposición de la Directiva 95/46/CE, y siguiendo la traza de su anterior normativa (18), fijó dos tipos de regímenes jurídicos: uno, para el ámbito público (*soggetti pubblici)* y otro, para el privado (y los *enti pubblici economici).* No obstante, la peculiaridad de esta dualidad no radica tanto en la separación en sí, sino en el fundamento y en los elementos diferenciadores de la misma: el consentimiento y el presupuesto de «svolgimento delle funzioni istituzionali» (cumplimiento de funciones institucionales). Estas son, verdaderamente, las notas características; pero permítase que se conozcan los detalles de las mismas.

La Directiva, como ahora el Reglamento, no exigía diferenciación alguna en el tratamiento de datos personales, sino que simplemente habilitaba una serie de garantías objetivas y alternativas cuya aplicación (y cumplimiento) se presumía suficiente para alcanzar un nivel adecuado y equivalente de protección, máxima esta última de la ya hoy derogada norma europea. De esta forma, el legislador italiano acogió, entre las varias opciones que ofrecía la Directiva (artículo 7, «Principios relativos a la legitimación del tratamiento de datos»), dos condiciones fundamentales para legitimar el tratamiento de datos: *a)* cuando el «interesado ha dado su consentimiento de forma inequívoca» y *e)* cuando «es necesario para

---

12», en Giannantoni, E., - Losano, M. G., *e* Zeno-Zencovich, V., *La tutela dei dati personali*, Padova, 1997, pp. 113-166; Cuffaro, V., «Il consenso dell'interessato», en Cuffaro, V.,–Ricciuto, V., (a cura di), *La disciplina del trattamento dei dati personali*, Giappichelli, Torino, 1997, pp. 201-223; Oppo, G., «Sul conseno dell'interessato», en Cuffaro, V.; Zeno-Zencovich, V., Ricciuto, V., (a cura di), *Trattamento dei dati e tutela della persona*, Giuffrè, Milano, 1998, pp. 123-128; Patti, S., «Commento all'art.11», en Bianca, C. M.,- Busnelli, F. D., (a cura di), *Tutela della privacy,* pp. 359-365; Putignani, A., «Consenso e disposizione della privacy», en Clemente, A., (a cura di), *Privacy,* pp. 231-258.

(18) La norma anterior, la *legge 31 dicembre 1996, n. 675 del 1996, sulla Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*, ya establecía esta diferenciación de regímenes entre ámbito público y privado. Entonces, se criticó la sucinta referencia al ámbito público, dedicándole sólo un precepto al tratamiento por parte de las Administraciones Públicas (artículo 27) teniendo en cuenta la trascendencia de la protección de datos en el sector público. En sentido, Cardarelli definió como «*confinata*» la circunstancia de que sólo se regulara en un solo precepto las normas para la Administración Pública («Il trattamento dei dati personali in ámbito pubblico: i soggetti ed i rapporti tra le fonti», *en Cardarelli, F., Sica, S., Zeno-Zencovich, V., Il códice dei dati persoanli. (Temi e problema)*, Giuffrè, Milano, 2004, p. 203); «racchiuso», fue el término empleado por De Tura, A., «Le regole ulteriori per i soggetti pubblici», en Cuffaro, V., D'Orazio, R., Ricciuto., V. (a cura di), *Il Codice del trattamento dei dati personali*, Giappichelli, Torino, 2007, p. 163; En el mismo sentido, Cirillo señalaba que el régimen diferenciado más que un problema de «*contrasto* de normas», fue un problema de «*vouto* normativo», en la medida que la *legge n. 675 de 1996* no contenía normas especificas, y necesarias, para el tratamiento publico de datos («Trattamento pubblico dei dati personali e responsabilità civile della p.a.», *Il Diritto dell'informazione o dell'informatica*, fasc. 4-5, 1999, pp. 843. En la normativa actual, la regulación para los *soggetti publici* se regula, generalmente, en los artículos 18-22 del *Codice*, para los datos *comuni*, y en los artículos 59 a 74 del *Codice*, para los datos *particolari*. Esta circunstancia ha sido clave para que algún autor, como Masucci, ha sostenido que existe un verdadero «statuto dell'informazione (personale) in ambito pubblico» («Tutela della riservatezza e obbligui di rispetto dei soggetti pubblici», en Pardolesi, R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Tomo II, Giuffrè, Milano, 2003, p. 567).

el cumplimiento de una misión de interés público». Y, en base a estas dos disposiciones, se normalizó el previo requisito del consentimiento del interesado para el tratamiento de datos en el ámbito privado (y los *enti pubblici economici)* y la excepción del consentimiento para el ámbito público, amparandosé en las categorías objetivas provistas por la Directiva 95/46/CE. Es decir, y esto es lo destacable, lo planteado en la norma europea en términos objetivos se transpusó al régimen italiano al ámbito subjetivo, argumentando la diferente estructura y organización del sector público respecto al sujeto privado, lo que implicaba ciertas peculiaridades en la aplicación de la normativa (19). O, dicho de otro modo, el legislador italiano no autoriza el procesamiento de datos en función de la actividad de interés público que pueda ejercer un sujeto, sino que es la específica naturaleza del sujeto el elemento concluyente que distingue este doble régimen. El consentimiento del interesado, por tanto, autoriza el tratamiento de datos personales para los privados (y los *enti pubblici economici*), pero esta anuencia es intrascendente para el sector público (20). Esto no significa, por otro lado, una «libre licencia» para tratar datos personales en el ámbito público; muy al contrario, la indulgencia de solicitar el beneplácito del interesado se reemplaza por una subordinación al interés público y al principio de legalidad, principios propios y primarios de la actuación administrativa. La particular posición de supremacía de la Administración Pública, de preeminencia frente al interesado, el irremediable servicio al interés general y su sometimiento al principio de legalidad justifican la dispensa de la aquiescencia del interesado y, por ende, la imperiosa previsión de un régimen diferente no tanto –o no sólo– por la propia actividad administrativa o por el elevado número de operaciones de datos que realiza sino por garantizar al ciudadano, de forma adecuada, su derecho a la protección de datos personales que, en su relación con la Administración Pública, se encuentra en general en una posición de inferioridad (21).

---

(19) Así lo puso de manifiesto en las primeras criticas al texto de la *legge 31 dicembre 1996, n. 675* Comandé, G., «*Privacy* informatica: prospettive e problemi», *Danno e responsabilità*, núm. 2, 1997, p. 145. Al respecto, *vid.* Cardarelli quien sostenía lo anterior al comprobar, por ejemplo, la dificultad en la identificación y distinción entre la figura del titular, el responsable y el encargado de los datos en el sector público («Il trattamento dei dati personali in ámbito pubblico: i soggetti ed i rapporti tra le fonti», *op. cit.*, p. 208).

(20) Este principio general de irrelevancia del consentimiento en el ámbito público encuentra una excepción, para «los profesionales sanitarios y los organisimos sanitarios públicos». Éstos sí deberán requerir el consentimiento al interesado (Artículo 18, *comma* 4 del *Codice della Privacy*). Giuffrè, Milano, 2003, pp.199. R.a instrumentalidad supoorto di conoscenze pinziale offensitivi

(21) Así lo argumentaba Acciai, agregando que esta separación ha dado lugar a un «*sistema piuttosto articolato di regole nel quale tuttavia non è dato rinvenire un regime di privilegio per le pubbliche amministrazione*», (*Privacy e banche dati pubbliche (Il trattamento dei dati personali nelle pubbliche amministrazioni)*, CEDAM, Padova, 2001, pp. 47 y 50). En el mismo sentido, Buttarelli también defendía que la razón de esta distinción se originaba en la necesidad de garantizar la tutela de derecho al interesado, sosteniendo que «Il rilievo costituzionale dei diritti della personalità sembra non ammettere un indebolimento della loro tutela in ragione del

Esta distinción, en su momento abiertamente criticada, y así se manifestó por no pocos autores, aseguraba que, al exceptuar a la Administración Pública de la obligación de solicitar el consentimiento el régimen aplicable al sector público se encontraba «attenuato» (22). Pero esto no es del todo cierto: en primer lugar, porque el hecho de que el régimen sea diferente no implica un régimen de «privilegio» para los *soggetti pubblici*, pues la obligación de alcanzar un nivel análogo de protección no presupone unas reglas uniformes (23). Pero, es más, esta distinción sólo se refiere a la condición de acceso –a la legitimización– en el tratamiento de datos y no determina el entero parámetro de validez en las operaciones que lleve a cabo la Administración Pública, pues ésta deberá someterse, como los demás sujetos, a los principios comunes y generales de la protección de datos personales.

Es cierto, no obstante, que el fundamento de esta original excepción registrada por el legislador italiano ha sido también muy diverso; lo que ha dado lugar a varias razones, esgrimidas para justificar esta «desigualdad» de trato, no de derecho (24). Por un lado, se ha afirmado que el motivo de

---

fatto che i dati personali siano trattati da una pubblica amministrazione anziché da un privato». Es más, añadía que el ciudadano disfruta hoy de mayores garantías frente a la Administración, por eso, resulta «impropio» basar la tutela del derecho a la protección de datos en el presupuesto del consentimiento, que continuaría colocando al ciudadano en una posición de «sostanziale disparità». (*Banche dati e tutela della riservatezza*, *op. cit.*, p. 286 y 427). Lugaresi, al respecto, defiende esta diferenciación de regímenes por varios motivos, intrínsecamente relacionados con la propia naturaleza de la Administración y de la acción administrativa, como son: «la mole dei dati, la rilevanza e la diffusione dei trattamenti, l'incrocio degli interessi, le dinamiche amministrativistiche sottese, la potenziale offensività dei comportamenti dei soggetti pubblici, la necesittà di garantire i principi propri dell'azione amministrativa, quali efficienza, efficacia, transparenza, publicità» («Il trattamento dei dati nella pubblica amministrazione», en Monduci, J., y Giovanni, S., *Il códice in materia di protezione dei dati personali. (Commentario sistematico al D. Lgs. 30 giugno 2003 n. 196)*, CEDAM, Padova, 2004, p. 237).

(22) Al respecto, entre otros, *vid.* las «lógicas» críticas de Bin, M., «Privacy e trattamento dei dati personali: entriamo in Europa», *Contratto e impresa/Europa*, 1997, pp. 459-481; y Giannaccari, A., «L´ambito di applicazione della legge, l´importazione e l´esportazione dei dati personali», en Pardolesi, R. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Tomo I, Giuffrè, Milano, 2003, p. 185. Sin embargozones. La primera, porque esta diferenciaci al interesado, ci»icie datos. El legislador italiano, acogiendose

(23) En este sentido, Buttarelli ya sostenía que este régimen no sólo no constituía un «privilegio» sino, muy al revés, *«completa il quadro di garanzie che opera nei confronti degli organi pubblici»*. Añade, además, que la voluntad del legislador de evitar distintos niveles de protección se demuestra en la remisión al juez ordinario de todas las controversias que pueda suscitar la ley (*Banche dati e tutela della riservatezza. La privacy nella Società dell´Informazione. (Commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria ed internazionale)*, Giuffrè, Milano, 1997, pp. 426-427). A favor de esta distinción tambíen se situaba Maietta que, al respecto, establecía que la diferenciación posibilita un tratamiento por parte de la Administración Pública *«snello»* y *«veloce»*, *«ma ancorato a capisaldi normativi che garantiscono, in ogni caso, l'interesato»* («Il trattamento dei dati effettuato da soggetti pubblici. (art. 18)», en Sica, S., y Stanzione, P., *La nuova disciplina della privacy. (Commento al d.lgs. 30 giugno 2003, n. 196)*, Zanichelli, Torino, 2005, pp. 77).

(24) Acciai asevera que «in ambito pubblico la centralità del consenso lascia il posto al pubblico interesse ad al principio di legalità». (*Privacy e banche dati pubbliche*, *op. cit.*, p. 49). En términos semejantes se muestra Mucio, quien asegura que *«La ragione di tale impostazione consiste evidentemente nel fatto che le amministrazioni effettuano trattamenti di dati nell´espletamento di funzioni istituzionali finalizzate al raggiungimento di interessi pubblici» (Codice della privacy*

esta elección responde a razones pragmáticas y funcionales para la normal actuación administrativa; otros, en cambio, interpretan que el mero fin del interés general, al que sirve siempre la Administración Pública, y el propio principio de legalidad, al que está sometida, son argumentos más que suficientes para explicarlo. Más concretos han sido quienes sostienen que existe una imperante finalidad «istituzionale» que permitiría el procesamiento de datos personales por parte de las Administraciones Públicas sin previa autorización del ciudadano, pues el legislador, en verdad, fundamenta todo tratamiento de datos personales realizado por las Administraciones Públicas en que éstas persigan «lo svolgimento delle funzioni istituzionali» (el artículo 18 del *Codice della Privacy*, sobre los «principios aplicables a todos los tratamientos realizados por los entidades públicas» especifica en el apartado 2 que: «todos los tratamientos de datos personales por parte de las entidades públicas sólo está permitido en cumplimiento de funciones institucionales») (25).

Es, por tanto, la remisión al cumplimiento de estas «funciones institucionales», y no al principio del consentimiento, la peculiaridad –y la diferencia con los privados y los *enti pubblici economici*– que habilita a la Administración Pública al tratamiento de datos personales; porque, en fin, si el tratamiento de datos es necesario para el desempeño de unas determinadas «*funzioni istituzionali»,* el consentimiento del ciudadano no es preceptivo, y si, por ejemplo, el tratamiento no fuera necesario para el desempeño de unas determinadas «*funzioni istituzionali»,* sería ilegitimo cualquier tratamiento aun solicitando el consentimiento al ciudadano (26). En el fondo, el sustento en el que poder basar esta singularidad,

---

e pubblica amministrazione. (Diritto di acceso e riservatezza nella p.a. e negli enti locali), IPSOA-Wolters Kluwer Italia, Assago, 2005, p. 77). Una razón pragmática y funcional, reconocen, por el contrario, Barilà y Caputo, quienes aseguran que «*la scelta legislativa di rendere irrilevante il consenso dell'interessato in ambito pubblico risulta del tutto ragionevole, ed anzi necessitata, per tutte le fattispecie in cui la pubblica amministrazione persegue fini pubblici indisponibili, la cui attuazione deve poter essere assicurata prescindendo da condizionamenti da parte degli interessati*». (*La tutela della privacy nella pubblica amministrazione (Riservatezza e gestione dell´informazione nel settore pubblico)*, Giuffrè, Milano, 2000, p.102). En el mismo sentido, Orestano manifiesta que se justifica por la necesaria «strumentalità» en el cumplimiento delle *funzioni istituzionali.* («La circolazione dei dati personali», en Pardolesi, R., (a cura di), *Riservatezza e circolazione dei dati personali*, Giuffrè, Milano, 2003, p. 199.) Señala Buttarelli que el principal motivo de esta elección «è collegata all´esigenza di assicurare che la pubblica amministrazione possa svolgere le proprie funzioni senza essere condizionata dal consenso della persona, laddove il potere abbia natura autoritativa», es decir, hace referencia a una finalidad *istituzionale.* (*Banche dati e tutela della riservatezza*, *op. cit.*, p. 286).

(25) El artículo 18, *comma* 2 del *Codice della privacy* transcribe apenas sin cambios sustanciales al precepto 27 de la *legge n. 675/1996.*

(26) Al respecto, *vid.* Zucchetti, A., «Commento all'art. 18», en Italia, V. (coord.), *Codice della Privacy. (Commento al Decreto Legislativo 30 giugno 2003, n.196 aggiornato con le più recenti modifiche legislative)*, Tomo I, Giuffrè, Milano, 2004, pp. 277-278. Troiano, P., «Commento art. 18. (Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici)», en Bianca, C. M., y Busnelli, F. D., (A cura di), *La protezione dei dati personali. (Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»)*, *Tomo I*, Cedam, Padova, 2007, p. 468. En este mismo sentido, el *provvedimento* del *Garante*, de 5 de diciembre de 2001, *Bolletino*, n.º 23, p. 142, punto 6 que señala

lejos de suponer una débil garantía (27), se encuentra en los rígidos requisitos a los que se somete a las entidades públicas y, en consecuencia, más que suprimir un presupuesto legitimador del tratamiento, el legislador impide que la Administración pueda felizmente valerse del consentimiento del ciudadano para efectuar tratamientos de datos sin los requisitos que marca la Ley (28). Se advierte entonces la dicotomía que ocasiona para el procesamiento de datos personales la irrelevancia del consentimiento porque, a pesar de lo que a primera vista pueda parecer, supone una verdadera garantía para los ciudadanos y una contrariedad para las Administraciones Públicas: éstas tendrán que observar adecuadamente los presupuestos que legitiman su actuación que, de otra forma, hubieran simplemente solicitado el consentimiento del interesado para proceder a una comunicación de esos datos.

En efecto, el *Codice della Privacy* circunscribe toda actuación de la Administración Pública en materia de datos personales a la existencia de este elemento objetivo, que opera como requisito indispensable en toda operación de datos en el ámbito público: «cumplimiento de las funciones institucionales». O, dicho de otro modo, sólo es válido aquel tratamiento de datos personales efectuado por la Administración Pública que sea necesario para el desempeño de estas *«funzioni istituzionali»*. Se trata de un presupuesto, amén de un verdadero límite: pues actúa con una doble vertiente: por una parte, es requisito indispensable para que la Adminis-

---

que: «La rilevata carenza di presupposti giuridici per la raccolta ed il trattamento dei dati in esame non può essere superata attraverso il consenso degli acquirenti, dal momento che la legge n. 675/1996 esclude che i soggetti pubblici, e dunque anche i soggetti da questi designati come responsabili del trattamento, possano supplire con una diversa procedura alla mancanza di fondamenti normativi»; Finocchiario, por el contrario, no excluye esta posibilidad. De hecho, indica que en la «prassi operativa» las Administraciones Públicas deciden requerir el consentimiento del interesado para excluir o limitar su responsabilidad ante una posible infracción del derecho del interesado y del eventual resarcimiento del daño causado por el tratamiento. (*Privacy e protezione dei dati personali. (Disciplina e strumenti operativi)*, Zanichelli, Bologna, 2012, p. 150). En contra de esta opinión, se muestra Troiano quien afirma que el requerimiento del consentimiento por parte de la Administración constituye un acto «non solo inidoneo» para producir efectos legitimadores sino «contrario» al «doveri d'ufficio del funcionario o agente publico», comprometiendo y ralentizando la acción administrativa («Commento art. 18. (Principi applicabili a tutti i trattamenti effettuati da soggetti pubblici)», *op. cit.*, p. 469).

(27) Para Bassoli, «nei rapporti con la p.a. il consenso ha sempre avuto un significato più sfumato, più debole, in virtù della particolare posizione di potere e di supremazia degli interessi pubblici in cui si esplica l´attività della stessa pubblica amministrazione» («Commento art. 18. (Principi applicabili a tutti i trattamenti effettuati da soggeti pubblici)», en Cassano, G., y Fadda, S., *Codice in materia di protezione dei dati personali. (Commento articolo per articolo al testo único sulla privacy d.lgs. 30 giugno 2003, n. 196)*, IPSOA, Assago, 2004, p. 137).

(28) Se recoge un magnífico razonamiento de Barilà y Caputo (*La tutela della privacy nella pubblica amministrazione (Riservatezza e gestione dell´informazione nel settore pubblico)*, Giuffrè, Milano, 2000, p. 103) construido en base a una acertada reflexión de Buttarelli, quien afirma que «*deve quindi escludersi che il consenso possa legittimare un organo pubblico ad utilizzare i dati per finalità diverse da quelle perseguite istituzionalmente, oppure per superare i limiti che specifiche disposizioni di legge o di regolamento prevedono in tema di comunicazione o diffusione e di trattamento dei dati sensibili» (Banche dati e tutela della riservatezza. La privacy nella Società dell Informazione, op. cit.*, p. 287).

tración Pública pueda efectuar un tratamiento de datos personales y, por otra, fija la extensión de su ámbito de actuación. De esta formulación «funzioni istituzionali», en cambio, deriva una difícil concretización y alcance un tanto indeterminado: propuestas que oscilan entre la interpretación más restrictiva de este presupuesto; esto es, aquella que valida solamente aquellos tratamientos de datos realizados por la Administración para el desempeño de sus propias funciones o, por el contrario, una interpretación amplia, por la que este requisito se acomodaría a toda actuación administrativa de tratamiento de datos personales que persigue el «interese pubblico» de la Administración. Se destacan también aquellas fórmulas que vinculan este presupuesto con, por ejemplo, el propio «principio de finalidad» (29), el «principio de competencia» (30), un «principio funcional» (31) o como un «criterio funcional» (32). Se advierte, sin embargo, que una interpretación sumamente amplia no se puede aceptar en

(29) En este sentido, Buttarelli señala que «Il principio di finalità permea l´intero trattamento ed implica, anzitutto, che ciascuna pubblica amministrazione debba astenersi dall´effettuare le operazioni di raccolta, di modificazione, di elaborazione, ecc. che risultino esuberanti rispetto agli scopi perseguiti in linea primaria.» (*Banche dati e tutela della riservatezza. La privacy nella Società dell´Informazione. (Commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria ed internazionale)*, Giuffrè, Milano, 1997, p. 432). En el mismo sentido, Bozzi se ha referido como un «principio di finalità istituzionale». («I soggetti coinvolti nell'attività di trattamento», en Cuffaro, V.,–Ricciuto, V. (a cura di), *La disciplina del trattamento dei dati personali*, Giappichelli, Torino, 1997, p.113).

(30) Así, Zucchetti sostiene que, en virtud del principio de competencia, «il trattamento ha, così, un carattere strumentale ed autonomo rispetto allo svolgimento delle funzioni di interesse pubblico.» («Commento all'art. 18», en Italia, V. (coord.), *Codice della Privacy. (Commento al Decreto Legislativo 30 giugno 2003, n.196 aggiornato con le più recenti modifiche legislative)*, Tomo I, Giuffrè, Milano, 2004, p. 265). Esta formulación, aunque completada por Zucchetti, fue originariamente enunciada por Travaglini, L. G., «Commento all´art. 27», en Giannantoni, E., Losano, M. G., e Zeno-Zencovich, V.,(a cura di), *La tutela dei dati personali. (Commentario alla l. 675/96*), Padova, 1997, p. 248.

(31) En particular, Troiano, defensor de un interpretación más amplia, propone que *«la nozione di «funzione istituzionale» sia stata itlizzata nel suo significato piú ampio, cosí da ricomprender l'intero ambito dei compiti che possono essere istituzionale assegnati ad enti pubblici non economici, sia che si tratti dell'esercizio di funzioni pubbliche in senso stretto sia che si tratti di attività di erogazione di servizi»*, encontrando el fundamento de este «*principio funzionale»* en el *consagrado* principio de legalidad *«che impone agli enti pubblici di operare esclusivamente per il perseguimento dei fini ad essi affidati dalla legge»*. («Commento art. 18. (Principi applicabili a tutti i trattamenti effettuati da soggeti pubblici)», en Bianca, C. M., y Busnelli, F. D., (A cura di), *La protezione dei dati personali. (Commentario al d. lgs. 30 giugno 2003, n. 196 («Codice della privacy»), Tomo I*, Cedam, Padova, 2007, pp. 468-469).

(32) Barbiero mantiene una posición extensiva sobre este presupuesto (excesiva, quizá), apuntando que *«nel concetto di «fini istituzionali» possono essere ricomprese: a) Le funzioni previste dalla legge, dallo statuto e dai regolamenti; b) le funzioni svolte sulla base di intese, accordi di programma, convenzioni o strumenti di programmazione negoziata; c) ogni altra funzione, o compito, strettamente configurabile come «di interesse pubblico»*. («Per un regolamento sulla tutela della riservatezza di dati personali contenuti in archivi e banche dati comunali», *Nuova Rassegna*, n.º 15-16, 1997, p. 1626).

En este contexto, otros, como Ferrara se refiere a esta condición como «vincolo di scopo» («Premesse ad uno studio sulle banche dati della pubblica amministrazione: fra regole della concorrenza e tutela della persona», *Diritto amministrativo: rivista trimestrale*, 1997, fasc. n.º 4, p. 561); Cacciari, en esta misma línea, «scopi di pubblico interesse attinenti alle propie funzioni istituzionali» («Il trattamento dei dati sensibili e giudiziari e gli obblighi delle pubbliche amministrazioni», *Il merito*, 2005, fasc. n.º 2, p. 102).obligatorio retacicyficil amente, el criterio del ici tratti di attivitenti pubblici non economici, sia che si tratti dell'

su versión más extensa pues, como acertadamente se ha apuntado (33), otorgarle esta consideración generaría el desafortunado efecto de expandir su alcance y, consecuentemente, de «vaciar» su significado. Por su parte, el criterio del *Garante per la protezione dei dati personali* en la aplicación de este presupuesto de «lo svolgimento delle funzioni istituzionali», no ha perfilado una definición clarividente: la fluctuante «giurisprudenza» (34) del *Garante*, abrazando, en ocasiones, una noción abierta del mismo; y otras, en cambio, ciñéndose rigurosamente a la interpretación más delimitada, no ha aportado en esta ocasión un inequívoco esclarecimiento. Habría que entender que estas «funciones institucionales» lo que obedecen es a «al cumplimiento de una misión de interés público o inherente al ejercicio del poder público», licitud que se hallaba en el artículo 7 *e)* de la Directiva 95/46/CE y ahora en términos semejantes en el artículo 6.1.*e)* del RGPD. A este respecto, este fundamento jurídico europeo para situaciones en las que «el tratamiento es necesario para el cumplimiento de una misión de interés público», será intensamente empleado para el procesamiento de datos por el sector público, al limitar el RGPD que puedan «valerse» bien del consentimiento (considerando 43) o bien del interés legítimo (35) (artículo 6.1 *in fine*) para el procesamiento de datos personales.

El todavía impúber Reglamento, que no excluye el uso del presupuesto de «misión de interés público» por parte de privados, habida cuenta de que en gran cantidad de Estados miembros existen entidades privadas que realizan tareas públicas, indica asimismo que el tratamiento que se efectúa en cumplimiento de esta habilitación ha de tener «base en el Derecho de la Unión o de los Estados miembros» (considerando 45), «sustento» que se ha interpretado como «leyes ordinarias u otra normativa jurídica» y «suficientemente específica y precisa a la hora de definir el tipo de tratamiento, sin que se exija para ello que el responsable tenga que actuar «en virtud de una obligación jurídica» (36). Esta habilitación de tratamiento comprendería dos específicas situaciones: la primera, cuando el responsable del procesamiento ostenta una potestad pública o una mi-

(33) Acciai, R., *Privacy e banche dati pubbliche (Il trattamento dei dati personali nelle pubbliche amministrazioni)*, CEDAM, Padova, 2001, p. 65.

(34) *Vid.*, por ejemplo, la nota del *Garante* de 19 de abril de 2001, *Bolletino*, n.º 19, p. 8-9.

(35) Sobre el alcance de este concepto de interés legítimo véase además del Dictamen 06/2014 del Grupo de Trabajo sobre Protección de Datos del Artículo 29 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, adoptado el 9 de abril de 2014. 844/14/ES. WP 217, p. 28 y ss; una audaz crítica sobre la «defectuosa» transposición de éste en España en Fernández-Samaniego, J., y Fernández-Longoria, P., «El interés legítimo como principio para legitimar el tratamiento de datos», en Rallo Lombarte, A., y García Mahamut, R., *Hacia un nuevo derecho europeo de protección de datos*, Tirant lo Blanch, Valencia, 2015, pp. 411-461.

(36) Dictamen 06/2014 del Grupo de Trabajo sobre Protección de Datos del Artículo 29 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, adoptado el 9 de abril de 2014. 844/14/ES. WP 217, p. 26.

sión de interés público y dicha operación de datos sea necesaria para el ejercicio de la predicha potestad o se debe desempeñar la misión; o bien que un tercero con potestad pública requiera al responsable de un tratamiento, aunque no tenga éste potestad alguna, la revelación de unos determinados datos personales (37). Lo que resulta claramente invariable es esa «potestad pública» que debe tener o bien el responsable del tratamiento o bien el tercero al que se comunican dichos datos. Otra «pista» en la interpretación del concepto de «interés público» de este fundamento se encuentra en el Reglamento n.º 45/2001 (38): el considerando 27 señala que «la realización de las «áreas de interés público» abarca el procesamiento de datos necesarios para la «gestión y el funcionamiento de dichas insticiones y organismos». Por tanto, y además del requisito de «potestad pública» que en todo caso debe concurrir, se abre la posibilidad a que dentro del concepto de «misión de interés público» se admita aquel tratamiento que sea necesario para la normal «gestión» y «funcionamiento» de las Administraciones Públicas lo que, sin duda, comprende un alto grado de adaptabilidad de este presupuesto.

En definitiva, se quiere dejar constancia que la irrelevancia del consentimiento, introducida ahora por el Reglamento europeo, pero que lleva ya tiempo aplicándose en la práctica jurídica italiana, viene acompañada por la imposición-restricción de perseguir siempre el interés público y de someterse al principio de legalidad en cualquier tratamiento de datos. En este caso, ambas condiciones, consentimiento-interés público, se establecen por sí solos como infalibles criterios legitimadores para las operaciones de datos personales; considerándose equivalentes en la tutela de la protección de datos. Dualidad de regímenes que demuestra, una vez más, la capacidad de adaptar el sistema jurídico al permitir la individualización en las formas y técnicas justas para la tutela de la protección de datos de los ciudadanos incluso, como declara Cirillo, prescindiendo de «*inutile dogmatismi*» (39).

4. UNA EXPERIENCIA PRÁCTICA: EL SISTEMA DE INFORMACIÓN DEL MERCADO INTERIOR (IMI) ¿OBJETIVO EUROPEO CUMPLIDO?

La Unión Europea ha tomado buena nota: conocedor de que el sector público ha de servir como un valioso combustible para la economía europea –sino quiere convertirse en su peor enemigo– instó vigorosamente a

(37) *Ibidem*, pp. 25 y26.

(38) Reglamento (CE) n.º 45/2001 del Parlamento Europeo y de Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8, de 12 de enero de 2001, pp. 1-22).

(39) («Trattamento pubblico dei dati personali e responsabilità civile della p.a.», *op. cit.*, p. 862).

que los Estados miembros adoptasen medidas, coherentes y compatibles para que obtener superiores beneficios de la era digital. Uno de ellos, sin duda urgentísimo, es la interacción entre las propias Administraciones, como entre éstas y con los ciudadanos. Reflexión compartida por la Comisión, en efecto, al sostener que «los servicios públicos digitales reducen la carga administrativa de las empresas y de los ciudadanos haciendo que las interacciones con las administraciones públicas resulten más rápidas y eficientes, más cómodas y transparentes, y menos costosas». La hoy Unión Europea ha contribuido enérgicamente a materializar la utópica idea de crear sistemas para intercambiar datos y documentos entre Administraciones Públicas; el Sistema de Información del Mercado Interior (IMI) y el éxito de su futura evolución es prueba de ello. El problema, o la lentitud, de mayores éxitos deriva, fundamentalmente, de la falta de competencia directa de la Unión en materia de Administración Pública, lo que se ha traducido en la escasez de disposiciones jurídicas vinculantes, sin demeritar el vastísimo conjunto de acciones políticas de la Unión, y la previa preocupación en su relación con el derecho fundamental consagrado en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea (40). Por un lado, y como explicó Gamero Casado, a propósito de la interoperabilidad, no era posible la «imposición de normas vinculantes», entre otras razones, por la distinta realidad socioeconómica en los Estados Miembros, «no sólo porque [podía] suponer un serio obstáculo para ciertos Estados en los que el grado de implantación de las tecnologías de la información [era] menor, sino también en los Estados más desarrollados, cuyas decisiones previas [podían] resultar incompatibles con el marco europeo» (41). Sin olvidar, asimismo, la diferente cultura administrativa y de trabajo. En todo caso, tampoco ha sido óbice para intervenir, como así ha sido, en pro del Mercado Interior o invocando, noblemente, el principio de subsidiariedad para llevar a cabo diferentes y numerosas iniciativas. No obstante, lo que se quiere (y se debe) recalcar es que la función de fomento de la Unión Europea ha servido de acicate y revulsivo para algunos Estados Miembros, pues para ciertas ma-

(40) Se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la UE que: 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan; 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente (DOCE C 364/20, de 18 de diciembre del 2000).

(41) En este sentido, Gamero Casado, E., «Interoperabilidad y Administración electrónica: conéctense, por favor», *Revista de Administración Pública*, núm. 179, p. 306. *Cfr.*, Moreno Molina, A. M., *La ejecución administrativa del derecho comunitario: régimen europeo y español*, Universidad Carlos III, Madrid,1998.

terias «está claro que lo que no haga la Unión Europea, […] posiblemente no lo vaya a hacer nadie» (42).

Pero centrándonos en este paradigma europeo de intercambio de datos entre Administraciones Públicas, el Sistema de Información del Mercado Interior (IMI) es, justamente un instrumento de cooperación administrativa, implantado en la Unión Europea en 2008, que permite la comunicación electrónica entre todas las Administraciones Públicas europeas, en diferentes ámbitos legislativos del Mercado Interior. Lo que significa, dicho de otro modo, que «cualquier» Administración Pública europea puede consultar, o verificar en tiempo real, los datos de «cualquier» ciudadano europeo en aquellos trámites administrativos que estén desarrollando. Así, por ejemplo, cuando un dentista finlandés desee prestar sus servicios en Francia y solicita que se le reconozcan sus cualificaciones profesionales, la Administración Pública francesa las podrá comprobar rápidamente a través del sistema IMI.

El Reglamento IMI, marco jurídico de este sistema, lo define como «aquella aplicación informática accesible a través de internet, realizada por la Comisión en colaboración con los Estados miembros, cuyo propósito es servir de ayuda a estos últimos para que puedan cumplir en la práctica las exigencias de intercambio de información establecidas en los actos jurídicos de la Unión a través de un mecanismo de comunicación centralizado que permita el intercambio transfronterizo de información así como la asistencia recíproca» [considerando segundo] (43). Y es que, en efecto, este servicio, fruto de los programas europeos *IDAbc* e *ISA*, es además el resultado del trabajo conjunto entre la Comisión y las distintas administraciones de los Estados miembros. Su uso, no obstante, se circunscribe a las relaciones entre las Administraciones de los Estados miembros, (incluidos Islandia, Liechtenstein y Noruega) y rara vez con la propia Comisión.

Esta herramienta –segura, multilingüe y respetuosa con la protección de datos personales– funciona a través de: *a)* consultas, *b)* alertas, *c)* notificaciones y *d)* repositorios, mientras que los flujos de datos se establecen entre sendas Administraciones, entre una Administración y varias o, a través de una base de datos dentro del IMI. Y se afirma el respeto de esta plataforma con el derecho a la protección de datos porque ésta ha cumplido con lo los flamantes principios desde el diseño o por defecto (44)

(42) Alabau Muñoz A., *La Unión Europea y su política para el desarrollo de la Administración electrónica*, *op. cit*., p. 153.

(43) Reglamento (UE) 1024/2012 del Parlamento Europeo y del Consejo de 25 de octubre de 2012, relativo a la cooperación administrativa a través del Sistema de Información del Mercado Interior y por el que se deroga la Decisión 2008/49/CE de la Comisión («Reglamento IMI») (DO L 316, de 14 de noviembre de 2012).

(44) Un inmejorable análisis general de ellos se puede encontrar en Cavoukian, A., *Privacy by Design: From Rhetoric to Reality*, Information and Privacy Ontario, Toronto, 2012. *Cfr.*, asimismo,

(art. 25 del RGPD) y con unas férreas directrices sobre protección de datos para los usuarios del IMI (45). La idea latente de este sistema era reemplazar «las relaciones bilaterales entre los Estados Miembros de la UE por una interfaz única» (46), como representa el IMI. Y se ha conseguido eliminando diversos obstáculos, por ejemplo, respecto a la clásica incertidumbre del destinatario, las diferencias de cultura administrativa y de prácticas de trabajo que se producen en el seno de la Unión. Así, el IMI ha conseguido ofrecer un «método de trabajo» uniforme aceptado por todos los Estados Miembros, lo que sin duda originará un indudable éxito. Respecto a los sectores en lo que se utiliza, si bien comenzó en el ámbito de servicios (47) y sobre cualificaciones profesionales (48), se ha extendido a otros, como a los derechos de los pacientes (49); SOLVIT (50), que es un servicio que resuelve los problemas ocasionados por una Administración Pública de otro Estado Miembros de la UE que no aplica correctamente la normativa europea; transporte transfronterizo de fondos en euros (51); en el contexto de los desplazamientos de trabajadores (52) y en cuanto a la restitución de bienes culturales (53). Además, se están implementado di-

---

con el particular examen de ellos en el RGDP que se realiza en Duaso Calés, R., «Los principios de protección de datos desde el diseño y protección de datos por defecto», en Piñar Mañas, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad*, *op. cit.*, pp. 295-320.

(45) http://ec.europa.eu/internal_market/iminet/docs/data_protection/data_protection_guidelines_es.pdf

(46) Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de Las Regiones «Mejorar la gobernanza del mercado único mediante una mayor cooperación administrativa: una estrategia para ampliar y desarrollar el sistema de Información del Mercado Interior («IMI»). COM (2011) 75 final, Bruselas, 21 de febrero de 2011.

(47) Directiva 2006/123/CE del Parlamento Europeo y del Consejo de 12 de diciembre de 2006 relativa a los servicios en el mercado interior (DO L 376, de 27 de diciembre de 206) y Decisión de la Comisión de 2 de octubre de 2009 por la que se establecen las medidas prácticas del intercambio de información entre Estados miembros por vía electrónica, de conformidad con lo dispuesto en el capítulo VI de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo relativa a los servicios en el mercado interior (DO L 263, de 7 de octubre de 2009).

(48) Directiva 2013/55/UE del Parlamento Europeo y del Consejo de 20 de noviembre de 2013 por la que se modifica la Directiva 2005/36/CE relativa al reconocimiento de cualificaciones profesionales y el Reglamento (UE) no 1024/2012 relativo a la cooperación administrativa a través del Sistema de Información del Mercado Interior («Reglamento IMI») (DO L 354, de 28 de diciembre de 2013).

(49) Directiva 2011/24/UE del Parlamento Europeo y del Consejo de 9 de marzo de 2011 relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (DO L 88, de 4 de abril de 2011).

(50) Recomendación de la Comisión de 17 de septiembre de 2013 sobre los principios por los que se rige SOLVIT (DO L 249, 19 de septiembre de 2013).

(51) Reglamento (UE) n 1214/2011 del Parlamento Europeo y del Consejo de 16 de noviembre de 2011 relativo al transporte profesional transfronterizo por carretera de fondos en euros entre los Estados miembros de la zona del euro (DO L 316, de 29 de noviembre de 2011).

(52) Directiva 2014/67/UE del Parlamento Europeo y del Consejo de 15 de mayo de 2014 relativa a la garantía de cumplimiento de la Directiva 96/71/CE, sobre el desplazamiento de trabajadores efectuado en el marco de una prestación de servicios, y por la que se modifica el Reglamento (UE) no 1024/2012 relativo a la cooperación administrativa a través del Sistema de Información del Mercado Interior («Reglamento IMI») (DO L 159, de 28 de mayo de 2014).

(53) Directiva 2014/60/UE del Parlamento Europeo y del Consejo de 15 de mayo de 2014 relativa a la restitución de bienes culturales que hayan salido de forma ilegal del territorio de un

versos proyectos pilotos sobre comercio electrónico, licencias de conducción de trenes y contratación pública y se espera que próximamente puedan incluirse también sectores como el de las máquinas móviles no de carretera y el de los documentos públicos en la Unión Europea.

En definitiva, este sistema IMI logra la unión de las distintas Administraciones de los Estados Miembros, facilitando el intercambio de información entre éstas, creando nuevos métodos de trabajo entre ellas y, en consecuencia, fortaleciendo el Mercado Único y contribuyendo al bienestar de los ciudadanos europeos en sus quehaceres administrativos. Todo ello sin poner en peligro el derecho de las personas a la protección de datos personales.

5. CONCLUSIÓN

No se descubre nada al afirmar que la interconexión masiva de datos e información puede potencialmente entrar en colisión cuando éstos son de carácter personal. En efecto, el ciudadano, en sus relaciones con la Administración Pública, autoriza la circulación de esos datos personales, pero no por ello, y sin que signifique esto una antinomia, cesa su preocupación por el uso inadecuado que se pueda hacer de ellos. En no pocas ocasiones, de hecho, se escuchan voces que aducen argumentos entre los cuales se imputa al derecho a la protección de datos personales la responsabilidad de no poder inaugurar, de una vez para siempre, un completo régimen de comunicación directa entre Administraciones Públicas. Estas aseveraciones, sin embargo, se demuestran superadas pues sólo garantizando sus derechos es posible lograr un adecuado régimen de intercambio de datos; el poder de disposición y de control sobre los datos personales, clásica definición de este derecho, será, en todo caso, un límite al que los sistemas de colaboración deberán ajustarse; pero nunca un obstáculo. La normativa del derecho a la protección de datos de carácter personal, supone un límite –no así un impedimento– para el intercambio interadministrativo de datos. Y, sin duda, el derecho de control y disposición que tienen los ciudadanos sobre sus datos personales no es óbice para la implementación de sistemas de transmisión de datos entre Administraciones Públicas. Es más, sólo desde el más absoluto respeto al derecho de protección de datos de carácter personal es posible que éstos se apliquen.

En este sentido, y a pesar de la existencia de mayores contrastes entre ordenamientos que sobre esta cuestión se advertían –sencillamente por los distintos presupuestos legitimadores en el tratamiento de datos personales por parte de las Administraciones Públicas– ahora uniformizados en

Estado miembro, y por la que se modifica el Reglamento (UE) no 1024/2012 (refundición) (DO L 159, 28 de mayo de 2014).

el potente Reglamento europeo, se puede afirmar sin temor a errar que se permite la transmisión de datos personales entre las Administraciones Públicas de los Estados miembros. De este éxito se debe, fundamentalmente, al buen hacer de las autoridades administrativas independientes de protección de datos personales que, con su gran labor aclarativa de los a veces oscurecidos preceptos que versan sobre la comunicación de datos personales entre Administraciones Públicas –sobre todo, en el caso de la normativa española– solventan complicadas situaciones como la que en estos instantes interesa. La elemental relación entre la cooperación interadministrativa y la siempre compleja ponderación con el derecho a la protección de datos personales son claves para las personas en este nuevo entorno digital que la innovación tecnológica posibilita. Su defensa y garantía de todos.

CAPÍTULO 16

DRONES Y PRIVACIDAD

JAVIER FERNÁNDEZ-SAMANIEGO
BLAS PIÑAR GUZMÁN
Abogados, Samaniego Law

1. INTRODUCCIÓN

En 2013, un dron-paparazzi se coló en la boda de Tina Turner que se celebraba en Suiza por todo lo alto para hacer fotos y venderlas a la prensa. En otra ocasión, otro de estos pequeños vehículos aéreos hizo saltar las alarmas de la Casa Blanca cuando se introdujo en el jardín y acabó estrellándose contra la parte trasera de la casa presidencial.

El uso de drones ha crecido exponencialmente en los últimos años. Hay drones para todo tipo de usos, desde la videovigilancia aérea hasta la fumigación. La empresa Amazon está implementando su uso para realizar envíos aéreos ultrarrápidos. Se pueden encontrar drones de diversos pesos y tamaños que le pueden conferir una mayor o menor manejabilidad. Debido a su pequeño tamaño y peso, y al hecho de que puede permanecer suspendido en el aire, un dron es un aparato muy manejable que puede volar por espacios muy reducidos e inaccesibles. Esto lo convierte en un ente especialmente invasivo. La incorporación de una cámara, máxime en el marco del actual despliegue de la red 5G, convierte en especialmente peligroso el impacto que su uso supone en nuestra privacidad.

Es precisa una breve digresión acerca de qué se entiende por «dron», qué se entiende por «privacidad» y cuál sería la interacción entrambos conceptos, donde se sitúa el *quid* que justifica el presente capítulo. Proveniente del inglés *drone*, el vocablo «dron» se refiere a toda aeronave no tripulada o sin piloto, lo que también se conoce como vehículo aéreo no tripulado o UAV (por sus siglas en inglés, *Unmanned Aerial Vehicle*). Ahora bien, estos UAVs pueden ser, o bien aeronaves pilotadas por control remoto (los RPAs o *Remotely Piloted Aircraft*), o bien aeronaves completamente autónomas. En coherencia con la práctica internacional más extendida, que prohíbe el uso de las aeronaves autónomas en los respectivos espacios aéreos nacionales, al hablar de «drones» se hará siempre referencia a aquellos UAVs que son RPAs.

Por su parte, bajo el vocablo «privacidad» subyacen conceptos jurídicos susceptibles de diferenciación. Sin entrar en este momento en la diferente aproximación a la que responde la noción de *privacy* en el derecho de matriz estadounidense respecto de aquella de intimidad y otros dere-

chos conexos propia del ámbito europeo, debe quedar claro que, al menos a los efectos del presente capítulo, por «privacidad» se engloban tanto la protección de datos de carácter personal como la protección de la intimidad personal y familiar y de la propia imagen. Lejos de ser caprichosa o voluntarista, esta acepción amplia responde, en realidad, a unos estrechos lazos. De un lado, la Carta Europea de los Derechos fundamentales entronca expresamente el derecho a la protección de datos con el artículo 8 del Convenio Europeo de Derechos Humanos, que se refiere a la vida privada. Y el Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal se refiere al derecho a la vida privada partiendo de la base de que la protección frente a la libertad de circulación de información personal es necesaria para proteger derechos como el respeto a la vida privada, la no discriminación o el derecho a un proceso equitativo, e incluso otros intereses legítimos en materia de empleo o de crédito al consumo. De otro lado, la propia dinámica del artículo 18.4 de la Constitución Española, que prefiguró el –posteriormente reconocido– «derecho fundamental a la protección de datos personales» (1) anclándolo a la protección del honor y de la intimidad personal y familiar de los ciudadanos. Finalmente, la normativa en materia de protección de datos personales distingue un núcleo duro de datos «sensibles» o «especialmente protegidos» que coinciden con la esfera de intimidad tradicionalmente protegida (2).

En palabras de Emilio Guichot,

> «[e]l tema nuclear de las relaciones entre derecho a la intimidad y derecho a la protección de datos […] no se encuentra resuelto ni en el Derecho comparado ni en el Derecho español. A falta de un reconocimiento específico, la jurisprudencia no encuentra obstáculo alguno en derivar la protección de la información personal, y los principios y facultades necesarios para su garantía, del derecho a la intimidad o vida privada, e incluso allá donde se han aprobado normas reguladoras de la protección de datos, éstas se declaran encaminadas a proteger los derechos y libertades y, en especial, el derecho a la intimidad o vida privada. Y, aún más, en el razonamiento judicial, derecho a la intimidad o vida privada y derecho a la protección de datos a menudo se manejan de forma indiferenciada. La jurisprudencia comunitaria es un buen ejemplo, como también lo es la española. … [L]as similitudes estriban en que ambos buscan un mismo objetivo, garantizar la vida privada, y tienen los mismos límites. Las diferencias radicarían en que el derecho a la intimidad es insuficiente para alcanzar este objetivo frente al flujo automatizado de datos personales, ya que no se extiende a toda información sobre una

(1) *Vid.* STC 292/2000, de 30 de noviembre.
(2) *Cf.* arts. 8 de la Directiva 95/46/CE, 7 de la Ley Orgánica 15/1999, de 13 de diciembre, y 9 del RGPD.

> persona, sino sólo a la relativa a determinados aspectos de su vida, los que tengan la consideración de íntimos, ni implica facultades positivas, esto es, derecho a obtener prestaciones de terceros, sino que se limita a una vertiente negativa, consistente en la facultad del titular del derecho de imponer a terceros una abstención de intromisión o injerencia en la parcela de realidad protegida por el derecho. Sin embargo, garantizar la vida privada, hoy, precisa del reconocimiento al individuo de un poder de control sobre todos sus datos personales…» (3).

Pues bien, a la hora de abordar la incidencia de los drones en la privacidad de las personas, ya en 2015 el Parlamento Europeo se hizo eco de una creciente preocupación: «En materia de riesgos para la privacidad y la protección de datos, los drones portan habitualmente videocámaras para permitir su pilotaje. Las imágenes pueden ser fácilmente grabadas y almacenadas, y con frecuencia son subidas a Internet. La intimidad de la vida privada y la propiedad pueden ser perturbadas y vulneradas cuando los drones captan imágenes de las personas en sus casas o jardines. Toda una serie de aplicaciones diferentes pueden ser instaladas en los drones, permitiéndoles la obtención y tratamiento de datos personales e infringiendo así, potencialmente, los derechos de los ciudadanos a la intimidad y a la protección de datos» (4). La Agencia Europea de Seguridad Aérea explica a este respecto que «[l]os riesgos para la intimidad y la protección de datos están relacionados esencialmente con la posibilidad de que el dron incorpore una cámara o cualquier otro sensor capaz de captar información personal. La mayoría de los drones disponibles en el mercado, incluso si son muy pequeños, están equipados con cámaras. Estos varían desde juguetes con posibilidades muy limitadas a nano drones capaces de portar cámaras de alta resolución» (5). A la misma cuestión se refiere el Grupo de Trabajo del Artículo 29 (6): «… debe quedar claro que lo relevante, desde el punto de vista de la intimidad y la protección de datos, no es el uso del dron en sí mismo, sino el equipo de procesamiento de datos a bordo del dron y el subsiguiente tratamiento de estos que pueda tener lugar. En efecto, es el tratamiento de imágenes (incluyendo imágenes de individuos, viviendas, vehículos, matrículas de estos, etc.), sonido, datos de geolocalización o cualesquiera otras señales electromagnéticas relacionadas con una persona física identificada o identificable llevada a cabo por el equipo de proce-

(3) Guichot, Emilio; Transparencia *versus* protección de datos.

(4) Privacy and Data Protection Implications of the Civil Use of Drones; In-depth analysis for the LIBE Committee (PE 519.221).

(5) Opinion 1/2018 of the European Aviation Safety Agency on Introduction of a regulatory framework for the operation of unmanned aircraft systems in the «open» and «specific» categories.

(6) «Grupo de protección de las personas en lo que respecta al tratamiento de datos personales» creado por el artículo 29 de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

samiento de datos a bordo del dron lo que puede tener un impacto en la privacidad y la protección de datos y, por lo tanto, motivar la aplicación de la legislación en materia de protección de datos» (7).

2. ENFOQUES REGULATORIOS

2.1 **Regulación en España**

En línea con los países de nuestro entorno y con objeto de regular el uso de drones, el Gobierno dictó el Real Decreto 1036/2017, de 15 de diciembre (8), que establece el marco jurídico definitivo (9) aplicable a la utilización civil de los RPAs no directamente sujetos a la normativa comunitaria (esto es, todos aquellos de masa máxima al despegue inferior a los 150 kg, así como los de masa máxima al despegue superior excluidos del ámbito de aplicación del Reglamento (CE) n.º 216/2008). Dispone el apartado f de su artículo 26 que todo operador de RPAs deberá «[a]doptar las medidas necesarias para garantizar el cumplimiento de lo dispuesto en materia de protección de datos personales y protección de la intimidad en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, sus normas de desarrollo y normativa concordante». Se hace, así pues, un llamamiento explícito a la protección de la privacidad en el ámbito de la utilización de drones, introduciendo de lleno a los operadores en el cumplimiento de la normativa en materia de protección de datos y de los derechos fundamentales a la intimidad y a la propia imagen.

No ofrece dudas la referencia a la Ley Orgánica 1/1982 que, como es harto sabido, desarrolla el artículo 18 de la Constitución Española y se mueve en el siempre delicado ámbito de colisión con el derecho fundamental a la libertad de expresión y su variante de libertad informativa (a informar y a ser informado). Mediante la técnica de la ponderación de derechos, a lo largo de los últimos lustros el Tribunal Constitucional y el Tribunal Supremo han creado un cuerpo doctrinal no uniforme ni exento de contradicciones que ofrece, no obstante, unos asideros con los que

(7) Opinion 1/2015 of the Article 29 Data Protection Working Party on Privacy and Data Protection Issues relating to the Utilisation of Drones.

(8) Real Decreto 1036/2017, de 15 de diciembre, por el que se regula la utilización civil de las aeronaves pilotadas por control remoto, y se modifican el Real Decreto 552/2014, de 27 de junio, por el que se desarrolla el Reglamento del aire y disposiciones operativas comunes para los servicios y procedimientos de navegación aérea y el Real Decreto 57/2002, de 18 de enero, por el que se aprueba el Reglamento de Circulación Aérea (BOE de 29 de diciembre de 2017).

(9) Anteriormente correspondía al artículo 50 de la Ley 18/2014, de 15 de octubre, de aprobación de medidas urgentes para el crecimiento, la competitividad y la eficiencia; la cual, asimismo, modificó el artículo 11 de la Ley 48/1960, de 21 de julio, sobre Navegación Aérea, para establecer que los RPAs son aeronaves sujetas a la legislación aeronáutica civil.

poder discernir la solución jurídica a los casos concretos. La sola prudencia aconseja, en consecuencia, no adentrarse en innovaciones legislativas en esta materia. Si el impacto que la irrupción de los teleobjetivos tuvo en estos derechos ya fue objeto de un específico desarrollo jurisprudencial (10), cabe esperar que la aparición de los drones lo será en un futuro más o menos cercano. De hecho, la STS 2.ª 329/2016, de 20 de abril, FJ 2.º *in fine*, razona que «*… la protección constitucional frente a la incursión en un domicilio debe abarcar, ahora más que nunca, tanto la entrada física del intruso como la intromisión virtual. La revolución tecnológica ofrece sofisticados instrumentos de intrusión que obligan a una interpretación funcional del artículo 18.2 de la CE. La existencia de drones, cuya tripulación a distancia permite una ilimitada capacidad de intromisión en recintos domiciliarios abiertos es sólo uno de los múltiples ejemplos imaginables*».

La invocación, sin embargo, de la Ley Orgánica 15/1999, de 13 de diciembre, nace herida de muerte toda vez que el Reglamento General de Protección de Datos (RGPD) (11) se encuentra en vigor desde mayo de 2016 y resulta plenamente aplicable desde el 25 de mayo de 2018 en adelante, momento a partir de cual deroga y desplaza aquella normativa nacional que se le oponga. En cualquier caso, todo operador de drones debe cumplir, en calidad de responsable o de encargado del tratamiento de datos personales, con las obligaciones inherentes a dicho estatus que prevé el RGPD, obligaciones susceptibles de cierto desarrollo por parte de la nueva Ley Orgánica de Protección de Datos de Carácter Personal dictada con ocasión, precisamente, del RGPD. Hasta el momento, la Agencia Española de Protección de Datos no ha elaborado directrices específicas sobre los drones, más allá de advertencias muy genéricas (12) o de la remisión a informes sobre cámaras *on board* (13).

Cabe mencionar que la Unidad de Aeronaves Pilotadas con Control Remoto de la Agencia Estatal de Seguridad Aérea (AESA) difunde un folleto informativo titulado «¿Qué podemos hacer con nuestro Dron?» (14). En él se advierte hasta en dos ocasiones de lo siguiente: «No te olvides de cumplir la Ley de Protección de datos, la del Derecho al Honor, Intimidad y propia imagen y las restricciones de toma de imágenes aéreas».

(10) *Vid.*, por ejemplo, la STS de 29 de marzo 1988 o la STC 176/2013, de 21 de octubre.

(11) Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

(12) Punto 2 del «Decálogo con consejos prácticos de privacidad y seguridad en dispositivos conectados».

(13) Informe Jurídico 546/2015 sobre el tratamiento de imágenes con cámaras *on board*.

(14) http://www.seguridadaerea.gob.es/media/4629387/que_podemos_hacer_con_nuestro_dron.pdf

2.2 **Regulación comparada. Breve referencia**

Los más conspicuos miembros de la Unión Europea han seguido un camino muy similar al de España. En general, se hace una remisión genérica a la respectiva normativa sobre videovigilancia por compartir algunos aspectos con el uso de drones.

En Francia, la Guía para el Uso de Drones con Fines Recreativos de la Dirección General de la Aviación Civil establece en sus puntos 7 y 8 que el operador de drones siempre deberá respetar la privacidad de los demás y que nunca deberá divulgar imágenes de terceros sin su consentimiento. Aconseja preguntar e informar a aquellos que puedan verse afectados por el uso del dron. La *Information Commissioner's Office* del Reino Unido ofrece en su sitio web una serie de recomendaciones, más bien etéreas, dirigidas a los usuarios de drones (15).

En EE. UU. la regulación federal sobre drones civiles tampoco aborda aspectos referidos a la privacidad. De la treintena de Estados americanos que han legislado en algún sentido sobre drones, algunos se refieren a la captación de imágenes sin consentimiento. Desde el punto de vista jurisprudencial, preeminente en el sistema de *Common law*, la cuestión parece decantarse en torno a la Cuarta Enmienda a la Constitución (16). Si en el pasado el Tribunal Supremo ha sostenido que dicha Enmienda no otorga a los ciudadanos ningún derecho con respecto a la vigilancia aérea, con fundamento en el hecho de que cualquiera puede observar desde el aire, el impacto de tecnologías potencialmente invasivas –como el escáner corporal o el localizador GPS– sí han sido contrastadas con la Cuarta Enmienda a los efectos de determinar su constitucionalidad y límites.

3. NUEVAS DIMENSIONES DE LA PRIVACIDAD ANTE EL FENÓMENO DE LOS DRONES. ESPECIAL CONSIDERACIÓN DEL RGPD

El RGPD no regula de forma específica los tratamientos de datos de carácter personal realizados mediante la utilización de drones por cuanto, con buen criterio, la norma parte de que la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas, como recuerda su Considerando 15. Pese a esa ausencia, lo cierto es que prácticamente todas las consideraciones realizadas por el Grupo de Trabajo del Artículo 29 –actual Comité Europeo de Protección de Datos– en su *Dictamen 1/2015 de 16 de junio de 2015 sobre la pro-*

(15) https://ico.org.uk/for-the-public/drones/

(16) Amendment IV to the Constitution of the United States of America: *«The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized».*

blemática del uso de drones para la protección de datos y privacidad resultan de aplicación, *mutatis mutandis*, bajo el prisma del vigente RGPD por cuanto dicha Opinión tuvo ya muy en cuenta la entonces Propuesta de Reglamento Europeo.

A continuación expondremos las principales obligaciones que establece el RGPD para que los tratamientos de datos realizados usando drones se adecuen a sus preceptos, deteniéndonos previamente en aquellos supuestos de tratamiento de datos que se encontrarían excluidos de su ámbito de aplicación, así como en algún supuesto de tratamiento específico.

3.1 **Tratamientos de datos excluidos del ámbito de aplicación del RGPD**

Como es sabido, el RGPD no se aplica a aquellos tratamientos de datos que, conforme a al artículo 2.2, están fuera de su ámbito de aplicación material, entre los que se encuentran aquellos «efectuados por una persona física en el ejercicio de actividades exclusivamente personales o domésticas», y los realizados «por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención».

3.1.1 Excepción «doméstica»

En relación con la denominada «excepción doméstica», ésta debe interpretarse de forma muy restrictiva. Aunque un dron se utilice para «fines domésticos», en el momento en el que trate datos de terceros –incluso de familiares o amigos– y no se limite a realizar tratamientos de la esfera más íntima de su titular, o bien ese círculo íntimo y el tratamiento puedan tener efectos o difusión fuera de tales ámbitos, no podría aplicarse la referida excepción, en consonancia con el criterio marcado por los tribunales y la AEPD al respecto (17).

3.1.2 Excepción «policial»

También el RGPD excluye de su ámbito de aplicación los tratamientos realizados por Fuerzas y Cuerpos de Seguridad y, en este sentido, la conocida como «Directiva policial» de protección de datos (18) (publicada en el DOUE

(17) STJUE, caso C-101/01, Bodil Lindqvist de 6 de noviembre 2003, párrafo 47, Informe 77/2013 de la AEPD, o SAN de 15 junio de 2006.

(18) Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

el mismo día que el RGPD) recuerda que las autoridades policiales no tienen vedado *per se* la realización de investigaciones encubiertas o la videovigilancia (debemos entender que tampoco la videovigilancia realizada a través de drones) cuando tales actividades se realicen con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas para la seguridad pública, siempre que estén previstas en la legislación y constituyan una medida necesaria y proporcionada en una sociedad democrática, con el debido respeto a los intereses legítimos de la persona física afectada.

En España, la derogada LOPD remitía a legislación específica los tratamientos procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad. Obviamente, aunque la «Directiva policial» de protección de datos se encuentra todavía pendiente de trasposición en España, cualquier tratamiento de datos realizado mediante drones por las Fuerzas y Cuerpos de Seguridad deberá realizarse siempre con esas salvaguardas y con pleno respeto al artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, que garantiza el derecho al respeto a la vida privada y familiar. Será particularmente relevante que, además de todas esas salvaguardas, las Fuerzas y Cuerpos de Seguridad puedan demostrar que los datos personales objeto de tratamiento mediante drones lo han sido debido a que la finalidad del tratamiento no podía lograrse razonablemente por otros medios.

3.2 **Tratamientos de datos realizados por drones con finalidades periodísticas**

Ya se ha aludido a lo que supuso, en su día, el advenimiento de los teleobjetivos con fines periodísticos y las colusiones con los derechos fundamentales que implicó. En esa misma línea, los tratamientos de datos que permiten técnicamente realizar los drones multiplican exponencialmente esta problemática.

El RGPD no excluye de su ámbito de aplicación los tratamientos de datos con fines periodísticos, si bien hace una llamada en su artículo 85 a que sean los Estados miembros quienes concilien por ley el derecho a la protección de los datos personales con el derecho a la libertad de expresión y de información, incluido el tratamiento con fines periodísticos. En España se ha decidido, con buen criterio a nuestro juicio, no hacer uso de dicha previsión en la nueva Ley Orgánica de Protección de Datos y seguir dejando que sean los tribunales quien realicen esa conciliación de ambos derechos fundamentales.

En el Dictamen 1/2015, el Grupo de Trabajo del Artículo 29 se refiere a un Código de Conducta europeo de la profesión periodística para la autorregulación del uso de drones. Ahora bien, considerando que el Tribunal

de Justicia de la Unión Europea no restringe esos fines periodísticos a la labor de los periodistas o medios de comunicación profesionales (19), se plantea el debate –relacionado con la excepción doméstica antes aludida– del periodismo ciudadano y el hecho de que imágenes tomadas por drones «domésticos» puedan pasar a tener interés periodístico y sean objeto de difusión pública. Ante tan delicados equilibrios, no parece que haya norma que pueda llegar a detallar toda la casuística posible. Lo más sensato, más allá de la deseable autorregulación, es el control judicial conforme a los criterios que en cada momento vaya marcando la doctrina jurisprudencial y constitucional.

3.3 **Licitud, cumplimiento de los principios de tratamiento y de información y transparencia que exige el RGPD a los tratamientos de datos realizados por drones**

3.3.1 Supuestos que legitiman que el tratamiento de datos por drones sea lícito

Todo tratamiento de datos, para ser lícito, debe ampararse en alguno de los supuestos previstos en el artículo 6 del RGPD. Si bien la obtención del consentimiento del interesado es el supuesto legitimador del tratamiento por excelencia, su obtención no resulta muy factible en el contexto de los datos personales captados por drones –particularmente en espacios públicos– resultando también problemática, en relación con el principio de transparencia y de información, la forma de cumplir con el derecho de información de los interesados sobre los tratamientos que están siendo llevados a cabo.

En determinadas situaciones –compras de productos cuya entrega puede realizarse mediante la utilización de drones– el supuesto legitimador previsto en el artículo 6.1.b del RGPD (*el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales*) podría operar. También pueden darse los supuestos previstos en los apartados c) (*tratamiento necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento*) o d) (*tratamiento necesario para proteger intereses vitales del interesado o de otra persona física*) en los que el tratamiento se realice mediante drones de forma lícita, como serían el caso de drones empleados en catástrofes naturales o en accidentes con sustancias peligrosas.

(19) Tribunal Europeo de Derechos Humanos, sentencia Társaság a Szabadságjogokért v Hungary 14 abril 2009, para. 27.

Asimismo, el supuesto que legitime multitud de tratamientos pretendidos será el del interés legítimo del artículo 6.1.f (*el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero*), sin olvidar las salvaguardas que exige este supuesto legitimador (*siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño*). Habrán de tenerse en cuenta las orientaciones proporcionadas sobre el uso del interés legítimo como supuesto legitimador (20) y el criterio de los tribunales en cada momento.

3.3.2 Particular reseña en relación con el cumplimiento de los principios de información y transparencia

Debido al particular contexto y circunstancias en el que los drones pueden llevar a cabo tratamientos de datos de carácter personal, cumplir con el principio de información al afectado (artículos 12 y siguientes del RGPD) es, tal vez, uno de los mayores retos jurídicos que se plantean. El Grupo del Trabajo del Artículo 29 sugiere en su Dictamen 1/2015 que los responsables cumplan desde una aproximación «multicanal» similar a la adoptada en materia de videovigilancia, donde se ha consolidado ya mediante la colocación de un dispositivo informativo en lugar suficientemente visible identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del RGPD. También se plantea que el operador del dron pueda ser fácilmente localizable y visible (por ejemplo, con un chaleco que contenga un símbolo intuitivo de la actividad que realiza).

Sin embargo, frente al carácter estático de las cámaras de videovigilancia que permite la colocación de esos carteles informativos, el fenómeno dron –salvo en el supuesto de áreas videovigiladas por drones de forma continuada y permanente– se caracteriza por una evidente volatilidad y lo desapercibidos que en ocasiones son estos aparatos, por lo que resulta esencial buscar mecanismos alternativos que permitan cumplir con esta obligación. Las sugerencias que realiza el Grupo de Trabajo del Artículo 29 a este respecto (21) son muy acertadas y van desde la utilización de símbolos en los propios drones, información en los sitios web de los operadores, colocación de paneles en lugares sometidos a videovigilancia permanente por drones, etc. Ello sin olvidar las iniciativas que abogan por la

(20) Opinión 2014 sobre la noción del interés legítimo del «responsable» del Grupo de Trabajo del Artículo 29 de 9 de abril de 2014, WP 217.

(21) Dictamen 1/2015. *Op. cit.* pp. 15 y 16.

individualización de los drones mediante una placa identificativa o un número de matrícula como es el caso español (22). Desde nuestro punto de vista, debería abordarse específicamente esta cuestión en futuros Códigos de Conducta que sería deseable fuesen aprobados conforme el artículo 40 del RGPD.

3.3.3 Cumplimiento de los principios relativos al tratamiento exigidos por el RGPD realizado con drones y particular relevancia de los principios de protección de datos desde el diseño y por defecto

A la hora de cumplir con los principios relativos al tratamiento de datos que exige el artículo 5 del RGPD, particularmente el principio de licitud, lealtad y transparencia (apartado1.a) y el denominado principio de «minimización de datos» (que exige que los datos sean *adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados* en el contexto de los datos tratados por drones), resulta particularmente relevante tener en cuenta los principios de protección de datos desde el diseño y por defecto, a los que se refiere el artículo 25 del RGPD.

Una forma de respetar el principio de minimización en este contexto podría consistir en que el dron permita la seudonimización de las imágenes u otros datos captados, o incluso si el fabricante estableciese que, por defecto, sólo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del mismo, llevando a cabo de forma automática el pixelado de rostros, matrículas y otros elementos identificadores de las personas físicas.

Lógicamente debido a la multitud de tipologías de drones y de finalidades que pueden perseguirse con los tratamientos de datos, tanto fabricantes como responsables deberán aplicar dichos principios sin olvidar que, si los tratamientos a realizarse, por su naturaleza, alcance, contexto o fines, pudieran entrañar un alto riesgo para los derechos y libertades de las personas físicas, se tendrá que realizar una evaluación del impacto de las operaciones de tratamiento conforme al artículo 35 del RGPD.

3.3.4 Seguridad

Las previsiones relativas a la seguridad de datos previstas en los artículos 32 y siguientes del RGPD deben ser obviamente tenidas en cuenta por los responsables –particularmente si se produjesen ciberataques o violaciones de seguridad de datos personales– y, una vez más, los mecanismos de certificación previstos en el artículo 42 del RGPD pueden ser instrumentos adecuados para cumplir con esas obligaciones.

(22) *Vid.* artículos 8 y 9 del Real Decreto 1036/2017, de 15 de diciembre.

3.4 **Importancia de la autorregulación y códigos de conducta**

El RGPD ha sido aprobado con la experiencia acumulada tras más de veinte años de vigencia de la Directiva 95/46/CE, ofreciendo un marco sólido y pretendidamente estable de instituciones jurídicas referidas a la protección de los datos personales de los ciudadanos de la Unión Europea. Se trata, pues, de una inmejorable oportunidad para evitar el fenómeno –tan en boga– de incontinencia normativa, o «legislación motorizada» a decir del Prof. García de Enterría (quien lo tomó, a su vez, de Carl Schmitt). Ante la tentación siempre latente de reclamar una «norma sobre drones y privacidad», y sin perjuicio de las funciones propias de las autoridades administrativas y de los tribunales de justicia, el sector podrá dotarse de códigos de conducta, certificados y sellos de los previstos en los artículos 40 y 41 del RGPD, autorregulando su actividad y sometiéndola a supervisión privada competente. Aspecto crítico será el de la formación básica y continua de los operadores de drones en materia de privacidad: de que reciban nociones de protección de datos, intimidad y propia imagen o no lo hagan dependerá tanto su concienciación sobre la gravedad de la cuestión como el éxito en la garantía de los derechos fundamentales de los ciudadanos en la era digital.

IV

CONDICIONES BÁSICAS PARA GARANTIZAR LA IGUALDAD EN UN MUNDO DIGITAL

CAPÍTULO 17

LA NECESARIA RECONFIGURACIÓN DE LAS GARANTÍAS JURÍDICAS EN EL CONTEXTO DE LA TRANSFORMACIÓN DIGITAL DEL SECTOR PÚBLICO

JULIÁN VALERO TORRIJOS
Catedrático de Derecho Administrativo
Coordinador iDerTec-Grupo de investigación «Innovación, Derecho y Tecnología»
Universidad de Murcia

1. PLANTEAMIENTO GENERAL: LA NECESIDAD DE ADOPTAR UN ENFOQUE MÁS AMPLIO

Desde el punto de vista jurídico, los importantes desafíos que ha de afrontar la sociedad europea han sido resaltados al afirmarse que resulta imprescindible un entorno claro que fomente la innovación y, al mismo tiempo, facilite la equidad y el equilibro entre los diversos agentes involucrados (1). Sin embargo, las garantías jurídicas en las que tradicionalmente se ha asentado la regulación no han seguido –al menos no lo han hecho con la necesaria agilidad e intensidad– el vertiginoso ritmo impuesto por la innovación tecnológica; especialmente por lo que respecta a las garantías jurídico-administrativas que constituyen el objeto de este trabajo. De la misma manera, el análisis doctrinal que podría haber ayudado a replantear y, en su caso, reconducir la degeneración del proceso legislativo (2), se ha centrado en gran medida en el análisis de las soluciones normativas (3) quizás ante la necesidad de abordar, en primer lugar, un estudio más descriptivo que permitiera comprender el alcance de la aplicación práctica de la tecnología en la gestión interna y, sobre todo, las comunicaciones *ad extra*.

Las consecuencias de esta actitud son todavía más graves si cabe cuando la inercia doctrinal centra su esfuerzo principalmente en glosar y analizar las novedades legislativas que, en definitiva y según el funcionamiento actual del procedimiento de su elaboración, en última instancia terminan por satisfacer las necesidades de su autor inicial –esto es, el Gobierno y en concreto los departamentos y entidades que lideran la mo-

(1) *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, relativa a la revisión intermedia de la aplicación de la Estrategia para el Mercado Único Digital. Un mercado único digital conectado para todos*, COM(2017) 228 final.

(2) A este respecto, ya afirmamos en su momento que la reforma de 2015 había sido en gran medida una oportunidad perdida desde la perspectiva de la innovación. Véase Valero Torrijos, J.: «La reforma de la Administración electrónica: una oportunidad perdida», *Revista Española de Derecho Administrativo*, núm. 172, 2015, pp. 13-26.

(3) Sobre la evolución de la atención doctrinal en esta materia, véase Cerrillo i Martínez, A.: «Las tecnologías de la información y la comunicación en el debate del Derecho Público contemporáneo», *Autonomies. Revista catalana de Derecho Público*, núm. 35, 2007, pp. 357-382. Más recientemente, Valero Torrijos, J.: «De la digitalización a la innovación tecnológica: valoración jurídica del proceso de modernización tecnológica de las administraciones públicas españolas en la última década (2004-2014)», *Revista Internet, Derecho y Política*, núm. 19, 2014, pp. 117-129.

dernización tecnológica desde la Administración estatal–; por mucho que quiera afirmarse la autonomía formal del procedimiento de elaboración de las leyes en sede parlamentaria, sin duda distorsionado en mayor medida cuando se trata de normas que aparentemente se caracterizan por su aparente dimensión técnica y una supuesta neutralidad política, como es el caso de la LPAC y la LRJSP.

Ciertamente, en muchos casos la moda de la innovación tecnológica únicamente nos presenta meras *etiquetas* impuestas por avanzados procesos de marketing y comunicación, muy frecuentes en el contexto del sector público dada la necesidad de impulsar continuamente nuevas ofertas tanto políticas como económicas –frecuentemente por avezadas consultoras y empresas de servicios–. Ahora bien, no es menos cierto que también estamos asistiendo a un cambio de paradigma que debiera ser objeto de una mayor atención, en particular por lo que se refiere al análisis doctrinal. De lo contrario, podemos encontrarnos con que la innovación tecnológica termine por deslumbrarnos y nos impida percibir los cambios que efectivamente están teniendo lugar, de manera que las garantías jurídicas se conviertan en un lastre y, por tanto, sean menospreciadas en su auténtico valor; o, incluso, que no se alcance a percibir su importancia real en un ecosistema de continuas novedades tecnocráticas, cuyos protagonistas sólo perciban los límites de la tecnología como única exigencia final a la que someterse, convirtiéndose así el Derecho en un mal menor que ha de intentase respetar sólo desde la literalidad y el mero formalismo o, incluso, directamente ignorarse.

Pues bien, desde estas premisas es necesario advertir que de la misma manera que la tecnología se ha ido implantando progresivamente en la realidad administrativa y se ha convertido en una herramienta de uso generalizado, también el marco normativo aplicable se ha ido adaptando de manera paulatina, pudiendo observarse con el paso de los años un creciente interés doctrinal que, en última instancia y como antes destacábamos, ha estado condicionado en gran medida por dicho avance fáctico y normativo. Sin embargo, existe el peligro de que la perspectiva doctrinal sea determinada en exceso por la evolución del marco legislativo y, por tanto, se acabe diluyendo la reflexión dogmática en las urgencias del análisis del Derecho positivo.

En consecuencia, más allá del mero análisis de las previsiones legales y reglamentarias, de una parte resulta imprescindible examinar hasta qué punto el marco normativo vigente establece soluciones jurídicas suficientemente garantistas en atención al contexto tecnológico actual en que se ha de desenvolver la actividad administrativa; y, en un segundo momento, valorar en qué medida las bases conceptuales en las que se sustenta dicha regulación son adecuadas a dicho contexto, caracterizado

sustancialmente por una creciente complejidad que puede privar a las previsiones normativas de su función tuitiva de los diversos intereses potencialmente afectados.

2. LA REGULACIÓN SOBRE RÉGIMEN JURÍDICO DEL SECTOR PÚBLICO Y PROCEDIMIENTO ADMINISTRATIVO COMÚN: ¿UNA PERSPECTIVA INSUFICIENTE Y DISFUNCIONAL?

Hasta la reforma de 2015, la disciplina jurídica del uso de las herramientas tecnológicas en el ámbito del sector público se ha basado sustancialmente en adaptar las tradicionales garantías jurídico-formales propias de la actuación administrativa y, en particular, el procedimiento administrativo. Tras la entrada en vigor de la LPAC y la LRJSP, dicha afirmación ha de mantenerse sustancialmente con algunas matizaciones.

En efecto, de una parte es preciso reconocer que la nueva regulación ha supuesto importantes avances en el empeño de dotar al sector público de los instrumentos jurídicos que permitan avanzar en la definitiva modernización de su gestión. Sin embargo, al mismo tiempo ha supuesto una regresión –o, al menos, la confirmación de ciertas prácticas restrictivas ya existentes– por lo que se refiere a las garantías jurídicas de quienes han de entablar relaciones jurídicas con las entidades del sector público, ya sean particulares o, incluso, otros sujetos públicos. No obstante, más allá de una mera valoración inicial de conjunto, resulta imprescindible llevar a cabo un análisis pormenorizado de las previsiones legales teniendo en cuenta el hilo conductor de este trabajo: hasta qué punto las garantías jurídicas del proceso de modernización en que se encuentran inmersas las entidades del sector público están consagradas legalmente de manera adecuada. Para, en su segundo momento, tal y como analizaremos más adelante, valorar si son o no suficientes a la hora de afrontar los retos de la transformación digital que, cada vez con mayor frecuencia, se plantean para superar las limitaciones y disfunciones a que se enfrentan los proyectos e iniciativas que se promueven en este contexto.

2.1 **La redefinición del ámbito subjetivo en la reforma de 2015 y sus consecuencias sobre el modelo de gestión electrónica**

Una de las principales novedades que, con carácter general, ha consagrado la reforma operada por la LPAC y la LRJSP se refiere a la redefinición de los sujetos que se encuentran obligados a cumplir sus previsiones. En efecto, tal y como señala el artículo 2 de ambas leyes es necesario distinguir entre las Administraciones Públicas en un sentido estricto –las tradicionalmente denominadas *Administraciones territoriales*– de aquellas otras personificaciones que, al no reunir las condiciones fijadas

legalmente, son relegadas al estatuto de meras entidades que forman parte del sector público institucional. A este respecto, las entidades con personificación jurídico-pública son consideradas por el legislador Administraciones Públicas y, en consecuencia, las previsiones específicas que se contemplan sobre el uso de medios electrónicos les resultan plenamente aplicables. En consecuencia, aquellas otras cuya forma de personificación sea privada, aun cuando se encuentren vinculadas o dependan de aquellas, tienen una disciplina parcialmente distinta que, en última instancia, puede llevar a producir disfunciones relevantes desde la perspectiva del uso de medios electrónicos (4).

En este sentido, es preciso tener en cuenta el diferente alcance de la regulación legal en algunos aspectos concretos. Por lo que se refiere a los registros de apoderamientos, se trata de una herramienta de gran importancia práctica a la hora de gestionar la representación de las personas interesadas en los procedimientos administrativos, en particular si tenemos en cuenta que según el planteamiento del legislador –art. 5.4 LPAC– pueden existir diversas modalidades con alcance ciertamente heterogéneo. Así pues, resulta imprescindible disponer de mecanismos de consulta automatizada e inmediata, para lo cual se configura una obligación legal inequívoca dirigida únicamente a la Administración General del Estado, las Comunidades Autónomas y las Entidades Locales, que son los únicos sujetos que habrán de disponer necesariamente de un registro electrónico general de apoderamiento a partir del 2 de octubre de 2018 (5). Ahora bien, esta obligación legal no impide que el resto de organismos, sin distinguir acerca de su naturaleza, puedan crear registros particulares, aunque una interpretación sistemática nos lleva a considerar que dicha posibilidad sólo se admitiría para las entidades con personificación pública, puesto que el objeto de los poderes es únicamente la actuación ante las Administraciones Públicas.

La distinción acerca del tipo de sujeto obligado por la regulación legal de 2015 también plantea una importante incidencia por lo que se refiere a la existencia de los Registros Electrónicos Generales, herramienta que sólo han de implantar las entidades consideradas Administraciones Públicas en sentido estricto –las que hemos venido a denominar *territoria-*

(4) Sobre esta problemática, *cfr.* Gamero Casado, E.: «La estructura de la legislación sobre procedimiento administrativo común y régimen jurídico básico del sector público y sus criterios de aplicación», en E. Gamero (dir.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público*, Tirant lo Blanch, Valencia, 2017, tomo I, pp. 244-257.

(5) En todo caso, debe advertirse que la obligación legal puede cumplirse a través de mecanismos de colaboración interadministrativa, lo que resulta de especial importancia en el ámbito local. Sobre esta posibilidad, véase Martínez Gutiérrez, R.: *El Régimen Jurídico del nuevo procedimiento administrativo común*, Thomson-Reuters Aranzadi, Cizur Menor, 2016, p. 151.

les– (6), sin perjuicio de que los organismos públicos también puedan crear el suyo, pero en este caso voluntariamente al no alcanzarles la obligación legal del artículo 16 LPAC. Ahora bien, en el caso de que decidan su puesta en marca, el acceso habrá de garantizarse desde el registro de la Administración Pública a la que se encuentren vinculados, de manera que todos se encuentren plenamente interconectados (7).

Por lo que se refiere al archivo electrónico único contemplado en el artículo 17 LPAC, el legislador alude genéricamente a que habrán de contar con él las Administraciones Públicas, sin hacer referencia alguna a los organismos públicos como sucedía en el caso de los registros de apoderamientos y los registros electrónicos de presentación de escritos y solicitudes. Dada esta diferencia en cuanto al resto de instrumentos, no queda otra opción que entender las entidades públicas que no sean consideradas Administraciones Públicas en sentido estricto no podrían disponer de un archivo único *propio*. Ahora bien, el alcance de esta exigencia ha de ser relativizado para evitar consecuencias absurdas, de manera que ha de interpretarse que la intención del legislador es que, en caso de disponer de un archivo, no pueda ser gestionado de manera separada respecto de aquel que hubiese puesto en marcha la Administración Pública de la que dependan o a la que se encuentren vinculados. En otras palabras, si se pretende hacer efectivo el derecho a no presentar documentos regulado en el artículo 28 LPAC, los organismos y entidades con personificación pública habrán de integrar su archivo electrónico en el sistema de la correspondiente Administración, de manera que ante cualquier intento por parte de otra entidad de consultar el mismo al amparo del artículo 155 LRJSP no sea preciso realizar la consulta a través de un sujeto intermediario –la entidad u organismo público–, sino que habrá de accederse directamente al sistema de archivo de la respectiva Administración territorial. Sin perjuicio, claro está, que esta derive la consulta a otro sistema de archivo interconectado, pero advirtiendo claro que la responsabilidad en términos jurídicos, organizativos y técnicos acerca de la accesibilidad y disponibilidad de la información corresponde a las respectivas Administraciones territoriales.

Por otro lado, tal y como se ha planteado anteriormente, el derecho a no presentar datos y documentos que configura el artículo 28 LPAC únicamente se refiere a los que ya obren en poder de las Administraciones Públicas o, en su caso, hubieran sido elaborados por ellas. Al igual que en los supuestos anteriores podría surgir la duda interpretativa acerca de su al-

(6) A este respecto nos remitimos al análisis de Rego Blanco, M.D.: «La presentación de solicitudes, escritos y documentos ante las Administraciones Públicas», en E. Gamero (dir.), *Tratado de procedimiento administrativo…*, ob. cit., tomo I, pp. 1039-1047.

(7) Martínez Gutiérrez, R.: *El Régimen Jurídico...*, ob. cit., p. 209.

cance subjetivo, si bien en este caso nos encontramos ante un supuesto cualitativamente distinto, ya que la regulación legal objeto de análisis no se refiere a instrumentos o herramientas que deban crearse sino, por el contrario, al alcance de un derecho subjetivo de las personas interesadas en un concreto procedimiento administrativo. Desde esta premisa no sería admisible una interpretación restrictiva que limitase el objeto del derecho, sobre todo si tenemos en cuenta que la naturaleza de los organismos puede variar según la Administración Pública a la que se encuentre vinculado el ente instrumental; lo que en última instancia supondría condicionar la titularidad de un derecho en función de la decisión organizativa adoptada por aquella, que podría ser diversa en cada Comunidad Autónoma o, por qué no, en función del ámbito local al que nos refiramos. En consecuencia, la seguridad jurídica parece reclamar que la referencia a las Administraciones Públicas se interprete en sentido amplio y, de esta manera, el derecho a no presentar datos y documentos se aplique, cuando menos, respecto de los que tengan en su poder cualesquiera entidades con personalidad jurídico-pública. Más discutible sería respecto de las entidades jurídico-privadas vinculadas al sector público al no poder considerarse Administración Pública en modo alguno según la regulación legal, a pesar de que *lege ferenda* debiera considerarse una ampliación del derecho.

Por su parte, en el caso de las Universidades públicas, la aplicación de este régimen jurídico sobre el uso de medios electrónicos –y en general la disciplina legal establecida en 2015 para el sector público y el procedimiento administrativo común– sólo tendrá lugar con carácter supletorio, lo que ha dado lugar a un intenso debate doctrinal de consecuencias inciertas (8). Idéntica conclusión cabe mantener para las Corporaciones de Derecho Público, al menos por lo que se refiere al ejercicio de las funciones públicas que les hayan sido asignadas legalmente o por delegación de una Administración. En conclusión, desde la perspectiva del objeto de este trabajo, la seguridad jurídica parece reclamar que, a salvo de una prohibición expresa o de una previsión en contrario por parte de su normativa específica, también les resulten de aplicación las disposiciones analizadas en este epígrafe.

2.2 **La regulación de los problemas en las comunicaciones**

Una de las principales novedades por lo que se refiere a las relaciones telemáticas entre las entidades públicas y la ciudadanía consiste en el establecimiento *ex lege* de una amplia obligación de utilizar medios electróni-

(8) Sobre esta problemática, Rivero Ortega, R.: «La aplicación de las Leyes 39 y 40/2015 a las universidades públicas: eliminando interrogantes», *Revista de Administración Pública*, núm. 201, pp. 279-302.

cos tanto para presentar escritos, recursos y solicitudes como, en su caso, recibir notificaciones. En efecto, a diferencia de las previsiones vigentes desde 2007 en que se remitía dicha decisión a la vía reglamentaria con ciertas garantías adicionales en cuanto a la disponibilidad de los medios adecuados (9) –disposición que se mantiene ahora únicamente para las personas físicas–, el legislador ha considerado necesario establecer una obligación directamente aplicable dirigida a las personas jurídicas, a los profesionales e, incluso, a las entidades sin personalidad jurídica. Aunque en principio podría considerarse que se trata de un avance razonable y proporcionado dada la naturaleza de los sujetos obligados, lo cierto es que supone una importante merma de garantías en algunos casos, tal y como puede suceder con un amplio número de entidades sin ánimo de lucro –caso, por ejemplo, de muchas asociaciones– o de numerosas entidades sin personificación –las comunidades vecinales son un caso paradigmático–, que en última instancia se verán obligadas a contar con los servicios de un profesional simplemente para el cumplimiento de obligaciones o el ejercicio de derechos ante las Administraciones Públicas. Con el agravante de que, al menos legalmente, no tienen reconocido el derecho a ser asistidos por parte las Administraciones Públicas en dichas situaciones, opción legislativa ciertamente criticable teniendo en cuenta la realidad de los sujetos aludidos que puede llegar a convertirse en imposibilidad de llevar a cabo la relación jurídica de existir problemas técnicos (10).

Por lo que respecta a la utilización de los registros, se ha regulado por primera vez con carácter general la ampliación de los plazos en los casos de problema técnicos, si bien las medidas del artículo 32.4 LPAC resultan excesivamente genéricas (11) por cuanto nada indican acerca del límite máximo ni el tipo de procedimiento al que se refieran las incidencias, lo que parece especialmente problemático en los de naturaleza competitiva por cuanto la medida puede afectar a derechos de terceros. Asimismo, la alusión expresa a la subsanación de la presentación realizada en soporte

(9) No obstante, el legislador ha fijado escasos límites a la potestad reglamentaria, lo que se añade a una interpretación jurisprudencial que los ha terminado por desdibujar. A este respecto, véase Cotino Hueso, L.: «El derecho y el debe de relacionarse por medios electrónicos (art. 14 LPAC). Asistencia en el uso de medios electrónicos a los interesados (art. 12 LPAC)», en E. Gamero (dir.), *Tratado de procedimiento administrativo común…*, tomo I, ob. cit., pp. 503-506.

(10) Por ello, según Cotino, resulta imprescindible «buscar una interpretación favorable [al derecho de asistencia] para salva la constitucionalidad de la ley» (Cotino Hueso, L.: «El derecho…», ob. cit., p. 520); si bien, nada impediría que cada Administración pueda ampliar el reconocimiento de este derecho también a los sujetos obligados al uso de medios electrónicos (Martínez Gutiérrez, R.: *El régimen jurídico…*, ob. cit., pp. 128 y 129). Así pues, en ambos casos parece justificada la necesidad de realizar interpretaciones tendentes a facilitar el ejercicio de los derechos y el cumplimiento de las obligaciones dada la restrictiva visión del legislador básico, más preocupado de evitarle problemas de gestión a las Administraciones Públicas que de asegurar la tutela de todos los intereses en juego.

(11) *Cfr.* Velasco Rico, C.: «Novedades en materia de Administración electrónica», en la obra colectiva que ella misma dirige, *Reflexiones sobre la reforma administrativa de 2015*, Marcial Pons, Madrid, 2017, p. 142-143.

papel cuando se está obligado al uso de medios electrónicos puede resultar disfuncional, en particular debido a la previsión legal –art. 68.4 LPAC– de que el trámite se entenderá realizado únicamente cuando se lleve a cabo la actuación utilizando dichos medios. Se trata, pues, de una fuente de inseguridad jurídica ya que no queda claro si procede aplicar el requerimiento general de diez días o, en su caso, qué sucedería cuando la subsanación se realice una vez cumplido ya el término o plazo establecido con carácter general (12).

Desde la perspectiva de las notificaciones, es necesario reconocer que se han incorporado novedades importantes, si bien al mismo tiempo la regulación legal de las mismas no permite afirmar de manera rotunda que se hayan reforzado las garantías jurídicas de los destinatarios, sobre todo si tenemos en cuenta que cada Administración Pública podrá utilizar su propia sede y, en consecuencia, resultará preciso acudir a cada una de ellas específicamente. Así pues, la insuficiencia de la regulación resulta especialmente clara en relación al aviso informativo que con carácter obligatorio ha de remitirse a los destinatarios de las notificaciones. En efecto, a pesar de la contundente e incondicionada obligación legal, lo cierto es que el propio legislador afirma sin rubor –art. 41.6 LPAC– que su falta no impedirá que la notificación sea considerada válida, por lo que resulta necesario reconfigurar las garantías jurídicas desde la perspectiva de la eficacia. Sólo de este modo se podría evitar la indeseable consecuencia de la indefensión (13), ya que parece desproporcionado en muchos casos hacer recaer sobre ciertos sujetos una exigencia absoluta de consulta de las sedes o direcciones electrónicas cuando la propia Administración Pública ha incumplido una obligación legal que, en última instancia, está dirigida a facilitar el conocimiento de la existencia de una notificación pendiente de acceso.

Asimismo, una deseable exigencia de refuerzo de la seguridad jurídica obligaría a ampliar la práctica existente en el ámbito tributario, donde se contempla el derecho de los interesados de señalar los días en los que la Agencia Estatal de Administración Tributaria no podrá poner notificaciones a su disposición en la dirección electrónica habilitada. Pues bien, teniendo en cuenta la celeridad de los plazos previstos desde que se pone a disposición la notificación hasta que empiezan a computarse los efectos de su rechazo –tan sólo diez días naturales–, parece más que justificado ampliar el ámbito de este derecho no sólo a otras entidades sino, asimis-

(12) En palabras de Cotino, el requerimiento «sólo parece tener sentido si se practica antes de que haya transcurrido el plazo de que se trate y el administrado tiene el tiempo de subsanar» (Cotino Hueso, L.: «El derecho y el deber…», ob. cit., p. 516).

(13) Martín Delgado, I.: «Ejecutividad y eficacia de los actos administrativos», en E. Gamero (dir.), *Tratado de procedimiento administrativo común…*, ob. cit., tomo II, p. 2164.

mo, a las notificaciones que se practiquen en ámbitos materiales distintos del tributario.

Por último hay que tener en cuenta que ha desaparecido una previsión legal de gran transcendencia que, en última instancia, estaba destinada a reforzar la posición jurídica de la persona destinataria de las notificaciones. En concreto, se trata de la referencia a la imposibilidad técnica o material del acceso como causa obstativa del comienzo de la eficacia de la notificación puesta a disposición –a la que se refería el art. 28.3 de la Ley 11/2007, de 22 de junio–, de la que no queda rastro tras la reforma de 2015. Aun cuando dicha previsión resultaba ciertamente complicada de interpretar debido a la multiplicidad de supuestos imaginables (14), permitía tener en cuenta una serie de circunstancias de diversa índole que podían justificar sobradamente la ineficacia de la notificación y, sobre todo, que el plazo para realizar las actuaciones correspondientes no diera comienzo. En última instancia, al igual que se afirmó en relación al aviso informativo, dicha medida justificaba tener en cuenta circunstancias relevantes desde la perspectiva de la indefensión que, de lo contrario, se produce cuando por razones ajenas a la voluntad de la persona destinataria de la notificación y suficientemente justificadas resulta imposible tener conocimiento del acto notificado. Ahora bien, en este caso ha de matizarse que la notificación siempre podría obtenerse a través de la personación en las oficinas administrativas una vez que ya se tiene conocimiento de la puesta a disposición; posibilidad que ha de valorarse igualmente a la hora de ponderar el alcance de la dificultad técnica y, por tanto, de la eficacia del acto administrativo objeto de notificación.

2.3 **La proyección de la tecnología en la gestión documental**

Desde la entrada en vigor de la reforma de 2015, los actos administrativos han de tener necesariamente formato electrónico, salvo que su propia naturaleza exija otra forma más adecuada de expresión y constancia, tal y como señala el artículo 26 LPAC. Sin embargo, la realidad de la gestión actual demuestra que dicha obligación no se cumple si quiera de manera generalizada, por lo que todavía persiste la tramitación en soporte papel como la forma normal de documentar los actos y los expedientes administrativos (15).

---

(14) Sobre esta problemática y la casuística a que daba lugar, véase Valero Torrijos, J.: *El régimen jurídico de la e-Administración. El uso de medios informáticos y telemáticos en el procedimiento administrativo común*, 2.ª ed., Comares, Granada, 2007, pp. 177-180.

(15) A este respecto, se ha llegado a afirmar que «no es realista caer en brazos de la «alquimila legal», es decir, de la convicción de que la letra de la ley puede transformar el formato papel en formato digital y, más aún, la gestión digital en una gestión eficaz y eficiente sin más ni más» (Cierco Seira, C.: «El «nuevo» procedimiento administrativo común», en C. Velasco (dir.): *Reflexiones sobre la reforma administrativa de 2015*, Marcial Pons, Madrid, 2017, p. 90.

La principal pregunta que puede plantearse a estos efectos se ha de referir necesariamente al alcance de este incumplimiento (16). Así, difícilmente cabe entender que concurra alguna de las causas de nulidad de pleno derecho que contempla el artículo 47 LPAC, por lo que necesariamente hemos de partir de la interpretación de la disciplina de la anulabilidad. A este respecto, el defecto de forma sólo tendrá fuerza invalidante en los casos en que impida al acto cumplir su finalidad o, en su caso, produzca indefensión. Esta última consecuencia podría darse cuando se hubiese indicado un medio electrónico de notificación o, en su caso, hubiese una obligación legal de utilizar dicha vía y se practicase por otra distinta, de manera que la persona destinataria no llegara a tener conocimiento del acto notificado. O, por lo que respecta al incumplimiento de los fines de la forma, también podría darse el caso de que no fuese posible acceder a datos o documentos al no encontrarse en soporte electrónico, dejando sin efecto el derecho a no presentarlos. Ahora bien, la consecuencia invalidante sólo se produciría cuando hubiese un perjuicio derivado de un retraso en la tramitación o, incluso, en la preclusión de un trámite o la caducidad del procedimiento por no haberse realizado la aportación, lo que exigiría una interpretación excesivamente rigorista y claramente ilegal por parte de la Administración responsable del trámite o del procedimiento.

Por el contrario, más allá de la genérica referencia del artículo 14 LPAC, no existe una clara y terminante obligación castigada legalmente de manera rotunda –con la correspondiente inequívoca sanción legal para los casos de incumplimiento–, de que cualquier trámite o actuación de los particulares pueda ser llevada a cabo utilizando medios electrónicos. Por esta razón, a pesar de la aparente contundencia de la regulación legal, todavía es práctica habitual en muchas entidades seguir exigiendo la utilización del papel o, al menos, instar a hacerlo ante los perjuicios que se pueden derivar para quien pretenda realizar el trámite por medios electrónicos o ejercer el derecho a no presentar datos o documentos que ya obren en poder de las Administraciones Públicas. Por el contrario, estas últimas sí que pueden sustentar su posición en la existencia de una reduplicada obligación de utilizar dicha vía para los sujetos obligados al amparo del artículo 68.4 LPAC; que, además, está reforzada de manera rotunda con la presunción de validez de sus decisiones según contempla el artículo 39 LPAC.

Más allá de la forma de los actos y los documentos, la implantación de la tecnología en la gestión documental requiere reconfigurar el concepto

(16) En particular si constatamos que el legislador no se pronuncia incomprensiblemente al respecto, como se destaca en Galán Vioque, R.: «Anulabilidad e irregularidades no invalidantes», en E. Gamero (dir.), *Tratado de procedimiento administrativo común…*, tomo II, ob. cit., p. 2057.

de expediente administrativo. A este respecto, el artículo 70 LPAC ha incorporado no sólo una definición sino, además y por lo que ahora nos interesa, una delimitación negativa, de manera que no formarán parte del mismo «la información que tenga carácter auxiliar o de apoyo, como la contenida en aplicaciones, ficheros y bases de datos informáticas». Desde la perspectiva de la efectividad de las garantías jurídicas se trata de una regulación no ya excesivamente restrictiva sino manifiestamente contraria a la defensa de los derechos e intereses legítimos de las personas interesadas en el correspondiente procedimiento administrativo por cuanto, de aplicarse en sus propios términos este precepto legal, se les impediría acceder a datos e información que podría ser determinantes para su posición jurídica (17). Como pude comprenderse no se trata ni mucho menos de una cuestión menor, sobre todo en un contexto tecnológico como el actual donde precisamente la utilización de los medios electrónicos puede dar lugar a sorpresas sin duda curiosas. Basta simplemente con pensar en la facilidad con que se puede recopilar hoy día información basada en tratamientos de *big data* que, posteriormente, cabría utilizarse para iniciar un procedimiento sancionador sin que pudiera llegar a conocerse su origen y, en su caso, el contexto donde inicialmente figuraban los datos.

2.4 **La insuficiente regulación legal de las garantías tecnológicas**

La efectividad de las garantías jurídicas en un contexto digital descansa, en última instancia, en el cumplimiento de las garantías de naturaleza tecnológica. Desde esta premisa, no se contempla con nitidez y de manera tajante una obligación legal de carácter general en orden al cumplimiento del Esquema Nacional de Seguridad y del Esquema Nacional de Interoperabilidad, ya que el artículo 156 LRJSP no constituye, precisamente, un ejemplo de rigor en la exigencia de su cumplimiento; sobre todo si nos atenemos a la inexistencia de consecuencias concretas para su contravención en la regulación legal (18). En consecuencia, es preciso acudir a otras previsiones más específicas para reforzar la exigibilidad de las nomas técnicas, tal y como sucede singularmente con el archivo electrónico único –art. 17 LPAC–, el archivo electrónico de los documentos –art. 46 LRJSP–, las copias auténticas –art. 27 LPAC– y la remisión del expediente electrónico –art. 70.3 LPAC–. Sin embargo, el legislador estatal sí que se ha preocupado de establecer dicha exigencia de manera

(17) Cierco Seira, C.: «El "nuevo" procedimiento administrativo...», ob. cit., p. 110. En todo caso, se podría plantear que dicha información se incorpore al proceso judicial, aunque la principal dificultad radicaría en conocer su existencia (Velasco Rico, C. «Novedades…», ob. cit., p. 137).

(18) Por lo que se refiere a las posibilidades de impugnación, ciertamente muy restringidas por más que se pueda forzar la interpretación a nivel doctrinal, véase Fondevila Antolín, J.: «Seguridad en la utilización de medios electrónicos. El Esquema Nacional de Interoperabilidad», en E. Gamero (dir.), *Tratado de procedimiento administrativo común*…, tomo I, ob. cit., pp. 663-665.

clara, indubitada y exigible para las Comunidades Autónomas y las Entidades Locales al permitirles que utilicen sus propias plataformas y registros únicamente cuando, al margen de las consideraciones que contempla la disposición adicional segunda LPAC sobre estabilidad presupuestaria y eficiencia, se justifique el cumplimiento de los citados Esquemas.

Una valoración similar puede realizarse por lo que se refiere a la protección de los datos de carácter personal, en particular desde la perspectiva de la nueva regulación europea en la materia. En efecto, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 ha supuesto un cambio de gran trascendencia en el enfoque la tutela de este derecho, incorporando la exigencia de una serie de medidas funcionales, estructurales y organizativas tendentes a garantizar no ya sólo el mero cumplimiento formal sino, además y sobre todo, demostrar que efectivamente se respetan las medidas adoptadas. Desde esta perspectiva se abre una nueva etapa en la que resta por determinar qué consecuencias llevará aparejado el eventual incumplimiento de esta normativa por las entidades públicas; si bien, cualquier valoración que se pueda hacer al respecto dependerá en última instancia de la regulación que se establezca a nivel estatal. En concreto, el legislador español debería prestar una especial atención a las medidas de seguridad tanto tecnológicas como, asimismo, organizativas y funcionales, adoptando disposiciones contundentes dirigidas a garantizar el efectivo respeto a los datos personales de las personas físicas y, en general, a la protección de la información. Una postura tibia a nivel legislativo difícilmente podría considerarse compatible con el mandato del artículo 18.4 del Texto Constitucional.

3. ALGUNAS CLAVES JURÍDICAS EN LAS QUE HA DE SUSTENTARSE EL PROCESO DE TRANSFORMACIÓN DIGITAL DEL SECTOR PÚBLICO

Una vez advertidas las principales insuficiencias y disfuncionalidades del marco normativo vigente sobre el uso de medios electrónicos en el sector público es necesario adoptar una visión prospectiva que parta de la caracterización general de los proyectos e iniciativas que tienen por objeto no ya la mera modernización tecnológica sino, en definitiva, la transformación digital de las Administraciones Públicas y el resto de entidades que forman parte del sector público. Para ello resulta imprescindible superar una visión reduccionista que, tanto a nivel normativo como doctrinal, se ha sustentado principalmente en el acto y el procedimiento administrativos, perspectiva que ha resultado esencial desde que en el año 1992 se aprobase la primera regulación legal básica en la materia, pero que hoy día se

encuentra claramente superada por el actual estado de la tecnología (19). En consecuencia, es preciso ajustar el análisis jurídico a la realidad que nos plantea esta última pues, de lo contrario, no podrá afrontarse el proceso de transformación digital a que se enfrenta el sector público; o, lo que sería incluso más preocupante, dicho proceso se llevaría llevarse a cabo al margen de las garantías jurídicas, que podrían quedar confinado al mero cumplimiento formal y aparente de una serie de previsiones cuya eficacia sustantiva vinculante quedaría en gran medida desnaturalizada.

3.1 **Las nuevas premisas en las que se han de fundamentar las garantías jurídicas**

3.1.1 La necesaria transformación del procedimiento administrativo

El procedimiento administrativo constituye uno de los ejes en torno a los cuales se ha sustentado doctrinal y legalmente el correcto funcionamiento de las Administraciones (20), hasta el punto de que una de las principales causas de invalidez de los actos administrativos se refiere a la vulneración de las normas procedimentales. Nos encontramos, pues, ante una concepción del procedimiento como el cauce natural para la formación de la voluntad de la Administración Pública, esto es, un proceso de toma de decisiones que representa un método, de ahí que haya sido contemplado tradicionalmente como un mecanismo «formal», y haya operado más bien a modo de elemento auxiliar al servicio de la aplicación del Derecho.

El uso de medios electrónicos –y de manera más intensa incluso cuando se trata de la innovación– presenta una incidencia directa sobre esta concepción clásica del procedimiento ya que afecta a una de sus principales exigencias: que los sucesivos actos que lo integran se deban producir necesariamente en un determinado momento de la tramitación y, en concreto, tras la finalización de los anteriores; planteamiento que también se proyecta sobre su reflejo documental y, en concreto, la conformación de los expedientes (21). En consecuencia, resulta imprescindible ofrecer planteamientos doctrinales, interpretativos y regulatorios más flexibles que, sin

(19) Incluso, conceptos relativamente modernos, alumbrados por el legislador en 2007, como el de la sede electrónica ya se encuentran claramente desbordados por la realidad tecnológica, tal y como se destaca en Alamillo Domingo, I.: «La regulación de la tecnología: la superación del modelo papel como elemento de transformación digital innovadora», en I. Martín (coord.), *La reforma de la Administración electrónica: una oportunidad para la innovación desde el Derecho*, Instituto Nacional de Administración Pública, Madrid, 2017, pp. 80 y ss.

(20) Sobre esta idea, véase Ponce Solé, J.: *Deber de buena Administración y derecho al procedimiento administrativo debido*, Lex Nova, Valladolid, 2001, en especial pp. 108-118.

(21) Valero Torrijos, J.: *Derecho, Innovación y Administración electrónica*, Global Law Press, Sevilla, 2013, pp. 274 y ss.

pérdida de las garantías jurídicas, permitan dar respuesta a las posibilidades de innovación y transformación que facilitan las tecnologías de la información y la comunicación. En definitiva, se trata de alumbrar lo que se ha venido a denominar el procedimiento administrativo adecuado (22).

3.1.2 De los documentos a los datos

Desde la perspectiva de la gestión documental, la modernización tecnológica conlleva una consecuencia cuya trascendencia no se puede minusvalorar desde la perspectiva que ahora nos ocupa: no basta con limitarse a un mero cambio en el soporte y simplemente sustituir la gestión de los documentos en papel por sus equivalentes en soporte electrónico y, en definitiva, requerirlos y remitirlos por medios telemáticos (23). En efecto, el uso avanzado de medios electrónicos requiere inexcusablemente desvincular los datos del documento original donde se pudiesen contener y, de este modo, llevar a cabo su procesamiento independiente, lo que suscita el desafío de asegurar que las garantías generales de los documentos en cuanto a integridad y autenticidad puedan consagrarse incluso cuando se incorporen a otros documentos o sean objeto de tratamiento, sobre todo automatizado. Ahora bien, este tipo de planteamientos de gestión avanzada han de superar una difícil barrera, ya que la realidad actual en el sector público parte en gran medida de un modelo diseñado fundamentalmente para el ámbito de cada entidad e, incluso, para la unidad u órgano que tramite cada uno de los expedientes; más aún, para cada uno de los procedimientos específicamente considerado. En última instancia, la adecuada gestión de los datos no sólo constituye una exigencia para la eficacia de la actividad administrativa y la protección de los intereses jurídicos implicados sino, incluso, de las obligaciones, principios y derechos propios de la buena regulación (24).

3.1.3 La multiplicación de los actores en el contexto digital

Otra de las principales notas distintivas del actual desarrollo tecnológico en que se prestan los servicios electrónicos se refiere al incremento de la complejidad desde una perspectiva subjetiva, característica que aboca a la participación de diversos prestadores de servicios; a diferencia de

(22) Gamero Casado, E.: «Hacia la simplificación de los procedimientos administrativos: el procedimiento administrativo adecuado», en L. Míguez, M. Almeida y D. Santiago (coords.), *La simplificación de los procedimientos administrativos. Actas del IX Congreso de la Asociación Española de Profesores de Derecho Administrativo*, Escuela Gallega de Administración Pública, Santiago de Compostela, 2014, pp. 75 y ss.

(23) Valero Torrijos, J.: *Derecho, Innovación...*, ob. cit., pp. 300-303.

(24) Canals Ametller, D.: «El acceso público a datos en un contexto de transparencia y buena regulación», en D. Canals (ed.), *Datos. Protección, Transparencia y Buena Regulación*, Documenta Universitaria, Girona, 2016, pp. 19 y 20.

los parámetros en los que se había venido basando tradicionalmente la relación entre la Administración Pública y los ciudadanos, en la que la intermediación se limitaba básicamente a la actuación mediante representante. En consecuencia, resulta imprescindible que las regulaciones normativas tengan en cuenta esta singularidad y adopten las medidas tendentes a asegurar el correcto funcionamiento de las aplicaciones y sistemas de gestión de la información.

A este respecto ha de tenerse en cuenta una doble dimensión. De una parte, las implicaciones de esta constatación respecto de las entidades públicas, que han de cambiar los parámetros técnicos, organizativos y jurídicos en los que han venido asentando sus relaciones, esto es, sustancialmente a partir del procedimiento administrativo, los informes y los documentos formalizados. Y, de otra parte, es preciso constatar el creciente protagonismo de los sujetos privados, tanto los propios destinatarios de la actuación administrativa como, sobre todo, nuevos prestadores de servicios de intermediación imprescindibles en el contexto digital, especialmente dado el incremento de las interconexiones, tal y como demuestra paradigmáticamente el caso de las ciudades inteligentes (25).

3.1.4 El reduplicado protagonismo de los destinatarios: hacia la cocreación de servicios públicos

Con la popularización de la web 2.0 se puso de manifiesto que a los destinatarios de los servicios públicos no sólo se les debía reconocer una posición reforzada en cuanto al acceso a la información sino que, sobre todo, esta circunstancia les confería una función de singular protagonismo en el propio proceso de difusión (26). Pues bien, este cambio de paradigma está llamado a reforzarse en el actual contexto digital, donde ya no basta con que las entidades públicas adopten una posición de iniciativa y superioridad por cuanto la tecnología permite y facilita una relación más horizontal. Incluso, el uso de medios electrónicos supone un avance ciertamente cualificado en cuanto a esta relación (27), hasta el punto de que cabe afirmar que la tecnología puede actuar como un eficaz catalizador

(25) Valero Torrijos, J.: «Ciudades inteligentes y datos abiertos: implicaciones jurídicas para la protección de datos de carácter personal», *Istituzioni del federalismo. Rivista di studi giuridici e politici*, núm. 4, 2015, pp. 1030-1033.

(26) Cerrillo i Martínez, A.: «Web 2.0 y la participación ciudadana en la transparencia administrativa en la sociedad de la información», en L. Cotino (ed.), *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías*, Universidad de Valencia, 2011, pp. 131-148. Libro electrónico accesible en https://www.uv.es/cotino/elibertades2010.pdf#page=132 (último acceso: 28/02/2018).

(27) Soares Barbosa, L.: «Digital Governance for Sustainable Development», en A. K. Kar y otros, eds., *Digital Nations. Smart Cities, Innovation, and Sustainability*, Springer, Cham, 2017, pp. 85-93.

que sirva para reforzar los principios del Estado democrático de Derecho (28).

Pues bien, desde la perspectiva del Gobierno Abierto resulta imprescindible dar un paso adelante no ya por lo que se refiere a la transparencia y la participación sino, sobre todo, la colaboración. En ese sentido, la cocreación de los servicios públicos es un concepto que está comenzando a abrirse paso desde planteamientos ajenos al ámbito jurídico, de manera que resulta necesario enfocar sus contenidos y consecuencias desde el Derecho. A este respecto, aun cuando la innovación social y tecnológica parece abrirse paso tímidamente en el ámbito de la contratación pública, lo cierto es que resulta imprescindible superar las restricciones formales y conceptuales en que se sustenta el instrumento contractual; todo ello a la búsqueda de una mayor flexibilidad que en modo alguno puede sustentarse en las posiciones de exclusividad ni en la actividad de fomento directo a través de las subvenciones. Sin duda que la compra pública de innovación podría ser un instrumento adecuado, pero ciertamente insuficiente teniendo en cuenta que ha de servir para reforzar las exigencias de participación y de legitimación social, evitando así la consagración de sistemas autocráticos de tipo paternalista y tecnológico (29).

3.2 **El necesario alcance de las garantías jurídicas: una visión prospectiva**

A partir de las anteriores premisas y, en particular, teniendo en cuenta las singularidades de la tecnología expuestas, procede ahora apuntar cómo sería preciso reconfigurar las garantías jurídicas, de manera que el Derecho pueda cumplir de manera sustantiva y no meramente formal el papel que está llamado a desempeñar. Se trata, en definitiva, de intentar reconfigurar el equilibrio entre la innovación tecnológica y las garantías jurídicas como premisa inexcusable para facilitar la transformación digital del sector público sin menoscabo de la seguridad jurídica (30).

3.2.1 La aprobación formal de las aplicaciones, exigencia ineludible

La aprobación formal de las aplicaciones que utilizan las Administraciones Públicas y el resto de entidades del sector público para el ejercicio de sus competencias y, en particular, sus potestades no es una cues-

(28) Cerrillo i Martínez, A.: «El papel de los medios electrónicos en la lucha contra la corrupción», *Revista Vasca de Administración Pública*, núm. 104, 2016, pp. 199-235.

(29) Ramió, C.: *La Administración Pública del futuro (Horizonte 2050). Instituciones, política, mercado y sociedad de la innovación*, Tecnos, Madrid, 2017, p. 137.

(30) Sobre esta idea, véase Rivero Ortega, R.: «Gestión pública inteligente, innovación e información: oportunidades y riesgos del Big data administrativo», *Presupuesto y Gasto Público*, núm. 86, 2017, pp. 150-151.

tión menor carente de relevancia. Por esta razón, tal y como se ha señalado (31), la desaparición de esta exigencia en la regulación general de la Administración electrónica del año 2007 –confirmada tras la reforma de 2015– ha supuesto una clara regresión en la transparencia de la actuación administrativa y, en general, desde la óptica de la seguridad jurídica.

En concreto, la opción de su autorización a través de un acto administrativo se ha de concebir como una premisa esencial a fin de garantizar el pleno sometimiento de la actuación administrativa al Ordenamiento Jurídico. En última instancia esta es la vía a través de la cual tiene lugar la asunción formal por parte de la Administración y, en su caso, la entidad pública correspondiente, del resultado del funcionamiento de la aplicación informática, de modo que si no ha existido el acto de imputación no se garantiza, en definitiva y con las garantías jurídicas adecuadas, la responsabilidad por parte de la entidad a la hora de hacer suyas las decisiones o actuaciones que corresponden a su propio ámbito competencial; en particular, a través de la posibilidad de impugnar formalmente una decisión que no ha existido en términos jurídicos.

3.2.2 Transparencia más allá de las previsiones legales

En los últimos años hemos asistido al proceso de puesta en marcha de una novedosa regulación sobre transparencia y acceso a la información del sector público que, al menos en mi opinión, ha de considerarse excesivamente restrictiva en cuanto al objeto, las limitaciones y, sobre todo, las garantías que establece. Esta insuficiencia –que por otra parte no resulta sorprendente, puesto que entronca con la tradición española en la materia (32)– resulta especialmente grave cuando se refiere a la temática de este trabajo, tanto desde una perspectiva objetiva (33) como, asimismo, de los planteamientos de innovación tecnológica (34).

(31) Cantero Martínez, J.: «El principio de transparencia en la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos», en J. L. Piñar (dir.), *Administración electrónica y ciudadanos*, Thomson-Reuters, Civitas, 2011, pp. 320-321.

(32) Boix Palop, A.: «Spanish administrative traditions in the context of European common principles», en M. Ruffert, ed., *Administrative Law in Europe. Between Common Principles and National Traditions*, Europa Law Publishing, Groningen, 2013, p. 93.

(33) Muñoz Soro, J.F. y Bermejo Latre, J.L.: «La redefinición del ámbito objetivo de la transparencia y el derecho de acceso a la información del sector público», en J. Valero y M. Fernández (coords.), *Régimen jurídico de la transparencia del sector público*: *del derecho de acceso a la reutilización de la información*, Thomson-Reuters-Aranzadi, Cizur Menor, 2014, pp. 195-198.

(34) Martín Delgado, I.: «Transparencia, reutilización y datos abiertos. Algunas reflexiones generales sobre el acceso libre a la información pública», en J. Valero y M. Fernández (coords.), *Régimen jurídico de la transparencia*…, ob. cit., pp. 385-390. Más reciente, incorporando el análisis de la reforma de 2015, Valero Torrijos, J.: «El acceso y la reutilización de la información del Sector Público desde la perspectiva de la reforma de la Administración electrónica», en I. Martín (coord.), *La reforma de la Administración electrónica*..., ob. cit., pp. 433 y ss.

Pues bien, teniendo en cuenta la singular incidencia que tiene la tecnología en la posición jurídica de los ciudadanos, la garantía relativa a la transparencia y el acceso a la información debería ser completada con el reconocimiento expreso a nivel normativo –o, al menos, como una exigencia hermenéutica de la garantía constitucional que se establece para la defensa de los derechos e intereses legítimos– de un derecho más extenso del que contempla la vigente legislación sobre transparencia y, asimismo, la regulación legal del expediente administrativo. En concreto, la complejidad tecnológica actual exige que pueda obtenerse toda aquella información que permita la identificación de los medios y aplicaciones utilizadas, así como del órgano bajo cuyo control permanezca el funcionamiento de la aplicación o el sistema de información; debiendo incluir en su objeto, asimismo, no sólo el conocimiento del resultado de la aplicación o del sistema informativo que le afecte específicamente a su propio círculo de intereses sino, además y sobre todo, el origen de los datos empleados y la naturaleza y el alcance del tratamiento realizado, es decir, cómo el funcionamiento de aquellos puede dar lugar a un determinado resultado.

3.2.3 Efectivo cumplimiento de las normas técnicas

La especial incidencia de los elementos tecnológicos en la actividad de las entidades que integran el sector público requiere que las garantías jurídicas se encuentren plenamente adaptadas a la singularidad que aquellos plantean y, además, que su incumplimiento acarree de manera efectiva consecuencias proporcionadas a la gravedad del mismo. Como en páginas anteriores se ha razonado, la reforma de 2015 ha supuesto una inadmisible regresión que, no obstante, en otros aspectos podría calificarse como una opción legislativa simplemente inadecuada. Lejos de minimizar las consecuencias del incumplimiento de tales normas técnicas, su respeto debería constituir una exigencia ineludible para las entidades públicas incluso si esta medida obliga a paralizar servicios públicos ya que, de lo contrario, se estaría dando carta de naturaleza jurídica al menosprecio de las normas técnicas cuando es precisamente su exigencia rigurosa la que en última instancia puede ayudar a reforzar las garantías jurídicas (35).

(35) Valero Torrijos, J.: «Seguridad, tecnología y Administración Pública electrónica: la necesaria reconfiguración del alcance de las garantías jurídicas ante la innovación tecnológica», en J. R Gil-García y otros (eds.), *Tecnologías de Información y Comunicación en la Administración Pública: Conceptos, Enfoques, Aplicaciones y Resultados*, Infotec, México, 2017, pp. 142 y 143. El trabajo se encuentra accesible en https://www.infotec.mx/work/models/infotec/Resource/1274/1/images/cap5.pdf (última visita: 28/02/2018).

Así pues, resulta de gran relevancia llevar a cabo un proceso –tanto a nivel normativo, jurisprudencial y doctrinal– de decantación de las consecuencias jurídicas que supone la vulneración de las normas técnicas, especialmente las relativas a seguridad. En efecto, de nada sirve con la mera previsión en disposiciones jurídicas de las garantías tecnológicas si las consecuencias del incumplimiento no se encuentran aseguradas suficientemente. En consecuencia, al margen de las implicaciones referidas a la invalidez de los actos (36), se debería reconocer normativamente de manera expresa la potestad de inmovilización de las aplicaciones y los sistemas de información en aquellos supuestos de incumplimiento más grave de las reglas de seguridad, especialmente si pueden verse afectados los derechos y libertades de los ciudadanos o la correcta adopción de las decisiones administrativas. No obstante, nada impide que, teniendo en cuenta las concretas circunstancias del caso, dicha decisión pueda adoptarse provisionalmente por el órgano judicial –o incluso administrativo– en aplicación del régimen jurídico general sobre las medidas cautelares.

3.2.4 La interoperabilidad y su importancia para la perspectiva jurídica

El análisis de la interoperabilidad en el contexto de la Administración electrónica ha sido una de las principales aportaciones de la doctrina a la hora de afrontar la reconfiguración de las garantías jurídicas. En este sentido, los varios y destacados trabajos realizados sobre la interoperabilidad (37), combinados con los que se han centrado en la automatización (38), nos ayudan a sentar las bases dogmáticas a partir de las cuales abordar una reconfiguración del principio en su dimensión jurídica: de una parte ampliando su alcance en los términos de los cambios de para-

(36) Sobre estas implicaciones, véase Palomar Olmeda, A.: *La actividad administrativa efectuada por medios electrónicos*, Aranzadi, Cizur Menor, 2007, pp. 268-275; Valero Torrijos, J.: *Derecho, Innovación…*, ob. cit., pp. 198-203; Cacharro Gosende, F. y Marquina Fuentes, J.: «La aplicación de las causas de invalidez de los actos administrativos en el marco del expediente electrónico», en C. Campos (dir.), *El nuevo procedimiento administrativo local tras la Ley 39/2015*, Wolters-Kluwer-El Consultor, Madrid, 2016, pp. 387-393; así como Menéndez Sebastián, E.: *Las garantías del interesado en el procedimiento administrativo electrónico*, Tirant lo Blanch, Valencia, 2017, pp. 101 a 108.

(37) Por todos, Cerrillo i Martínez, A.: «Cooperación entre Administraciones Públicas para el impulso de la Administración electrónica», en E. Gamero Casado y J. Valero Torrijos (coords.), *La Ley de Administración electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*, 3.ª ed., Thomson-Aranzadi, Madrid, pp. 757-810; Gamero Casado, E.: «Administración electrónica e interoperabilidad», en I. Martín (dir.), *La reforma de la Administración electrónica: Una oportunidad para la innovación desde el Derecho*, Instituto Nacional de Administración Pública, Madrid, 2017, pp. 500-517; Martínez Gutiérrez, R.: *El régimen jurídico del nuevo…*, ob. cit., pp. 68-78.

(38) *Cfr.* Palomar Olmeda, A.: *La actividad administrativa…*, *ob. cit.*, pp. 59 y ss.; I. Martín Delgado: «Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada», *Revista de Administración Pública*, núm. 180, 2009, pp. 353-386; J. Valero Torrijos: *Derecho, Innovación…*, ob. cit., 67-71.

digma examinados y, de otra, concretando su alcance efectivo para garantizar que, más allá de planteamientos genéricos y abstractos, su inobservancia conlleve consecuencias concretas que permitan fortalecer las garantías jurídicas.

En efecto, por lo que se refiere a la protección de los datos personales, la intensificación de las interconexiones requiere una perspectiva más amplia de la gestión de la información que no se centre exclusivamente en el consentimiento de los afectados o en la mera previsión formal de una habilitación legal. Desde otra perspectiva, las exigencias de las ciudades inteligentes, los proyectos colaborativos, el *big data* o la inteligencia artificial exigen de un replanteamiento más amplio de las garantías jurídicas desde parámetros mejor adaptados a la gestión avanzada de la información que permitan superar los temores que alimentan la desconfianza mutua (39). Por último, no es posible basar la tutela de los ciudadanos únicamente en el derecho fundamental a la protección de datos, ya que no sólo se sustenta en una lectura excesivamente restrictiva de la dicción literal del texto constitucional (40) sino que, además, puede tener consecuencias indeseables en cuanto a la efectividad de las garantías que está llamado a asegurar el legislador con el mayor nivel de protección constitucional ya que, en última instancia, conlleva una interpretación reduccionista del alcance que ha de tener el artículo 18.4 de la Norma Fundamental según sus propias palabras.

Así pues, desde la perspectiva del contenido de este principio y la exigencia de concreción antes aludida, la dimensión jurídica de la interoperabilidad ha de ir más allá de la mera actividad reguladora y, por tanto, desde planteamientos inexcusables de buena gobernanza (41) debería proyectarse sobre la efectiva integración de las garantías jurídicas en las perspectivas semántica, organizativa y técnica del principio.

4. REFLEXIÓN FINAL

La innovación tecnológica no puede consistir en un fin en sí mismo sino que, por el contrario, ha de convertirse en una herramienta esencial que ayude a transformar el sector público. Sin embargo, existe el riesgo de que la tensión entre eficacia, eficiencia y garantías jurídicas se decante definitivamente a costa de estas últimas, ya que ante las posibilidades de innovación que permite la tecnología pueden percibirse como un obstácu-

(39) García Macho, R.: «Procedimiento administrativo y sociedad de la información y el conocimiento», en J. Barnés, ed., *La transformación del procedimiento administrativo*, Global Law Press, Sevilla, p. 221.

(40) Martínez Martínez, R.: *Una aproximación crítica a la autodeterminación informativa*, Thomson-Citivas-APDCM, Madrid, 2004, pp. 343-347.

(41) Gamero Casado, E.: «Administración electrónica e interoperabilidad», ob. cit., pp. 513 y 514.

lo sin sentido. Más aún si las normas jurídicas, la práctica judicial y los parámetros doctrinales no se adaptan a la singularidad del contexto digital, de manera que incluso se pueda llegar a plantear que los requerimientos jurídicos carecen de sentido por considerarse obsoletos. Sólo partiendo de la constatación de este problema es posible ofrece respuestas adecuadas que ayuden a recuperar el auténtico papel que corresponde al Derecho –y sobre todo al Derecho Administrativo– en la actual sociedad de la información y el conocimiento.

CAPÍTULO 18

EL DERECHO DE ACCESO A INTERNET

PABLO GARCÍA MEXÍA, J. D., PH. D.
Jurista digital. Letrado de las Cortes. Of Counsel, Ashurst LLP.
Vicepresidente de Internet Society (Capítulo español)

1. INTERNET COMO RED ABIERTA

De entre los diversos rasgos que explican el fulgurante éxito de Internet (1) (descentralización, flexibilidad gracias a la conmutación de paquetes, simplicidad «extremo a extremo»), probablemente el de mayor relevancia, al menos a los fines del presente Capítulo, es la extrema compatibilidad del protocolo TCP/IP con otras redes (2).

Internet se diseña desde su inicio compatible porque se pretende que incorpore otras redes y otros dispositivos (3). Una red que en sus comienzos apenas si vinculaba a unos cuantos científicos y centros académicos, logra por ello mismo escalar exponencialmente, y en muy poco tiempo, hasta convertirse en el recurso esencial que hoy es (Post 2009, 60-89). Internet triunfa pues gracias a su apertura. E Internet es consustancialmente abierta.

Si ello es así, el acceso a Internet debe también, casi «por naturaleza», considerarse abierto. Sus creadores no le pusieron traba alguna. Ha sido ese éxito sobrevenido e inesperado por sus inventores el que ha ido generando barreras. A estas barreras, a sus posibles remedios y al futuro de unas y otros dedicamos este Capítulo.

---

(1) Motivos de edición han llevado a esta ubicación de la bibliografía del capítulo, que es la siguiente: J. Abbate (1999), *Inventing the Internet. Inside Technology*, Cambridge, Mass.: MIT Press; R. Baena Zapatero (2018), «Big Data y Derecho de la competencia», ponencia presentada en el seminario *Big data, privacidad y competencia*, Ashurst, Madrid, 28 de febrero de 2018; M. Barrio Andrés (2017), *Fundamentos del Derecho de Internet*, Madrid: Centro de Estudios Políticos y Constitucionales; P. De Filippi (2016), «The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies», *Journal of Peer Production*, 2016, https://hal.archives-ouvertes.fr/hal-01382006/document; P. García Mexía (2017), *La Internet Abierta. Retos regulatorios de una Red nacida libre*, Madrid: RDU; (2014), *Derechos y libertades, Internet y TICs*, Valencia: Tirant lo Blanch; P. García Mexía y C. Perete Ramírez (2018), «Internet y el Reglamento General de Protección de Datos», en J. López Calvo, coord., *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, Las Rozas de Madrid: Wolters Kluwer; D. Hunter (2003), «Cyberspace as Place and the Tragedy of the Digital Anticommons», *California Law Review*, vol. 91, pp. 447 y ss.; G. Huston (2012), «The Concept of Quality of Service in the Internet», https://goo.gl/JCYfMX; (2010), «A Rough Guide to Address Exhaustion (in 12 easy questions)», September 2010, http://goo.gl/1m1yoa; M. Mueller, D. L. Cogburn, J. Mathiason, J. Hofmann (2007), «Net Neutrality as Global Principle for Internet Governance», *GigaNet: Global Internet Governance Academic Network, Annual Symposium 2007*, https://ssrn.com/abstract=2798314; D. Post (2009), *In Search of Jefferson's Moose. Notes on the State of Cyberspace*, Oxford University Press; A. Preukschat (2017), «La descentralización de Internet y la identidad digital», en A. Preukschat, coord., *Blockchain: La Revolución industrial de Internet*, Barcelona: Gestión 2000.

(2) *Cfr.* García Mexía (2012, 57).

(3) Así lo hace ver Vinton G. Cerf, uno de los dos inventores del propio protocolo TCP/IP, y por ello de Internet, en el delicioso prólogo a mi obra: *La Internet abierta. Retos regulatorios de una Red nacida libre*, Madrid: RDU, 2017.

2. LAS AMENAZAS A LA INTERNET ABIERTA

Las barreras a la apertura se han venido proyectando sobre las tres grandes facetas de Internet: lógica (estándares y protocolos), física (infraestructura de comunicaciones electrónicas) y humana (aplicaciones y contenidos) (4).

2.1 **La gobernanza estatalista de Internet**

El peculiar modo como Internet se gobierna a escala mundial está inexorablemente marcado por las singularidades de esa capa lógica recién citada. Uno y otra vienen sufriendo presiones políticas muy intensas desde el mismo origen de la Red, presiones que se han acentuado con el arranque del siglo XXI. Y que por supuesto inciden decisivamente sobre el acceso a Internet.

Internet se gobierna a través de ICANN (Internet Corporation for Assigned Names and Numbers), un organismo no gubernamental, pero que desde su origen mantuvo un vínculo contractual con el Departamento de Comercio de los EE. UU. (a resultas de que Arpanet, la «red madre» de Internet, nació a fines de los cincuenta de la cooperación entre el Departamento norteamericano de Defensa y un grupo de cinco universidades del oeste de aquel país). ICANN gestiona el llamado sistema de nombres de dominio (DNS), verdadera «llave» de la Red, en cuanto que los nombres de dominio, gracias a su correspondencia con las llamadas direcciones IP (5), hacen posible que Internet localice en su interior los puntos concretos entre los que se ha de establecer comunicación.

Pese al inicial vínculo de ICANN con el gobierno estadounidense, la gestión cotidiana de la Red vino obedeciendo a pautas primordialmente técnicas, gracias a su vez a la intensa colaboración entre ICANN y otro ente clave, el IETF (Internet Engineering Task Force), auténtico núcleo tecnológico de Internet, en cuyo seno se elaboran los estándares y protocolos que la hicieron nacer. A la vez, ICANN aglutina en órganos internos de asesoramiento a representantes de gobiernos, empresas y sociedad en general, lo que ha permitido bautizar este esquema de gestión como «modelo multilateral» («multistakeholder»).

Todo ello explica que, desde hace algunos años, ICANN haya sido el foco principal de controversia, y por qué no decirlo, de lucha abierta, a

(4) Un ejemplo tan reciente como relevante de estas tres facetas de Internet, tan destacadas a efectos expositivos en las Ciencias Sociales, puede hallarse en el Manual de Tallin, el texto mundial de referencia sobre la regulación de la ciberguerra y la ciberdefensa, el cual lo emplea para definir de este modo el ciberespacio. El Manual publicaba en 2017 su segunda edición, el llamado Manual de Tallin 2.0. *Cfr. Tallinn Manual 2.0 on the International Law Applicable to Cyberoperations*, Cambridge University Press, 2017.

(5) Quizá por extraordinariamente simple, la mejor definición de dirección IP que he manejado es la del tecnólogo australiano Geoff Huston (2010), quien la concreta como «end-point identifier» (o «identificador de extremo»).

propósito del gobierno de Internet (6). La controversia y la pugna en el seno de la Cumbre mundial se basa en la pretensión de determinados países emergentes (en especial China y Rusia) de privar a los EE. UU. de su hasta entonces posición hegemónica en el gobierno de la Red (gracias al indicado vínculo con ICANN). En otros términos, se trataba de poner fin al modelo multilateral, para transformarlo en otro que, bajo la veste de las Naciones Unidas, permitiera un mayor control por parte de los Estados.

Ese mayor control estatal debía por supuesto proyectarse en el DNS, que dejaría de operar con arreglo a esos criterios exclusivamente técnicos originarios, para comenzar a ser permeable a pautas políticas, dependientes de las necesidades de cada Estado. Sobra decir el resultado que esta pretensión habría generado sobre el acceso a la Red, especialmente en países carentes de libertades. Internet habría quedado «balkanizada» en mucho mayor medida de lo que ya lo está y además de un modo prácticamente repentino (7).

2.2 **Tensiones procedentes de los proveedores de acceso a Internet**

Junto a factores como el desnivel regulatorio frente a los proveedores de contenidos (cuyos mayores, aunque evidentemente no únicos, exponentes son sin duda las denominadas empresas GAFAM) (8), la pugna por un mismo mercado de servicios digitales ha venido conduciendo a los operadores de comunicaciones a reivindicar frente a aquéllas, singularmente las gigantes norteamericanas, acuerdos económicos compensatorios por el uso de su infraestructura de red. Y frente al regulador –ya sea a escala global (Unión Internacional de Telecomunicaciones, UIT) (9), ya europea, ya nacional–, medidas regulatorias de «reequilibrio».

Este trasfondo tiene su reflejo frente a los usuarios, a propósito del acceso a Internet. Por principio, y evidentemente, los operadores están del todo interesados en que ese acceso se produzca del modo más generalizado posible, pues son al cabo sus redes las que se emplean a tal fin. Donde en cambio surgen los problemas es a propósito de la calidad de ese

(6) Esa controversia se hizo patente en un foro auspiciado por las Naciones Unidas (más concretamente, por el organismo especializado de ellas dependiente, la Unión Internacional de Telecomunicaciones o UIT): la llamada Cumbre mundial sobre la sociedad de la información, que se celebra regularmente desde 2003. *Cfr*: http://goo.gl/NO3ky.

La reunión de la Cumbre celebrada en Túnez en 2006 creaba a su vez otro ámbito de discusión más específico, el llamado Foro para la Gobernanza de Internet, *cfr*: http://www.intgovforum.org

(7) Un panorama general de este «astillamiento» de Internet puede encontrarse en la obra del consultor estadounidense Scott Malcomson, *Splinternet How Geopolitics and Commerce are Fragmenting the World Wide Web.* Or Books: 2017. Éste es por otro lado el planteamiento general de García Mexía (2012).

(8) Acrónimo de creciente difusión alusivo a Google, Apple, Facebook, Amazon y Microsoft.

(9) G. Huston (2012) llega incluso a referirse a una afinidad de intereses entre proveedores de acceso y reguladores, que fraguó en el plano internacional, de la mano del intento de los operadores de consagrar la noción de «calidad de servicio» en las International Telecommunications Regulations (ITRs) de la UIT.

acceso, en un doble sentido. Por un lado, los operadores están obligados a garantizar dicha calidad, lo que a su vez genera evidentes tensiones de precios (10). Por otro, los proveedores de acceso vienen blandiendo la noción de «calidad de servicio», con el principal fin inmediato de gestionar sus redes del modo necesario para prestar los llamados «servicios especializados u optimizados», a su vez orientados a competir frente a los proveedores de contenidos. En lo que aquí interesa, es la llamada calidad de servicio el problema principal, al poder entrar en pugna con lo que más adelante denominaremos «acceso justo» a Internet, al tiempo bien jurídico principal de la normativa sobre neutralidad de la Red.

2.3 «Velos» y «vallas» sobre contenidos de la Red

El acceso a Internet se ve asimismo amenazado por la presión sobre sus contenidos (aplicaciones y servicios). Dicha presión puede obedecer a políticas públicas, lógicamente procedentes de gobiernos: son los que llamamos «velos» sobre el contenido de Internet. O bien puede tener orígenes económicos: son las «vallas» que impiden que los contenidos fluyan sin obstáculos por la Red.

2.3.1 Los «velos»: el bloqueo político de contenidos

Por razones de políticas públicas, y con mayor o menor amparo legal, gobiernos de todo signo, democráticos y no democráticos, recurren con cada vez más frecuencia al bloqueo de contenidos en Internet. No es éste el lugar para dilucidar la mayor o menor legitimidad de estas medidas, que de ordinario dan lugar a órdenes judiciales (o resoluciones administrativas), y que pueden justificarse con argumentos como la protección de la seguridad nacional (11), la salvaguarda de la privacidad de terceros (12), la propiedad intelectual e industrial (13), hasta un largo etcétera. Tampoco es éste el lugar para calibrar su posible legitimidad, en función de que, conforme al

(10) Esta perspectiva encontró acomodo desde 2002 en la legislación europea de comunicaciones electrónicas, de la mano del concepto jurídico de «acceso funcional a Internet» (a propósito del servicio universal de telecomunicaciones), más tarde previsto en la Directiva 2009/136/CE, de 25 de noviembre de 2009, de servicio universal (art. 1.3); y, en España, en la Ley 9/2014, de 9 de mayo, general de telecomunicaciones (art. 25.1.a) y disp. adicional 18.ª).

(11) En contextos democráticos, es paradigmática en esta línea la *Patriot Act* norteamericana de 2001, con sus diversas reformas posteriores. En España, basta citar las reformas introducidas en la Ley de enjuiciamiento criminal por la Ley orgánica 1/2015, de 30 de marzo.

Tan relevante como polémica en este sentido, la ley alemana que obliga a las redes sociales a retirar en 24 horas contenidos ofensivos o ilegales, en particular de discurso de odio o «noticias falsas-fake news». *Cfr. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz-NetzDG)*, de 01.09.2017, en vigor desde 01.01.2018.

(12) Un ejemplo claro sería el derecho al olvido [art. 17 Reglamento (UE) 2016/679, comúnmente conocido como RGPD], siendo justamente la censura el riesgo de crearlo, como el Abogado General del caso *Mario Costeja c. Google* (C-131/12) advirtió en sus conclusiones ante el TJUE de 25 de junio de 2013.

(13) Claro ejemplo es el inacabable rosario de cierres de webs a resultas de las descargas ilegales de contenidos que se vienen produciendo en Internet desde mediados de los noventa.

ordenamiento de que se trate, la medida en cuestión respete los principios y el procedimiento legalmente establecidos. El derecho de la UE prevé de hecho estos supuestos como una de las excepciones al principio de neutralidad de la Red, en el bien entendido de que la gestión de tráfico que los proveedores de acceso lleven a cabo con esta cobertura de «cumplimiento de legislación de la UE o nacional (o de medidas que pretendan darle efecto)» habrá de respetar la Carta de Derechos Fundamentales de la UE, y en particular su artículo 52, que requiere que dicha legislación (o las medidas) se hayan dictado legalmente y que respeten la esencia de dichos derechos y libertades (14).

El único motivo para tratar aquí esta cuestión es poner de manifiesto que el bloqueo por políticas públicas constituye indiscutiblemente una barrera, por más que pueda ser legal y legítima, para el acceso a la Red.

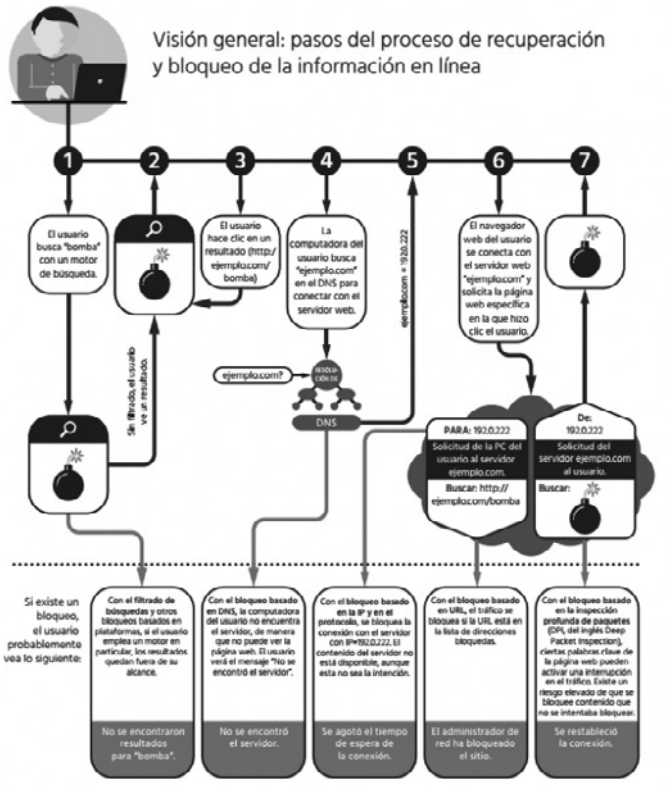
En lo que aquí importa, el bloqueo por políticas públicas se puede llevar a efecto a escala nacional o en el plano de los proveedores de servicios (ya sean éstos de acceso o de contenidos) (Internet Society 2017) (15). En el primero, bien se bloquean contenidos de la Red a partir de un «cuello de botella» centralizado controlado por el gobierno en cuestión (es el modelo de Irán); bien se efectúa el bloqueo, siempre a lo largo y ancho del territorio nacional de que se trate, por parte de proveedores de servicios que siguen las instrucciones políticas del gobierno (es el modelo chino). Sobra decir que, debido a su naturaleza sistemática, este tipo de bloqueo a escala nacional solo es propio de regímenes no democráticos. El bloqueo meramente basado en la actuación de los proveedores de servicios es en cambio el empleado también en los países democráticos, cuando las autoridades requieren actuaciones basadas en disposiciones legalmente previstas.

Cinco son las principales técnicas de bloqueo de contenidos por razones políticas (Internet Society 2017): a) Bloqueo basado en el protocolo y en la IP, gracias a barreras en la Red, que bloquean todo el tráfico hacia un grupo de direcciones IP. b) Bloqueo basado en la inspección profunda de paquetes (DPI), que usa dispositivos entre el usuario final y el resto de Internet para filtrar por contenido, patrones o tipos de aplicaciones específicos. c) Bloqueo basado en el URL, merced a un filtro que intercepta el flujo de tráfico web (HTTP) e intercepta la URL que aparece en la solicitud HTTP, si ésta se encuentra incluida en una base de datos local o en un servicio en línea. d) Bloqueo basado en plataformas (motores de búsque-

(14) Así lo apunta el órgano que agrupa a los reguladores europeos de comunicaciones electrónicas (BEREC), en su interpretación de la disposición que establece esa excepción, el artículo 3.3.a) del Reglamento (UE) 2015/2120, sobre Internet abierta (BEREC 2016, 21).

(15) Internet Society (2017) hace notar que uno de los modos más eficaces de bloquear contenido no deseado es llevarlo a cabo en la red local o incluso en el dispositivo del usuario («punto de conexión») (ej. software antimalware, o de control parental, o de bloqueo de contenidos pornográficos). El bloqueo por políticas públicas, sin embargo, no se lleva a cabo en puntos de la Red tan cercanos al usuario.

da, aunque también redes sociales o tiendas de aplicaciones móviles), previo acuerdo con la autoridad nacional en cuestión. e) Bloqueo basado en el DNS, en que el tráfico DNS se desvía a un servidor de DNS modificado, que bloquea las búsquedas de ciertos nombres de dominio.



Fuente: Internet Society, goo.gl/wCCstz

2.3.2 Las «vallas»: La Internet de las grandes plataformas

Sir Tim Berners-Lee lleva años denunciando cómo empresas de importancia decisiva para la Red, como las citadas GAFAM (aunque también algunas de las principales operadoras de telecomunicaciones), estarían propiciando la fragmentación de Internet en múltiples «silos» de datos (sus propias plataformas), datos que, aun cuando sean suyos, el usuario no puede trasladar de un sitio online a otro (16).

(16) Tim Berners-Lee, «Long Live the Web: A Call for Continued Open Standards and Neutrality», *Scientific American Magazine*, diciembre de 2010, goo.gl/xKsQNy.

Más allá de la amenaza que todo ello supone para la privacidad del usuario, es claro que esta fragmentación va en contra de la apertura de Internet y por ende supone una traba para un acceso libre.

3. LA SALVAGUARDA DEL ACCESO A INTERNET

La panoplia de amenazas al acceso a Internet que se ha expuesto ha ido suscitando respuestas en dos grandes planos, territorial (con remedios a escala global, regional o nacional) y funcional (según que se trate de salvaguardar la capa lógica, la infraestructura de comunicaciones o los contenidos de Internet).

3.1 **La gobernanza multilateral de Internet**

Ante la presión más atrás narrada de China, Rusia y otros países emergentes en favor de una estatalización de la gobernanza de Internet, la posición de España, como la del resto de sus socios en la Unión Europea, ha venido siempre siendo la de mantener el actual modelo multilateral de gobierno de Internet, como la fórmula más compatible con su naturaleza de red abierta (17).

Por otro lado, y sin duda como respuesta a esta presión, la Administración del Presidente norteamericano Barack Obama decidía el 14 de marzo de 2014 abrir un proceso para transferir las funciones de última garantía sobre el DNS que hasta entonces los EE. UU. venían ejerciendo (18). Dicho proceso fraguaba en una cumbre que ICANN celebraba entre el 5 y el 10 de marzo de 2016 en Marraquech (su 55.ª Reunión), de la que salió un acuerdo que establece en lo esencial un esquema de gobierno basado en «ciudadanía» (un pluriverso de organismos consultivos y de apoyo en representación de los distintos sectores interesados), un «ejecutivo» (la Junta de gobierno) y un poder «judicial» (en cuanto que proceso de revisión independiente), todos ellos con participación «multilateral» de gobiernos, empresas y comunidad de Internet; nota muy importante es que los gobiernos solo han de ser expresamente consultados si así lo exigiera

---

Al denunciar esto, el padre de la World Wide Web reactivaba una discusión académica que ya se suscitó en los EE. UU. a mediados de los años noventa: su principal exponente, el profesor Dan Hunter (2003), definía esta misma idea como «la tragedia de la tabicación de la Red» («the tragedy of the digital anti-commons»).

(17) Ambas posturas volvieron a evidenciar su pugna en la reunión del Foro para la Gobernanza de Internet celebrada en Nairobi en septiembre de 2011, así como en la de la Conferencia Mundial sobre las Telecomunicaciones Internacionales, celebrada bajo los auspicios de la UIT en Dubai en diciembre de 2012.

Sobre los orígenes tecnológicos del problema, *cfr.* J. Abbate (1999).

(18) http://goo.gl/1bUwXY.

por unanimidad, respecto de alguna determinada decisión, el órgano consultivo en que éstos están representados (19).

En síntesis, y en lo que aquí interesa, el balón de oxígeno que el modelo multilateral lograba en Marrakech en 2016 ha supuesto por tanto evitar que el DNS hubiera podido convertirse en lo que los pioneros de Internet jamás, ni de lejos, pensaron que pudiera llegar a ser, una traba para el acceso libre a Internet.

3.2 **El acceso a Internet, derecho ciudadano**

Desde comienzos del siglo XXI, la garantía del acceso a la infraestructura física, que a su vez permite acceder a Internet, se ha instrumentado en forma de auténtico derecho ciudadano, el derecho de acceso a la Red (20).

Varias organizaciones internacionales han venido considerando el acceso a Internet como un derecho básico: es el caso de la Unión Europea, desde el paquete de directivas sobre telecomunicaciones del año 2002; o la Organización para la Seguridad y la Cooperación en Europa (OSCE), desde 2011 (21).

También las propias Naciones Unidas, a través de dos iniciativas: una de ellas calificaba el acceso a Internet como un derecho instrumental, consecuencia de la libertad de expresión, a raíz de un informe de mayo de 2011 de la Oficina del Alto Comisionado para los Derechos Humanos (22); otra, más relevante y asimismo más reciente, fue la Resolución del Consejo de Derechos Humanos de las Naciones Unidas de 5 de julio de 2012, en cuanto proclama que los mismos derechos que las personas tienen «offline» deben también protegerse online, en particular la libertad de expresión (23).

Mientras que diversos Estados han ido dando pasos relevantes en igual sentido. Por una parte, y en la misma línea de la UE y la OSCE, una serie de países introdujeron el acceso a Internet como un derecho básico: se trataba de Estonia desde 2000, Grecia desde 2001 (lo hizo incluso como un derecho constitucional), España y Finlandia desde 2003, o Alemania desde 2004, por solo citar los más relevantes.

En otros países, la vía seguida fue la citada de Naciones Unidas en su documento de 2011: reconocer el acceso a Internet como derecho instru-

(19) Una excelente síntesis del acuerdo de Marrakech puede encontrarse en: *The Economist*, «We the Networks», 5 de marzo de 2016, http://goo.gl/IgZ4LJ.

(20) Un derecho que por cierto no se ha de confundir con otro más específico, clásicamente encuadrado en el elenco de derechos de la protección de datos, el de acceso a los datos (art. 15 RGPD).

(21) *Cfr*: http://goo.gl/ejCFA

(22) *Cfr*: http://goo.gl/jWMFr.

(23) *Cfr*: http://goo.gl/Ek47z

mental derivado de la libertad de expresión; los ejemplos más relevantes son los de Portugal, Rusia o Ucrania (24). En este grupo destaca el caso de Francia, donde los tribunales han sido decisivos para considerar el acceso a Internet como derecho derivado de la libertad de expresión, desde 2009 (25).

Un paso más allá lo daban Finlandia en octubre de 2009 (26) y España, en marzo de 2011, al conceder un derecho de acceso a Internet, no por cualquier medio, sino por banda ancha, es decir, de alta velocidad, con un mínimo de 1 Mb por segundo en sentido descendente (27). De nuevo Finlandia avanzaba aún más y en 2015 consagraba un derecho de acceso a Internet con conexión de 100 Mb por segundo en sentido descendente.

Es justamente el carácter vital de Internet en la sociedad actual (reconocido por el propio Tribunal Europeo de Derechos Humanos en el citado caso *Ahmet Yildirim*) lo que a mi juicio basta y sobra para propugnar el acceso a Internet como un auténtico derecho ciudadano, *autónomo* respecto de cualesquiera otros derechos o libertades (incluidas las libertades de expresión e información). Además, el acceso a la Red garantiza, no solamente el ejercicio de las libertades de expresión e información, sino el de tantas otras, desde la de pensamiento o el derecho de asociación o a la participación política, hasta la libertad de empresa, por no mencionar más que estos ejemplos.

Quizá también por ello, un texto de importancia clave, la Guía de derechos humanos para usuarios de Internet del Consejo de Europa (2014) (28), lo ha incluido entre sus postulados. Y lo ha hecho reivindicando además un acceso libre de discriminaciones, a lo que en consecuencia sería una Red neutral (29). Esa Red neutral debe garantizar lo que podríamos denominar un derecho de acceso (a ser posible, de alta velocidad) «libre de brechas digitales», es decir, sin discriminación alguna por razón de edad, sexo, discapacidad, lugar de residencia o cualquier otra condición. En una palabra, un acceso *justo* (30).

---

(24) *Cfr*. http://goo.gl/ejCFA.

(25) Así lo hizo el Consejo Constitucional francés, *cfr*. http://goo.gl/j7H4o. También el Tribunal Europeo de Derechos Humanos, en su sentencia de 18 de diciembre de 2012, correspondiente al caso *Ahmet Yildirim*, *cfr*. http://goo.gl/ulAH2.

(26) *Cfr*. http://goo.gl/ejCFA.

(27) *Cfr*. Ley 2/2011, de 4 de marzo, de economía sostenible (art. 52), desarrollada por Real decreto 726/2011, de 20 de mayo, por el que se modifica el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios, aprobado por Real decreto 424/2005, de 15 de abril.

(28) *Cfr*. https://goo.gl/kJbYdc.

(29) Ya desde 2011, los Países Bajos regulaban el primer derecho europeo a disfrutar de una Red neutral. Otros países fuera de la Unión Europea que han regulado la Neutralidad de la Red son Chile en 2010, Brasil en 2014, e India o Rusia en 2016, entre otros.

(30) *Cfr*. García Mexía (2017, 76-78). Y en esto insiste igualmente el Consejo de Europa (2014).

3.3 **La neutralidad de la Red como garantía de acceso justo a Internet**

BEREC, el organismo que agrupa a los reguladores europeos de telecomunicaciones, probaba en un interesante estudio que el de neutralidad de la red es un concepto que resulta abstruso para la generalidad de los europeos (BEREC 2015, 9).

Siempre según ese estudio, sin embargo, con lo que sí nos familiarizamos más los europeos es con la necesidad de que los operadores gestionen sus redes, que son las que nos permiten el acceso a Internet. Ahora bien, y aquí está la clave, aceptamos esta gestión siempre y cuando no se haga a expensas del acceso a la Red de nadie, ni en particular de nuestra propia calidad de acceso a Internet. Es decir, que como asegura BEREC (2015, 9): «Los consumidores europeos manifestamos una elevada sensibilidad hacia la justicia en cuanto se refiere a la neutralidad de la Red.» En otras palabras: el usuario europeo quizá no sepa definir la neutralidad de la Red, pero, paradójicamente, sabe perfectamente en qué consiste.

En el fondo, la neutralidad de la Red busca que el tráfico de Internet fluya libre de discriminaciones injustificadas respecto de aplicaciones o de servicios, en el sentido de que nadie pueda evitar nuestro acceso a Internet, en que nadie pueda perturbar nuestra calidad de navegación (por ejemplo ralentizando cierto tráfico) y en que nadie pueda obtener beneficios económicos por priorizar tráfico alguno sobre otro, si ello perjudica una u otra cosa. Nada de esto quiere decir que los operadores no puedan gestionar las redes, pero habrá de ser, se desprende de lo dicho, por razones justas (31).

3.3.1 La normativa europea sobre neutralidad de la Red

Tras años de titubeos, se dictaba el Reglamento (UE) 2015/2120 sobre Internet abierta, que, en línea con lo que venimos diciendo, pretende garantizar un tráfico en Internet sin discriminaciones (32). Esta normativa permite una gestión «razonable» del tráfico en Internet. Para ajustarse a ese estándar de «razonabilidad», dicha gestión habrá de ser transparente, no discriminatoria y proporcionada, así como no obedecer a criterios co-

(31) Es interesante la perspectiva aportada entre nosotros por Barrio Andrés (2017, 356 y ss.), para quien la neutralidad de la Red «esconde un problema de precios. En efecto, se trata de determinar si los proveedores de acceso a Internet cobran a los consumidores solo una vez por el acceso a Internet, no favorecen a un proveedor de contenidos sobre otro y no cobran a los proveedores y plataformas de contenidos por enviar información a través de líneas de banda ancha a los usuarios finales.»

(32) La iniciativa es muy importante, pues, hasta entonces, la Unión no había ido más allá de una mera proclamación de principios, que figuraba en la «Declaración de la Comisión sobre la Neutralidad de Internet», contenida en la Directiva 2009/140/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009.

merciales. Tampoco podrá implicar supervisión de contenidos, ni extenderse más allá del tiempo necesario. A la par que establece esos principios, el Reglamento (UE) 2015/2120 limita a cuatro los fines posibles de la gestión de tráfico que en su caso lleven a cabo los operadores: tres de ellos son habitualmente considerados indiscutibles, tratándose de cumplimiento legal [ya comentado más atrás, art. 3.3.a)], seguridad [art. 3.3.b)] y congestión [art. 3.3.c)].

Ahora bien, ninguno de estos fines justifica que los proveedores de acceso incurran en las que BEREC (2016, 6) ha denominado ofertas de «sub-internet». No digamos fines comerciales, como es el caso de algunos operadores en Europa, que dividen Internet en función de sus contenidos: vídeo (con YouTube, Vimeo, etc.), mensajería (con WhatsApp, etc.), redes sociales (con Facebook, etc.), entre otros, para cobrar diferentes tarifas a sus abonados en función de que se suscriban a un paquete, a algunos o a todos. Éstas son prácticas que BEREC (2016, 6; 11, 15) ha declarado abiertamente incompatibles con el Reglamento (UE) 2015/2120, por cuanto implican «el bloqueo de aplicaciones y/o discriminación, restricción o interferencia respecto del origen o destino de la información.» Otro tanto sucedería con ofertas que implicasen limitar el acceso a «partes predefinidas» de Internet (por ejemplo, solo ciertos sitios web) (BEREC 2016, 6).

El cuarto fin de la gestión de tráfico es mucho más polémico, consistiendo en la prestación de los comúnmente llamados «servicios especializados» («optimizados», en la terminología del Reglamento) que exijan un adecuado «nivel de calidad de servicio» (calidad «técnica» es la expresión utilizada en el Reglamento) (art. 3.5); un claro ejemplo lo constituyen los paquetes de contenidos de entretenimiento (películas, series, música, etc.). BEREC (2016, 26-27) hace notar que estos servicios solo podrán considerarse como tales en el supuesto de requerir un nivel de calidad que no se pueda prestar a través de los servicios de acceso a Internet, cosa que los reguladores nacionales deberán evaluar caso por caso. Es también un requisito el que la red tenga suficiente capacidad para prestarlos, junto a los servicios de acceso a Internet que el operador en cuestión viniera suministrando (art. 3.5).

Pese a haber implicado un gran avance, esta normativa europea presenta cierta laxitud, por dos razones principales.

La primera es justamente su regulación de los servicios especializados, que ha llevado a autorizadas voces a afirmar que, a su amparo, «cualquier operadora podrá implantar carriles rápidos [de uso de Internet], bastando para ello con que los etiquete como tales “servicios especializados”» (33).

(33) B. Van Schewick, en *The Economist*, «A multi-speed Europe», 28 oct. 2015, http://goo.gl/Lf7h7z.

Puede que esta visión sea algo exagerada, pero lo que es claro es que los estándares son aquí muy vagos, sin que, como se ve, BEREC haya podido concretar mucho más.

La segunda razón: algunos operadores europeos han comenzado a ofrecer, sin ir más lejos en España, no cobrar a sus clientes «si se quedan sin megas», respecto de algunos servicios o aplicaciones predeterminados por el propio operador (un determinado servicio de mensajería instantánea, por ejemplo), mientras que han de pagar el exceso «de megas» respecto de todos los demás. Es lo que se conoce como «zero-rating». En sus pautas interpretativas del Reglamento (UE) 2015/2120, BEREC (2016, 11) descarta de plano la legalidad del zero-rating que implique (además del cobro extra) bloquear o ralentizar todas las aplicaciones que no sean las sujetas a la oferta del operador; por el contrario, abre la puerta a que los reguladores nacionales acepten cualesquiera otras ofertas de zero-rating, siempre y cuando, «por su escala», no «conduzcan a situaciones en que las opciones de los usuarios finales se vean significativamente reducidas en la práctica», o bien «puedan menoscabar aspectos esenciales de este derecho [de acceso del usuario final]».

3.3.2 Internet (y Europa) ante la política anti-neutralidad de la Red de la Administración norteamericana

La Federal Communications Commission (FCC) estadounidense decidía el 14 de diciembre de 2017 eliminar la normativa sobre neutralidad de la Red de 2015, elaborada por la anterior Administración presidencial, y que prohibía bloquear, ralentizar o cobrar por priorizar aplicaciones o servicios (34). Es decir, que, desde el 14 de diciembre de 2017, en EE. UU. ninguna norma impedirá que los operadores desarrollen estas prácticas.

Los defensores de la eliminación arguyen que ninguno de esos males inadmisibles había llegado a ocurrir antes de 2015. También que lo que se busca es aumentar las opciones para el consumidor. Y potenciar la innovación.

Puede ser cierto. Aunque también puede serlo que nunca antes de 2015 había sido tan probable esa «balcanización» en los contenidos de Internet, siendo ese riesgo aún mayor en 2017 (lo atestiguan algunos de los ejemplos anteriores de Europa). Y es igualmente verdad que esas mayores opciones para el consumidor no son elegidas por él mismo, sino por el operador correspondiente, en función de sus intereses comerciales.

(34) La normativa procedente de la Administración Obama era FCC 15-24 (*Order on Remand*), de 26 de febrero de 2015. La que la revoca, FCC 17-166 (*Restoring Internet Freedom Order*), de 14 de diciembre de 2017.

Y en cuanto a potenciar la innovación, qué mejor para ello que una red como es por esencia Internet, abierta «de extremo a extremo», una red «tonta» aunque «conecte máquinas inteligentes» (D. Post 2009, 66; 83), porque se limita a permitir la comunicación, sin que importen ni la tecnología subyacente ni la naturaleza de los contenidos que se enlazan. Es indudable que si no hubiera sido por esa apertura y esa «ceguera» respecto de lo que se enlaza y distribuye, aplicaciones y servicios nacidos de la nada y que hoy han llegado a ser algunas de las mayores empresas mundiales, difícilmente habrían superado la mediocridad.

Internet, como toda obra humana, tiene defectos y entraña riesgos. Unos y otros empiezan a ser crecientemente conocidos, conforme toda una ola de pensamiento «ciberescéptico» va surgiendo a la luz. Aunque difícilmente se podrá negar que esta Red ha llegado a convertirse en un instrumento imprescindible para la libertad y para el progreso de la Humanidad. Y a esto se ha llegado gracias a ese ADN inescindible de la propia Internet, que es su neutralidad. Al fin y al cabo, con la neutralidad de la Red nos jugamos lo que más valoramos en nuestro acceso a Internet, que se lleve a cabo de un modo justo (35).

Es pues de esperar y de desear que Europa no siga los últimos pasos dados en este campo por la Administración de los EE. UU., y se mantenga fiel a los postulados de la neutralidad de la Red, por laxos que resulten al amparo del Reglamento (UE) 2015/2120.

3.4 **Una privacidad centrada en el ciudadano también ayuda a la Internet abierta**

El ya citado RGPD, directamente aplicable desde 25 de mayo de 2018, bien puede considerarse como un remedio más en favor del acceso a Internet. Así es porque el RGPD presenta como una de sus novedades capitales la de establecer un régimen de privacidad y protección de datos centrado en el usuario, en el ciudadano, a su vez gracias al refuerzo del principio de transparencia (y con ello de los derechos de información y consentimiento) (García Mexía y Perete Ramírez 2018, 128).

Junto a los mencionados y otros (como el de oposición al trazado de perfiles, art. 13.3 RGPD), esto se concreta en nuevos derechos, singularmente el de portabilidad (regulado en el art. 20), que incrementan el control de los ciudadanos sobre sus datos. Gracias al derecho de portabilidad, los responsables de los datos deben posibilitar que los titulares recuperen

(35) Tras denunciar las presiones que sobre Internet vienen ejerciendo tanto Estados como agentes privados, Mueller *et al.* (2007, 16) tendían ya entonces puentes entre las capas lógica y física de la Red, al concluir que «la neutralidad de la Red constituye un baluarte, en tanto que principio alternativo de gobernanza de Internet, que prioriza el valor de una comunicación y una información abiertas y universales».

fácilmente sus datos personales y los trasladen de un entorno digital a otro (ya sea a sus propios sistemas, a los sistemas de terceros de confianza o a los de ulteriores responsables). Merced a todo ello, el derecho de portabilidad constituirá un arma importante frente a cualquier «valla» en Internet.

Probablemente reste un paso más, como sería el reconocimiento en favor del ciudadano de un derecho de propiedad sobre sus datos personales, de raíz estrictamente patrimonial y por supuesto complementario del tradicional (de raigambre constitucional). Parece natural, en un entorno Big Data, donde el dato constituye un activo de máximo y creciente valor económico. Aunque el RGPD no ha llegado tan lejos, es claro que su encuadre «user-centric» permite aventurar que esa vertiente patrimonial de la privacidad podría no tardar en llegar (García Mexía y Perete Ramírez 2018, 130-131). Y si lo hiciera, es también evidente que Internet resultaría aún mucho más abierta para todos.

3.5 **La normativa sobre competencia, nueva punta de lanza en pro del acceso a la Red**

Esa vertiente patrimonial del dato se está en cambio reconociendo y estudiando ya sin rubor alguno en un contexto legal de cada vez mayor importancia para el entorno digital, como es el Derecho de la competencia.

En España, una muestra muy representativa de ello es la opinión de la Autoridad Catalana de la Competencia (2016, 36), para quien los datos en poder de una empresa habrían de ser indudablemente considerados parte de su activo a la hora de fiscalizar posibles concentraciones; a nadie se oculta, añado, que, si empresas como Google, Facebook o Amazon están hoy entre las cinco mayores del mundo, indiscutiblemente se debe al incalculable valor de los datos que atesoran. En parecida línea, esta misma fuente propugna «la propiedad del usuario» sobre «toda la información que de él ha sido recabada de tal forma que pueda controlar quién tiene acceso a la misma, lo que a su vez podría facilitar el acceso al mercado de nuevos operadores» (Autoridad Catalana de la Competencia 2016, 45).

Autoridades europeas de competencia como la alemana y, aunque en menor medida otras, como la francesa, han abierto brechas decisivas en esta línea (36). Lo han hecho con el argumento de que, sin perjuicio de los poderes de las autoridades de protección de datos, también las de competencia deben velar por que los ingentes volúmenes de datos en poder de

(36) También la Comisión Europea (2017, 10-11), mediante su objetivo de «conseguir una economía de plataformas equitativa y favorable a la innovación», dentro de su *Estrategia revisada de Mercado Único Digital para Europa*.

empresas como las citadas no deriven en abusos de posición dominante (Baena Zapatero 2018).

Es claro que, de por sí, o en conjunción con el empoderamiento del usuario propiciado por la nueva normativa sobre privacidad, estos avances en competencia pueden también generar una Internet más libre de barreras.

4. EL ACCESO A INTERNET EN EL FUTURO (INMEDIATO Y NO TANTO)

Dos son los vectores de avance tecnológico que en mi opinión más influjo tendrán sobre el acceso a la Red: uno, la convergencia tecnológica; el otro, Blockchain.

4.1 **El impacto de la convergencia tecnológica sobre el acceso a la Red**

Indica la OCDE (2014):

> «Si la última década [2004-2014] representó el surgimiento generalizado de la banda ancha y de Internet como fenómeno verdaderamente global, la siguiente década probablemente entrañará la integración de las redes fijas de voz, video, datos y servicios de máquina a máquina (M2M) en plataformas integradas ("converged") basadas en Internet.»

En una palabra: la noción de «plataforma» está llamada a englobar, no solo a los proveedores de contenidos, sino también a los de acceso (y hasta a ciertos servicios audiovisuales), todos vinculados por su común uso del protocolo TCP-IP. Y cada vez mayor número de unos y de otros crecientemente dedicados a todo tipo de servicios digitales, en un auténtico «entrecruzamiento de los roles tradicionales».

A la vista de esta evolución, parece evidente que Internet estará dominada por esas «plataformas integradas», siendo ya irrelevante que sus componentes procedieran originariamente de uno u otro subsector digital (acceso, contenidos, audiovisual). Y si eso es lo que sucederá, el acceso a la Red deberá entonces salvaguardarse justamente frente a estos nuevos agentes del entorno digital. Será pues frente ellos como se habrá de preconizar el derecho a acceder a la misma infraestructura, el derecho a que ese acceso sea justo (en cuanto a que tenga la calidad necesaria y esté libre de discriminaciones) y el derecho a la propiedad (o cuando menos a la portabilidad) sobre la información personal.

Esa convergencia de roles antes dispares, que está haciendo *ya* que titulares de redes y proveedores de contenidos sean los mismos (Telefónica explota redes y con cada vez mayor ahínco comercializa contenidos en línea), generará una muy importante consecuencia en el plano regulatorio.

Se trata de la necesidad de aplicar las mismas normas para cualesquiera actores del entorno digital (sin que importe su subsector de origen, si es que acaso lo tuvieron), debiendo éstas ser «las generales de competencia, consumidores o derechos de autor» (Gobierno de Suecia-A. Focus 2015, 13-14; 23; 87). Cierto que la materialización de este principio abocaría a la extinción de la actual regulación sectorial de las telecomunicaciones. Aunque a la par privaría de sentido a una potencial regulación - paralelamente sectorial- de los proveedores de contenidos, como en su *Estrategia de Mercado Único Digital para Europa* se había propuesto estudiar la Comisión Europea (2015, 14), para posteriormente descartarlo (Comisión Europea 2016, 10-11) (37).

4.2 ¿Por qué influirá Blockchain sobre el acceso a Internet?

La tecnología de las cadenas de bloques o Blockchain, una de las de mayor potencial disruptivo de nuestro tiempo (OCDE 2016, 107-110), posibilita compartir información a través de Internet y mantenerla actualizada de modo distribuido y a la vez criptográficamente seguro.

Su germen revolucionario a nuestros efectos radica en dos factores. El primero de ellos es el hecho de que Blockchain permitirá pasar, de la Internet centralizada actual, construida alrededor del DNS, a una Internet descentralizada, en cuanto que libre de servidores («serverless»), donde los usuarios almacenarán los datos en su propia nube, sin puntos centrales de error y fallo (Preukschat 2017, 121). Por lo dicho, y mientras que en la actualidad resulta capital mantener el DNS al margen de una gestión estatalizada, una Internet basada en Blockchain reduciría desde luego la potencial repercusión de la injerencia política sobre la capa lógica de la Red. En otras palabras, sería mucho más difícil, por no decir virtualmente imposible, que ningún Estado interfiriese con éxito en el funcionamiento de la capa lógica de una Internet basada en Blockchain: una buena noticia para el posible futuro del acceso a la Red.

El segundo gran factor de disrupción que impulsará Blockchain es absolutamente consustancial a esta tecnología, que lleva por así decir en su «ADN», la posibilidad de eliminar intermediarios. En la actual Internet, intermediarios como Google, Facebook o Amazon, entre tantos otros, aportan confianza en sus respectivos campos; es más, es casi un axioma de Internet que, en ella «siempre hay un intermediario», siendo quizá el mejor ejemplo el del buscador. Ahora bien, como De Filippi (2016, 5) hace notar, en una red basada en Blockchain, «cada nodo de la red se comunica

(37) En línea con la posición inicial de la Comisión Europea se manifestó el Gobierno de España (MINETUR 2015, 3). Es de suponer que la *Estrategia digital para una España inteligente*, aún en elaboración al cierre de este trabajo, se definirá de nuevo sobre la cuestión, especialmente a la vista de la nueva posición de la Comisión.

con todos los demás, sin necesidad de pasar por una autoridad central de confianza» y la seguridad se garantiza «mediante validaciones y verificaciones llevadas a cabo de forma transparente por todos y cada uno de los nodos de la red». Como suele explicarse en entornos Blockchain, la seguridad y la autenticidad de las comunicaciones se consigue por consenso. La consecuencia es clara: en la medida en que la criptografía garantiza la posibilidad de confiar en cualquier otro partícipe de una red basada en cadena de bloques, el intermediario sobra. Y si el intermediario sobra, una Internet futura basada en Blockchain podría también ser una Red mucho más abierta.

5. CONCLUSIONES

El acceso a Internet proporciona una perspectiva privilegiada, de evidente perfil subjetivo, para avizorar los principales problemas de esta Red como red abierta, así como para percibir las salvaguardas que se han ido arbitrando para remediarlos.

Una de las mayores enseñanzas de este trabajo es la de que las amenazas en él descritas van en aumento. Pese al acuerdo de Marrakech de 2016, la gobernanza de Internet va a seguir sufriendo la presión de Estados como China o Rusia para estatalizar elementos tecnológicos determinantes de esta Red. Es presumible que los operadores de telecomunicaciones pretendan esgrimir con al menos el mismo ahínco la llamada «calidad de servicio», para recuperar terreno perdido frente a las grandes empresas «de Internet». Es evidente que los bloqueos de contenido por motivos de políticas públicas se están generalizando por todo el mundo, con cada vez mayor frecuencia sin suficiente justificación legal, incluso en países democráticos. En tanto que comienza a ser paradigmático señalar a las llamadas GAFAM como empresas tecnológicas que probablemente habrían llevado demasiado lejos sus «silos» de información, y con ello las trabas a un «deambular» libre de «vallas» por Internet.

La segunda gran conclusión es la de que, lamentablemente, son solo los países occidentales los que de verdad asumen compromisos serios a la hora de salvaguardar el carácter abierto de Internet, y aun así, de modo marcadamente desigual, como por ejemplo demuestra el retroceso norteamericano de diciembre de 2017 en materia de neutralidad de la Red. Esa casi total «soledad» de Occidente queda de manifiesto a la hora de impulsar la gestión multilateral de la Internet global, precisamente frente a Estados abiertamente opuestos a sus valores y a sus líneas generales de acción política; en lo que se refiere a la consideración del acceso a Internet como un derecho ciudadano (por más que algunos de esos Estados no occidentales no bloqueen al menos su proclamación en organizaciones como Naciones Unidas u OSCE); desde luego en materia de neutralidad

de la Red, principio prácticamente exclusivo de los EE. UU. (con muchos matices desde 2017) y de Europa; y por supuesto, en lo que hace al control de los usuarios sobre sus datos en Internet, donde sin duda es Europa la líder en solitario, con países como Japón, Corea del Sur y algunos latinoamericanos (México, Brasil, Argentina o Chile) siguiendo atentamente sus pasos, mientras los EE. UU. permanecen fieles a su modelo de gran eficacia práctica pero únicamente reactivo, en tanto que China o Rusia proclaman legalmente una «privacidad» muy lejana a lo que aquí entendemos por ella. Sobra por fin decir que las iniciativas en materia de competencia que aquí hemos analizado son de nuevo exclusivamente europeas; y aunque el escándalo Facebook de marzo de 2018 podría impulsar en las autoridades norteamericanas acciones hasta hace poco impensables en este ámbito, éstas continúan en lo esencial a la expectativa de lo que desde aquí se viene decidiendo.

El futuro invita sin embargo al optimismo. La convergencia tecnológica, por una parte, está homogeneizando los roles de los agentes del entorno digital, y permitirá por tanto homogeneizar también, más de lo que «de facto» estén ya, las reglas de juego para unos y otros, ayudando a rebajar conflictos motivados por iniciales asimetrías regulatorias.

Por otro lado, esa Internet sin intermediarios que Blockchain parece prometernos, con todas las cautelas ante una tecnología aún incipiente, y que por tanto tampoco permite aún calibrar su verdadera potencialidad futura, podría de alguna forma devolvernos, o siquiera acercarnos, a la Red sin barreras, abierta «de extremo a extremo», que sus inventores crearon.

CAPÍTULO 19

LOS MENORES Y SUS DERECHOS EN LA SOCIEDAD DIGITAL

M.ª Belén Andreu Martínez
Profesora Titular de Derecho Civil (Universidad de Murcia)

1. LOS MENORES EN LA RED, USOS Y RIESGOS. APROXIMACIÓN EN EL CASO ESPAÑOL

La revolución tecnológica del siglo xxi, como todas las revoluciones que han tenido lugar en épocas anteriores, ha cambiado la forma en que entendemos el mundo y a nosotros mismos. Hay un replanteamiento tanto desde el punto de vista sociológico, psicológico, ético, político y como no, también jurídico. El nuevo espacio de comunicación e interacción que es Internet influye decisivamente en la configuración, ejercicio y disfrute de los derechos fundamentales y plantea nuevos retos para el legislador, que intenta abordar con bastante dificultad. Y a esto no son ajenos los menores (1). Es ya un lugar común hablar de nativos digitales respecto de

(1) Como ya señalara Perez Luño, A. E., «La protección de los datos personales de los menores en Internet», *Anuario de la Facultad de Derecho de la Universidad de Alcalá*, n.º 2, 2009, p. 153,

los nacidos en el nuevo milenio e incluso de huérfanos digitales si se pone el acento en la brecha digital o en la falta de apoyo o acompañamiento en el uso de las TIC por parte de los padres o profesores. Los datos nos confirman año tras año esta realidad, con avances constantes en la digitalización de la sociedad, un descenso en la edad de inicio para conectarse, una constante evolución en los hábitos en el uso de medios electrónicos y, en consecuencia, en un internet más ubicuo y omnipresente en la vida diaria de los menores (2).

En este contexto, la protección de los menores y el ejercicio de sus derechos es un tema clásico, que sigue preocupando en la actualidad tanto a nivel nacional como internacional, y en el que se avanza, aunque probablemente no tan rápido como nos gustaría. Existen numerosos estudios que se han detenido a analizar tanto la influencia del ámbito digital en el desarrollo de los menores como, en particular, los riesgos que éste supone.

El papel que se viene reconociendo al menor en la sociedad en los últimos decenios como un menor activo, participativo y con una capacidad creciente para el ejercicio de sus derechos, se ha trasladado de facto al mundo virtual, que es donde de forma mayoritaria ejercen sus derechos. En este sentido, se crean una identidad digital, una biografía digital, una reputación online… (3). Los menores ejercitan su libertad ideológica y de conciencia y su libertad de expresión e información a través de las TIC y desarrollan su personalidad mediante la participación en foros, blogs, chats y, particularmente, redes sociales. La participación en comunidades virtuales ayuda a conformar estos derechos y les permite implicarse en la vida social, cultural, educativa, recreativa y a ejercitarse como ciudadanos activos, siempre conforme a su propia evolución y desarrollo físico y psíquico (4).

Los riesgos de los menores en el mundo digital también han sido objeto de numerosos estudios. A título de ejemplo, se puede citar la clasificación

---

Internet ha redimensionado las relaciones del menor con la utilización de su espacio vital, con los demás y consigo mismo.

(2) Pueden verse los datos de la encuesta del INE (2017) sobre equipamiento y uso de las TIC en los hogares españoles (http://www.ine.es/prensa/tich_2017.pdf). De entre los muchos estudios en la materia se pueden citar para España Garmendia Larrañaga, M. y otros, *Net Children Go Mobile: Riesgos y oportunidades en internet y el uso de dispositivos móviles entre menores españoles (2010-2015)*, Red.es/ Universidad del País Vasco, Madrid, 2016; y a nivel europeo, la red Eu KidsOnline (www.eukidsonline.net).

(3) Sobre el uso de estos términos, *vid.*, entre otros, Burguera Ameave, L., «Autodeterminación informativa de los menores (I)», en Pérez Álvarez, S. y otros (directores), *Menores e Internet*, Thomson Reuters-Aranzadi, Cizur Menor, 2013, pp. 332 y ss.; Alamillo Domingo, I., «La identidad digital en la Red», en Rallo Llombarte, A. y Martínez Martínez, R. (editores), *Derecho y redes sociales*, Thomson Reuters-Civitas, Cizur Menor, 2013, pp. 39 y ss.

(4) Fernández Coronado, A. y Pérez Álvarez, S., «La libre formación de la conciencia del menor a través de Internet», en Pérez Álvarez, S. y otros (directores), *Menores e Internet*, Thomson Reuters-Aranzadi, Cizur Menor, 2013, p. 211.

realizada por la Ponencia conjunta de estudio sobre riesgos derivados del uso de la red por parte de los menores del Senado (5), y que distingue entre riesgos de Internet (relativos a los cambios cognitivos y relacionales, uso excesivo o conductas adictivas a Internet) y riesgos en Internet (de contenidos, ya sean ilícitos o perjudiciales para el menor; y de contactos). Entre estos últimos, destacarían los asociados a la integridad física o psíquica del menor (*ciberbullying*, *cibergrooming*, juego on line…) o a la privacidad y protección de datos personales (*sexting*, cosificación de la identidad digital, uso malicioso de información personal…). Evidentemente los riesgos y las conductas van evolucionando. Se habla así de *morphing* (cuando la imagen difundida es modificada o manipulada, incluso con connotaciones sexuales o vejatorias), o en relación con el acoso, el llamado *ciberstalking* (o acoso repetido y continuado a través de las TIC impidiendo a la persona llevar una vida normal), o el *happy slapping* (agresión física difundida por la red) (6).

Para abordar el escenario descrito se ha realizado una intervención desde diferentes ángulos: protección frente a contenidos ilícitos, a la explotación sexual o al ciberacoso; gestión de la información y acceso a contenidos apropiados; gestión de la privacidad, identidad digital y reputación online… Y a través de diferentes herramientas: legislativas, autorregulación, sensibilización y educación de usuarios, padres y educadores, fomento de contenidos apropiados…

En el caso español, y más allá de las iniciativas de autorregulación o de las acciones de sensibilización y formación a las que se hará referencia en este trabajo, la intervención legislativa específica para el ámbito digital ha sido escasa y básicamente centrada en el ámbito penal. Así, se han introducido en el CP (especialmente tras la reforma llevada a cabo por la LO 1/2015, 30 marzo) figuras delictivas para reprimir algunas de las conductas descritas, como el acoso insistente mediante el uso de nuevas tecnologías (*ciberstalking*, art. 172 ter), *sexting* (art. 197.7 CP), el *child grooming* (art. 183 ter.1) o el embaucamiento de un menor para el intercambio de material pornográfico (art. 183 ter.2), sin perjuicio de que otras puedan tener cabida en tipos penales generales (ej., *ciberbullying* en los delitos contra la integridad moral, art. 173.1 CP) (7). Es evidente que la intervención desde el punto de vista penal es absolutamente necesaria,

(5) BOCG 3-10-2014; que, como señala, utiliza en parte la del proyecto EU Kids Online.

(6) Guardiola, M., «Menores y nuevas tecnologías: los nuevos retos en el sector legal en España», *La Ley Derecho de Familia*, n.º 14, 2017 (LA LEY 5019/2017), pp. 2 y ss.

(7) Sobre el tema, puede verse, entre otros, Aparicio Torres, C. y López Jara, M., «La protección penal del menor víctima de ciberdelitos. Primeras actuaciones», *La Ley Derecho de Familia*, n.º 14, 2017. *Vid.* asimismo, las obligaciones asumidas en el Convenio del Consejo de Europa relativo a la Protección de los niños contra la explotación y abuso sexual, de 25 de octubre de 2007, y a la Directiva del Parlamento Europeo y del Consejo 2011/93/UE, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil.

pero no suficiente. Por otra parte, pone de relieve una aproximación quizá excesivamente centrada en el riesgo, control y la restricción. No en vano, conforme a la clasificación realizada en 2013 por el proyecto EU Kids Online, España pertenecería a la categoría de países donde los niños están «protegidos mediante restricciones» (se caracterizan por un nivel relativamente bajo de riesgos, probablemente porque el uso de internet es más limitado), frente a otros como Suecia, que entrarían dentro de los menores «exploradores experimentados con apoyo» (se exponen a más riesgos sexuales *on-line*, pero con mayor implicación parental) (8).

Ahora bien, los nuevos hábitos de conexión (desde edades más tempranas, en contextos más variados y con dispositivos más avanzados como *tablets* y *smartphones*) conllevan que los riesgos aumenten y lo vayan a seguir haciendo. Como se ha señalado, a más oportunidades más riesgos; pero esto también implica más habilidades y no necesariamente un aumento de los daños en la misma proporción como consecuencia de la mayor exposición al riesgo (9). Frente a ello se propone que por los distintos actores se prioricen medidas como la clasificación de contenidos, los servicios adecuados a la edad, las configuraciones de privacidad o los sistemas de denuncia sencillos (10).

A la vista de lo anterior, en las siguientes páginas abordaremos desde una óptica jurídica aspectos como: la posición del menor en la actualidad en nuestro ordenamiento jurídico, qué reconocimiento se realiza de sus derechos en el ámbito digital, así como el papel que le corresponde a los representantes legales; la intervención legislativa realizada o pendiente de realizar en ámbitos especialmente problemáticos como la privacidad del menor o el uso de servicios de comunicación audiovisual; para, por último, realizar una breve referencia a otras medidas adicionales para un mejor disfrute y protección de los derechos de los menores en Internet, en particular, en lo que se refiere a la formación y educación.

2. EL *STATUS* JURÍDICO DEL MENOR Y EL EJERCICIO DE SUS DERECHOS EN EL MUNDO DIGITAL. LA INTERVENCIÓN DE LOS REPRESENTANTES LEGALES

Como sabemos, uno de los textos básicos de protección de los menores en nuestro ordenamiento es la LO 1/1996, de 15 de enero, de protección jurídica del menor (LOPJM), que incorpora las previsiones y principios contenidos en tratados internacionales, en particular, en la Convención de la ONU de los Derechos del Niño, de 20 de noviembre de 1989

(8) Helsper, E. y otros, *Country classification: opportunities, risks, harm and parental mediation*. EU Kids Online, The London School of Economics and Political Science, London, 2013.
(9) Garmendia Larrañaga, M. y otros, *op. cit.*, pp. 97 y ss.
(10) Garmendia Larrañaga, M. y otros, *op. cit.*, p. 96.

(CDN). Esta Ley recogió ya en 1996 el cambio en el status social del menor y el nuevo enfoque en la construcción de los derechos humanos de la infancia que se derivaba de dichos tratados internacionales y que se plasmó, entre otros, en elementos que hoy en día podemos seguir considerando clave para entender el rol de nuestros menores (11): el reconocimiento pleno de la titularidad de derechos en los menores de edad y de una capacidad progresiva para ejercerlos, así como una interpretación restrictiva de las limitaciones a su capacidad de obrar (12); su consideración como sujetos activos, participativos y creativos, con capacidad de modificar su propio medio personal y social; o el interés superior del menor como principio básico que debe primar en las actuaciones y decisiones que le conciernan (Preámbulo, apdo. 2; art. 2).

La LOPJM no deja de reflejar la tensión existente entre la visión tradicional del menor como destinatario de medidas de protección y tutela y la potenciación de su autonomía (13). Dicotomía que acertadamente supera al entender que «la mejor forma de garantizar social y jurídicamente la protección a la infancia es promover su autonomía como sujetos», de manera que puedan ir construyendo progresivamente una percepción de control acerca de su situación personal y de su proyección de futuro (Preámbulo, apdo. 2). Esta visión sigue teniendo plena vigencia, más aún si cabe en la actualidad a la vista de la especial vulnerabilidad del menor en el ámbito digital, de la necesidad declarada de reforzar las medidas de protección y de la construcción de un ambiente seguro que no debe por ello llevarnos a olvidar su autonomía como sujetos, todo ello conforme a las necesidades de su proceso evolutivo.

Ahora bien, y partiendo de esta premisa, hay que remarcar que apenas existen menciones o una regulación sobre el ejercicio de estos derechos en el mundo digital o a cómo éste pueda verse afectado por el uso de Internet. Es evidente que el menor disfruta de sus derechos también en el ámbito digital (con independencia de que exista o no un expreso reflejo normativo); y también es evidente que el escenario actual es otro y las posibilidades de control también son diferentes a las existentes hace vein-

(11) Aunque ya el artículo 162 CC o el artículo 3 LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen reconocieron la capacidad del menor para el ejercicio de derechos de la personalidad conforme a sus condiciones de madurez.

(12) De hecho se predica una asunción de responsabilidad unida a esta ampliación de la capacidad del menor, *vid.* entre otros, Muñoz García, C, «Responsabilidad civil de los grandes menores a la luz de las últimas reformas. Algo falta por hacer», *Diario La Ley*, n.º 8719, 2016 (LA LEY 871/2016); Grimalt Servera, P., *La responsabilidad civil por los daños causados a la dignidad humana por los menores en el uso de las redes sociales*, Comares, Granada, 2017, pp. 39 y ss., 137 y ss.

(13) Sobre esta dicotomía y su reflejo en las políticas sobre Infancia e Internet desde el análisis del discurso, *vid.* Ramiro Vázquez, J., «Virtualizando infancias. Del niño competente al menor en riesgo a través de Internet», en Pérez Álvarez, S. y otros (directores), *Menores e Internet*, Thomson Reuters-Aranzadi, Cizur Menor, 2013, pp. 31 y ss.

te años, y que nos movemos en un escenario global en el que es necesaria una actuación coordinada a niveles supranacionales, pero esto no exime de una mínima revisión de la normativa interna. Sorprende, por ello, que una reforma integral de los mecanismos de protección de menores, como la llevada a cabo en el año 2015 (a través de la Ley 26/2015, de 28 de julio y LO 8/2015, de 22 de julio, de modificación del sistema de protección a la infancia y a la adolescencia), no se haya detenido en estos aspectos. Apenas encontramos alguna mención al ejercicio de los derechos en el ámbito digital en el artículo 5, a propósito del derecho a la información. En concreto, y tras la reforma de 2015, se incluyeron referencias a la alfabetización digital y mediática (como herramienta imprescindible para que los menores puedan desarrollar su pensamiento crítico y tomar parte activa en una sociedad participativa y en un mundo actual); y a la labor de las Administraciones en la sensibilización «sobre la oferta legal de ocio y cultura en Internet y sobre la defensa de los derechos de propiedad intelectual», o en el fomento de la autorregulación en los medios de comunicación para evitar el acceso a contenidos lesivos (sin mayor precisión al respecto, en un momento en el que además los límites entre la comunicación audiovisual tradicional y en la Red se difuminan, tal y como señalaremos posteriormente). Por otra parte, la aproximación del artículo 5 LOPJM no deja de reflejar esa idea de «menor en riesgo» a la que antes aludíamos. Queda, por tanto, en el tintero una actualización al ámbito digital de los derechos que se reconocen en la LOPJM, en particular de la libertad de expresión, el derecho de participación y los derechos al honor, intimidad y propia imagen (en relación con éste último, y en concreto, sobre lo dispuesto en el art. 4.3, volveremos más adelante).

Curiosamente sí encontramos algún desarrollo mayor al nivel de las Comunidades Autónomas. Quizá uno de los ejemplos más paradigmáticos haya sido el Decreto andaluz 25/2007, de 6 de febrero, por el que se establecen medidas para el fomento, la prevención de riesgos y la seguridad en el uso de Internet y las TIC por parte de las personas menores de edad. Aunque los fines declarados en la norma son la concienciación, prevención del riesgo y de los usos inadecuados y la promoción de un acceso seguro (art. 3), se recogen una serie de derechos de los menores en el acceso y uso de Internet y las TIC, claramente inspirado en el decálogo de Unicef de los e-derechos de los niños y las niñas (14): derecho al acceso y uso de internet, al desarrollo personal y la educación, a buscar, recibir y difundir información e ideas a través de internet y las TIC, al ocio y esparcimiento por estos medios…; aunque con algunas ausencias

(14) Resulta también ilustrativa la iniciativa sobre los e-derechos de la Infancia llevada a cabo por Pantallas Amigas, accesible en: http://www.pantallasamigas.net/otros-webs/e-derechos-infancia.shtm.

significativas como las referencias a la libertad de expresión o el derecho a la intimidad en Internet.

En una futura actualización de esta materia puede presentar especial interés la Guía de los derechos humanos para los usuarios de Internet, adoptada por el Consejo de Ministros del Consejo de Europa el 16 de abril de 2014 (15), y que parte de la aplicación por igual de los derechos y libertades fundamentales a entornos dentro y fuera de la red. La guía dedica un apartado específico a los niños y jóvenes, deteniéndose en aspectos clave, de los que destacaríamos dos:

— El derecho a expresar libremente su opinión, a participar activamente en la sociedad, a ser oído y a participar en la toma de decisiones que le afecten, de acuerdo a su grado de madurez y edad, a través de Internet y otras TIC. Lo que incluye también la posibilidad de recibir información sobre cómo ejercer estos derechos, así como medios y recursos de reparación efectivos cuando consideren que se ha violado su derecho a participar.

— Y la posibilidad de solicitar que se retire en un plazo razonable el contenido creado por el propio menor o por terceros sobre el menor (salvo prensa y editores) y que pueda afectar a su dignidad, vida privada, seguridad u otros derechos, ya sea en ese momento o en una etapa posterior de su vida.

En esta línea, entre las enmiendas al Proyecto de LOPD, de 24 de noviembre de 2017 (enmiendas núms. 246, 298 ss.) (16), se encuentra la propuesta de modificación del título de la Ley y la adición de un título X sobre garantía de derechos digitales.

Otra de las cuestiones fundamentales en la materia es la de compatibilizar el ejercicio de estos derechos por los menores y las responsabilidades parentales. La irrupción de las TIC ha aumentado la dificultad para ejercer las funciones derivadas de la patria potestad o tutela, por la multiplicación de las situaciones de riesgo y la omnipresencia y la perdurabilidad de un medio como Internet, pero también por las mayores posibilidades técnicas de control que las tecnologías nos ofrecen.

Aún así consideramos que las herramientas proporcionadas por la CDN siguen siendo válidas: el interés superior del menor como criterio rector de actuación y el proceso evolutivo y madurez como elemento delimitador de la intensidad de la intervención. En este sentido, creemos que debe entenderse, por ejemplo, la reforma operada en el artículo 162 CC a propósito del ejercicio de los derechos de la personalidad por parte del menor de acuerdo con su madurez, al haberse añadido la intervención en estos casos

(15) Recomendación CM/Rec(2014)6.
(16) *BOCG*. Congreso de los Diputados 18 de abril de 2018.

de los representantes legales «en virtud de sus deberes de cuidado y asistencia». Esta precisión incorporada en 2015 no supone sino positivizar los mencionados criterios y reconocer algo que ya se podía y, de hecho, se venía aplicando en virtud del «deber de velar» previsto en el artículo 154 CC. Por lo tanto, no se trata ni de eliminar la posibilidad de ejercicio por *sí* solo del menor de sus derechos, ni de un acceso o control ilimitado de los padres a las actividades de sus hijos, pero sí una posibilidad de intervención de estos más o menos intensa atendiendo a las circunstancias del caso, y un acompañamiento, apoyo y seguimiento en su formación derivada de la propia configuración de la patria potestad adaptada a la nueva realidad social y status del menor en nuestro Derecho (17).

En este sentido, creemos que debe entenderse también el criterio seguido en la STS de 10 de diciembre de 2015, cuando afirma la plena titularidad (y habría que añadir también el ejercicio) del derecho a la intimidad por parte de una menor de 15 años, debiendo ésta consentir el acceso de sus padres a su cuenta de Facebook, pero legitima en ciertos casos el acceso por el representante legal (por ej., ante signos claro de actividad presuntamente criminal contra su hija) con base en los deberes inherentes a la patria potestad (18).

Adicionalmente, hay que hacer referencia en este tema a los posibles límites que puedan tener las herramientas y aplicaciones para controlar la actividad de los menores (19). Estas constituyen un mecanismo útil que se ofrece a los padres para que puedan llevar a cabo su labor de cuidado y

(17) *Vid.* Grimalt Servera, P., *op. cit.*, pp. 130 y ss.; Fernández-Coronado, A. y Pérez Álvarez, S., *op. cit.*, p. 212, que señalan actuaciones que pueden constituir una extralimitación injustificada en el ejercicio de la patria potestad lesiva de la libertad de conciencia del menor. Por su parte, propone García González, J., «Oportunidad criminal, internet y redes sociales. Especial referencia a los menores de edad como usuarios más vulnerables», *Indret* 4/2015, pp. 25-26, un reconocimiento legal expreso para que los progenitores/tutores de un menor de 14 años puedan intervenir ante los proveedores de servicio y/o cualquier otro responsable de contenidos y solicitar la retirada de contenidos o el cese de comunicaciones con terceros con la simple demostración de ser los representantes legales.

(18) STS 864/2015, de 15 de diciembre (RJ 2015/6401), aunque la discusión en el caso se limitaba a la validez como medio de prueba en el proceso penal de los datos obtenidos por la madre de la red social de su hija. Como señala el TS: «No puede el ordenamiento hacer descansar en los padres unas obligaciones de velar por sus hijos menores y al mismo tiempo desposeerles de toda capacidad de controlar en casos como el presente en que las evidencias apuntaban inequívocamente en esa dirección. La inhibición de la madre ante hechos de esa naturaleza, contrariaría los deberes que le asigna por la legislación civil». Puede verse también la SAP Pontevedra (Secc. 2.ª) 893/2017, de 25 de octubre de 2017 (JUR 2017/308428), que, ante la denuncia presentada por la ex cónyuge, considera que no constituye un delito del artículo 197.1 CP, el hecho de que el padre revisara con su hija de 9 años ciertas conversaciones de whatsapp de la menor. Sobre otro tema, también relevante, como es la publicación de imágenes de menores por los padres en redes sociales, puede verse la SAP Pontevedra (Secc. 1.ª), 208/2015, de 4 de junio de 2015 (JUR 2015/163149) y Gil Membrado, C., «Límites a la autonomía de la voluntad en la disposición de la imagen del menor a través de las Redes Sociales», *La Ley Derecho de Familia*, n.º 13, 2017, pp. 10 y ss.

(19) *Vid.*, por ej., la noticia que saltó recientemente sobre la prohibición en Alemania del uso en menores de smartwach que tuvieran función de espionaje (https://www.bundesnetzagentur.de/SharedDocs/Downloads/EN/BNetzA/PressSection/PressReleases/2017/17112017_Verbraucherschutz.pdf?__blob=publicationFile&v=4).

asistencia al menor y para protegerles frente al acceso a contenidos ilícitos o inadecuados o contactos riesgosos. Aunque hay que tener en cuenta que ofrecen cada vez más funcionalidades, desde geolocalización, a cómo gestionar tiempos de acceso, contactos e incluso una monitorización completa de lo que el menor hace con un dispositivo electrónico (20). Se hace, por tanto, preciso aplicar también en este ámbito los criterios antes señalados, esto es, el equilibrio entre el respeto a los derechos del menor y la labor de velar de los padres, atendiendo a su proceso evolutivo y a su interés superior; y, por tanto, limitando las posibilidades de control conforme el menor va adquiriendo madurez y capacidad para actuar por sí mismo (21). En esta línea y en relación con la privacidad, ya se pronunció el Grupo de Trabajo del Artículo 29 en diversos dictámenes, en los que insistía en la necesidad de encontrar un equilibrio entre la intimidad de los menores y su seguridad, debiendo evitarse un control excesivo que limitara su autonomía o acostumbrarlos a estar permanentemente vigilados (22). Reflexiones que pueden aplicarse también a otros ámbitos, como puede ser el educativo, evitándose actuaciones de sobre vigilancia de menores o que puedan suponer una vulneración de su derecho a la intimidad (23).

3. LA INTERVENCIÓN LEGISLATIVA RELACIONADA CON LOS DERECHOS A LA INTIMIDAD Y PROTECCIÓN DE DATOS DEL MENOR

Más allá de conductas delictivas (como las relacionadas con la indemnidad sexual del menor o el *ciberbullying*), uno de los riesgos que más preocupan es el relacionado con la privacidad, la protección de la imagen y los datos personales del menor en el ámbito digital. En ello influyen di-

(20) Guardiola, M., *op. cit.*, pp. 3 y ss. Destaca la autora que alguna de ellas (como Teen Safe o My mobile wachtdog) son especialmente polémicas al permitir el control de toda la actividad del dispositivo del menor.

(21) Sobre la mediación parental y los posibles beneficios de una mediación activa en lugar de restrictiva, *vid.* Garmendia Larrañaga, M. y otros, *op. cit.*, pp. 77 y ss, 99 y ss.

(22) *Vid.*, entre otros, los Dictámenes 5/2005, de 25 de noviembre, sobre el uso de los datos de localización; 2/2009, de 11 de febrero, sobre la protección de los datos personales de los niños; o 13/2011, de 16 de mayo, sobre servicios de geolocalización en aparatos inteligentes. En concreto, respecto de los servicios de geolocalización, considera que se corre el riesgo de perturbar las relaciones normales de confianza mutua entre padres e hijos y, además, de acostumbrarlos desde edades muy tempranas a estar permanentemente controlados, de manera que de adultos ya no lo percibirán como una intromisión en sus derechos. De ahí que entienda que, cuando las circunstancias aconsejen el uso de dispositivos de control, deberá ser informado y participar en la toma de decisiones tan pronto como sea posible.

(23) Pueden consultarse, por ejemplo, los informes jurídicos de la Agencia Española de Protección de Datos (AEPD) 65/2015, sobre control de acceso a comedor por huella dactilar o 475/2014, sobre sistemas de videovigilancia en guarderías; o las polémicas SAN (Sala de lo Contencioso) de 26 septiembre de 2013 (JUR 2013\317703), que avaló el acceso por el director de un Colegio al terminal móvil (historial de navegación, contenido multimedia) de un menor que había mostrado un vídeo de contenido sexual a una compañera; o STS 155/2018, de 5 de febrero (RJ 2018/360), sobre el consentimiento de los estudiantes para publicar imágenes suyas (videos) en abierto en internet como tarea escolar (aunque la discusión judicial se redujo al tema de la legitimación activa). *Vid.* asimismo, Grimalt Servera, P., *op. cit.*, pp. 151 y ss.

versos factores, como el propio modelo de negocio en la Red, que se basa en la recopilación de información de los usuarios (siendo, además, los menores un target importante, actual y futuro) o la concepción de los menores de su privacidad, unida a otras características propias de la edad, y que les lleva a una sobreexposición de su vida privada (24). En este ámbito la intervención legislativa ha sido dispar, con una preponderancia de la normativa de protección de datos personales, en detrimento de otros aspectos, y una sensación de insuficiencia frente al propio funcionamiento de la Red (25).

Así, si nos detenemos en la normativa de protección de datos personales, los resultados alcanzados no son del todo satisfactorios. Por un lado, el artículo 13 Real Decreto 1720/2007, de 21 de diciembre (RLOPD dejando a un lado que se tratara de una norma reglamentaria) intentó recoger la experiencia de la *Children Online Privacy Protection Act* (COPPA) estadounidense, aunque sin demasiado éxito. La norma habría requerido algún tipo de desarrollo para detallar aspectos relativos, por ejemplo, a la información a facilitar a los representantes legales o los mecanismos de verificación del consentimiento parental. Ello ha hecho que en la práctica su cumplimiento no haya sido óptimo (26).

El nuevo Reglamento europeo de protección de datos personales (Reglamento UE 2016/679, de 27 de abril; RGPD) ha venido a llenar el vacío existente en la Directiva 95/46/CE en relación con los menores. No obstante, el resultado al que se ha llegado tampoco colma las expectativas, a pesar de la necesidad de protección de este colectivo que el propio Reglamento se encarga de remarcar (considerando 38). Ciertamente se menciona a los menores a propósito de diversas cuestiones, algunas las iremos señalando en las siguientes páginas. Pero el precepto específicamente destinado a ellos (art. 8 RGPD) se limita a regular el tratamiento de los

(24) La evolución del concepto de privacidad, tanto en general como respecto de los menores, ha sido un tema al que se le ha prestado atención en numerosos estudios (se habla de «extemidad», de publicitación de lo privado…), por citar algunos: Sibilia, P., *La intimidad como espectáculo*, Fondo de Cultura Económica, Buenos Aires, 2008, pp. 11 y ss.; Perez Luño, A. E., *op. cit.*, pp. 145 y ss.; Orozco Pardo, G., «Intimidad, privacidad, «extimidad» y protección de datos del menor ¿Un cambio de paradigma?», en Boix Reig, F. J. (director), *La protección jurídica de la intimidad*, Iustel, Madrid, 2010, pp. 390 y ss.; Piñar Mañas, J. L., «El derecho fundamental a la protección de datos y la privacidad de los menores en las redes sociales», en Piñar Mañas, J. L. (director), *Redes sociales y privacidad del menor*, Reus, Madrid, 2011, pp. 69-70.

(25) Sánchez Gómez, A., «Las nuevas tecnologías y su impacto en los derechos al honor, intimidad, imagen y protección de datos del menor. Mecanismos jurídicos de protección: carencias, interrogantes y retos del legislador», *Rev. Boliv. de Derecho*, n.º 23, 2017, p. 172, señala la insuficiencia de la regulación actual y la necesidad de que el legislador habilite mecanismos que impidan que el nuevo entorno digital se edifique sobre el recorte o desprotección de derechos como una consecuencia inevitable.

(26) Martínez Martínez, R., «Menores y redes sociales. Condiciones para el cumplimiento del artículo 13 del Reglamento de desarrollo de la Ley orgánica de protección de datos», en Rallo Llombarte, A. y Martínez Martínez, R. (editores), *Derecho y redes sociales*, Thomson Reuters-Civitas, Cizur Menor, 2013, pp. 216 y ss.

datos personales de los menores en los servicios de la sociedad de la información (SSI) específicamente dirigidos a ellos. Sigue así la línea de la COPPA estadounidense (aunque con carencias) y desiste de realizar una regulación más amplia y armonizada, puesto que permite a los Estados establecer la edad de «madurez» del menor para consentir el tratamiento de sus datos personales entre los 13 y los 16 años. Hay aspectos que habrá que concretar, por ejemplo, qué se va a considerar como esfuerzos razonables (conforme a la tecnología disponible) para verificar que el consentimiento se ha prestado por los representantes legales (art. 8.2). Y otros que habrá que resolver, como el relativo a la verificación de la edad del usuario, o si las webs que no están específicamente dirigidas a menores deben o no realizar algún tipo de control. La experiencia estadounidense en esto debería ayudarnos (27).

En cualquier caso, el margen que queda para el legislador nacional sigue siendo amplio en esta materia y debería aprovecharse de cara a la aprobación de la futura Ley Orgánica de Protección de Datos Personales [PLOPD (28)]. En este sentido, puede ser razonable el descenso de edad para consentir el tratamiento de datos a los 13 años, con la excepción de aquéllos supuestos en los que la ley exija la intervención de los representantes legales (previsto en el art. 7), si lo miramos desde la óptica de una unificación (en lo que se refiere a los SSI) con la edad prevista en la COPPA estadounidense (especialmente importante en un ámbito sin fronteras como el digital). Pero como contrapartida debería complementarse con previsiones específicas sobre la obligación de los responsables en materia de verificación de edad y consentimiento de los representantes legales (realización de «esfuerzos razonables conforme a la tecnología disponible») que completaran las previstas en el RGPD (que, además de ser insuficientes, se refieren únicamente al ámbito de los SSI dirigidos específicamente a menores). Con ello evitaríamos que el nivel de protección fuera inferior al que actualmente concede el artículo 13 RLOPD (ya que el art. 8 RGPD regula únicamente la oferta directa de SSI destinados a menores), y al mismo tiempo supliríamos alguna de las carencias del artículo 8 RGPD (en cuanto a la verificación de edad y consentimiento de los padres).

Ahora bien, una buena regulación del consentimiento del menor y de las facultades de intervención de los representantes legales no es suficiente y debe necesariamente complementarse con otras actuaciones tanto en el

(27) Sobre el tema, *vid.* Andreu Martínez, M. B., *La protección de los datos personales de los menores de edad*, Thomson Reuters-Aranzadi, Cizur Menor, 2013, pp. 48 y ss.; Piñar Real, A., «Tratamiento de datos de menores de edad», en Piñar Mañas, J. L. (Director), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016, pp. 187 y ss.; Brito Izquierdo, N., «Tratamiento de los datos personales de los menores de edad: supuestos, límites, retos y desafíos», *La Ley Derecho de Familia*, n.º 14, 2017, pp. 4 y ss.

(28) Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal (121/000013), de 24 de noviembre de 2017.

ámbito de la protección de datos personales como fuera de él (29). En este sentido, la nueva forma en que los menores manejan su intimidad hace que se venga planteando con fuerza, por las consecuencias que esa sobre exposición puede acarrearles en el futuro, la posibilidad de eliminar la información producida durante esta etapa de la vida. Una de las propuestas para hacer frente a esta realidad es la relativa al derecho al olvido, en este caso aplicado a los menores (30). El RGPD ha sido sensible a esta cuestión y se pronuncia, en principio, de forma amplia sobre esta posibilidad en su considerando 65 (que destaca la pertinencia de este derecho cuando el interesado dio su consentimiento siendo un niño, sobre todo en internet), si bien la concreta regulación contenida en el artículo 17 se limita a los datos recabados en el marco de la oferta directa a niños de servicios de la sociedad de la información (conforme a lo dispuesto en el art. 8.1 del propio Reglamento). En este sentido, las carencias señaladas del artículo 8 RGPD pueden hacer que se limite este derecho de supresión en relación con los menores. Nótese, por ejemplo, que no se define cuándo nos encontramos ante una oferta directa de SSI a menores; por otra parte, podríamos dejar fuera un amplio espectro de actividad de los menores en la Red, quizá la más importante, puesto que no entrarían SSI que no se cataloguen como «oferta directa» a niños. Por ello, una regulación más clara en la futura LOPD que permita ejercitarlo respecto de los datos suministrados en el marco de los SSI siendo menor a solicitud del titular (o, en su caso, representante legal) daría una mayor protección en este ámbito (31).

Con todo, hay que reconocer que la aplicación del derecho al olvido en la práctica plantea dificultades que, evidentemente, son extensibles e incluso se amplían en el caso de los menores. Y, por otra parte, se ha cuestionado que pueda hablarse propiamente de derecho al olvido digital en el ámbito de las redes sociales (que es donde de forma mayoritaria comparten la información los menores). Como se ha señalado, este derecho surge para hacer frente a los dilemas jurídicos que plantea la arquitectura de la Red, como son la perennidad de la información (noticias, resoluciones…) y el efecto multiplicador de los motores de búsqueda, se fundamenta en el principio de calidad de los datos y se concreta en los derechos de cancelación y oposición. Dilemas que son distintos a los que se producen en las

(29) De hecho, como más adelante se señalará, es la propia idea del que el consentimiento es suficiente para una correcta protección del afectado la que está en discusión (sin por ello entender que debe procederse a limitar la autonomía de los menores).

(30) Al respecto *vid.* Cobacho López, A., «Autodeterminación informativa de los menores a través de Internet (y II)», en Pérez Álvarez, S. y otros (directores), *Menores e Internet*, Thomson Reuters-Aranzadi, Cizur Menor, 2013, p. 364.

(31) Ya existe, además, un precedente al respecto: el artículo 40.2 Ley francesa de protección de datos (Loi n.° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés), en su redacción dada por la Ley para una república digital de 7 octubre 2016 y la enmienda núm. 259 al PLOPD va en este sentido.

redes sociales, donde es el propio usuario el que comparte la información personal y en donde hay una imposibilidad material de saber si la red social conserva los datos o con qué fines los utiliza. De ahí que en estos casos se ha dicho que lo que procede más bien es una correcta gestión del consentimiento por parte de las redes sociales (32).

Si optamos por este enfoque, esto nos lleva al tema de la virtualidad (y límites) del consentimiento en este ámbito. Por un lado, no hay que olvidar que el consentimiento, en cuanto base jurídica para el tratamiento de datos (art. 6.1.a RGPD), puede retirarse en cualquier momento (art. 7.3 RGPD). Pero también son necesarias medidas que incidan en otros momentos del proceso de gestión de datos. Así, hay que tener en cuenta que en el momento inicial de recabar el consentimiento éste se basa en políticas de privacidad que, como gráficamente se ha señalado, constituyen un *take it or leave it*, es decir, o se aceptan unas condiciones (que pueden llegar a ser abusivas) o no es posible la utilización del servicio, lo que plantea enormes dificultades desde el punto de vista de la exclusión de servicios «básicos», por ejemplo, de cara a la socialización en el caso de los menores. Frente a ello se propone el establecimiento de normas imperativas que limiten este tipo de cláusulas y que establezcan un mínimo en lo que a privacidad se refiere (33). Esta postura se enmarca en una línea de debate más amplia sobre los posibles límites del consentimiento como base jurídica para el tratamiento de datos en el entorno digital. En efecto, como ya hemos señalado, hoy en día el modelo de negocio en la Red está basado en el uso de la información de los usuarios. Frente a ello, y desde el ámbito europeo con el nuevo RGPD, se ha optado por seguir haciendo pivotar el sistema en el consentimiento del usuario, con ciertas medidas de reforzamiento (principio de minimización de datos, privacidad desde el diseño, reforzamiento de la transparencia e información…). Ahora bien, es dudoso que el consentimiento sin más (34) pueda ser en cualquier caso la base jurídica adecuada para el tratamiento de datos en un ámbito caracterizado por el desequilibrio o asimetría entre las posiciones

(32) Simón Castellano, P., *El reconocimiento del derecho al olvido digital en España y en la UE*, Bosch, Barcelona, 2015, pp. 311-312. No obstante, el RGPD no diferencia al regular esta cuestión entre motores de búsqueda y redes sociales.

(33) En este sentido, Simón Castellano, P., *ibidem*; al que le sigue en este punto Sánchez Gómez, A., *op. cit.*, p. 186. Señala también el primero de los autores mencionados el papel que pueden jugar los principios de privacidad desde el diseño y por defecto (actualmente regulados en el art. 25 RGPD). Aunque, como indica este autor, al final el problema es garantizar este respeto a la normativa de protección de datos y, en especial, al consentimiento cuando se trata de empresas con sede y servidores fuera de Europa.

(34) Algunos lo califican como «divulgación no espontánea de datos». *Vid.* Lorente López, M. C., «La vulneración de los derechos al honor, a la intimidad y a la propia imagen de los menores a través de las Nuevas Tecnologías», *Revista Aranzadi Doctrinal*, n.º 2/2015 (BIB 2015/258).

de las partes y en el que plantea dudas la especificidad y libertad de dicho consentimiento (35).

Por otra parte, también es necesario trascender del limitado ámbito de la protección de datos, al que se ha visto en gran medida reducida la protección de la privacidad en el ámbito de internet (y en el que sigue siendo un elemento clave el consentimiento del sujeto, que como hemos señalado, no resulta necesariamente el mecanismo más eficaz de protección en el actual escenario tecnológico), y profundizar en un concepto más amplio de privacidad y otras vías de protección (36). En esto, la LO 1/1982, de 5 de mayo, de protección civil de los derechos al honor, intimidad y propia imagen (LOPDH) y el propio artículo 4.3 LOPJM son elementos a tener en cuenta. Lo que ocurre es que se trata de normas que necesitan una actualización al actual escenario tecnológico (que tampoco se ha hecho en la reforma del año 2015).

Ya se han señalado aspectos de la LOPDH que merecen una reflexión (37): la inclusión de nuevos supuestos de intromisiones ilegítimas; o la incorporación de nuevos criterios, adaptados al ámbito digital, para la determinación del perjuicio o de las medidas que se pueden adoptar (art. 9). Pero podríamos destacar también aquí los relacionados con el consentimiento en la gestión y protección de los derechos a la intimidad y propia imagen. Así, habría que clarificar el conflicto entre la edad para consentir el tratamiento de datos (art. 8 RGPD o, en su caso, la que establezca el PLOPD) y el criterio de la madurez del artículo 3 LOPDH o el del artículo 4.3 LOPJM; o la coordinación del papel del consentimiento del menor/representante legal en el artículo 3 LOPDH y en el artículo 4.3 LOPJM (38), y si el criterio previsto en éste último para los medios de comunicación se extiende al ámbito digital (o, al menos, se relativiza la eficacia legitimadora del consentimiento del menor en estos derechos), incorporándose la protección reforzada del derecho a la propia imagen del menor corroborada por la jurisprudencia del TS y del TC (39); la relevancia que para delimitar el ámbito de pro-

(35) *Vid.*, entre otros, Oliver-Lalana, A. D. y Muñoz Soro, J. F., «El mito del consentimiento y el fracaso del modelo individualista de protección de datos», en Valero Torrijos, J. (coordinador), *La protección de los datos personales en Internet ante la innovación tecnológica*, Thomson Reuters-Aranzadi, Cizur Menor, 2013, pp. 154 y ss.; y en el mismo libro, Andreu Martínez, M. B. y Plana Arnaldos, M. C., «El poder de disposición del titular como facultad principal del derecho a la protección de datos personales: su efectividad en el actual escenario tecnológico», pp. 144 y ss.

(36) Burguera Ameave, L., *op. cit.*, pp. 323 y ss.

(37) Sánchez Gómez, A., *op. cit.*, pp. 181 y ss. Sobre la necesidad de reforma de la LOPDH, con especial atención a la notoriedad y la vulnerabilidad de las personas ofendidas, se pronuncia el Informe de la subcomisión de estudio sobre las redes sociales del Congreso *(BOCG* 9-4-2015). *Vid.*, asimismo, Escribano Tortajada, P., «Algunas cuestiones sobre la problemática jurídica del derecho a la intimidad, al honor y a la propia imagen en internet y en las redes sociales», en Fayos Gardó, A., *Los derechos a la intimidad y a la privacidad en el siglo* xxi, Dykinson, Madrid, 2014, p. 85.

(38) Habría que tener en cuenta también lo dispuesto en el artículo 7.1 Ley 7/2010, de 31 de marzo, General de la Comunicación Audiovisual (en adelante, LGCA).

(39) Sobre estas cuestiones, *vid.*, entre otros, Grimalt Servera, P., *op. cit.*, pp. 46 y ss.; Castilla Barea, M., *Las intromisiones legítimas en el derecho a la propia imagen*, Thomson Reuters-Aranzadi, Cizur Menor, 2011, pp. 203 y ss.

tección de estos derechos se le va a conceder a los propios actos del perjudicado o a los usos sociales (art. 2.1 LOPDH), a la vista del concepto de intimidad que tienen los propios menores en la actualidad y de la exposición pública que de ella se hace (40); así como una actualización del papel que corresponde al Ministerio Fiscal en la defensa de estos derechos (arts. 3.2 LOPDH y 4 LOPJM) (41).

4. EL ACCESO A CONTENIDOS NOCIVOS Y LA PUBLICIDAD DIRIGIDA A MENORES EN LOS SERVICIOS DE COMUNICACIÓN AUDIOVISUAL

Otra de las cuestiones en las que se ha centrado la protección de los menores en el entorno digital es la relativa a las medidas para evitar el acceso a contenidos ilícitos, reservados a adultos o, en general, que puedan perjudicarle en su desarrollo. Y, junto a éste, aunque en menor medida, la publicidad destinada a menores, con el fin de evitar prácticas abusivas o perjudiciales (42).

Estas preocupaciones han tenido desde el inicio un reflejo en la regulación en materia audiovisual. Actualmente el artículo 7 LGCA (conforme a las previsiones de la Directiva 2010/13/UE, de 10 de marzo de 2010, de servicios de comunicación audiovisual, DSCA) establece medidas específicas para los contenidos audiovisuales (prohibición de emisión de ciertos contenidos, etiquetado de contenido por edades, sistemas de filtrado, franjas horarias de emisión, mecanismos de bloqueo en el acceso a contenidos por catálogo perjudiciales para menores…) y respecto a la comunicaciones comerciales (no deben incitar a la compra aprovechando su inexperiencia o credulidad, o a persuadir a los padres o terceros para la compra, ni deben mostrar al menor en situaciones peligrosas…). Adicio-

(40) Para el ámbito penal también destaca García González, J., *op. cit.*, pp. 7-8, cómo la redefinición del concepto de «intimidad» que se da en el caso de los menores, puede modificar el alcance y eficacia de los delitos aparejados a una posible vulneración de este derecho. En este sentido, considera que la «tesis del despojamiento de la intimidad» u otra mantenida por el TS deberá revisarse ante la «extemidad» con la que actúa la hipotética víctima de ciberdelincuencia intrusiva. Pero, incluso, también puede tener relevancia a la hora de incriminar o no la conducta denunciada; como señala este autor existen precedentes en nuestro ordenamiento en los que se niega la protección penal frente a delitos «facilitados» por la propia víctima y de hecho ya se plantea en relación con el delito previsto en el artículo 197.7 CP.

(41) Y, en coordinación con estos, los arts. 59 y 60 de la Ley 15/2015, de 2 de julio, de la jurisdicción voluntaria. La Instrucción 2/2006, de la Fiscalía General del Estado, sobre el fiscal y la protección del derecho al honor, intimidad y propia imagen de los menores (con un apartado, además, dedicado a estos derechos en Internet), ya realizó una primera aproximación a la materia.

(42) No hay que obviar que la publicidad influye también en la visión que el menor tiene de sí mismo, de sus relaciones con el entorno y, en general, en su desarrollo como persona. *Vid.* Andreu Martínez, M. B., *op. cit*, pp. 168 y ss. Y el estudio sobre las repercusiones en el comportamiento de los niños del marketing a través de las redes sociales, los juegos en línea y las aplicaciones móviles (accesible en: http://collections.internetmemory.org/haeu/20171123130248/http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/impact_media_marketing_study/index_en.htm).

nalmente, y para el tema de la publicidad, también existen previsiones específicas tanto en la Ley 34/1988, de 11 de noviembre, General de Publicidad, por ejemplo, considerándose ilícita la publicidad a menores con las características antes señaladas (art. 3.b), o en la Ley 3/1991, de 10 de enero, de Competencia Desleal, que reputa desleal la publicidad ilícita y regula también ciertas prácticas publicitarias agresivas en relación con menores (arts. 18, 30) (43).

La base última de estas normas se encuentra en el artículo 20.4 CE y en derechos reconocidos al menor en la CDN (y LOPJM), como la libertad de expresión, y otros relacionados con éste, como la libertad de pensamiento y de conciencia, el respecto a su vida privada, el derecho a la educación, a participar en la vida cultural y artística y al juego y, en última instancia, al libre desarrollo de su personalidad. La CDN considera a los medios de comunicación como un pilar básico en el derecho de acceso a la información por el menor (art. 17), debiendo alentárseles a que difundan información y materiales de interés social y cultural para el niño. Por lo tanto, el bienestar del menor constituye un elemento fundamental en su derecho de acceso a la información, con el fin último de potenciar su propio desarrollo y su formación como persona.

No obstante, y al igual que se ha señalado anteriormente para otros ámbitos, sigue pendiente una plena incorporación de estas cuestiones al ámbito digital. En esta línea ya se pronunció la Comisión Europea en su «Estrategia europea a favor de una internet más adecuada para los niños», de mayo de 2012 (44). Como señaló la Comisión, las necesidades particulares de este sector de la población y sus puntos vulnerables merecen un tratamiento específico que permita que Internet se convierta en un lugar en el que los menores puedan acceder al conocimiento, comunicarse, desarrollar aptitudes y mejorar sus expectativas laborales (45). Para la Comisión, la línea a seguir era fomentar las normas autorregulatorias en esta materia, testigo que ha sido recogido por el artículo 5 LOPJM (tras la reforma de 2015), al incluir una referencia a la autorregulación en lo relacionado con el acceso a contenidos ilícitos.

---

(43) Un amplio análisis de este tema, tanto en la DSCA como en la normativa española, puede verse en Martínez Otero, J. M., *La protección jurídica de los menores en el entorno audiovisual*, Thomson Reuters-Aranzadi, Cizur Menor, 2013, pp. 114 y ss., 183 y ss.; destacando esta autor, entre otros, la necesidad de una mayor concreción de qué debe considerarse contenido perjudicial para el menor.

(44) COM (2012) 196 final.

(45) Por ello, dentro de esta estrategia, estableció como el primero de sus pilares el «fomento de unos contenidos en línea de calidad para los niños» y, dentro del tercer pilar (garantizar la seguridad en línea de los menores), se incluyó como objetivo el evitar la publicidad inadecuada en línea (promoviendo que las normas sobre publicidad en sitios web para niños tengan un nivel de protección equiparable al de la publicidad en los servicios audiovisuales y evitando la exposición de los menores a publicidad inadecuada en cualquier medio en línea).

Esta tarea de adecuación al mundo digital pretende llevarse a cabo en parte a través de la Propuesta de reforma de la DSCA, de 25 de mayo de 2016 (46), en la que se reconocen los cambios en los hábitos de consumo de contenidos audiovisuales (con la convergencia entre la televisión tradicional y los contenidos distribuidos a través de internet) y se pretende una unificación normativa y de niveles de protección para todos los agentes del sector. Precisamente uno de sus objetivos es reforzar la protección de los menores. Así, por ejemplo, se establece la obligación de informar sobre contenidos que puedan perjudicar a menores (a través de advertencias acústicas, símbolos visuales...) y se amplían las medidas para impedir el acceso a contenidos perjudiciales o nocivos, que se aplicarán a cualquier servicio de comunicación audiovisual (ya sean los tradicionales o a petición). También se contienen previsiones para reforzar lo relativo a la publicidad de alimentos poco saludables, tabaco y alcohol, a través de la autorregulación y la corregulación. Pero la verdadera novedad es la inclusión de las plataformas de distribución de vídeos, esto es, las que incluyen contenidos creados por los propios usuarios (como YouTube) a ciertos efectos. En concreto, obliga a los Estados a adoptar medidas adecuadas para proteger a los menores frente a contenidos perjudiciales (sin, por ello, modificar la exención de responsabilidad por contenidos ilícitos alojados en la web en los términos de los arts. 14 y 15 de la Directiva 2000/31/CE, de comercio electrónico, DCE). Las medidas estarán relacionadas con la organización de los contenidos, no con el contenido en sí mismo (por ej., mecanismos de verificación de edad, control parental, sistemas de calificación de contenidos por el usuario, de denuncia de contenidos ilícitos…) (47). La opción de la Directiva en este caso es el establecimiento de una obligación de medios a estas plataformas a través de la corregulación.

Las reformas a nivel europeo conllevarán la necesaria modificación de la LSCA en lo relativo al reforzamiento de la protección de menores frente a contenidos y comunicaciones comerciales perjudiciales (48). No obstante, a nuestro entender las medidas en relación con estas últimas son poco ambiciosas, se limitan a ciertos productos nocivos y se remiten a la adopción de códigos de conducta, cuando el impacto publicitario, en particular a través de un medio como Internet, puede tener una gran influencia en el desarrollo del menor. Por otra parte, también se podrían complementar con el reforzamiento de ciertas medidas en relación con la protección de

(46) COM(2016) 287 final.

(47) Sobre el tema puede verse Mendoza Losana, A. I., «La nueva regulación europea del mercado audiovisual. Propuesta de revisión de la Directiva 2010/13/UE», *Revista CESCO de Derecho de Consumo*, n.º 18, 2016, pp. 166 y ss.

(48) Y, en su caso, otras como el artículo 5 LOPJM o su coordinación con la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico (LSSI).

datos de menores. En concreto, para la publicidad orientada a comportamientos y perfiles en línea ya apuntó la Comisión europea en su Estrategia a favor de una internet más adecuada para los niños (2012) que no deberían crearse segmentos para niños (49) y que deberían basarse en normas de autorregulación (50). En este punto, el nuevo RGPD no recoge, sin embargo, de forma clara esta limitación [*vid.* art. 22 (51)], oportunidad que podría aprovecharse en el artículo 18 del PLOPD.

Ahora bien, el verdadero reto lo sigue constituyendo, más allá de los servicios de comunicación audiovisual, el acceso a contenidos ilícitos, nocivos o comunicaciones comerciales perjudiciales en general en el ámbito de Internet y las redes sociales. Éstas últimas quedan fuera de las previsiones de la propuesta de reforma de la DSCA de 2016, que se aplica a las plataformas de distribución de vídeos (52). La norma básica en este ámbito sigue siendo la DCE, aplicable a los prestadores de SSI (53); y, sobre esta base se avanza, sobre todo, a nivel supranacional y en coordinación con la propia industria, por ejemplo, para la mejora de los mecanismos de notificaciones o la implementación de medidas activas (incluidas las automatizadas) en la detección de contenidos ilícitos (sin perjuicio de las reglas de responsabilidad y sus exenciones previstas en dicha Directiva) (54).

5. UN ÚLTIMO APUNTE: OTRAS VÍAS DE INTERVENCIÓN Y UNA ASIGNATURA PENDIENTE

De todo lo dicho anteriormente es fácilmente deducible que la intervención legislativa es necesaria. De hecho, sería deseable una mayor determinación por parte del legislador español para no ir únicamente a rebufo de las obligaciones derivadas de la normativa europea. Ahora bien, como se ha apuntado, la verdadera protección de los menores en el ámbito digital conlleva la implicación de los diversos actores, dotando de herramientas a los propios usuarios (a los que se considera como verdaderos

(49) En este sentido, también el Grupo de Trabajo del Artículo 29 en su Dictamen 2/2010, de 22 de junio, sobre publicidad comportamental en línea.

(50) Y señalaba como modelo a seguir las definidas por la Alianza Europea por la Ética en la Publicidad (*European Advertising Standards Alliance*, EASA) para la publicidad comportamental.

(51) Únicamente en el considerando 38 se señala que la protección específica de la que son merecedores los menores debe aplicarse al ámbito de la elaboración de perfiles de personalidad o usuario.

(52) La finalidad principal de las redes sociales no es *a priori* la de ofrecer programas y vídeos generados por los usuarios al público en general, conforme a la definición que da la propuesta DSCA de 2016 para dichas plataformas (art. 1).

(53) Acerca de la normativa aplicable a Internet y redes sociales (en particular, la regulación en la LSSI) y las posibles respuestas antes contenidos ilícitos o nocivos en redes sociales, *vid.* Martínez Otero, J. M., *op. cit.*, pp. 239 y ss.

(54) Entre las últimas actuaciones en esta línea se puede citar (aunque con carácter general y no solo destinada a contenidos ilícitos relacionados con menores) la Recomendación (UE) 2018/334 de la Comisión, de 1 de marzo de 2018, sobre medidas para combatir eficazmente los contenidos ilícitos en línea. Sin perjuicio de que también se adopten medidas legislativas, como las Directivas 2011/92/UE, de 13 diciembre de 2011 o 2017/541, de 15 de marzo de 2017.

protagonistas en la protección de sus derechos), padres, educadores y fomentando la implicación de la industria.

En este sentido, como también hemos visto, uno de los instrumentos que se ha potenciado es la autorregulación y la corregulación. La dimensión global de internet y la dificultad de las legislaciones para adaptarse a los rápidos cambios que se producen en el ámbito tecnológico han sido, entre otras, las razones de peso para potenciar esta vía (55). La iniciativa autorregulatoria se ha visto reflejada en muy diferentes campos (publicitario, SSI, telefonía móvil…), del que podríamos destacar aquí la Alianza para una mejor protección en línea de los menores (formada por empresas tecnológicas y de telecomunicaciones, del sector de juegos y entretenimiento infantil, y ONGs) que puso en marcha en 2017 una iniciativa dirigida a luchar contra contenidos, conductas y contactos perjudiciales (56). También el nuevo RGPD potencia la adopción de Códigos de Conducta en esta materia (entre otros, para especificar lo relativo a la información a menores y el tratamiento de sus datos personales, art. 40.2) y la existencia de organismos de supervisión de su cumplimiento independientes (art. 41).

Otro de los ejes básicos de actuación son las medidas de sensibilización de los usuarios, en particular de los propios menores, los padres y la comunidad educativa. Estas forman parte de los diversos planes y acciones impulsados por los organismos nacionales y europeos, y por la propia sociedad civil. De hecho, en la estrategia europea a favor de una Internet más segura para los niños 2012 (estrategia BIK) uno de los pilares lo constituyó la sensibilización y la capacitación. Con base en esta acción se han creado en todos los países europeos los SIC (por sus siglas en inglés, Centros para una internet más segura), que vienen desarrollando estas acciones de sensibilización ciudadana y líneas telefónicas de ayuda (pertenecientes a la red INSAFE), en las que los padres e hijos pueden obtener asesoramiento y ayuda; así como líneas directas de denuncia de contenidos ilícitos (coordinadas por la red INHOPE) (57). En España, junto a las

(55) Fernández Pérez, A., «La protección de los derechos fundamentales de los menores en Internet desde la perspectiva europea», *Ius et Praxis*, Año 22, n.º 1, 2016, pp. 388 y ss.; Martínez Otero, J. M., *op. cit.*, pp. 236 y ss.; Bendito Cañizares, M. T., *La autorregulación: una alternativa para la protección de los menores digitales*, UNED, Madrid, 2012.

(56) Accesible en: https://ec.europa.eu/digital-single-market/en/news/safer-internet-day-2017-european-commission-welcomes-alliance-industry-and-ngos-better-internet. Como se señala, esta iniciativa podría preparar el terreno para mecanismos de autorregulación y corregulación más formales que la propuesta de DSCA pretende promover. Por otra parte, con esa iniciativa se complementan otras anteriores como la Coalición CEO para hacer de Internet un lugar mejor para los niños; los principios de la UE para unas redes sociales más seguras o el Marco europeo para un uso más seguro del móvil por niños y adolescentes. *Vid.* la información al respecto en: https://ec.europa.eu/digital-single-market/en/self-regulation-and-stakeholders-better-internet-kids.

(57) Más información en https://www.betterinternetforkids.eu/. Por otra parte, según el informe final del programa europeo una Internet más segura 2009-2013 (Informe de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las

acciones de organizaciones sociales y profesionales, hay que destacar la labor realizada por entidades estatales como INCIBE y Red.es (58). Y dentro de ésta, la reciente creación de IS4K, que es el Centro de Seguridad en Internet (SIC) para menores de edad en España, que tiene asignadas tareas fundamentalmente de formación y concienciación, organiza en España el Día de la Internet Segura, ofrece materiales y contenidos relacionados con el uso seguro y responsable de las TIC y los servicios de línea de ayuda y de reporte, entre otros (59).

Junto a estas actividades de formación y capacitación impulsadas por las distintas entidades públicas y organizaciones sociales, queda pendiente una verdadera introducción de estas materias en la formación reglada. La importancia de la educación en competencias digitales como la mejor vía para una protección eficaz de los menores ha sido puesta de relieve desde diversas instancias. Por citar un ejemplo, la propia Comisión europea, en su informe final de evaluación del programa Una Internet más Segura 2016, destaca la necesidad de que los menores adquieran competencias digitales, idealmente a través de los planes de estudio escolares (60). Por tanto, una vez creado el SIC en España y sin perjuicio de que se siga apoyando y reforzando sus tareas, el siguiente paso que habrá que abordar necesariamente desde las instancias competentes es un impulso de la introducción en los planes curriculares de materias que aborden la ciberseguridad o la gestión de la identidad digital por los menores. Ello lleva también necesariamente la capacitación del profesorado, no solo mediante la «educación informal» o formación especializada adicional, sino en los propios grados de educación. Celebramos por ello una enmienda como la 302 al PLOPD (dedicada al derecho a la educación digital) y que de incluirse en el texto que finalmente se apruebe constituiría un

---

Regiones, COM (2016) 364 final) de 6 de junio de 2016, una de las acciones que se consideraron más importantes y en las que se consiguió un mayor impacto fue la sensibilización, junto con la educación, formación y herramientas y materiales destinados a ser utilizados por los niños. También destaca los avances en concienciación de padres y menores, Garmendia Larrañaga, M. y otros, *op. cit.*, p. 100.

(58) Sin ánimo exhaustivo y respecto de la labor llevada a cabo por otras entidades, puede citarse, por ej., el portal «Tu decides en Internet», de la AEPD (http://www.tudecideseninternet.es/agpd1/), o la organización Pantallas Amigas (http://www.pantallasamigas.net/).

(59) Puede consultarse su contenido en: https://www.is4k.es/. Un análisis de esta herramienta en Davara Fernández De Marcos, L., «IS4K, Nueva herramienta sobre el «tema de moda»: Menores y seguridad en Internet», *Actualidad Administrativa*, n.º 4, 2017 (LA LEY 2528/2017).

(60) *Vid.* también la Ponencia conjunta de estudio sobre riesgos derivados del uso de la red por parte de los menores del Senado (BOCG 3.10.2014) y el Informe de la subcomisión de estudio sobre las redes sociales del Congreso (BOCG 9.4.2015), así como la Proposición no de Ley (162/000384) presentada por el Grupo Parlamentario Socialista, sobre protección de los derechos digitales de la ciudadanía (BOCG Congreso de los Diputados 7.04.2017). Sobre la obligación de los centros educativos de formar en el uso de las TIC, Davara Fernández De Marcos, L., *Menores en internet y redes sociales: derecho aplicable y derechos de los padres y centros educativos*, AEPD/Agencia estatal BOE, Madrid, 2017, pp. 65 y ss. En relación con la privacidad, se puede hacer referencia al proyecto europeo ARCADES (Introducing Data Protection and Privacy Issues at Schools in the European Union): http://arcades-project.eu/.

paso significativo en esta dirección. Un avance también importante lo constituye el Marco Común de Competencia Digital Docente (2017) de INTEF (Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado), con un área 4 de Seguridad que incluye competencias en protección de datos personales, de la identidad digital y uso responsable y seguro, entre otras.

CAPÍTULO 20

MAYORES Y CIUDADANÍA DIGITAL

LEOPOLDO ABAD
Profesor Titular (Universidad San Pablo-CEU)

1. LAS PERSONAS MAYORES ANTE LOS NUEVOS PARADIGMAS DERIVADOS DE LA SOCIEDAD DE LA INFORMACIÓN

Las Tecnologías de la Información y de la Comunicación son, sin duda, uno de los principales escenarios de la socialización de un sujeto del siglo XXI y requieren ciudadanos que se actualicen permanentemente debido a que la cultura digital está en constante transformación, tanto de sus contenidos como de sus formas (1). Esta necesidad de acceso a las tecnologías de la información son fundamentales en la presente realidad histórica y social denominada genéricamente como Sociedad de la Información.

En este contexto, no podemos obviar la situación de envejecimiento demográfico a las que están sometidas las sociedades occidentales, y especialmente la española. Actualmente, y según datos del INE a 1 de julio de 2017 un 18,27% de la población española es mayor de 65 años. Pero si valoramos la proyección poblacional española, en 2050 seremos el segun-

(1) AREA MOREIRA, M., *et alii*, *Alfabetización digital y competencias informacionales*. Fundación Telefónica. Editorial Ariel. Madrid, 2012, p. 20.

do país más envejecido del mundo tras Japón, con un 34% de personas mayores de 65 años y un 15% de población mayor de 80 años. Este profundo cambio demográfico se produce a la par que una revolución similar a la que supuso la imprenta o la Revolución Industrial: Internet y el desarrollo de las TIC. Una población que va envejeciendo supone un cambio en las estructuras económicas, sociales y tecnológicas para un país. Las personas mayores se ven compelidas por las circunstancias a la necesidad de desarrollar habilidades y destrezas en el uso de las TIC y así disminuir la brecha digital entre conectados (jóvenes y adultos) y no conectados (personas mayores).

Sin embargo, los datos del INE de octubre de 2017 sobre el uso de las TIC por las personas mayores, muestran como sólo un 36,4% ha usado el ordenador en los últimos tres meses, sólo un 38% de los mayores de 65 años usa Internet una vez por semana (frente al 91% en Luxemburgo o el 87% en Islandia) y sólo un 10,6% realiza compras on-line.

Ello parece indicar la existencia de la denominada brecha digital generacional, conceptualizada como la diferencia en el acceso, uso y capacitación para el empleo de las TIC entre las distintas generaciones. Parece por tanto una evidencia que el uso provechoso de las TIC es beneficioso para este grupo poblacional como elemento clave en los procesos de envejecimiento activo. Esta nueva realidad socio-tecnológica a la que se enfrentan las personas mayores está caracterizada por una serie de cambios en los paradigmas sociales que tienen una influencia decisiva en la forma de entender la ciudadanía digital, pero especialmente condicionan la participación cívica vinculada a las TIC de las personas mayores (2).

Tanto es así, que este empleo de las TIC ha llegado a ser configurado como un derecho más dentro de los que la persona puede reivindicar. No podemos perder de vista, que el manejo de las TIC se convierte en fundamental para que el ciudadano puede estar informado en toda su amplitud de las cuestiones que de forma directa le afectan y así participar realmente en la vida comunitaria tanto desde una perspectiva societaria como política. Como señala Martínez Nicolás (3) «la continuidad conceptual y práctica que debe existir entre el acceso a las NTIC y la participación ciudadana en la vida pública, de forma tal que esta última dimensión –y no solo el acceso– también debe quedar atendida en las estrategias de im-

(2) Estos paradigmas son resumidos por Lancho: igualdad digital, sensación de presentismo, globalización, mestizaje, omnipresencia tecnológica, participación social, consumo inmoderado, sacralización de la juventud, expansión del ocio, conectividad constante y espectacularización de los hechos. Lancho, J., «Los nuevos paradigmas sociales y su repercusión en los procesos de aprendizaje», en Jiménez Frías, R. (Coord.), *Educación de personas adultas en el marco del aprendizaje a lo largo de la vida*, UNED, Madrid, 2009, pp. 14-24.

(3) Martínez Nicolás, M., «De la brecha digital a la brecha cívica. Acceso a las tecnologías de la comunicación y participación ciudadana en la vida pública», en *Revista TELOS (Cuadernos de Comunicación e Innovación)*, enero-marzo 2011, p. 2.

plantación de la Sociedad de la Información y el Conocimiento (SIC) cualquiera que sea el nivel de intervención (local, estatal, supranacional)».

En este contexto de participación ciudadana creemos importante destacar el concepto de cultura participativa, entendida como la posibilidad de actuación del sujeto en sus ámbitos sociales más cercanos a través de interacciones culturales empleando los distintos medios de comunicación (digitales y no digitales) a su alcance. Jenkins (4) considera que debemos centrarnos más en el concepto de culturas de participación en lugar de en el concepto de tecnologías interactivas. La interactividad es una propiedad de la tecnología, mientras que la participación es una característica de la cultura. Focalizarse en ampliar el acceso a las nuevas tecnologías nos lleva sólo hasta cierto punto si no lo hacemos también fomentando las habilidades y conocimientos culturales necesarios para implementar dichas herramientas hacia nuestros propios fines.

En definitiva, el uso de las TIC tiene como meta sustantiva facilitar el proceso de la construcción del individuo como ciudadano culto y democrático y de su socialización en los ecosistemas comunicacionales digitales. De este modo, los objetivos de la participación digital deberían dirigirse a que todos, pero creemos que especialmente las personas mayores, que se encuentran en muchas ocasiones en situación de vulnerabilidad digital:

— Logren las competencias de dominio de los mecanismos y de las formas de comunicación de las distintas herramientas digitales.

— Adquieran criterios de valor que les permitan discriminar y seleccionar aquellos productos, informaciones o contenidos de mayor calidad cultural.

— Sepan sacar a la luz los intereses económicos, políticos e ideológicos que están detrás de toda empresa, proyecto y producto mediático.

— Sean capaces de comunicarse y colaborar en redes sociales.

— Tengan las habilidades para expresarse y crear productos en distintos lenguajes expresivos.

— Tomen conciencia crítica del papel de las tecnologías en nuestra vida cotidiana, económica y social.

2. LOS DERECHOS DE LOS MAYORES EN LA SOCIEDAD DE LA INFORMACIÓN

Quizá no sea este el lugar para reflexionar sobre las diversas generaciones de derechos y específicamente sobre la existencia de derechos de

(4) Jenkins, H., *Confronting the Challenges of Participatory Culture: Media Education for the 21st Century*, The MacArthur Foundation, Chicago, 2008, pp. 7-8.https://mitpress.mit.edu/sites/default/files/titles/free_download/9780262513623_Confronting_the_Challenges.pdf.

nueva generación de carácter tecnológico, aunque trataremos el tema de forma tangencial al final del presente epígrafe. No obstante, sí parece lógico considerar que si el Derecho debe tener finalidad la obtención de la justicia en la clásica definición de Ulpiano (5), nada es más justo que dar un tratamiento específico a aquellos en situación de vulnerabilidad, reconociéndoles determinadas peculiaridades así como abogar por la acción de los Poderes públicos para que su participación en la sociedad sea real, y específicamente darles acceso a las posibilidades que ofrece la tecnología en la actualidad en el marco de la denominada Sociedad de la Información.

Si nos atenemos al reconocimiento de los derechos de las personas mayores como grupo social diferenciado, encontramos referencias en el artículo 25 de las Declaración Universal de Derechos Humanos de 10 de diciembre de 1948, que establece que «Toda persona tiene derecho a un nivel de vida adecuado que le asegure, así como a su familia, la salud y el bienestar, y en especial la alimentación, el vestido, la vivienda, la asistencia médica y los servicios sociales necesarios; tiene asimismo derecho a los seguros en caso de desempleo, enfermedad, invalidez, viudez, vejez u otros casos de pérdida de sus medios de subsistencia por circunstancias independientes de su voluntad» (6).

También podemos destacar el compromiso de la Unión Europea (UE) con la agenda de envejecimiento activo, que se basa en sus valores fundamentales, definidos en los Tratados. El Tratado de Lisboa de 2009 confirmó que «La Unión se fundamenta en los valores de respeto de la dignidad humana, libertad, democracia, igualdad, Estado de Derecho y respeto de los derechos humanos [...] La Unión combatirá la exclusión social y la discriminación y fomentará la justicia y la protección sociales, la igualdad entre mujeres y hombres [y] la solidaridad entre las generaciones».

Por su parte, la Carta de los derechos fundamentales de la Unión Europea (2000/C 364/01) (7) establece en su Capítulo III dedicado a la Igual-

---

(5) *Iustitia est constans et perpetua voluntas ius suum cuique tribuendi;* «La justicia es la constante y perpetua voluntad de dar (conceder) a cada uno su derecho».

(6) Otras referencias las encontramos en la Carta Social Europea de 18 de octubre de 1966 (revisada en 1996) del Consejo de Europa que establece en su epígrafe 23 que «Toda persona de edad avanzada tiene derecho a protección social», también el Código Europeo de Seguridad Social (Estrasburgo, 16 de abril de 1964, ratificado por España el 4 de febrero de 1994) dedica su Parte V a las «Prestaciones de vejez», podemos también citar el Convenio n.º 128, de 29 de junio de 1967, de la Organización Internacional del Trabajo relativo a las prestaciones de invalidez, vejez y sobrevivientes, así como la Carta comunitaria de los Derechos Sociales de los Trabajadores (9 de diciembre de 1989) donde se recoge la protección de las personas de edad avanzada y específicamente sobre la protección social por jubilación, al decir que « De acuerdo con las modalidades de cada país: 24. Al llegar a la Jubilación todo trabajador de la Comunidad Europea debe poder disfrutar de recursos que le garanticen un nivel de vida digno. 25. Toda persona que haya alcanzado la edad de jubilación, pero que no tenga derecho a pensión y que no tenga otros medios de subsistencia, bebe poder disfrutar de recursos suficientes y de una asistencia social y médica adaptadas a sus necesidades específicas».

(7) http://www.europarl.europa.eu/charter/pdf/text_es.pdf.

dad en su artículo 20 (Igualdad ante la ley) que «Todas las personas son iguales ante la ley», y en su artículo 21 (No discriminación) que «Se prohíbe toda discriminación, y en particular la ejercida por razón de sexo, raza, color, orígenes étnicos o sociales, características genóticas, lengua, religión o convicciones, opiniones políticas o de cualquier otro tipo, pertenencia a una minoría nacional, patrimonio, nacimiento, discapacidad, edad u orientación sexual». Específicamente en el artículo 25 (Derechos de las personas mayores) se declara que «La Unión reconoce y respeta el derecho de las personas mayores a llevar una vida digna e independiente y a participar en la vida social y cultural» (8).

En el ámbito americano se ha promulgado la Convención Interamericana sobre la protección de los derechos humanos de las personas mayores (9) que en su artículo 1 bajo el epígrafe «Ámbito de aplicación y objeto» declara que «el objeto de la Convención es promover, proteger y asegurar el reconocimiento y el pleno goce y ejercicio, en condiciones de igualdad, de todos los derechos humanos y libertades fundamentales de la persona mayor, a fin de contribuir a su plena inclusión, integración y participación en la sociedad. Entre los principios generales aplicables a la Convención incluidos en el artículo 3 destacan la promoción y defensa de los derechos humanos y libertades fundamentales de la persona mayor; la valorización de la persona mayor, su papel en la sociedad y contribución al desarrollo; o la participación, integración e inclusión plena y efectiva en la sociedad.

Especialmente esta Convención recoge que los Estados miembros signatarios se comprometen específicamente a «promover la educación y formación de la persona mayor en el uso de las nuevas tecnologías de la

(8) La preocupación por las personas mayores en los poderes públicos tiene una larga trayectoria. Específicamente en el ámbito de la Unión Europea, el interés por las personas mayores se manifiesta desde hace años a través de diversas iniciativa. Un resumen de dichas iniciativas podemos encontrarlo en Pérez Serrano, G., «Estereotipos, vez y bienestar social», en Pérez Serrano, G. (Coordinadora), *Calidad de vida en personas mayores (2.º ed.)*, Dykinson, Madrid, 2006, pp. 53-54; o en Pérez De Gatta Sánchez, D., «La política y las acciones de la Unión Europea sobre la dependencia derivada del envejecimiento de la población», en *Noticias de la Unión Europea n.º 303, abril 2010*, p. 10. Un resumen detallado de todas ellas pueden consultarse en el epígrafe «Unión Europea, envejecimiento activo y alfabetización digital» en Abad Alcalá, L., *Alfabetización mediática par la e-inclusión de personas mayores»*, Dykinson, Madrid, 2017, pp. 88-102. Destacamos entre dichas iniciativas, la Comunicación de la Comisión «Envejecer mejor en la sociedad de la información. Una iniciativa i2010. Plan de Acción sobre Tecnologías de la Información y Comunicación y envejecimiento» [COM (2007) 332 final]; el Informe de la Comisión de Cultura y Educación del Parlamento Europeo publicado el 24 de noviembre de 2008 '/TitreType''Titre'sobre la alfabetización de los medios de comunicación en un mundo digital [A6-0461/2008], las 'DocRef' Conclusiones del Consejo, de 22 de mayo de 2008, sobre «Un planteamiento europeo de la alfabetización mediática en el entorno digital» [2008/C 140/08] o la Recomendación de la Comisión de 20 de agosto de 2009 sobre la alfabetización mediática en el entorno digital para una industria audiovisual y de contenidos más competitiva y una sociedad del conocimiento incluyente [2009/625/CE]. '/DocRef'

(9) 57http://www.oas.org/es/sla/ddi/tratados_multilaterales_interamericanos_A70_derechos_humanos_personas_mayores.asp.

información y comunicación (TIC) para minimizar la brecha digital, generacional y geográfica e incrementar la integración social y comunitaria».

Por su parte la Constitución española, y al margen de la aplicación de algunas de estas declaraciones en virtud de su artículo 10.2 (10), el artículo 10 reconoce en su punto 1 que «La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social», y en su artículo 14 la no discriminación por edad incluido en el genérico principio de igualdad ante la ley que no permite discriminación por condición o circunstancia personal o social. Más específicamente, y donde podría encontrarse el amparo constitucional a cualquier iniciativa de inclusión digital de las personas mayores es en el artículo 50, que bajo el epígrafe «Derecho a acceder a prestaciones sociales y asistenciales» establece que «Los poderes públicos […] promoverán su bienestar (el de los ciudadanos durante la tercera edad) mediante un sistema de servicios sociales que atenderán sus problemas específicos de salud, vivienda, cultura y ocio». Entendemos que la necesidad de la inclusión digital puede ser catalogado como un problema específico de cultura, ocio e incluso salud, que requiere dicha intervención de los poderes públicos.

Uno de los aspectos que algunos autores destacan como limitativos de este principio de promoción del bienestar de las personas mayores es la imposibilidad de acceder a la información que a menudo está disponible en formatos (muchos de ellos digitales) que no son accesibles o adecuados para las personas mayores, dificultando su participación en la sociedad (11) y especialmente la imposibilidad de cumplimiento del artículo 20 de la Declaración Universal de Derechos Humanos (12). Este aislamiento social tiene efectos a largo plazo sobre la integración social, el acceso a la información, e incluso el acceso a la ley. Una sociedad basada en el conocimiento y en los servicios, existente en muchos países desarrollados y que muchos países en vías de desarrollo aspiran a tener, requiere de políticas que garanticen el acceso permanente a la educación y la forma-

(10) Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España.

(11) Martin, C. *et alii*, *Human Rights of Older People*, Springer, Nueva York, 2015, p. 43.

(12) «Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión». *Vid.* al respecto Abad Alcalá, L., «El derecho a la información en los textos universales» en Bel Mallén, J. I. y Corredoira y Alfonso, L. (Dir.), *Derecho de la información: el ejercicio del derecho a la información y su jurisprudencia*, Centro de Estudios Políticos y Constitucionales, Madrid, 2015, pp. 49-68.

ción (13). Como indica la Carta Europea de los derechos y responsabilidades de las personas mayores que necesitan atención y asistencia a largo plazo (14) en su artículo 6 «A medida que pasan los años y puede llegar a depender de otros para el apoyo y la atención, se sigue teniendo el derecho a relacionarse con los demás, a participar en la vida cívica, al aprendizaje permanente y a la actividad cultural». El acceso a Internet y a la alfabetización informática puede tener un dramático efecto positivo en el ejercicio del derecho de acceso a la información, la libre asociación y la participación en la sociedad (15).

Por tanto, el derecho de acceso a la información, mucha de ella en formatos digitales, se configura como un derecho de raigambre individual que permite el libre desarrollo de la personalidad en la línea del artículo 10.1 de la Constitución española (16). Así lo entiende Sánchez de Diego al considerar que el acceso a la información pública «es requisito para la participación pública, pero también es una mecanismo para que las personas puedan satisfacer otros intereses, incluso privados. Es definitiva, el acceso a la información es un requisito previo de la participación del ciudadano en la *res pública,* pero su finalidad la participación, pues se constituye en un auténtico derecho fundamental que busca la realización de la persona en una sociedad globalizada, en donde la información es clave del desarrollo, del progreso y, en definitiva, del éxito» (17). La información constituye el elemento básico de la conformación de una visión personal de la existencia y frente a posturas que limitan esta búsqueda a los profesionales de la información, no puede entenderse el artículo 10 de la Constitución española sin reconocer este derecho a todo individuo. El libre desarrollo de la personalidad requiere de los instrumentos necesarios para que este procese se lleve a cabo y entre ellos, el derecho de acceso a la información se convierte en requisito indispensable para proveer de materia prima al sujeto sobre el que edificar su propia conformación personal de la existencia.

Bustamente incluso ha configurado lo que denomina «cuarta generación» de los derechos humanos como expansión del concepto de ciudadanía digital, que presenta tres dimensiones. En primer lugar, como amplia-

(13) Judge, L. (2008). *The rights of older people: International Law, Human Rights Mechanisms and the Case for New Normative Standards, en* www.globalaging.org/elderrights/world/2008/internationallaw.pdf.

(14) http://www.age-platform.eu/images/stories/22204_AGE_charte_europeenne_EN_v4.pdf.

(15) Martin, C…., *op. cit.*, p. 175.

(16) «La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la Ley y a los derechos de los demás son fundamento del orden político y de la paz social».

(17) Sánchez de Diego, M., «Un derecho fundamental a acceder a la información pública», en Sánchez de Diego, M. (Coord.), *El derecho de acceso a la información pública*, Universidad Complutense, Madrid, 2008, p. 30.

ción de la ciudadanía tradicional, enfatizando los derechos que tienen que ver con el libre acceso y uso de información y conocimiento, así como con la exigencia de una interacción más simple y completa con las Administraciones Publicas a través de las redes telemáticas. En segundo lugar, ciudadanía entendida como lucha contra la exclusión digital, a través de la inserción de colectivos marginales en el mercado de trabajo en una Sociedad de la Información (SI) (políticas de profesionalización y capacitación). Por último, como un elemento que exige políticas de educación ciudadana, creando una inteligencia colectiva que asegure una inserción autónoma a cada país en un mundo globalizado (18). Concluye Bustamante, que deben garantizarse previamente otros fines intermedios: un nivel de pericia técnica suficiente para utilizar el voto electrónico, acceso abierto y barato a la Red, un nivel de educación y de discernimiento para filtrar y seleccionar información, capacidad de contrastar la información en circulación, etc. En definitiva, considera que puede ser un error centrar la discusión poniendo demasiado énfasis en la promoción de derechos fundamentales, descuidando lo que podríamos llamar derechos intermedios de cuarta generación.

En definitiva, como expresa la Recomendación de la Comisión Europea de 20 de agosto de 2009 en su epígrafe 16, «Una sociedad instruida en el uso de los medios de comunicación sería a la vez un estímulo y una condición previa para el pluralismo y la independencia de los medios. La expresión de distintas ideas y opiniones, en idiomas diferentes y representando a diferentes grupos, ya sea en el ámbito de una misma sociedad o de varias, ejerce un efecto positivo sobre los valores de la diversidad, la tolerancia, la transparencia, la equidad y el diálogo. Por tanto, se debe promover el desarrollo de la alfabetización mediática en todos los sectores de la sociedad y se deben seguir de cerca sus avances».

3. INCLUSIÓN DIGITAL DE LAS PERSONAS MAYORES COMO GARANTÍA DE PARTICIPACIÓN CIUDADANA

Las competencias para poder acceder a la información en sus diversas manifestaciones, procesarla en su contexto y emplearla de forma ventajosa según las características de la persona está mucho más allá de su simple consideración como una elección vital más, transformándose en una necesidad perentoria para poder tener una participación social activa y aún más, poder disfrutar de significativas ventajas en la vida personal. En el caso de las personas mayores, esta perspectiva requiere de un esfuerzo

(18) Bustamante Donas, J., «La Sociedad de la Información Hacia la cuarta generación de Derechos Humanos: repensando la condición humana en la sociedad tecnológica», *Revista TELOS (Cuadernos de Comunicación e Innovación),* octubre-diciembre 2010, p. 2.

de todos los sectores implicados (Administraciones públicas (19), sociedad civil, los propios protagonistas) para que no queden al margen de esta realidad tecnológica y puede incardinarse en las posibilidades digitales a su alcance. Bajo el concepto de e-inclusión incluimos los procesos de empoderamiento digital que tienen como finalidad el acceso y la adquisición de las capacidades necesarias para el empleo provechoso de las oportunidades que ofrecen la tecnologías digitales en la sociedad actual.

La importancia de la inclusión digital ha sido puesta de manifiesto por los diversos documentos de la Cumbre Mundial sobre la Sociedad de la Información que tuvieron lugar en Ginebra en 2003 y Túnez 2005 auspiciada por la Unión Internacional de Telecomunicaciones dependiente de la ONU, y puede ser definida como el «conjunto de políticas públicas relacionadas con la construcción, administración, expansión, ofrecimiento de contenidos y desarrollo de capacidades locales en las redes digitales públicas, alámbricas e inalámbricas, en cada país y en la región entera» (20).

Diversos estudios (21) muestran la dificultad para integrar a los personas mayores para una utilización activa, ventajosa y productiva de las nuevas tecnologías. En este sentido, la necesidad de evitar la denominada brecha digital entre las personas mayores sin capacidades y habilidades para el uso eficiente de las TIC se hace imprescindible, dando lugar al concepto de e-inclusión. Dicha voluntad de inclusión en las TIC ha sido puesta de manifiesto en las conclusiones de la Carta para la Inclusión Digital y Social (22) donde se establecen los siguientes objetivos para lograrla: 1) Superar las barreras psicológicas es tan importante como resolver los problemas de acceso a la red y a los equipos, ya que la fractura digital no es sólo material: también existe en las mentalidades. 2) Hay que desarrollar programas de investigación para comprender mejor las necesidades de los distintos grupos excluidos de lo digital, así como las relaciones entre los distintos factores de exclusión, como la edad, el origen o el género. 3) Hay que buscar soluciones adaptadas a cada discapacidad. Se requieren esfuerzos suplementarios para identificar los campos más sensibles y evitar un enfoque generalista. 4) Insistir en la vertiente lúdica de las técnicas digitales refuerza la motivación de los que aprenden. No basta con destacar su importancia en el mundo profesional. 5) Convertir las TIC en un componente del estatus sociocultural es un factor de motivación para la inclusión. Sin embargo, para evitar bloqueos adicionales, con-

(19) Sobre la vinculación entre mayores y Administración electrónica nos permitimos citar nuestro trabajo Viñarás-Abad, M. *et alii*, «Administración electrónica y e-inclusión de las personas mayores», en *Revista Latina de Comunicación Social*, *72*, pp. 197-218.

(20) https://www.itu.int/wsis/index-es.html.

(21) Citamos este como paradigmático al respecto: Ala-Mutka, K. *et alii*, *Active Ageing and the Potential of ICT for Learning*. Institute for Prospective Technological Studies (IPTS) y European Commission, Bruselas, 2008. http://ftp.jrc.es/EURdoc/JRC45209.pdf.

(22) http://charte.velay.greta.fr/pdf/charter_E-learning_hacia_inclusion_social.pdf.

viene informar a los individuos de que también se puede vivir sin Internet. 6) Las actividades de formación pueden apoyarse con eficacia en los valores positivos que transmiten las TIC, ya que, incluso en un nivel modesto de utilización y dominio, las TIC son sinónimo de integración. 7) El *e-learning* debe ser participativo: no definir los interfaces a priori, a partir de los modelos preexistentes, sino implicar a los usuarios en fases anteriores para que puedan evaluarlos. 8) El *e-learning* debe favorecer el aprendizaje cooperativo: permitir que las personas de los grupos objetivo apoyen, se conviertan en una referencia y devuelvan la confianza a sus iguales. 9) Desarrollar modelos mixtos: la combinación del uso del ordenador con un contacto humano es más eficaz que el «todo *e-learning*». Las relaciones interpersonales con los educadores son necesarias cuando el aprendizaje es complejo y desalentador. 10) Las políticas y estrategias de inclusión deben favorecer asimismo el desarrollo personal de aquellos que, por razones económicas, personales o de gran discapacidad, no se incorporan a la sociedad de la información.

Internet, incluyendo el email, tiene el potencial para mejorar el apoyo social y el bienestar psicosocial para muchos adultos de diferentes formas. Ante todo, las personas mayores pueden usar los ordenadores para comunicarse con frecuencia, fácilmente y sin coste con sus familias y amigos quienes tienen acceso al email en el trabajo o en casa. Los mayores exploran intereses y hobbies a través de Internet, o obtienen información de consumo y acceso a recursos comunitarios. Pueden conocer nuevas personas con intereses similares a través de chats o tablones de anuncios virtuales. Además, Internet puede proporcionar una nueva vía para controlar sus opciones respecto a las interacciones con otros y uso del tiempo que no les sería de otra forma posible, lo que proporciona más autonomía a los adultos mayores. En esencia, relativamente aislados e incapacitados pueden reconectar, fortaleciendo y ampliando su conexión con el mundo exterior a través de la incorporación de la tecnología y los ordenadores a sus vida (23).

Entre las ventajas que supone Internet para las personas mayores, Muñoz Márquez (24) establece las siguientes:

— Facilitar la integración, comunicación e información entre los mayores: La lucha contra el aislamiento y la soledad es un seguro de ralentización de la vejez. Mediante la interacción se puede conseguir una mejor

(23) White, H. *et alii*, «A randomized controlled trial of the psychosocial impact of providing internet training and access to older adults.» *Aging & Mental Health 6 (3)*, 2002, p. 213.

(24) Muñoz Márquez, L.D., «Las personas mayores ante las tecnologías de la información y la comunicación. Estudio valorativo», en *Profesorado, revista de currículum y formación del profesorado, 6*, 2002, p. 2.

realización personal y la mayor participación social. La interactividad es la característica fundamental del ordenador e Internet.

— Mejorar la relación intergeneracional: en la actualidad, el mayor, al dejar su actividad laboral, deja también gran parte de su valiosa aportación a la sociedad. Afortunadamente comienza a emerger una nueva filosofía de educación de los mayores en la que se intenta que en una sociedad de objetivos productivos, cuando el anciano sale del ámbito laboral, no salga también de la consideración social, puesto que se desaprovecharía un cúmulo de conocimientos y sabiduría. Creemos que con las nuevas tecnologías se puede promover el principio de solidaridad entre generaciones y fomentar el voluntariado de las personas mayores hacia los jóvenes a la hora de transmitirles sus conocimientos y experiencias profesionales y de otro tipo. Internet sería entonces un punto de encuentro entre los mayores y las demás generaciones.

— Aprender algo nuevo sin limite de edad: La capacidad de mantenerse activo mediante un proceso educativo de amplia cobertura social incrementa la felicidad y la autorrealización. Para ello debemos acabar con el supuesto de que a las personas mayores les corresponde la inactividad.

— Mejora de la autoestima y la aportación creativa: el mayor ha de realizar actividades que le conduzcan al aumento de su autoestima. Un proyecto con el uso de Internet, deberá ser de aplicación inmediata, satisfacción garantizada e inyección de ánimo para futuros aprendizajes. Todos podemos incorporar una cierta dosis de creatividad cuando escribimos un e-mail, participamos en un chat o recogemos una información de una página web que nos sirva de inspiración para redactar por ejemplo una poesía.

— Fomentar la participación en la sociedad: El sistema social actual no deja mucho sitio en el juego social para aquellos que han entrado ya en la jubilación. La sociedad política por su parte es también propensa a olvidarse del segmento anciano, en el ejercicio del poder los mayores quedan relegados a ministerios y organismos casi de beneficencia. Con Internet tendremos una puerta abierta para propiciar un mayor grado de participación social; todo ello sería factible si por circunstancias determinadas nos sentimos incapacitados para hacerlo de una manera real.

La doctrina académica identifica tres fines generales a los que el empleo de los medios digitales puede contribuir (25) para lograr el objetivo de la e-inclusión especialmente vinculados con la necesidad de participación política, económica y con la autorrealización personal:

(25) Livinstong, S. *et alii*, *Adult Media Literacy. A review of research literatura*, Ofcom/ London School of Economics, Londres, 2005, p. 7.

Democracia, participación y ciudadanía activa: En una sociedad democrática, una persona capaz mediáticamente es más capaz de lograr una opinión informada sobre cuestiones cotidianas, y tiene la posibilidad de expresar sus opinión individual o colectivamente en los ámbitos públicos, cívicos y políticos. Una sociedad alfabetizada mediáticamente podría por tanto sustentar una esfera pública sofisticada, crítica e inclusiva.

Economía del conocimiento, competitividad y elección: En una economía de mercado que incrementa su base en la información, a menudo presentada de forma compleja y mediatizada, una capacitación mediática de los individuos es probable que tenga más que ofrecer y así lograr un mayor nivel en el mercado de trabajo, y una sociedad alfabetizada mediáticamente puede ser innovadora y competitiva, posibilitando una rica pléyade de opciones para el consumidor.

Aprendizaje a lo largo de la vida, expresiones culturales y autorrealización personal: Desde nuestro entorno simbólico fuertemente mediatizado por las informaciones, encuadrar las elecciones, valores y conocimientos da significado a nuestra vida cotidiana, la capacitación digital apoya las habilidades críticas y expresivas que sustentan una vida plena y con significado, y a una sociedad informada, creativa y ética.

Livinstong, Van Couveing y Trumim (26) establecen una serie de limitaciones que pueden encontrar las personas mayores cuando afrontan el acceso y uso de las TIC y por tanto limitar sus posibilidades para lograr dicha participación ciudadana:

Edad. La edad con frecuencia estratificó la población en cuanto al acceso y la respuesta a los medios de comunicación, pero funciona de manera distinta y a menudo contraria. Las personas mayores, en general, tienen menores niveles de acceso a los nuevos medios de comunicación, pero su comprensión crítica puede ser mayor que la de los jóvenes.

El estatus socioeconómico (SES). Dentro de la mayoría de las investigaciones, el SES es una barrera evidente, sobre todo para el acceso, pero también para la comprensión y la dimensión creativa de la acción digital. Si bien esto sugiere que in/exclusión digital puede ser explicada en términos similares a la in/exclusión social, existe más incertidumbre sobre si el efecto SES es principalmente por los ingresos, la educación, la clase social o alguna combinación de los mismos.

Género. Esta cuestión es cada vez menos importante. Sin embargo, sigue siendo significativo en relación con algunas de las habilidades más avanzadas subyacentes al acceso (navegación, control, regulación); siendo particularmente evidente en la creación de contenido donde los hombres superan a las mujeres en la creación de sitios web y medios comuni-

(26) *Ibidem*, pp. 54-56.

tarios. Ya que generalmente tiende a ser madres que median y regulan uso de los medios de comunicación (incluyendo Internet) de los niños en el hogar, las desigualdades de género también puede tener un impacto en la educación.

Discapacidad. En general, la discapacidad es una barrera clave para un segmento significativo de la población, e interactúan con otras barreras para multiplicar la exclusión. La investigación es especialmente deficiente de si y cómo las diferentes tecnologías aumentan –o, en algunos contextos, superan– los efectos de los diferentes tipos de discapacidad.

Etnicidad. Hay algunos hallazgos en la investigación científica que muestra que los grupos étnicos minoritarios están en desventaja comparativamente en relación con cierta dimensiones de la participación digital. Al igual que con otras barreras, es poco operativo el tratamiento de todos los grupos minoritarios como equivalentes (27).

Observa Cuevas (28) que durante las décadas pasadas, se ha producido una sobreestimación de la tecnología frente al proceso cognitivo que se produce en todo proceso de inclusión digital. Considera que debe observarse la inclusión digital también desde una perspectiva social, educacional y cultural más que tecnológica o política. Así, considera que la sociedad en la que vivimos depende de una compleja infraestructura tecnológica. Sin embargo, en orden a encontrar sentido a esta tecnología y no convertirla en meras herramientas, debemos ser capaces de interactuar con ella, beneficiarnos de ella, y convertirla en nuestra aliada. No es fácil, depende de la capacidad para incorporar una serie de habilidades asociadas a su uso, sobre la posibilidad de acceso e incluso la disposición para apropiárnosla; empoderamiento. La inclusión digital entendida como un factor de inclusión social está caracterizada por una actitud de cambio que incluye competencias digitales e informacionales, educación, conocimiento, pero también actitud y compromiso social. La dimensión ética es inseparable del concepto mismo de inclusión digital, pues nos permite una aproximación que contempla a las personas como sujetos críticos, autónomos

(27) En el mismo documento, los citados autores establecen una serie de elementos que pueden valorarse como facilitadores de la inclusión digital de los ciudadanos desfavorecidos donde podemos incluir a las personas mayores. Destacan entre ellos el diseño de los interfaz de las TIC; la educación en adultos adaptadas a sus necesidades; la sensibilización de los consumidores sobre diversos aspectos del uso de las TIC; el valor percibido de tal uso; la autosuficiencia que se deriva de dicho uso asociada a la noción de envejecimiento activo; las redes sociales como instrumento de interacción social de este grupo; la composición familiar influye, especialmente cuando hay niños y adolescentes en dicha composición; y los actores institucionales, que deben implicarse en la alfabetización digital de estos grupos.

(28) Cuevas Cerveró, A., «Digital inclusión: from connectivity to the development of information culture», en Passarelli, B. *et alii*, *Handbook of research on comparative approaches to the digital age revolition in Europe and the Americas*, IGI Global, Hershey, 2016, p. 41.

y activos y no como meros consumidores de tecnología y contenidos digitales (29).

McConnell y Straubhaar (30) consideran que la política de inclusión digital en los Estados Unidos históricamente ha hecho hincapié en el acceso a la banda ancha en el hogar ya que ha sido su prioridad política. Sin embargo, el suministro de hogares con acceso de banda ancha no puede hacer mucho para mejorar la capacidad de los individuos para hacer un uso significativo de Internet. Esto se debe a que proporciona acceso a Internet con poca posibilidad de interactuar en un contexto social más allá de la familia. Estos autores sobre la base de los conceptos de disposición, habito y múltiples formas de capital de Bourdieu, consideran que el uso de Internet debe situarse en su contexto social más amplio dando más importancia al acceso institucional, al uso de Internet en el trabajo o en la escuela, así como al desarrollo de las disposiciones y competencias necesarias para utilizar Internet de manera instrumentales, fomentando la aplicación de programas educativos o la comunicación con los gobiernos.

La inclusión digital es generalmente entendida como un fenómeno por el cual las personas marginadas pueden acceder y participar de manera significativa en las mismas actividades de aprendizaje, empleo, sociales y de participación ciudadana que el resto, a través del acceso y uso de las tecnologías digitales como de los ordenadores (31).

Un nuevo concepto está surgiendo en el campo de la información, la comunicación y la computación respecto a la inclusión digital denominado alfabetización informacional, que trasciende estos tres ámbitos del conocimiento. Debe ser considerado como un factor amplificador de la ciudadanía en la medida que completa el desfase en la apropiación del conocimiento, haciendo a los sujetos más independientes al tiempo que estimulan su competencia informacional (32). Esto es cierto tanto para una evaluación crítica como en su habilidad para participar en iniciativas políticas como ciudadanos. La inclusión digital puede promover la participación en el ciberespacio, sin embargo, la alfabetización informacional, puede promover mejoras en la participación en las decisiones de la esfera pública y facilitar la búsqueda de la ciudadanía.

---

(29) *Ibidem*, p. 42.

(30) McConnell, C. y Straubhaar, J. (2016). «Why the Institutional Access Digital Divide Might Be More Significant than the Home Broadband Divide» en Passarelli, B. *et alii*, *Handbook of research on comparative approaches to the digital age revolition in Europe and the Americas*, IGI Global, Hershey, 2016, pp. 56 y ss.

(31) Seale, J. *et alii*, «Digital agility and digital decision-making: conceptualising digital inclusion in the context of disabled learners in higher education», en *Studies in Higher Education*, vol. 35, Iss. 4, 2010, p. 445.

(32) Medeiros Neto, B. (2016). «From Information Society to Community Service: the Birth of E-citizenship», en Passarelli, B. *et alii*, *Handbook of research on comparative approaches to the digital age revolition in Europe and the Americas*, IGI Global, Hershey, 2016, p. 104.

La capacidad de un colectivo para tener el control sobre el ejercicio de sus derechos como ciudadanos, y en mayor medida si es un colectivo vulnerable, debe ser fundamental en una sociedad avanza. Surge el término empoderamiento para recoger esta situación que surge con especial interés a partir del desarrollo de las TIC e Internet.

El empoderamiento es un término multidimensional (33) que puede abordarse desde diversas perspectivas. En general, se ha definido como un conjunto de mecanismos que permite a las personas tener un control sobre sus propias vidas (34) y se refiere al desarrollo del control personal con cambios en la autopercepción, la confianza, la capacidad individual y las habilidades para negociar e influir en la toma de decisiones.

El propio uso de la Red pone de manifiesto una actitud proactiva por parte de los mayores que ven en Internet un compendio de recursos de gran utilidad en múltiples facetas de sus vidas. Esta percepción alzaría a la Red como instrumento clave para el empoderamiento de los mayores, dado que les facilita desarrollar un control sobre sus vidas a través de sus muy diversas potencialidades.

Todo ello redundaría en una transformación personal con efectos en el ámbito social, permitiendo la participación de los miembros de este grupo poblacional en todos aquellos asuntos de trascendencia colectiva o en palabras del Tribunal Constitucional en aquellos «hechos o acontecimientos que afectan al conjunto de los ciudadanos» (35). En definitiva, convirtiendo a los mayores en plenos ciudadanos digitales.

(33) Rodríguez Beltrán, M., «Empoderamiento y promoción de la salud». *Red de Salud 14*, 2009, pp. 20-31

(34) Silva, C. y Martínez, M.L., «Empoderamiento: Proceso, nivel y contexto», en *Psykhe 13 (2)*, 2004, p. 30.

(35) STC 134/1999, de 15 de julio (FJ 8.º).

CAPÍTULO 21
DISCAPACIDAD Y CIUDADANÍA DIGITAL

José Antonio Moreno Molina
Catedrático de Derecho Administrativo
Universidad de Castilla-La Mancha

1. LA NECESIDAD DE PROTECCIÓN JURÍDICA Y DE INTERVENCIÓN ADMINISTRATIVA A FAVOR DE LAS PERSONAS CON DISCAPACIDAD

El ordenamiento jurídico y las Administraciones públicas deben garantizar a las personas con discapacidad su desarrollo, realización personal e inclusión social, así como que puedan tener una vida en iguales condiciones que el resto de los ciudadanos, que les permita contribuir con sus importantes capacidades al progreso de la sociedad.

Los fundamentos y la raíz misma del Estado social y democrático de Derecho sufren de forma grave si los derechos a la libertad, la igualdad y la dignidad se ven limitados o restringidos de cualquier manera a las mujeres y hombres con discapacidad, lo que exige a todos los poderes públi-

cos una intervención activa para impulsar las medidas necesarias que eliminen toda discriminación y promuevan la igualdad de oportunidades (1).

Tanto la Convención de Naciones Unidas sobre los derechos de las personas con discapacidad (2) como el Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, así las últimas leyes autonómicas y los Estatutos de Autonomía reformados a partir de 2006, han llevado a un cambio de paradigma en la protección y garantía de los derechos constitucionales de las personas con discapacidad.

El derecho a la igualdad de oportunidades y no discriminación de las personas con discapacidad exige para su garantía y efectividad el respeto de los principios de vida independiente, dignidad y autonomía individual, incluida la libertad de tomar las propias decisiones, y la independencia de las personas; la participación e inclusión plenas y efectivas en materia laboral y en la sociedad; el respeto por la diferencia y la aceptación de las personas con discapacidad como parte de la diversidad y la condición humanas; el respeto al desarrollo de la personalidad de las personas con discapacidad; accesibilidad universal y diseño para todos; así como la transversalidad de las políticas en materia de discapacidad (3).

Estos principios específicos, junto a la participación a través del diálogo civil y por ende la estrecha colaboración entre el Estado y la sociedad, todos los cuales inspiran la Estrategia Española sobre Discapacidad 2014-2020 y su Plan de Acción 2014-2016 (4), están convirtiendo a velocidad de crucero al Derecho administrativo social en un «sector de referencia» para la construcción sistemática de la parte general del Derecho administrativo (5).

La Convención de la ONU ha supuesto un salto cualitativo en las políticas sociales en la materia, al plantear como objetivo principal la necesi-

---

(1) Un análisis competo de las políticas públicas de atención a las personas con discapacidad se puede encontrar en las magníficas monografías: Torres López, A., *La discapacidad en el Derecho Administrativo*, Civitas, Madrid, 2012 y AA. VV. (dir. Beltrán Aguirre, J. L. y Ezquerra Huerva, A.), *Atención y protección jurídica de la discapacidad*, Aranzadi, Pamplona, 2015.

(2) La Convención sobre los derechos de las personas con discapacidad de 13 de diciembre de 2006, adoptada por la ONU por medio de la resolución 61/106, conforme a su artículo 42, estaba abierta a la firma de todos los Estados y las organizaciones de integración regional desde el 30 de marzo de 2007. Ese mismo día, el 30 de marzo de 2007, firmó España la Convención y su Protocolo Facultativo.

(3) Véase Torres López, M. A., «Derecho a la igualdad de oportunidades y no discriminación. Derechos políticos y civiles de las personas discapacitadas accesibilidad universal, educación inclusiva, empleo público, contratación pública), AAVV (dir. Beltrán Aguirre, J. L. y Ezquerra Huerva, A.), *Atención y protección jurídica de la discapacidad*, Aranzadi, Pamplona, 2015, pp. 70 y ss.

(4) Aprobados por Acuerdos del Consejo de Ministros de 14 de octubre de 2011 y de 12 de septiembre de 2014, respectivamente.

(5) Véase Rodríguez De Santiago, J. M., *La administración del Estado social*, Marcial Pons, Madrid, 2007.

dad de garantizar que las personas con discapacidad gocen de los derechos humanos en igualdad de condiciones con los demás.

Se trata de un avance decisivo para el fomento, protección y plena realización de los derechos y libertades fundamentales de todas las personas con discapacidad y una manifestación más de la protección «multinivel» de los derechos (6), en un marco de globalización (7) que demanda la universalidad de los derechos, entre ellos destacadamente los del Estado social (8).

Así lo han entendido los procesos de reformas de los Estatutos de Autonomía desarrollados a partir de 2006, que han tenido como una de sus más destacadas novedades la incorporación de declaraciones de derechos relacionados principalmente con los objetivos del Estado social de Derecho –y que han dedicado una importante atención a la protección y al estatus jurídico de las personas con discapacidad–.

Se trata sin duda de normas llamadas a producir trascendentes cambios sociales (9).

En este sentido, debe destacarse el Libro blanco sobre acceso e inclusión en el empleo público de las personas con discapacidad (Instituto Nacional de Administración Pública, Madrid, 2015), proyecto impulsado por el INAP, la Fundación ONCE, el CERMI y FSC Inserta, en el que han intervenido diversos colectivos, y que se ha basado en el trabajo de investigación dirigido por el profesor Piñar Mañas.

El Libro blanco plantea nuevas medidas de acceso e inclusión en el empleo público y de provisión y desempeño del puesto de trabajo de las personas con discapacidad, y compara nuestro ordenamiento con otros modelos y sistemas jurídicos europeos.

---

(6) Véase Fioravanti, M., «Estado y Constitución», en *El Estado moderno en Europa*, Trotta, Madrid, 2004, p. 40.

(7) Véase Morcillo Moreno, J., «Una crisis marcada por la globalización: intervención, desregulación y autorregulación regulada», ponencia presentada al VI Congreso de la Asociación Española de Profesores de Derecho Administrativo, Palma de Mallorca, 11 y 12 de febrero de 2011. Disponible en http://www.aepda.es/EscaparateFamilia.aspx?id=71-Actividades-Congresos-de-la-AEPDA.aspx, fecha de consulta 30 de julio de 2015; González García, J. V., «Globalización económica, administraciones públicas y derecho administrativo: presupuestos de una relación», *Revista de Administración Pública*, núm. 164 (2004); Alli Aranguren, J. C., *Derecho Administrativo y Globalización*, Thomson-Civitas, Madrid, 2004; Domingo Oslé, R., *The New Global Law*, Cambridge University Press, New York, 2010.

(8) Garrido Cuenca, N., «La titularidad de los derechos sociales y de ciudadanía en los nuevos Estatutos de Autonomía, y en particular del extranjero», *Derechos sociales y Estatutos de Autonomía. Denominaciones de origen. Nuevo Estatuto del PDI universitario. Actas del IV Congreso de la Asociación Española de Profesores de Derecho Administrativo*, Lex Nova, Valladolid, 2009, p. 134.

(9) Como ilustrativamente ha señalado Muñoz Machado, la realidad social, a la que está íntimamente unido el Derecho, le aportan a éste continuamente innovaciones que provocan mutaciones, no sólo en los procedimientos sino también «en lo más característico de su sustancia» [«Las concepciones del Derecho Administrativo y la idea de participación en la Administración», *RAP* n.º 84 (1977), p. 521].

En el derecho español existe una importante tradición de normas orientadas a evitar la discriminación inicial que la discapacidad provoca en el acceso a la función pública, mediante el establecimiento de cuotas flexibles de reserva, como las que hoy consagra el artículo 59 del Estatuto Básico del Empleado Público aprobado por el Real Decreto Legislativo 5/2015, de 30 de octubre, el Real Decreto 2271/2004 y numerosa normativa autonómica (10). Estas disposiciones prevén supuestos de discriminación inversa racionalizada que el TC ha considerado constitucionales (con apoyo en los arts. 9.2, 14, 23.2 y 103.3 de nuestra norma constitucional).

La Estrategia Europa 2020 ha reconocido que la atención a la discapacidad constituye una prioridad europea y nacional dentro del ámbito más amplio de la lucha contra la pobreza (11). En dicho documento se declara que la Comisión procurará crear y aplicar programas para fomentar la inclusión social de los más vulnerables, en particular promoviendo una educación innovadora, oportunidades de formación y de empleo, y combatiendo la discriminación de las personas con discapacidad; asimismo insta a los Estados miembros a que establezcan y ejecuten, habida cuenta de sus obligaciones nacionales, medidas para abordar las circunstancias concretas de grupos con un riesgo específico de pobreza, entre las que figuran las personas con discapacidad.

El Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, tras reconocer en el artículo 7.1 que «las personas con discapacidad tienen los mismos derechos que los demás ciudadanos conforme a nuestro ordenamiento jurídico», obliga a las Administraciones públicas para hacer efectivo este derecho a la igualdad a promover «las medidas necesarias para que el ejercicio en igualdad de condiciones de los derechos de las personas con discapacidad sea real y efectivo en todos los ámbitos de la vida» y a proteger «de forma especialmente intensa los derechos de las personas con discapacidad en materia de igualdad entre mujeres y hombres, salud, empleo, protección social, educación, tutela judicial efectiva, movilidad, comunicación, información y acceso a la cultura, al deporte, al ocio así como de participación en los asuntos públicos, en los términos previstos en este Título y demás normativa que sea de aplicación» (apartados 2 y 3 del art. 7).

Asimismo, la norma contempla el deber de las Administraciones de protegerá de manera singularmente intensa a aquellas personas o grupo de personas especialmente vulnerables a la discriminación múltiple como las niñas, niños y mujeres con discapacidad, mayores con discapacidad,

(10) AA. VV., *Libro blanco sobre acceso e inclusión en el empleo público de las personas con discapacidad, Instituto Nacional de Administración Pública*, Madrid, 2015, p. 27.

(11) Comunicación de la Comisión relativa a la Estrategia Europa 2020, COM (2010) 2020.

mujeres con discapacidad víctimas de violencia de género, personas con pluridiscapacidad u otras personas con discapacidad integrantes de minorías.

Por influencia de la Convención, el Real Decreto Legislativo 1/2013 reconoce de forma expresa que el ejercicio de los derechos de las personas con discapacidad se realizará de acuerdo con el principio de libertad en la toma de decisiones.

2. IMPORTANCIA DEL PRINCIPIO DE TRANSVERSALIDAD DE LAS POLÍTICAS EN MATERIA DE DISCAPACIDAD

La Convención de Naciones Unidas recoge entre las obligaciones generales de los Estados firmantes de la misma el que tengan en cuenta «en todas las políticas y todos los programas, la protección y promoción de los derechos humanos de las personas con discapacidad» (art. 4.1.c).

En el Informe Mundial sobre la Discapacidad (12) se recomienda que las políticas y estrategias que se adopten estén dotadas de un amplio perfil integrador de ámbitos y personas y que contemplen la necesidad de incluir a las personas con discapacidad en todos los programas y medidas de erradicación de la pobreza, mejora de la educación y de la inclusión.

El Tratado de Funcionamiento de la Unión Europea (TFUE) estipula que la Unión, en la definición y ejecución de sus políticas y acciones, tratará de luchar contra toda discriminación por razón de discapacidad (art. 10) y que podrá adoptar acciones adecuadas para luchar contra la discriminación por motivo de discapacidad (art. 19).

La Estrategia Europea sobre Discapacidad 2010-2020 (13) destaca que el marco de gobernanza que establece el artículo 33 de la Convención (organismos gubernamentales, mecanismo de coordinación, mecanismo independiente y participación de las personas con discapacidad y sus organizaciones) debe abordarse respecto a los Estados miembros, en una amplia gama de políticas de la UE, a cuyo efecto ha establecido mecanismos de coordinación tanto entre los servicios de la Comisión y las instituciones de la Unión como entre la UE y los Estados miembros.

Trasladando la Estrategia Europea al ámbito nacional, la Estrategia Española sobre Discapacidad 2014-2020, aprobada por el Consejo de Ministros el 14 de octubre de 2011, fija las directrices de las políticas públi-

(12) Organización Mundial de la Salud y Banco Mundial, *Informe mundial sobre la discapacidad*, Ginebra, 2011, pp. 18 y ss.

(13) Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, «Estrategia Europea sobre Discapacidad 2010-2020: un compromiso renovado para una Europa sin barreras», SEC(2010) 1323 y 1324, p. 11.

cas españolas en materia de discapacidad y también destaca la transversalidad como principio inspirador de la misma y de su Plan de Acción (14).

El artículo 3 del Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, establece los principios de la norma y recoge «la transversalidad de las políticas en materia de discapacidad», que define como

> «el principio en virtud del cual las actuaciones que desarrollan las Administraciones públicas no se limitan únicamente a planes, programas y acciones específicos, pensados exclusivamente para estas personas, sino que comprenden las políticas y líneas de acción de carácter general en cualquiera de los ámbitos de actuación pública, en donde se tendrán en cuenta las necesidades y demandas de las personas con discapacidad.»

También la Ley 39/2006, de 14 de diciembre, de Promoción de la Autonomía Personal y Atención a las personas en situación de dependencia, reconoce entre sus principios el de la transversalidad de las políticas de atención a las personas en situación de dependencia [letra d) del art. 3].

Se pretende con ello fomentar la «normalización» (*mainstreaming* en terminología anglosajona), entendida como la incorporación de la dimensión de la discapacidad en todas las políticas sociales y económicas, más que en la formulación de una política específica para la discapacidad.

3. RETOS DEL SISTEMA ESPAÑOL DE PROTECCIÓN DE LAS PERSONAS CON DISCAPACIDAD. LA ACCESIBILIDAD EN LAS TECNOLOGÍAS DE LA INFORMACIÓN Y EN LA CONTRATACIÓN PÚBLICA

En España contamos en la actualidad con un avanzado sistema de regulación y protección social y jurídica de las personas con discapacidad, un modelo que se encuentra entre los más desarrollados del mundo y que sirve incluso como referencia a nivel comparado junto a otros como los de Países Escandinavos (15) y Holanda (16).

---

(14) Plan de Acción de la Estrategia Española sobre Discapacidad 2014-2020, aprobado por Acuerdo del Consejo de Ministros el día 12 de septiembre de 2014, p. 7.

(15) Véase AA. VV., *Capacidad jurídica y discapacidad. Cuaderno de trabajo*, n.º 11, Suecia, FUTUEX, 2010. Disponible en http://www.futuex.com/index.php/herramientas/biblioteca/category/8-p-p#, fecha de consulta 10 de febrero de 2018.

(16) El Libro Blanco elaborado por el Ministerio de Trabajo y Asuntos Sociales y el Instituto de Mayores y Servicios Sociales (IMSERSO) sobre la «Atención a las personas en situación de dependencia en España» (2005, disponible en http://www.imserso.es/dependencia_01/documentacion/documentos_de_interes/documentos_clave/libro_blanco/libro_blanco_x_capitulos/index.htmen, fecha de consulta 4 de febrero de 2018), expone en su capítulo XI diversos modelos de protección existentes en Europa (y en otros países, como Estados Unidos y Australia, o Japón y Suiza), esbozando grandes modelos, como el de protección universal y financiación mediante impuestos (países nórdicos, Holanda), el modelo bismarckiano de protección a través del sistema de la Seguridad Social (Alemania, Austria), y el modelo asistencial, dirigido esencialmente a ciudadanos carentes de recursos (países del sur de Europa).

No se puede entender en la actualidad el nivel de protección de las personas con discapacidad alcanzado en España sin subrayar el decisivo papel desarrollado por las organizaciones del denominado tercer sector (17), entidades de voluntariado, sin ánimo de lucro y no gubernamentales (18).

Pero todavía queda mucho por hacer, sobre todo en la aplicación práctica de los derechos que las normas reconocen –desde la crisis económica se redujeron las partidas presupuestarias del sistema prestacional (19)– y en la incorporación de las exigencias derivadas de la Convención sobre los Derechos de las personas con discapacidad (20). Entre los retos pendientes destaca la necesidad de aprovechar todas las oportunidades que ofrece la sociedad digital, con sus tecnologías y servicios.

La Estrategia Española sobre Discapacidad 2014-2020 (21) sirve en la actualidad como marco de referencia y directriz de todas las políticas públicas que se desarrollen en materia de discapacidad con una visión integral de las mismas.

El Plan de acción de la Estrategia Española sobre Discapacidad (PAEED) 2014-2020, plantea de forma destacada la necesidad de avanzar en un mayor desarrollo de la accesibilidad universal en todos los ámbitos asociados a las necesidades de las personas con discapacidad y, en este

---

(17) Véase Piñar Mañas, J. L., «Tercer Sector, sector público y fundaciones», *Congreso Italo-Español de Profesores de Derecho Administrativo*, Cedecs, Barcelona, 2003 y Piñar Mañas, J. L. (dir.), *El tercer sector en España e Iberoamérica. ONG, Fundaciones y Sociedad Civil*, Tirant lo Blanch, Valencia, 2000.

(18) La Ley 43/2015, de 9 de octubre, del Tercer Sector de Acción Social, ha venido, como destaca su artículo 1, a regular las entidades del Tercer Sector de Acción Social, reforzar su capacidad como interlocutoras ante la Administración General del Estado, respecto de las políticas públicas sociales y definir las medidas de fomento que los poderes públicos podrán adoptar en su beneficio. La norma define las entidades del Tercer Sector de Acción Social como «aquellas organizaciones de carácter privado, surgidas de la iniciativa ciudadana o social, bajo diferentes modalidades, que responden a criterios de solidaridad y de participación social, con fines de interés general y ausencia de ánimo de lucro, que impulsan el reconocimiento y el ejercicio de los derechos civiles, así como de los derechos económicos, sociales o culturales de las personas y grupos que sufren condiciones de vulnerabilidad o que se encuentran en riesgo de exclusión social» (art. 2).

(19) Véase Ruiz Ojeda, A. «Sobre la sostenibilidad económica de los derechos sociales reconocidos en los Estatutos de Autonomía», en AA. VV., *Derechos sociales y Estatutos de Autonomía. Denominaciones de origen. Nuevo Estatuto del PDI Universitario*, Lex Nova, Valladolid, 2009, pp. 331 y ss.; y Carro Fernández-Valmayor y Miguez Macho, «Servicios sociales y crisis económica: los límites del Estado asistencial», comunicación presentada al VI Congreso de la Asociación Española de Profesores de Derecho Administrativo, p. 9, disponible en http://www.aepda.es/, fecha de consulta 15 de septiembre de 2015.

(20) Como pone de manifiesto el estudio «La Convención internacional sobre los derechos de las personas con discapacidad y su impacto en el ordenamiento jurídico español», Informe elaborado por el Instituto de Derechos Humanos «Bartolomé de las Casas» de la Universidad Carlos III de Madrid en el marco del Proyecto de investigación «El impacto que la incorporación y ratificación de la Convención Internacional de los Derechos de las Personas con Discapacidad tiene en el Ordenamiento jurídico español», 2008 (recuperado el 29 de octubre de 2017 de http://www.cermi.es/es-ES/Biblioteca/Lists/Publicaciones/Attachments/55/Estudio1ImpactoCDPDParte1_2_3_4.doc).

(21) Aprobada por el Consejo de Ministros el 14 de octubre el 2011.

sentido, su «Objetivo operativo 1» es fomentar la accesibilidad en las tecnologías de la información y la comunicación.

Respecto al fomento de la accesibilidad en las tecnologías de la información, destaca el PAEED que se ha avanzado en el diagnóstico, pero aún no se ha elaborado un plan de acción específico.

Resulta importante la formación en nuevas tecnologías y en el aumento del uso por las personas con discapacidad. En este sentido se han celebrado diferentes convenios de colaboración entre Administraciones públicas y entidades privadas y se ha impulsado la investigación en pro de acercar la demanda y oferta de servicios y dispositivos tecnológicos a las necesidades concretas de las personas con discapacidad.

Por otra parte, hay que tener en cuenta que la Directiva 2014/24/UE del Parlamento Europeo y del Consejo, sobre contratación pública y en particular su artículo 42, establece que las especificaciones técnicas de todos los contratos destinados a ser utilizados por personas físicas, ya sea el público en general o el personal del poder adjudicador, deben estar redactadas, salvo en casos debidamente justificados, de manera que se tengan en cuenta los criterios de accesibilidad para las personas con discapacidad o el diseño para todos los usuarios.

Así lo ha recogido la nueva Ley española 9/2017, de contratos del sector público (LCSP 2017), que prevé que las prescripciones técnicas se redactarán de manera que se tengan en cuenta la Convención de las Naciones Unidas sobre los derechos de las personas con discapacidad, así como los criterios de accesibilidad universal y de diseño universal o diseño para todas las personas, tal y como son definidos estos términos en el texto refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social, aprobado mediante Real Decreto Legislativo 1/2013, de 29 de noviembre.

De no ser posible definir las prescripciones técnicas teniendo en cuenta criterios de accesibilidad universal y de diseño universal o diseño para todas las personas, deberá motivarse suficientemente esta circunstancia.

Sin perjuicio de lo anterior, siempre que existan requisitos de accesibilidad obligatorios adoptados por un acto jurídico de la Unión Europea, las especificaciones técnicas deberán ser definidas por referencia a esas normas en lo que respecta a los criterios de accesibilidad para las personas con discapacidad o el diseño para todos los usuarios.

La LCSP 2017 tiene una gran vocación social, lo que se puede apreciar desde su artículo 1.3, y ha querido desarrollar mucho más que sus antecesoras las reglas para las especificaciones técnicas, como demuestran los apartados 3 y 4 del artículo 126 que tienen en cuenta la protección de las personas con discapacidad.

Se trata de una manifestación más de la vinculación de la contratación pública a las políticas sociales y medioambientales, expresada destacadamente en la Directiva 2004/24 y recogida todavía de forma más decidida que la norma comunitaria por la LCSP 2017.

Como ha destacado Gimeno Feliú (22), si bien es cierto que la política de contratación pública está orientada a la consecución de objetivos de eficiencia económica, también lo está a la consecución de objetivos sociales y medioambientales (23).

4. ACCESIBILIDAD DE LOS SITIOS WEB Y APLICACIONES PARA DISPOSITIVOS MÓVILES DE LOS ORGANISMOS DEL SECTOR PÚBLICO

La Directiva (UE) 2016/2102 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público, establece los condicionantes, con respecto a su accesibilidad, que deberán cumplir todos los sitios web y aplicaciones móviles del sector público estatal, autonómico y local.

La Directiva tiene como objetivo garantizar que los sitios web y las aplicaciones para dispositivos móviles de los organismos del sector público sean más accesibles, al basarse en requisitos comunes de accesibilidad. Para poner fin a la fragmentación del mercado interior es necesaria la aproximación de las medidas nacionales a escala de la Unión, basada en unos requisitos de accesibilidad acordados que se apliquen a los sitios web y las aplicaciones para dispositivos móviles de los organismos del sector público. De esta forma se podrá reducir la incertidumbre para los desarrolladores y fomentar la interoperabilidad. El uso de requisitos de accesibilidad que sean neutros con respecto a la tecnología podrá también estimular la innovación.

Los ciudadanos se podrán beneficiar de un acceso más amplio a los servicios del sector público mediante sitios web y aplicaciones para dispositivos móviles, y obtendrán servicios e información que facilitarán su vida diaria y el disfrute de sus derechos en toda la Unión, especialmente de su derecho a circular y residir libremente en el territorio de la Unión, de su libertad de establecimiento y de su libertad de prestación de servicios.

Mediante la ratificación por parte de la mayoría de los Estados miembros y la celebración por parte de la Unión de la Convención de las Naciones Unidas sobre los derechos de las personas con discapacidad, adopta-

(22) Gimeno Feliú, J. M., *La nueva contratación pública europea y su incidencia en la legislación española*, Civitas, Madrid, 2006, p. 47.

(23) Véase AA. VV. (dir. Pernas García, J. J.), *Contratación pública estratégica*, Aranzadi, Cizur Menor, 2013.

da el 13 de diciembre de 2006, todos se comprometieron a adoptar las medidas adecuadas para garantizar el acceso de las personas con discapacidad, en igualdad de condiciones que los demás, a las tecnologías y los sistemas de información y comunicación, a desarrollar, promulgar y supervisar la aplicación de unas normas mínimas y unas directrices para la accesibilidad de las instalaciones y los servicios abiertos al público o de uso público, así como a fomentar el acceso para las personas con discapacidad a las nuevas tecnologías y sistemas de información y comunicación, con inclusión de internet, y se comprometieron a abstenerse de actos o prácticas que sean incompatibles con la Convención y a velar por que las autoridades e instituciones del sector público actúen de conformidad con la misma.

La Convención de las Naciones Unidas estipula asimismo que el diseño de productos, entornos, programas y servicios debe permitir que sean utilizados por todas las personas, en la mayor medida posible, sin necesidad de adaptación ni diseño especializado. Este tipo de «diseño universal» no debería excluir los dispositivos de apoyo para grupos concretos de personas con discapacidad, cuando ello sea necesario. Conforme a la Convención de las Naciones Unidas, por personas con discapacidad se entiende aquellas que tengan deficiencias físicas, mentales, intelectuales o sensoriales prolongadas que, unidas a otras barreras, impidan su participación plena y efectiva en la sociedad en igualdad de condiciones que las demás.

La Estrategia Europea sobre Discapacidad 2010-2020 establece medidas que han de tomarse en varios ámbitos prioritarios, entre ellos la accesibilidad de los sistemas y tecnologías de la información y las comunicaciones, y tiene por objeto garantizar la accesibilidad a los bienes y servicios (en especial los servicios públicos) y los dispositivos de apoyo para las personas con discapacidad.

Los Reglamentos (UE) n.º 1303/2013 y n.º 1304/2013 del Parlamento Europeo y del Consejo contienen disposiciones sobre la accesibilidad a las tecnologías de la información y la comunicación, pero no contemplaron, sin embargo, las especificidades de la accesibilidad de los sitios web y las aplicaciones para dispositivos móviles.

Horizonte 2020, el programa marco de investigación e innovación establecido por el Reglamento (UE) n.º 1291/2013 del Parlamento Europeo y del Consejo (24), apoya la investigación de los problemas de accesibilidad y el desarrollo de soluciones tecnológicas a esos problemas.

En su Comunicación de 15 de diciembre de 2010 titulada «Plan de Acción Europeo sobre Administración Electrónica 2011-2015 –Aprove-

(24) Reglamento (UE) n.º 1291/2013 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2013, por el que se establece Horizonte 2020, Programa Marco de Investigación e Innovación (2014-2020) y por el que se deroga la Decisión n.º 1982/2006/CE (*DO L* 347 de 20.12.2013, p. 104).

chamiento de las TIC para promover una administración pública inteligente, sostenible e innovadora», la Comisión pedía que se tomasen medidas para desarrollar unos servicios de administración electrónica que garanticen la inclusión y la accesibilidad. Ello incluye medidas destinadas a reducir la brecha en el uso de la TIC, y a fomentar su uso para superar la exclusión, de modo que se garantice que todos los usuarios puedan aprovechar al máximo las oportunidades que se presentan. Por su parte, en la Comunicación de 19 de abril de 2016 titulada «Plan de Acción sobre Administración Electrónica de la UE 2016-2020 – Acelerar la transformación digital de la administración», la Comisión reiteró la importancia de la inclusión y la accesibilidad.

La Directiva 2016/2102 debe ser transpuesta en los ordenamientos jurídicos nacionales de los Estados miembros de la Unión Europea antes del 23 de septiembre de 2018. En España se encuentra en trámite de audiencia pública un proyecto de Real Decreto (25) que incorporará las previsiones de la norma europea y vendrá a sustituir y mejorar las condiciones que ya se exigían a los portales de las Administraciones públicas en el Real Decreto 1494/2007.

(25) Puede verse en la web https://administracionelectronica.gob.es (consultada el 23 de febrero de 2018).

CAPÍTULO 22

EL DERECHO A LA INFORMACIÓN Y EL DERECHO AL VOTO (1)

RAFAEL RUBIO NÚÑEZ (2)
Profesor Titular Universidad Complutense

1. COMUNICACIÓN, DEMOCRACIA Y VOTO

El uso de la tecnología ha afectado siempre a la democracia, principalmente de tres maneras. Por un lado las instituciones no han dudado en aprovechar sus ventajas para cumplir sus funciones, por otro han tenido que buscar respuestas para las nuevas situaciones provocadas por su irrupción y, por último pero quizás más relevante, ha tenido que hacer frente al cambio cultural provocado por estas innovaciones, que ha gene-

(1) El contenido de este artículo ha sido desarrollado por el autor con más detalle en «La regulación de la campaña online» en «Derecho de sufragio y participación ciudadana a través de las nuevas tecnologías»/coord. por JORDI BARRAT I ESTEVE, ROSA MARÍA FERNÁNDEZ RIVEIRA, Aranzadi, Madrid, 2012 e «Información y propaganda: la comunicación política y electoral en época de gobierno abierto» en «Derecho de la información. El ejercicio del derecho a la información y su jurisprudencia». BEL, I. y CORREDOIRA, L. Cuadernos y Debates, 240. Centro de Estudios Políticos y Constitucionales, Madrid, 2015.

(2) Este trabajo ha sido elaborado con el apoyo de los Proyectos I+D+I de Excelencia del MINECO, «El avance del Gobierno Abierto. Régimen jurídico constitucional de la implantación de políticas de transparencia, acceso a la información, datos abiertos, colaboración y participación especialmente a través de las TIC y del gobierno electrónico» DER2015-65810-P (2016-2018), e «Interacción entre representación y participación en la producción normativa» DER2015-68160-C3-3-P. Así como del Grupo de Investigación UCM sobre participación, tecnología y democracia.

rado profundos cambios sociales y un cambio en las demandas de la sociedad a las instituciones (3).

Entre los cambios que está provocando la revolución tecnológica actual algunos afectan de manera directa a la opinión pública, verdadero fundamento de la democracia representativa (4). Esta representación, y así lo advierte Habermas, sólo es explicable desde la publicidad (5). Todo el edificio democrático se apoya sobre la opinión pública, opinión que para ser tal debería ser verdaderamente autónoma y del público. Como señala Pedro De Vega con acierto, «la representación burguesa no sería otra cosa que la traducción a nivel político y parlamentario de la opinión pública burguesa concebida como producto de la discusión entre particulares en el seno de la sociedad» (6).

El derecho a la información es la condición necesaria de esta opinión pública sobre la que se levanta la democracia representativa. Así lo recoge el Tribunal Constitucional español al señalar como la libertad de información «no sólo se protege un interés individual sino que su tutela entraña el reconocimiento y garantía de la posibilidad de existencia de una opinión pública libre, indisolublemente unida al pluralismo político propio del Estado democrático» (7).

La democracia es un proceso que se actualiza a diario pero en el que hay momentos más determinantes, especialmente aquellos en los que se realiza la elección de representantes a través del ejercicio del derecho al voto. El periodo electoral se concibe como un periodo determinante que condiciona el ejercicio de la democracia durante un periodo de tiempo, la duración del mandato, y en el que es preciso aumentar las garantías para que el derecho al voto, sobre el que se construye la elección, pueda ejercerse de manera libre (art. 23 CE). La libertad en el ejercicio del voto guarda una relación directa y estrecha con el derecho a la información, sólo con el libre acceso a información veraz será posible ejercer el derecho al voto de manera libre, de ahí la importancia de considerar de manera conjunta estos derechos y el impacto que la tecnología puede tener en ambos, del que en los últimos tiempos hemos visto reiterados ejemplos.

---

(3) Coello de Portugal, J. M. «Parlamento, Derecho Parlamentario y nuevas tecnologías: ¿una discusión nueva?» en Rubio Núñez, R. «Parlamentos abiertos. Tecnología y Redes para la democracia». *Cuadernos del Congreso de los Diputados*, 2013, pp. 65-71.

(4) Venn Dicey, A. Lectures on the Relation between Law and Public Opinion in England during the Nineteenth Century. 1905, p. 3 *cit.* en Sartori, G. ¿Qué es la democracia?, Taurus, Madrid, 2007.

(5) Habermas, J. (1999): «Tres modelos de democracia. Sobre el concepto de una política deliberativa», en *La inclusión del otro*, Paidós, Barcelona, pp. 231-246.

(6) De Vega, P, en «Significado constitucional de la representación política», en Obras escogidas de Pedro de Vega (ed. Rafael Rubio), Cepc, 2017, p. 406.

(7) STC 68/2008, de 23 de junio, FJ 3, STC 21/2000, de 31 de enero, FJ 4 por todas.

2. EL IMPACTO DE LO DIGITAL EN EL DERECHO A LA INFORMACIÓN

El Derecho a la información tiene la libertad de expresión y de prensa como punto de partida. Ambos son reconocidos inicialmente, y con fronteras difusas entre si, como derechos del hombre en los que corresponde al Estado el reconocimiento de los mismos, especialmente en lo que se refiere a la libre difusión de ideas políticas.

En los primeros textos Constitucionales, fruto de las revoluciones liberales (8), se habla de ellos en términos de libertad, una posibilidad de acción propia del ser humano, que es a su vez un derecho que corresponde garantizar al Estado. Desde entonces la libertad de información se ha ido consolidando muy vinculada a la consolidación de los medios de comunicación y la generalización de la prensa en la segunda mitad del siglo XIX, y la radio y la televisión en la primera y segunda mitad del siglo XX. Así lo señala Benkler cuando destaca que «por más de 150 años, las modernas y complejas democracias han dependido en gran medida de una economía de información industrial para sus funciones básicas» (9).

Así la declaración de derechos humanos de 1948 recoge en su artículo 19, el derecho a la libertad de opinión y expresión que incluye la información, el derecho a recibirla y a difundirla, como un derecho humano, la «más honda garantía de la circulación de informaciones e ideas para su transcendencia para la democracia» (Conferencia de la ONU sobre la libertad de información, Ginebra 1948). El derecho a la información se constituye así como un pilar democrático que apunta a la información como presupuesto indispensable para la formación de la opinión pública, presupuesto imprescindible a su vez de una sociedad democrática.

«El derecho a la información representa la vertiente social de más peso de la libertad de expresión» (10). La normativa internacional considera ambos derechos de una manera conjunta y así lo reconocen instrumentos internacionales como el Pacto Internacional de Derechos Civiles y Políticos (art. 19.2) o el Convenio para la protección de los derechos humanos y las libertades (art. 10.1). Por el contrario la Constitución Española, artículo 20, consagra la libertad de expresión y el derecho de la información, como dos derechos fundamentales diferentes, pero en íntima

(8) Declaración de los Derechos del Buen Pueblo de Virginia (1776) n. 12, Declaración de los Derechos del Hombre y del Ciudadano (1789) artículo 11 o la Constitución de Cádiz (1812) artículo 371.

(9) Benkler, Y. The Wealth of Networks. How social production transforms markets and freedom. New Haven and London, Yale University Press, 2006, citado por Garcia Sanz, R. M. Digital Journalism. Rethinking communications law to support democracy and viable business models. Academica Press. Palo Alto, 2017, p. 7

(10) Azurmendi, A. El proceso de configuración del derecho a la información en Bel, I. y Corredoira, l. Derecho de la información, CEPC, Madrid, 2015, p. 46.

conexión (11). Esta concepción dual tiene consecuencias al conceder autonomía a ambos. De esta manera si la libertad de expresión (20.1.a), tendría por objeto la libertad de expresión de pensamientos, ideas, opiniones, creencias y juicios de valor, el derecho a la información del 20.1.d), protegería la libertad de transmitir y recibir libremente información verdadera, sobre hechos, especialmente sobre aquellos noticiables (12).

El derecho a la información garantiza el derecho a comunicar la verdad en forma de hecho o de idea u opinión, pero este hecho se convierte en deber al ser un derecho para los demás (13). Derecho activo, del emisor, y pasivo, de la audiencia, al ser la comunicación, una relación que requiere la interactividad, cosa de, al menos dos. El ejercicio de este derecho a la información se realiza a través del mensaje. Toda información parte de los hechos pero, para ser transmitida, necesita de «la actividad informativa», «la puesta en forma de la realidad misma para posibilitar su vehiculación hasta el sujeto receptor» (14). Este proceso consiste en la selección de los hechos, la combinación de los mismos, la interpretación final y la distribución de la misma. En este momento la noticia, que busca originalmente la representación fidedigna de la realidad, pasa a ser interpretación de la misma, a través de un proceso de simplificación de los hechos, que suponen una cierta distorsión. Esta actividad se realiza por mediadores, que eran normalmente seres humanos y, en cuanto tal, era siempre subjetiva (15). El papel de estos mediadores es el de ofrecer interpretaciones que ordenan y dan sentido a los hechos, ante la complejidad de los mismos, y en este papel participaban tradicionalmente, de una manera determinante, los denominados como *gatekeepers* (periodistas, editores, o el propio Estado que en ocasiones puede permitir o no la distribución de una noticia). La elaboración de todo mensaje requiere de un proceso de construcción por parte del emisor y, dada la subjetividad de este proceso, es habitual que la imprescindible «puesta en forma» de la información, suponga un cambio de forma de la misma (16). Cuando el que informa crea un mensaje y lo difunde está desarrollando la actividad informativa y satisfaciendo este derecho fundamental a la información, de la misma manera que el público cuando lo recibe y valora ejerce también este derecho. Como consecuencia de esta exigencia aparece el requisito de la verdad, reiterado por el TC cuando señala como imponer o amparar

(11) STC 6/1981 de 16 de marzo.
(12) STC 107/88, de 8 de junio.
(13) STC 6/1988, de 21 de enero, FJ 5 «a efectos de que sea real la participación de los ciudadanos en la vida colectiva, de tal forma que de la libertad de información –y del correlativo derecho a recibirla– es sujeto primario la colectividad y cada uno de sus miembros, cuyo interés es el soporte final de ese derecho».
(14) Desantes, J. M. *La verdad en la información.* Instituto Cultural Simancas, 1976, p. 26.
(15) Hoy cada vez es más frecuente que estos trabajos se realicen de manera automatizada.
(16) Fraguas, M. *Teoría de la desinformación*, Ed. Alhambra, 1985, p. 4.

la transmisión de noticias que no responden a la verdad supone el menoscabo de los derechos reconocidos en el artículo 20.1.d (17).

Para estar protegido por este derecho la emisión debe centrarse estrictamente en información, y no en ideas y opiniones, que serían protegidas por la libertad de expresión. La verdad es el constitutivo esencial de la información hasta el punto de que la verdad es «la información misma» (18). La ausencia de verdad hace desaparecer la información y la sociedad queda privada de un derecho que le pertenece. La propia Constitución establece esta vinculación determinante entre el derecho de la información y la verdad al establecer como elemento constitutivo la obligación de veracidad, como algo sustancial y exigible a la comunicación de hechos. A la hora de determinar esta veracidad, se exige lo que conocemos como verdad lógica, la adecuación del conocimiento a la realidad, que se traduce en la exigencia al emisor de un específico deber de diligencia en la búsqueda de la verdad.

Entre todos los conflictos habituales que plantea el derecho a la información con otros derechos fundamentales quizás el más complicado es el que se plantea con la libertad de expresión. Por un lado porque los límites en el caso del ejercicio derecho a la información por parte del emisor no pueden ser los mismos que en el caso del ejercicio de la libertad de expresión, que incluye junto a los hechos, las ideas y opiniones, creencias y juicios de valor que de manera generalizada se presentan unidos en el mismo mensaje. Así al tener un objeto más amplio los mensajes de todo tipo asumen el objeto del derecho a la información, haciendo innecesario el componente de veracidad que la Constitución exige como componente esencial del derecho a la información. Como consecuencia de esto se produce el segundo conflicto, quizás el más complejo, por el que el derecho a la información de la opinión pública puede resultar perjudicado por la libertad de expresión. El TC ha enfrentado esta cuestión estableciendo que «en los supuestos en que pueden aparecer entremezclados elementos de una y otra significación, atender, para calificar tales supuestos y encajarlos en cada uno de los apartados del artículo 20, al elemento que en ellos aparece como preponderante» (19). En este punto también resulta relevante la opinión del TC cuando señala que el ejercicio de la libertad de expresión supone el ejercicio a la vez del derecho a comunicar y que «ha de salvaguardarse la delimitación constitucional de este derecho sino también el derecho que corresponde a los lectores a recibir una información veraz» (20). «Entendido así el requisito de la veracidad, es

(17) STC 168/1986, de 22 de diciembre.
(18) Desantes, J. M. *Comunicación social*, Unión Editorial, Madrid, 1998, pp. 75 y 155.
(19) STC 6/1988, de 21 de enero.
(20) STC 336/1993, FJ 7, de 15 de noviembre.

de especial importancia distinguir entre pensamientos, ideas, opiniones y juicios de valor, de un lado, y hechos, del otro, puesto que tal distinción delimita teóricamente el respectivo contenido de los derechos de libre expresión y de información, siendo propio de este último la recepción y comunicación de hechos. Ocurre, sin embargo, que en la práctica es frecuente y normal que en la información se incluyan elementos valorativos que no llegan a desnaturalizar el derecho a la información, siempre que el elemento preponderante de lo comunicado sea el informativo, debiéndose a este respecto señalar que la valoración de los hechos constituye también un elemento fundamental del derecho de información, en el que se incluye la actitud crítica, incluso enérgica o áspera, siempre que los términos en que se exteriorice no sean desmesurados o desproporcionados con la finalidad de oposición o repulsa que la misma pretende, no siendo, por ello, exigible que las informaciones difundidas por los medios de comunicación social, que no se limiten al simple comunicado de noticias, sean neutrales o estrictamente objetivas, ya que lo contrario equivaldría a limitar el principio de pluralismo más allá de lo que consiente su condición de valor esencial de la sociedad democrática, dejando reducida la libertad de información a inocua transmisión mecánica de hechos noticiables. Esta mezcla de descripción de hechos y opiniones, que ordinariamente se produce en las informaciones, determina que la veracidad despliegue sus efectos legitimadores en relación con los hechos, pero no respecto de las opiniones que los acompañen o valoraciones que de los mismos se hagan, puesto que las opiniones, creencias personales o juicios de valor no son susceptibles de verificación y ello determina que el ámbito de protección del derecho de información quede delimitado, respecto de esos elementos valorativos, por la ausencia de expresiones injuriosas, que resulten innecesarias para el juicio crítico, careciendo de sentido alguno introducir, en tales supuestos, el elemento de veracidad, puesto que, en todo caso, las expresiones literalmente vejatorias o insultantes quedan siempre fuera del ámbito protector del derecho de información» (21). «Tal valor preferente, sin embargo, no puede configurarse como absoluto, puesto que, si viene reconocido como garantía de la opinión pública, solamente puede legitimar las intromisiones en otros derechos fundamentales que guarden congruencia con esa finalidad, es decir, que resulten relevantes para la formación de la opinión pública sobre asuntos de interés general» (22).

Aristóteles en su Retórica señalaba como «pertenecen al mismo arte lo creíble y lo que parece creíble» (23). La verdad informativa requiere que

(21) STC 172/1990, FJ 3, de 12 de noviembre.
(22) STC 171/1990, de 12 de noviembre, FJ 5, STC 20/1992, de 14 de febrero, FJ 3.
(23) Aristóteles, *La Retórica.* Centro de Estudios Constitucionales, Madrid, 1985, p. 9.

la información verse sobre hechos objetivos y reales, aunque esto no supone ausencia de valoración sino la prohibición de manipularlos para desvirtuarlos. Así, busca restablecer la adecuación de lo realmente acaecido a la noticia difundida (24). El problema es que los hechos no pueden ser conocidos al margen de las interpretaciones, ni al margen de los testimonios de quienes dan fe de los mismos. La información basada en los hechos, para ser verdadera, deberá ser objetiva, significativa y válida, pero existen diversidad de formas de transmitir información, y estas se presentan a menudo de manera conjunta incluyendo interpretaciones, que suelen estar basadas en opiniones. Borrar esta línea divisoria es una de las muchas formas que la mentira puede asumir. Al poder exigir sólo la verdad a la verdad lógica, la de los hechos, que se presentarían inmunes a la subjetividad de las interpretaciones, la opinión transmitida como hechos se arroga la presunción de veracidad que se otorga a los hechos. La opinión además de estar fundada en hechos deberá respetar los principios de lógica. Tomar hipótesis por axiomas, y llegar a conclusiones, supuestamente objetivas, sobre esa base hipotética es otra técnica habitual de desinformación. De ahí que la libertad de opinión se convierta en una farsa cuando se confunden los hechos con la pura opinión o se convierten hipótesis en axiomas.

Además la intención informativa no suele aparecer aislada, y se acompaña de la voluntad incitativa, que une a la información la intención de mover el intelecto del receptor en una dirección determinada, pasando a formar parte de nuestra reflexión, o busca mover la voluntad, provocando una reacción determinada que sustituya, o se anticipe al proceso reflexivo. Toda comunicación tiene un componente informativo pero la comunicación suele basarse en mensajes referenciales, emotivos, incitativos, relacionales o estéticos. La verdad no suele aparecer en estado puro y cuando se comunica apelando a factores emocionales e intencionales, la comunicación comienza a derivar hacia la propaganda, y se convierte en una herramienta que sirve para modificar percepciones e influir en las acciones.

El derecho a la información requiere, por su vinculación con los canales y medios de comunicación, de una adecuación permanente. Especialmente cuando la inmensa mayoría de la información se encuentra digitalizada y circula a través de canales digitales. De ahí la necesidad de analizar algunos de los elementos que, como consecuencia de la tecnología, sufren un cambio y que ha hecho que en los últimos tiempos se hable cada vez con más frecuencia de las plataformas virtuales como una amenaza para la democracia.

(24) STC 105/1990, de 6 de junio, y STC 6/1988, de 21 de enero.

La supervivencia de los medios de comunicación, y su convivencia con otras fuentes informativas se revela así, desde el punto de vista del derecho a la información, como el primer elemento clave para la salud de la democracia. Una supervivencia que se ve afectada por el modelo de negocio, los derechos de los editores… Así lo reconoce la Unión Europea cuando, tras reconocer el papel esencial de los medios para el debate público y el funcionamiento de una sociedad democrática, advierte de los problemas que los editores están afrontando como consecuencia del uso online de sus contenidos, sin obtener ningún retorno económico a cambio y como el reconocimiento de estos derechos resulta con frecuencia complejo e ineficiente (25).

Causa de este problema es también la generalización de las posibilidades de emitir y distribuir de manera amplia información. La facilidad de creación de fuentes de información y la entrada de los ciudadanos en el proceso informativo multiplica el número de fuentes. El procedimiento informativo sufre como muchos otros sectores los cambios en los modelos de intermediación. Más fácil, más accesible y sin dependencia de los tradicionales ***gatekeepers*** y los reguladores. Algo en lo que contribuyen especialmente las redes, que hacen que el consumo de la información incluso de los medios tradicionales, se distribuya a través de referencias personales que difuminan la cabecera, que deja de ser un elemento determinante, adquiriendo protagonismo el autor de la noticia, e incluso los que distribuyen la información, lo que afecta al modelo de negocio y reclama una respuesta jurídica (26). Los individuos se unen a los medios, en ocasiones en términos de igualdad. Se crean así espacios personales de información, en los que el ciudadano acaba cobijándose, ante el diluvio de contenidos, en un reducido y manejable, confiable y seguro universo informativo dominado por las relaciones con sus más cercanos, desde el punto de vista personal, profesional, ideológico, etc Los ciudadanos hiperconectados con el mundo pero especialmente entre sí, al difundir de manera sencilla y masiva información, se convierten en protagonistas de la comunicación, poniendo en cuestión el concepto diferencial de medio de comunicación.

Esto aumenta el número de fuentes y diluye las referencias de autoridad que son aceptadas como intérpretes de la complejidad, que pasan a ser sospechosas. Esta abundancia y diversidad hace que se produzca una generalización que atribuye a los medios una pérdida de su carácter referencial y de autoridad. A esto contribuyen también los errores de los me-

(25) Proposal for a Directive of the European Parliamente and of the Conuncil on copyright in the Digital Single Market-COM (2016)593.

(26) Sobre estos efectos ha reflexionado con acierto García Sanz, R. M. *Digital Journalism. Rethinking communications law to support democracy and viable business models.* Academica Press. Palo Alto, 2017.

dios tradicionales, que como consecuencia de la inmediatez del procedimiento informativo y la confusión de las fuentes han cometido errores que desgastan el prestigio menguante de los medios (27).

En este contexto nos planteamos, si la protección del derecho a la información está restringida a los medios de comunicación o debería hacerse extensiva a cualquier persona. La jurisprudencia es clara, el derecho a la información se ejerce de acuerdo al principio de universalidad, por el que no puede restringirse en función del medio o el público. El TC señala en este punto que «El derecho a comunicar, que en cierto sentido puede considerarse como una simple aplicación concreta de la libertad de expresión y cuya explicitación diferenciada sólo se encuentra en textos constitucionales recientes, es derecho del que gozan también sin duda todos los ciudadanos, aunque en la práctica sirva sobre todo de salvaguarda a quienes hacen de la búsqueda y difusión de la información su profesión específica… Quienes hacen profesión de la expresión de ideas u opiniones o de la comunicación de información los ejercen con mayor frecuencia que el resto de sus conciudadanos, pero no deriva de ello ningún privilegio y desde luego no el de transformar en su favor lo que para el común de los ciudadanos es un derecho de libertad» (28).

En tercer lugar debemos hablar de los efectos de la tecnología sobre el contenido. El contenido es el elemento informativo donde se distingue principalmente la desinformación, el único lugar en el que es posible descubrir las discordancias entre la realidad representada y su representación. Aunque, como hemos visto, esto no es tarea fácil. En este sentido desde hace un tiempo se habla del peligro que las *fake news* suponen para la democracia. Se trata de una información creada por alguien, o transformada desde una noticia original que se distribuye sin referencia a su origen y su fundamento. Su fortaleza es ser difícilmente averiguable y es idóneo para preparar un terreno receptivo. Sin duda lo más relevante de esta nueva situación es la distribución de la misma a través de plataformas online. Las «fake news» como reflejo del auge de la propaganda y la bajada en la credibilidad de los medios de comunicación presentan ciertas peculiaridades respecto a otro contenido que circula por las redes, pero es precisamente el hecho de circular por las redes lo que convierte un contenido de propaganda tradicional en «fake news».

---

(27) El Presidente Trump ha utilizado algunos de estos fallos, reales o aparentes, para otorgar sus premios a las fake news: https://www.elconfidencial.com/mundo/2018-01-18/trump-fake-news-awards-noticias-falsas-premios_1508101/ (consultado el 25/01/2018).

También se puede consultar, como ejemplo, https://theintercept.com/2017/12/09/the-u-s-media-yesterday-suffered-its-most-humiliating-debacle-in-ages-now-refuses-all-transparency-over-what-happened/ (consultado el 25/01/2018).

(28) STC 6/1981, de 16 de marzo. *BOE* 14/04/1981.

La adaptación a los nuevos canales ha ocasionado que nos encontremos ante una comunicación con un claro predominio de la forma frente a la progresiva pérdida del interés por el fondo o el contenido. En este sentido, asistimos en lo que se refiere al contenido a la confusión entre lo real, lo virtual y la ficción, el predominio de la brevedad, y el protagonismo de la imagen como forma preponderante de transmisión de información (29), que afecta incluso a las propias palabras convertidas en imágenes que, como el resto de la información, son procesadas de manera inmediata en lugar de reflexionar sobre ellas. Así resulta a todas luces insuficientes para informar a la no informada opinión pública general. La brevedad, característica de las redes sociales, el peso de la imagen, o la facilidad de redifusión favorecen el uso de estas técnicas distorsionadoras de la realidad. Cuando la información se ve reducida a estímulos que afectan al receptor (30), el hombre reacciona cada vez más ante la persuasión y cada vez menos frente a la información. El protagonismo de la imagen genera además una dificultad importante para explicar conceptos complejos que requieren de abstracción. Los estímulos ante los cuales responde son casi exclusivamente audiovisuales, y gozan de la presunción de veracidad (31), pero sólo reacciona ante aquellas imágenes que entre un millón consiguen provocar en él alguna reacción; el hombre no puede evitar convertirse cada vez más en un ser sentimental. De ahí que las «fake news» suelan ser «noticias con contenido cargado de tensión, puestas en circulación sin garantías (…) y que se legitiman con una autoridad aparente» (32). La comunicación se convierte en espectáculo premiando los conceptos simples, los titulares engañosos, todo aquello que atrae la atención (el clickbait) aunque pueda resultar reduccionista. En el ecosistema de la posverdad prima la forma sobre fondo, las imágenes sobre las ideas, la búsqueda de respuestas simples, que dividen el mundo en blanco o negro, en sí o no, y no admiten matices.

Otro de los elementos que afecta al derecho a la información es la nueva concepción del tiempo. En el terreno de la información los tiempos periodísticos, de un día para otro, o televisivos, de un telediario al siguien-

(29) Sartori, G. *Homovidens*, Taurus, 1989.
(30) Schwartz, T. *La respuesta emocional.* Ed. Liderazgo democrático 2. Quito, 2001, p. 37.
(31) Ana Tudela nos recuerda en «Comunicación Propaganda y 'fake news': con nosotros mucho antes de la tecnología» https://retina.elpais.com/retina/2017/12/28/tendencias/1514460844_757457.html (consultado 25/01/2018) como «Las imágenes del cormorán agonizante embadurnado en petróleo emitidas y publicadas durante la Guerra del Golfo de 1991, desatada tras la invasión de Kuwait por Irak, eran un montaje que encajaba como un guante en el relato sobre el ecoterrorismo practicado por Saddam Husseim. No era posible que las cámaras de televisión de la ITN ni de la CNN hubieran podido grabar las aves mientras estaban allí los iraquíes, ni hay crías de cormorán en enero en el Golfo Pérsico, explicarían los ornitólogos cuando medios como el francés L'Evénément du Jeudi o el italiano Il Manifesto se encargaron de hacer fact-checking a aquellas imágenes que habían dado la vuelta al mundo.»
(32) Dovifat, E. *Política de la información.* EUNSA, Pamplona, 1980, p. 406.

te, han sido sustituidos por una actualización permanente que en ocasiones, en busca de atraer tráfico en la batalla por la atención, intenta anticiparse a la realidad (33), para llegar a un público en busca de respuestas inmediatas que olvida la realidad como proceso que se va haciendo, y ansioso de conocer y dar a conocer las noticias en tiempo real¸ teniendo muy en cuenta los efectos que esa difusión tendrá sobre nuestra propia imagen. Esto hace que la información se elabore según se va produciendo, sin las comprobaciones y la reflexión necesaria, y se distribuya de manera automática, en función del titular o la imagen que la encabeza y la persona a través de la que lo hemos recibido, pero sin tiempo de consultar, ni si quiera, su contenido. Generando una dinámica donde prima la velocidad y genera ciclos informativos que muchas veces no llegan a un día, y agotan determinadas informaciones, antes de que se publiquen en la prensa escrita del día siguiente. El problema de esta inmediatez es que deja huella. Si el almacenamiento de la información y su archivo hacía de la información algo pasajero, limitando su impacto a ciclos informativos de un par de días, la capacidad de almacenamiento, que es infinita, y su disponibilidad, accesible en segundos desde cualquier sitio, hace posible que cualquier declaración sea puesta en evidencia, siendo también estas contradicciones objeto de difusión masiva.

La información deja de ser un bien escaso a disposición de unos pocos privilegiados para convertirse en una *commodity* a la que todo el mundo tiene acceso. Sobre cada acontecimiento, sobre cada realidad, se generan de forma instantánea millares de análisis, de opiniones, de versiones, de datos que tratan de darles sentido, que además se van acumulando, de forma más o menos caótica, en las redes de información, y se distribuyen con una capilaridad casi infinita a través de los variados terminales a los que los ciudadanos están conectados. El receptor tiene gran capacidad para acceder rápidamente a infinitas fuentes de información, recibe una cantidad de información y de canales muy superior, y selecciona ésta en función de impulsos rápidos, no siempre razonados, que no suelen implicar una reflexión posterior. No existe una relación directa entre la calidad de la comunicación y la cantidad de información. Poner muchos datos sobre la mesa no es sinónimo de transparencia es más, habitualmente en el contexto actual, el exceso de información acaba dificultando el ejercicio del derecho a la información. Los datos resultan insuficientes, llegando a convertirse incluso en fuente de desinformación ocultando la realidad que se pretende mostrar u ofreciendo una visión diferente. A pesar de la abundancia de información siguen existiendo realidades opacas, que logran

(33) En España a la costumbre habitual, especialmente de Wikipedia, de dar por muertos a personas que gozan de buena salud, añadimos la particularidad de haber incinerado a una de ellas, la enfermera del Ebola, que se recuperó estupendamente del trance.

pasar desapercibidas por las dificultades que tiene su observación y se benefician de una atención dirigida a otras realidades más llamativas y de las que resulta más sencillo obtener información. Como señala Revel «La abundancia de información se relaciona menos con la importancia del acontecimiento, que con la facilitad de observarlo» (34), y su espectacularidad (añadiríamos nosotros). Paradójicamente una de las formas más sutiles de la posverdad es la transparencia radical.

La tecnología ha provocado la abundancia de información y facilitado el acceso a la misma, provocando por un lado el consumo aleatorio, no lineal de la información y permitiendo seleccionar las fuentes, directas o indirectas, institucionales o personales, de las que se recibe información. Creamos nuestro propio ecosistema informativo, un mundo muy personal, paralelo a otros mundos personales y terreno propicio de la posverdad. Un ecosistema formado por informaciones autorreferenciales que conservan, en el mejor de los casos la coherencia interna pero que no requieren ningún tipo de coherencia con textos anteriores, ni muchos menos con la realidad, provocando además la percepción de que todos aquellos que no comparten nuestro ecosistema informativo, lo hacen profundamente sesgados. La pluralidad de los medios de comunicación, que tradicionalmente se han contemplado como un espacio de encuentro y garantía de objetividad, generan una falsa impresión de estar informados. Esta parcialidad provoca una especialización en el conocimiento. Cuando uno se fija sólo en una parte de la información puede seleccionar dentro de la misma de una manera parcial, lo que le impide tener una visión general del problema, imprescindible para conocer la realidad del mismo.

Nunca han existido tantas posibilidades de acceso a la información… todas al servicio de reforzar las propias ideas, potenciando el sesgo de la confirmación, en el que se presta atención y credibilidad a la información que alimenta las creencias propias. Como hemos visto este mecanismo, humano y, como tal, universal, se viene reforzando como consecuencia de la ampliación de opciones entre los medios de comunicación que nos permite elegir aquellos más afines a nuestras creencias, pero además viene a reforzarse con herramientas de comunicación personal como *whatsapp* o las redes sociales, cuyo algoritmo detecta estas preferencias y nos las ofrece con mucha más frecuencia, reforzando nuestro conocimiento y adhesión a aquellas comunidades más afines. Así, a pesar de la pluralidad de opciones, que construye una falsa imagen de apertura del debate, pese a existir más información alternativa que nunca, no accedemos a ella o lo hacemos convencidos de su poca credibilidad. El sesgo anclaje provoca además, el prestar atención a un solo elemento, y descartar el resto, a la

(34) Revel, J. F. *Comment les democracies finisent*, Grasset, 1983, pp. 163-165.

hora de configurar una opinión y tomar las consiguientes decisiones, lo que podríamos denominar la «verdad a la carta». Podemos ignorar los hechos que no nos gustan y optar por narrativas personalizadas. Seleccionamos toda la información, incluidas las correcciones, para mostrar que estamos en lo correcto y que nuestros adversarios están equivocados (35). Esto se produce incluso en los casos de información verificada, que se comparte con mucha más frecuencia cuando refuerza creencias previas que cuando las cuestiona (36). Cuando los datos están de nuestro lado, los hacemos públicos. En cambio, cuando nos contradicen, los rechazamos o los ignoramos. Difícilmente le diremos al mundo que estábamos equivocados y creíamos en fantasías.

Este sesgo de la confirmación genera una fragmentación entre burbujas informativas (37), de mundos informativos paralelos, que dificulta la existencia de espacios comunes de debate. Frente a la opinión pública entendida como un entramado de relaciones comunicativas de diverso género desarrollada en distintos foros, que sustentaba la sociedad, asistimos a un proceso de reducción de una esfera pública general de la que todos formemos parte, hacia pequeños bloques tremendamente movilizados pero muy aislados entre sí, lo que David Roberts ha denominado como la era de las «epistemologías tribales» (38). La posibilidad de comunicar y de informarse de manera selectiva, casi personalizada, fundamentalmente a través de la tecnología y de las redes sociales, va generando microcomunidades que tienen muy poca relación entre sí. Se trata de grupos cerrados, de convencimiento mutuo donde la confirmación provoca la perseverancia de las creencias, y la consiguiente sospecha ante cualquiera que defienda puntos de vista diferente, aunque sustente sus afirmaciones en hechos objetivos. A esto se añade la costumbre de compartir de manera acrítica la información recibida dentro del grupo (39). Una mentira repetida cien veces en las redes sociales se vuelve realidad en su círculo de confianza. Nunca ha sido más fácil entender lo que piensan los demás y, a pesar de esto, nunca se ha practicado menos, debido a que, así como es más fácil que nunca conocer la intención de los otros,

(35) Sunstein, C., Scala, A., Quattrociocchi, W. Echo chambers on facebook. 2016. Disponible en:, https://ssrn.com/abstract=2795110 (consultado el 25/01/2018).

(36) Shin, Jieun, Thorson, Kjerstin. «Partisan Selective Sharing: The Biased Diffusion of Fact-Checking Messages» on *Social Media. Journal of Communication.* Vol. 67, 2017. Disponible en: http://onlinelibrary.wiley.com/doi/10.1111/jcom.12284/full (consultado el 25/01/2018).

(37) Parisier, E. *The filter bubble.* The Penguin Press. New York. 2011.

(38) Robert, D. https://vox.com/policy-and-politics/2017/3/22/14762030/donald-trump-tribal-epistemology (consultado el 13.5.2018).

(39) Según la revista Forbes un 59% de las noticias compartidas en las redes se transmiten sin ser leídas previamente. Disponible en: https://www.forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/jaysondemers/2016/08/08/59-percent-of-you-will-share-this-article-without-even-reading-it/&refURL=https://t.co/9QQBhdD9VR&referrer=https://t.co/9QQBhdD9VR#ce573742a648 (consultado el 25/01/2018).

también es más fácil reforzar la percepción propia y, al final, uno tiende a hacer lo más cómodo: tratar de informarse a través de gente que tiene un pensamiento afín. Esto provoca una percepción falsa de la realidad. Cuando uno se comunica siempre con los mismos y habla de lo mismo, corre el riesgo de acabar viendo la realidad de manera deformada o contraria a como es.

Estas microcomunidades autoreferenciales provocan una necesidad de destacar dentro de grupos uniformes que fomenta las posiciones más radicales y una falta de diálogo que dificulta la empatía, la posibilidad de conocer y ponerse en el lugar del otro (40). La suma de estos dos elementos alimenta la polarización y permite el establecimiento de un pensamiento único, al menos en los grupos cerrados que terminan por silenciar y expulsar al disidente. La relación entre ecosistemas informativos diferentes termina provocando el choque entre los mismos, y este choque retroalimenta la polarización, al desgastar las posiciones radicales de unos y otros la credibilidad, alimentando a su vez el discurso radical del otro (41).

En el plano jurídico se plantean distintas soluciones, la primera, de ámbito reducido, afectaría al contenido y sería el ejercicio del derecho de rectificación señalado por la LO 2/1984, y podríamos definirlo, con el TC, como «la facultad otorgada a toda persona, natural o jurídica, de rectificar la información difundida por cualquier medio de comunicación social de hechos que le aludan que considere inexactos y cuya divulgación pueda causarle perjuicio» (42). Este derecho que tiene una finalidad preventiva, para tratar de evitar el daño, tiene una serie de limitaciones claras para la realidad actual en la línea de lo analizado previamente, tanto en su definición, circunscrita a hechos inexactos que afecten a los derechos legítimos de una persona, como, sobre todo, en su ejecución. Como ha señalado parte de la doctrina, el derecho de rectificación se consolida como la facultad de toda persona de ejercer el derecho a comunicar para restablecer la verdad lógica de forma inmediata, sumaria y sencilla. Este ejercicio se plantea a través del contraste de opiniones, sin aportar la versión definitiva, que sería objeto de otro procedimiento. El restablecimiento de la verdad (lógica) se plantea así como el objeto principal del ejercicio de este derecho. El problema es que en la era de la información en *streaming* nada es lo que parece en un primer momento, ya que siempre se puede contar con más información que matiza, que da una nueva visión, que aporta nuevos datos, que los contrasta con otros ya existentes. Este entorno de verdadero diluvio informativo provoca la relativiza-

(40) Sunstein, C. R. «The law of group polarization». *Journal of political philosophy*, 10, 175-195 (2002).

(41) https://www.buzzfeed.com/charliewarzel/2017-year-the-internet-destroyed-shared-reality (consultado el 25/01/2018).

(42) STC 168/1986, de 22 de diciembre.

ción de los hechos y de los datos y hace que mostrar hechos para corregir errores de información no sea suficiente para corregir estos errores. De esta manera, aunque «el acceso a una versión disidente de los hechos publicados favorece, más que perjudica, el interés colectivo en la búsqueda y recepción de la verdad» (43), el problema es que esta solución resuelve sólo una parte del problema, aquella que afecta a terceros, pero en la práctica la delimitación del sujeto emisor, al difuminarse el concepto de medio de comunicación, los nuevos tiempos informativos y las posibilidades multidireccionales de la información, hacen imposible esa rectificación y la llegada a una audiencia similar a la de la información originaria que causa la lesión.

3. LA DIGITALIZACIÓN DE LAS ELECCIONES Y SUS EFECTOS EN EL DERECHO AL VOTO

Estos cambios en la producción, difusión y recepción de la información afectan también al derecho al voto. El ejercicio del derecho fundamental de participación política se realiza a través del voto libre, y este puede estar condicionado por la tecnología. El asunto ha adquirido nueva relevancia, e incluso cierta urgencia, tras los últimos procesos electorales, poniendo de manifiesto su importancia capital para la democracia y la necesidad de ofrecer respuestas jurídicas. Casos como el referéndum del Brexit o la campaña electoral norteamericana (con denuncias de la incidencia de Rusia y del uso de datos personales de más de 50 millones de norteamericanos), las amenazas al recuento electoral en Holanda, etc., ponen de manifiesto que, por lo general, la normativa electoral no está preparada para este nuevo escenario. Se repiten las denuncias en todo el mundo sobre la fragilidad del sistema electoral. Esta fragilidad tiene una relación directa con la tecnología, y afecta a las distintas fases del proceso electoral: campaña electoral, votación y recuento. Internet está transformando el modo de decidir y ejercer el voto. La regulación electoral existente no es suficiente para dar respuesta a los retos que plantean estos cambios. El respeto a los fines de la regulación de las campañas electorales, como elemento básico del sistema democrático, requiere una adaptación normativa a las nuevas formas de hacer campaña, especialmente en lo que afecta a los sujetos, el contenido, los espacios electorales, el tiempo de duración de la campaña y la privacidad de la información que se maneja durante la misma. Muy pocos son los países que han afrontado en serio éste asunto abordando reformas en su legislación para tratar de dar respuesta a este fenómeno, los más tratan de

(43) STC 168/1986, de 22 de diciembre, FJ 5.

aplicar las normas existentes a esa realidad cambiante provocando inseguridad jurídica.

Carreras y Vallés explican como «la campaña electoral es aquel periodo de tiempo anterior a la fecha de las elecciones en que los candidatos, a través de los medios de comunicación (mítines, prensa, radio, televisión, etc.) intentan ponerse en contacto con el cuerpo electoral para atraer el máximo número de votos. En los inicios del régimen liberal, este periodo no estaba regulado por leyes, pero hoy en día sí, de tal modo que la campaña electoral es aquel periodo de tiempo en que actos políticos que en otro momento no son regulados, en este periodo sí lo son» (44).

Esta regulación específica se debe a la importancia del momento político, y está determinado por una definición teórica de los conceptos de información y propaganda que en realidad forman parte de una misma realidad en la que es difícil deslindar los límites. El motivo de esta difusa distinción obedece a la percepción generalizada de que la democracia descansa sobre la base de una comunicación persuasiva. Una comunicación que oculta la existencia de una intencionalidad por parte de aquel que transmite un mensaje o idea y que, en el fondo, tiene tras de sí unos objetivos conscientes, prefijados y específicos que buscan la captación de votos. En este sentido se ha entendido durante mucho tiempo propaganda y publicidad como sinónimos, de forma que la propaganda emplearía las técnicas tradicionales de la publicidad para promover contenidos «políticos», ideas y creencias.

El objeto de esta distinción, según la exposición de motivos de la ley que reforma la normativa electoral aprobada por la Ley Orgánica 2/2011, de 28 de enero, por la que se modifica la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, es doble: por un lado, «la reducción del peso de la publicidad y propaganda» en el período electoral y correlativamente, «una mayor incidencia durante el mismo, de la exposición y debate de los programas y propuestas» de las formaciones políticas que participan en las elecciones. A pesar de lo anterior en los últimos tiempos se ha venido extendiendo la visión según la cual «publicidad y propaganda serían dos formas distintas de comunicación persuasiva, en la que la publicidad adoptaría formas persuasivas mientras que la propaganda utilizaría formas aparentemente no-persuasiva. De modo que la diferencia entre ambas formas de comunicación no estaría en los contenidos, sino en el método» (45). Si a esto le sumamos que vivimos en una suerte de permanente campaña electoral, y que las elecciones libres y competitivas se han

(44) Carreras, F. de y Vallés, J. M.ª, *Las elecciones. Introducción a los sistemas electorales*, Blume, Barcelona, 1977, p. 60.

(45) Mendiz Noguero, A., «Diferencias conceptuales entre publicidad y propaganda: una aproximación etimológica», *Questiones Publicitarias*, vol. I, n.º 12, 2008, pp. 43-61. (Citada por Feliu, 2014, p. 57).

convertido incluso en un símbolo de nuestra democracia, comprenderemos que determinar cuándo nos encontramos ante información política y cuándo ante propaganda, no resulte excesivamente sencillo. Esta dificultad para distinguir entre información y propaganda, y sus posibles consecuencias, se extiende mucho más allá del periodo electoral, cuando al referirnos a la comunicación del gobierno también tratamos de distinguir entre publicidad y comunicación, algo difícilmente sostenible si concebimos la publicidad como una forma de comunicación, que se entendería así compuesta por tres modos comunicativos: información, propaganda y publicidad aunque, tal y como destaca Fernández Souto, «en ocasiones se funden en uno solo» (46).

Hasta ahora la distinción se basa en cuatro elementos: un criterio temporal, los días previos a la elección; un criterio de contenido, la petición expresa del voto; un criterio de canal, la prohibición de usar canales publicitarios fuera de este periodo; y un criterio vinculado a los sujetos, partidos políticos y candidatos, y la actuación de los medios de comunicación. Pero esta distinción, difícil de mantener incluso en el plano teórico donde se configuran «las campañas electorales como un enorme y simbólico diálogo entre electores y elegibles, entre representados y representantes», se ve trastocada por «la revolución operada en los medios de comunicación (que) determina que ese impresionante diálogo colectivo sufra una conmoción notable, en la medida en que acaba haciendo sucumbir a los principios inspiradores de la conducta del homo sapiens ante los requerimientos y urgencias del homo videns» (47). Como consecuencia de esta evolución las campañas electorales han sido percibidas, y por tanto diseñadas normativamente, como periodos de alta intensidad en la utilización de técnicas de comunicación persuasiva. De ahí que, en el proceso de acceso al poder instrumentalizado a través de las elecciones periódicas observamos cómo incluso las reglas del juego han cambiado en favor de esta idea. Hoy todo se considera que es propaganda, todo apela a los sentimientos, a las emociones, al componente irracional de la política y por ello, los legisladores conscientes de esta deriva han enfocado su labor normativa.

Si esto ha sido así, especialmente tras la generalización del uso de la televisión, mucho más tras los cambios radicales que la comunicación ha sufrido desde los años 90, apareciendo a principios del siglo XXI, un nuevo paradigma en la comunicación política electoral. Las campañas electora-

(46) Fernández Souto, A. B., «Comunicación Política y RRPP desde las instituciones autonómicas: estudio de las estrategias y mensajes de las principales campañas llevadas a cabo desde la Xunta de Galicia (1990-1997)». Tesis doctoral. Universidad de Vigo, 2002. (Citado por Feliu, 2014, p. 39).

(47) De Vega, P., «Campañas electorales y democracia» en *Obras escogidas de Pedro de Vega* (ed. Rafael Rubio), Cepc, 2017, p. 775.

les están experimentando en los últimos años cambios sustanciales que, buscan aprovechar las últimas técnicas del marketing para lograr movilizar a los votantes propios y desmovilizar a los ajenos. Uno de los aspectos que condicionan estos cambios de manera más determinante es el uso de la tecnología.

Si el uso de la tecnología ha afectado siempre a la democracia, cuando se utiliza en estos momentos de especial intensidad democrática requiere especial atención del legislador y los órganos encargados de velar por la integridad del proceso.

Más allá de las posibilidades y retos que plantea la tecnología al ejercicio del voto, en torno al voto electrónico que desde hace años se han estudiado con profundidad (48), es necesario explicar los cambios más importantes que ha experimentado la comunicación en la campaña electoral y sus efectos. Junto a los cambios, ya mencionados, que ha experimentado la comunicación en general, y entre los que hemos destacado los nuevos espacios y tiempos comunicativos, el protagonismo que adquieren nuevos sujetos, la facilidad con la que se extienden informaciones no veraces, y la dificultad de contrarrestarlas, encontramos una serie de elementos que alteran específicamente el panorama de las campañas electorales.

En primer lugar vemos como se ha sustituido la tradicional publicidad por nuevas formas de comunicación personalizada, adaptando los mensajes a segmentos del electorado específicos. Para aquellos que diseñan las campañas, las grandes masas vuelven a ser irrelevantes, ya que la mayoría de los individuos ya están convencidos o perdidos, por tanto es necesario centrarse en el pequeño grupo de indecisos y las técnicas de campaña vuelven al *one to one* (como durante el siglo XIX), o al *many to many*, en lo que Joseph Pine ha denominado «personalización en masa», en una (49) evolución del mismo concepto facilitada por la tecnología. Las nuevas tecnologías permiten un conocimiento profundo, y prácticamente personalizado del electorado y esto permite adaptar mensajes generales a mensajes con un altísimo grado de personalización. Al conocimiento personalizado del electorado se une la posibilidad de llegar directamente a él a través de canales como las redes sociales, que permiten en la compra de publicidad una segmentación muy precisa. Esto, que es aplicable a cualquier tipo de publicidad, ha sido aprovechado por algunos en la arena electoral. Consultoras como Cambridge Analytics han obteni-

(48) Recientemente Guglielmi, G. y Ihl, O. El voto electrónico. Centro de Estudios Políticos y Constitucionales, Madrid, 2017. En España Barrat, J. «El voto electrónico y sus dimensiones jurídicas: entre la ingenua complacencia y el rechazo precipitado», Madrid, Iustel, 2016 o Barrat, J. y Fernández Riveira, R. *Derecho de sufragio y participación ciudadana a través de las nuevas tecnologías*, Cizur Menor, Civitas, 2011.

(49) Pine, B.J., II (1993). *Mass Customization: The New Frontier in Business Competition.* Harvard Business School Press, Boston.

do información detallada de un número considerable de los votantes, adaptando sus mensajes a estos perfiles. Aunque no está demostrada la correlación directa entre estas acciones publicitarias y el voto, este tipo de prácticas han puesto sobre la mesa el debate general sobre la privacidad en las redes sociales, y específicamente el debate sobre si esta información personal, y sensible, puede ser aprovechada para realizar publicidad electoral segmentada.

En segundo lugar deberíamos hablar de los canales de comunicación. En España la comunicación electoral se encuentra regulada por la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General (LOREG). Esta ley ha sufrido numerosas modificaciones, pero no ha incorporado una respuesta a los efectos que la tecnología está teniendo ya sobre las campañas. La ausencia de un tratamiento normativo específico lleva a la equiparación de los canales digitales con el resto de medios de comunicación social. Así lo recoge la Instrucción 4/2007, de 12 de abril de la Junta Electoral Central en la que se recuerda que las limitaciones establecidas en materia electoral para los medios de comunicación sociales son también aplicables a estos «medios electrónicos». Esta equiparación normativa de Internet con el resto de medios se mantiene, ya que tanto en la LO 2/2011, de 28 de enero como en la reciente Instrucción de 3/2011, de 24 de marzo, se utilizan expresiones como: «queda prohibida la realización de publicidad o propaganda electoral mediante carteles, soportes comerciales o inserciones en prensa, radio u otros medios digitales», o «está permitida la inserción de anuncios en prensa o revistas, o en cuñas radiofónicas, o en formatos publicitarios en Internet ("banners"), o en canales comerciales de televisión, o en otros soportes en medios digitales».

Un tercer elemento, vinculado a la aparición de nuevos actores, tiene que ver con la utilización masiva de *bots*, cuentas anónimas y automatizadas, y cuentas falsas que actúan como individuos en las redes y sirven para aumentar la distribución masiva de determinada información, buscando crear una corriente de opinión, de aceptación o rechazo a determinadas personas o ideas, de manera artificial (50). Estas cuentas permiten crear a distancia la apariencia de mayoría, que genera un efecto arrastre o *bandwagon*, provocando la aceptación de aquellas ideas compartidas por una aparente mayoría, y especialmente cuando es acogida por los medios de comunicación. Esto facilita la intervención de otros países en la campaña electoral, como la injerencia rusa denunciada en las últimas elecciones presidenciales norteamericanas.

(50) http://agendapublica.elperiodico.com/desde-rusia-bots/.

Por último no podemos dejar de mencionar los ciberataques, como el que durante la campaña presidencial norteamericana supuso la publicación de correos internos de miembros del equipo de campaña del Partido Demócrata. Estos ciberataques, que amenazan también los sistemas de votación y recuento, constituyen una amenaza a los gobiernos democráticos ya que en un mundo interconectado, un ataque contras las redes de una nación puede ser un ataque contra todos, lo que obliga a la creación de normas de comportamiento entre Estados que garanticen la protección de las redes comunes globales.

En lo electoral además las nuevas tecnologías también abren la puerta a elementos ignorados hasta ahora en el ámbito del voto y el recuento y que afectan al derecho al voto. Poder hacer frente a los mismos requiere, no sólo un impulso decidido de la administración electoral, sino la adopción de nuevas perspectivas que aborden escenarios impensables antes de la aparición de las nuevas tecnologías. Asuntos meramente logísticos como el ahorro de costes, la reducción del impacto medioambiental que tendría la reducción de papel y, especialmente, aquellos que reforzarían la legitimidad democrática como la financiación ciudadana de las campañas; la transparencia de esa financiación; la inscripción electrónica en el registro (en los países en que el registro es necesario para votar); la declaración de dominio público de la información electoral que los gobiernos, partidos políticos y candidatos ofrecen online, para garantizar a los votantes el derecho de usar, compartir y comentar esa información; la promoción por parte de las autoridades de la participación electoral, ya sea a través de campañas publicitarias de promoción de la participación electoral en soportes como las redes sociales o utilizando la tecnología para localizar en el mapa la ubicación de las casillas electorales, son sólo un ejemplo de la amplitud de las perspectivas que se abren ante nuestro sistema democrático, confiamos en que sepa aprovecharlas.

4. NUEVO ESCENARIO, NUEVAS RESPUESTAS

En resumen podemos decir que el gran reto de la regulación del derecho a la información en general, y su ejercicio durante las campañas electorales en particular, no es solamente el de adaptar la normativa vigente para acciones que puedan alterar de manera indebida la opinión pública y la consiguiente formación de la voluntad de los votantes, ya que este tipo de respuestas suelen resultar insuficientes, se trata de ir más allá y pensar en las nuevas situaciones que las nuevas tecnologías plantean a la democracia, más allá del esquema actual. Regular y juzgar estas cuestiones requiere un conocimiento técnico que permita comprender la naturaleza de las actuaciones y su posible impacto.

Esta respuesta además no puede ser sólo de carácter regulatorio y pase por otras vías, como la educación, el fortalecimiento de modelos informativos sostenibles, y un esfuerzo por compartir los datos de manera rápida y eficiente. Además es imprescindible tener en cuenta a las empresas privadas, que son elemento indispensable para el ejercicio de ambos derechos, con el establecimiento de mecanismos de buenas prácticas en las plataformas tecnológicas, que incluyan una mayor transparencia especialmente con investigadores independientes (51).

(51) https://maldita.es/wp-content/uploads/2018/03/HLEGReportonFakeNewsandOnlineDisinformation.pdf

V

CONFIANZA DIGITAL Y RESPONSABILIDAD EN LA RED

CAPÍTULO 23

DEFENSA DE DERECHOS Y NEUTRALIDAD DE LA RED

MERCEDES FUERTES
Catedrática de Derecho Administrativo (Universidad de León)

Avanzar por el nuevo mundo que nos han descubierto Internet y las tecnologías de la comunicación resulta emocionante. Son sorprendentes las sucesivas posibilidades que aparecen ante los trepidantes progresos técnicos. Sin embargo, si queremos mantener una sociedad abierta hemos de defender en ese mundo virtual algunas pautas jurídicas. Sería más que frustrante y cercano al absurdo, no poder disfrutar en esas experiencias de las grandes conquistas de la humanidad, en especial, de las libertades públicas. Pero, sobre todo, la razón primordial para que el Derecho impere en la Red sería que una desatención a los derechos fundamentales se trasladaría y contagiaría las relaciones personales y sociales en el mundo real. Ello pondría en riesgo el desenvolvimiento de la sociedad civilizada que conocemos. Tal es la trascendencia de sentar unas correctas bases jurídicas.

Dos son los firmes trazos iniciales que han de marcar las dimensiones del plano sobre el que edificar el Derecho del ciberespacio y las telecomunicaciones. Que Internet sea abierta y que la Red sea neutral.

Otros autores han aludido ya en esta obra a la pretensión de una Internet abierta. Me corresponde a mí resumir la necesidad de defender la neutralidad de la Red como presupuesto del adecuado ejercicio de los derechos de los ciudadanos (1). Hay que tener en cuenta que el debate en torno a la neutralidad de la Red, si se me permite la expresión, se ha «enredado» entre otras circunstancias por las imprecisiones sobre su sentido intrínseco (2); por las tensiones entre los diversos modelos de negocios de las distintas empresas de telecomunicaciones, de servicios y de contenidos que se desenvuelven en Internet (3); así como por la intención de algunos Gobiernos de controlar el tráfico en Internet. Por ello conviene asentar en primer lugar las razones de la defensa.

1. EL PLANO DE LA NEUTRALIDAD

La expresión «neutralidad de la Red» se generalizó en los Estados Unidos de Norteamérica con el nuevo milenio (4) y, en principio, persigue que los datos se transmitan sin discriminación, sin ser alterados, sin que

(1) De manera más extensa atiendo a esta relevante cuestión en mi monografía *Neutralidad de la Red ¿realidad o utopía?*, Marcial Pons, Madrid, 2014. Sin perjuicio de la bibliografía a la que haré referencia, quiero ya destacar en este momento los libros de S. Muñoz Machado, *La regulación de la red. Poder y Derecho en Internet*, Taurus, Madrid, 2000. M. L. Fernández Esteban, *Nuevas tecnologías, Internet y derechos fundamentales*, McGraw Hill, Madrid, 1998 G. Doménech Pascual, *Derechos fundamentales y riesgos tecnológicos*, CEPC, Madrid, 2006; J. Pérez Martínez (coord), *Neutralidad de Red: aportaciones al debate*, Fundación Telefónica, Madrid, 2011; M. Barrio Andrés, *Fundamentos del Derecho de Internet*, CEPC, Madrid, 2017; Ch. T. Marsden, *Network Neutrality. From policy to law to regulation*, Manchester University Press, 2017; así como la obra colectiva editada por L. Belli y P. de Filippe, *Net Neutrality Compendium. Human rights, fee competition and the future of the Internet*, Springer, 2016.

(2) Es frecuente que se incendien las discusiones con porfías sobre la velocidad de la red, el coste o la gratuidad, la férrea defensa de la libertad de expresión, la polémica sobre la propiedad intelectual... y así seguido, cuando la deliberación sobre la neutralidad de la Red ha de constituir algo previo pues implica el principio de no discriminación en las transmisiones; *vid. Neutralidad de la Red...*, cit, pp. 57 y ss.; J. Barata Mir, «El concepto de net neutrality y la tensión entre regulación pública y autorregulación privada de las redes», *Revista de Internet, Derecho y Política*, núm. 13/2012, pp. 57 y ss. (disponible en http://idp.uoc.edu).

(3) Son tensas las relaciones entre las empresas de telecomunicaciones, que apelan a las elevadas inversiones para la mejora de sus redes, así como la incorporación de las nuevas tecnologías que con tanta celeridad se superponen, con las empresas de servicios y de contenidos que no necesitan de tanta financiación para obtener unos significativos beneficios. Tal tensión es una de las principales causas que más complija el debate de la neutralidad de la Red.

(4) Resulta obligada la cita de los artículos de Lawrence Lessig y Tim Wu, principales catalizadores de esta tendencia. Sirva la referencia a su conocida carta «Ex Parte Submission in CS Docket 02-52» de 22 de agosto de 2003 (http://www.timwu.org/wu_lessig_fcc.pdf); T. Wu, «Network neutrality, broadband discrimination», *Telecomm & High Tech Law*, núm 2 de 2003 o «Why have a telecommunications law? Anti-discrimination norms in communications», *Telecomm & High Tech Law* núm. 15, 2006 (accesibles en su página web). Otros primeros estudios se recogieron en el libro dirigido por T. M. Lenard y R. J. May *Net neutrality or net neutering. Should broadband Internet services be regulated?*, Springer, 2006.

unos cuenten con preferencias mientras otros sufren postergaciones y todo ello con independencia de dónde procedan o a dónde se dirijan.

Un largo periplo ha recorrido y sigue recorriendo la concreción de los derechos de los usuarios y de las posibilidades de negocio de las empresas en los Estados Unidos de Norteamérica desde que el Presidente de la Comisión federal de telecomunicaciones anunciara las libertades de los ciudadanos que debían garantizarse en ese sector. En estos días pugnan las últimas decisiones de esa agencia americana alterando el régimen jurídico de Internet con las iniciativas en el Congreso y los acuerdos de algunas autoridades de los Estados federados que declaran la aplicación de la neutralidad en su ámbito (5). Un debate que nos ha de interesar sobremanera porque el predominio mundial de las empresas norteamericanas de telecomunicaciones genera el riesgo de que sus prácticas de negocio inunden el territorio europeo. El peligro de que esas humedades empapen los valladares levantados por las instituciones europeas para garantizar los derechos y libertades públicas y una Internet abierta y neutral en los Estados miembros y con el tiempo –un tiempo que corre veloz en el ámbito de las telecomunicaciones– genere unos desconchones y grietas que lleguen a abatir la fortaleza del Derecho de la Unión.

Hemos de estar, por consiguiente, muy atentos a lo que ocurre al otro lado del Atlántico.

En todo caso, ¿en qué consiste ahora mismo la defensa de la neutralidad en la Unión Europea? (6).

Contamos ahora con un texto básico –en concreto el Reglamento 2021/2015, de 25 de noviembre– que ha fijado unas normas comunes con el fin de garantizar un tratamiento equitativo y no discriminatorio del tráfico en la prestación de servicios de acceso a Internet y los derechos relacionados de los usuarios finales (7).

Este Reglamento europeo nos reconoce a los ciudadanos, a los usuarios de los servicios de telecomunicaciones, los derechos de acceso a la

(5) Sobre la historia de la regulación de las telecomunicaciones en los Estados Unidos de Norteamérica y los conflictos judiciales más relevantes puede verse M. Fuertes, *Neutralidad en la Red...*, cit. pp. 18 y ss. Hay que advertir que en diciembre de 2017, la Comisión Federal de telecomunicaciones revocó las medidas establecidas que garantizaban la neutralidad, facilitando que las empresas discriminen el tráfico en sus redes. Sin embargo, algunos Estados como Montana, Nueva Jersey y otras autoridades están firmando órdenes ejecutivas exigiendo el respeto de la neutralidad en los territorios donde extienden sus competencias.

(6) Sobre la historia del largo trayecto hasta la actual regulación, *vid.* M. Fuertes, *Neutralidad de la Red...*, cit., pp. 31 y ss.

(7) Resumen de manera suficiente y con buen espíritu crítico esta regulación: J. Vida Fernández, «Las garantías para el acceso a una Internet abierta en el Reglamento (EU) 2015/2120: una batalla perdida para la neutralidad de la Red», *Revista General de Derecho Europeo*, núm. 40/2016; y J.A. Martí del Moral, «La discutida configuración de la neutralidad de la Red: evolución normativa y el Reglamento de la Unión Europea 2015/2120, de 25 de noviembre», en la obra coord. por L. Parejo y J. Vida, *Los retos del Estado y la Administración en el siglo xxi. Libro homenaje al Prof. Tomás de la Quadra*, Iustel, Madrid, 2017, pp. 1611 y ss. del volumen II.

información, a su distribución, a suministrar aplicaciones y servicios, a utilizar las terminales que elijamos. En principio y con carácter general, las empresas han de considerar todo el tráfico de manera equitativa, sin discriminación, sin restricciones o interferencias con independencia de quién sea el emisor y el receptor de la comunicación, prescindiendo del contenido, de las aplicaciones o servicios utilizados, de los equipos y aparatos. Las empresas no pueden bloquear, ralentizar, alterar, restringir, interferir, degradar contenidos, aplicaciones o servicios concretos salvo excepciones lógicas en todo Estado de Derecho. A saber la necesidad de cumplir las leyes y sentencias judiciales; preservar la integridad de las Redes y evitar una inminente congestión (art. 3.º).

Es con relación a esta última excepción donde pueden presentarse riesgos que planten la semilla de la desigualdad entre los ciudadanos y con ello crezcan plantas que generen una densa jungla donde empiece a perecer el Estado social y democrático de Derecho.

Las empresas pueden y deben gestionar el tráfico. Es su misión. Ahora bien, tal gestión ha de ser «equitativa» y los criterios o medidas que introduzcan para la misma han de ser, como en tantos ámbitos de la prestación de servicios de interés general, medidas razonables, no discriminadoras, proporcionadas y transparentes.

Pero antes de precisar algunas técnicas para garantizar que esa gestión del tráfico no quiebre el principio de neutralidad de la Red, apunto otro riesgo que acoge el Reglamento europeo. Me refiero a la posibilidad de que las empresas formalicen contratos de «servicios especializados», esto es, aquellos servicios distintos al de acceso que ofrezcan unos mejores resultados.

Es cierto que se han establecido varios límites con el fin de mantener el equilibrio en la Red. En concreto, sólo podrán facilitarse tales servicios si, por un lado, la capacidad de la Red es suficiente. Por otro, no podrán ser utilizados tales servicios especializados como sustitución del acceso a Internet y, además, como tercer linde, no podrán generar un detrimento de la calidad de los servicios de acceso para los usuarios (art. 3.5 del Reglamento) (8). Existe, en consecuencia, un marco en el que deben desenvolverse tales servicios «especiales», que se considera suficiente para impedir la generación de una brecha de desigualdad. No obstante, a pesar de esta regulación, el peligro de la quiebra de la neutralidad persiste.

(8) El organismo europeo que agrupa a todas las autoridades nacionales responsables de las telecomunicaciones, ORECE, publicó una guía con ilustrativos criterios para facilitar la aplicación de ese Reglamento europeo (tiene como referencia BoR 16, 127, de 30 de agosto de 2016).

2. PAUTAS DE PROTECCIÓN DE LOS USUARIOS

En España la aprobación de este Reglamento europeo no ha alterado las previsiones normativas existentes sobre las condiciones de calidad de la prestación de los servicios de telecomunicaciones. En desarrollo de la Ley de telecomunicaciones es una Orden ministerial la que fija los criterios mínimos de calidad y exige facilitar la información de tales índices por parte de las empresas operadoras (en especial, art. 50 LT) (9). La rapidez de los avances tecnológicos y la multiplicación de posibilidades que ello genera me hace dudar de que esta regulación permita extraer todas las consecuencias para la protección de los derechos de los usuarios que la gestión del tráfico origina.

En resumen, impone obligaciones de información, con los actuales parámetros armonizados del Instituto europeo, a aquellas empresas que tengan un volumen de facturación superior a veinte millones de euros o una cuota de mercado del diez por ciento en cualquier ámbito geográfico. Tales compañías deben: garantizar los parámetros de calidad fijados, incorporar instrumentos de medida para su comprobación, facilitar dicha información a la Secretaría de Estado y difundirla a través de su página web. Además, deberán contratar a una empresa «solvente e independiente» para que audite las mediciones y contraste la información suministrada. El resto de empresas operadoras deberán proporcionar sus índices de calidad a través de su página web, como establece con carácter general el artículo 14 de la Carta de derechos de los usuarios. La Administración divulgará mediante unas guías básicas los umbrales esenciales de calidad de los servicios. Guías y orientaciones que proceden de los trabajos realizados por una Comisión específica, denominada de manera expresiva «para el seguimiento de la calidad del servicio» y que está integrada por una suficiente representación de las asociaciones de usuarios y de empresas con mayor presencia en el sector de las telecomunicaciones (10).

La reacción ante un significativo incumplimiento de tales parámetros, ante una degradación del servicio cuyos perfiles fija la propia Orden ministerial, se concretan en facultades de inspección para comprobar el

---

(9) Recuérdese que la Ley de telecomunicaciones retiene en el Ministerio de Energía, Turismo y Agenda Digital la competencia relativa a la protección de los usuarios [art. 69.f) LT] y, en concreto, depende de la Secretaria de Estado el órgano específico para la resolución de los conflictos entre las empresas operadoras y los usuarios: la Oficina de atención al usuario de telecomunicaciones. La Orden en estos momentos vigentes es la núm. 1090/2014, de 16 de junio.

(10) En la actualidad cada proveedor despliega unos sistemas de medidas y sondas de prueba en función del número de usuarios. Tales sistemas son aprobados por el Ministerio y son auditados por una organización independiente. Los resultados de tales mediciones –que se realizan constantemente– son publicados cada tres meses tanto por las empresas operadoras, como por el Ministerio. Puede verse, en este sentido:

http://www.minetad.gob.es/telecomunicaciones/es-ES/Servicios/CalidadServicio/Paginas/Calidad.aspx.

suceso y en la emisión de recomendaciones que podrán ser públicas (arts. 72 y ss LT) (11). Como se advierte, esas degradaciones están considerando más los grandes fallos de la red en su conjunto, que las perturbaciones voluntarias que pueda realizar la compañía. Es ahí donde más exposición corre el respeto a la neutralidad de la red.

No obstante, ha de insistirse en las obligaciones de las empresas de telecomunicaciones y me detengo brevemente en su recordatorio.

2.1 **La competencia como primera defensa**

Defender la neutralidad de Internet implica que no se podrá impedir, por regla general, la comunicación con servidores, páginas, contenidos, servicios... etc., siempre que el correspondiente contrato no contenga explícitas limitaciones (como permite la LT, art 53). Una vez que un usuario ha suscrito un contrato con un operador o accede a través de una red gratuita, ya sea pública o privada, ha de poder navegar, dirigirse a los destinos que quiera, utilizar los servicios que convenga, descargarse los contenidos que le interesen, usar los programas o aplicaciones que elija, disfrutar de las futuras utilidades que se creen o se inventen... En principio, el comportamiento neutral del operador exige ese acceso abierto y la adecuada comunicación sin interrupciones, detenciones o cortes (12).

Resulta inadmisible que mediante decisiones unilaterales y arbitrarias de la empresa operadora se impida la libre navegación. Y, así, la sentencia de la Audiencia provincial de Madrid de 29 de noviembre de 2012 (AC 2013\67) confirmó la condena impuesta y la responsabilidad patrimonial de una empresa operadora que bloqueó el acceso a la página web de una sociedad dedicada a la enseñanza de ilustración de libros. La página web era el único medio de esa compañía para relacionarse.

Del mismo modo, los usuarios tienen derecho a no soportar dificultades en lo que se considera un tráfico «adecuado», en no ver entorpecida

(11) Es el artículo 21 el que precisa qué ha de entenderse por degradación «significativa», por ejemplo una interrupción total o un incumplimiento de la calidad establecida en las guías de referencia del Ministerio si afecta a la imposibilidad de realizar llamadas de emergencia durante dos horas, a los usuarios de las islas, las ciudades autónomas o más de veinticinco mil usuarios de la península; o a más de cien mil usuarios durante una hora. Se consideran degradaciones menores las interrupciones que afecten a más de veinticinco mil usuarios durante dos horas entre las siete de la mañana y las doce de la noche. A mi juicio, una calidad del servicio acomodada a nuestros tiempos debería ser más exigente.

(12) El artículo 12 bis de la Ley de servicios de la sociedad de información de 11 de julio de 2002 establece la obligación de informar sobre las herramientas de filtrado y la restricción de acceso a contenidos no deseados o que sean nocivos para la infancia. *Vid.* P. A. de Miguel Asensio, *Derecho privado de Internet*, Civitas, 4.ª ed. 2011, pp. 181 y ss. Recordemos que la Declaración conjunta sobre libertad de expresión e Internet promovida por las Naciones Unidas considera que «los sistemas de filtrado de contenidos impuestos por gobiernos o proveedores de servicios comerciales que no sean controlados por el usuario final constituyen una forma de censura previa y no representan una restricción justificada a la libertad de expresión».

su navegación normal, en que su velocidad contratada no sufra restricciones, ni padezca estrangulamiento, ni una dificultad en las descargas y comunicaciones

Ahora bien, tales previsiones generales han de matizarse porque una empresa puede recibir un mandato público de bloqueo, así como la retirada de contenidos cuando se atente al orden público, a la salud pública, a la dignidad de la persona o sea necesario salvaguardar los derechos de propiedad intelectual (13).

Se asienta, en consecuencia, la defensa de la neutralidad de la Red en los contratos privados y en las prácticas mercantiles que surjan con el desenvolvimiento del mercado y de los negocios. Siendo relevantes las técnicas que ofrece el Derecho de la competencia, sin embargo, a mi juicio, no son suficientes. El mercado es muy variopinto y su desenvolvimiento nos sorprende con frecuencia. No hay que esperar a la aparición de un «cisne negro». Las prácticas mercantiles pueden conducir a que distintas empresas con diversos negocios, unos de proveedores de Internet, otras de programas de navegación, otras de servicios, se unan y pacten encauzar a sus clientes a través de sólo las empresas de ese concierto. Tales pactos podrían ser colusorios y, aunque como sabemos están proscritos por el Derecho de la competencia, su delimitación está definida con amplios criterios y la prueba no siempre es fácil. En principio, están prohibidos aquellos contratos que tienen como consecuencia clara limitar la competencia, además de todas aquellas recomendaciones o prácticas concertadas que se dirijan a tal fin (14). La amenaza es cercana por los anuncios de empresas norteamericanas que podrían generalizarse.

---

(13) Artículo 8 de la Ley de servicios de la sociedad de información y comercio electrónico (Ley 34/2002, de 11 de julio). En la *Declaración conjunta sobre libertad de expresión en Internet*, promovida por las Naciones Unidas, se considera el bloqueo obligatorio de sitios web enteros, direcciones IP, puertos, protocolos de red o ciertos tipos de usos una medida extrema *«que solo podría estar justificada conforme a estándares internacionales, por ejemplo, cuando sea necesaria para proteger a menores del abuso sexual»*. Desarrollo estos aspectos y recojo suficiente bibliografía y pronunciamientos de las autoridades de la competencia en Neutralidad de la Red..., cit. pp. 99 y ss.

(14) Recuerdo que uno los supuestos que indica el artículo 81.1.b) del Tratado como constitutivo de pacto colusorio es el de aquellos acuerdos que tienden a limitar o controlar la producción, el mercado, el desarrollo técnico o las inversiones. El Tribunal de Justicia de la CE ha venido ha señalar que el acuerdo colusorio es todo pacto verbal o escrito mediante el cual varios operadores económicos se ponen de acuerdo en realizar determinada conducta que tiene por objeto o efecto restringir la competencia señalando que habrá acuerdo siempre que haya un concierto de voluntades entre varias empresas independientes (STJCE de 20 de marzo de 1985, asunto Italia contra la Comisión, 19 de mazo de 1991, asunto Francia contra la Comisión; o 7 de marzo de 1990 asunto GB-Inmo-BM). Ilustrativa exposición de la aplicación de esta regulación y jurisprudencia en el ámbito de las telecomunicaciones ofrece L. A. Velasco San Pedro, «Regulación y competencia en el sector de las telecomunicaciones», en la obra dirigida por T. de la Quadra, *Regulación económica. IV. Telecomunicaciones*, Iustel, Madrid, 2009, en especial, pp. 743 y ss.

2.2 **Una gestión del tráfico adecuada**

Sucesivos avances técnicos han perfeccionado la arquitectura de las redes de tal modo que se han ido incorporando precisiones con el fin de conseguir una mejor comunicación. Las primeras pautas se apoyaron en el principio del transporte mercantil «de extremo a extremo» (15). Pero la necesidad de evitar ciertos riesgos, como la multiplicación de mensajes basura o la propagación de virus facilitó la incorporación de otras técnicas para dotar de confianza al tráfico (16) y, a partir de ahí, se buscó una gestión eficaz, que fuera la mejor posible (*best effort*) sin originar en ningún caso discriminaciones, como si la red fuera ciega.

La necesidad de proteger la red, de asegurar la transmisión ante el incremento de los peligros, defenderse de las plagas, impedir la instalación de herramientas autómatas que multiplican las malas prácticas y otras circunstancias son causas suficientemente poderosas que justifican la introducción de nuevas técnicas. Ha de facilitarse el buen desarrollo de unas transmisiones cada vez más exigentes que requieren una especial atención y ritmo –caso de las emisiones musicales o de vídeo, así como los juegos y apuestas, entre otras–.

Los especialistas van agregando nuevos diseños en los algoritmos para la distribución de los paquetes y se ha extendido la idea de distinguir diferentes «capas» de información (17). De manera muy resumida, diferencian los técnicos la estructura de la comunicación en diversas capas, entre las que resaltan cuatro: la integrada por las infraestructuras (las líneas, cables, fibra óptica, satélites...), la «lógica», (integrada por los protocolos de comunicación, nombres de dominio, identificadores como las direcciones IP); las relativas a las diversas aplicaciones (como las que identifican las páginas web, los correos electrónicos, la mensajería, el sistema VoIP, etc.); y, finalmente, la capa de contenidos concretos.

---

(15) *Vid.*, entre otros, J. H. Saltzer, D. P. Reed, D. D. Clark, «End to end arguments in system design» *ACM Transactions on computer sys*, 277, 1984; M. S. Blumenthal y D. Clark «Rethinking the design of the Internet: the end-to-end arguments vs. the brave new world», *ACM Transactions on Internet Technology* 2000; M. A. Lemley y L. Lessig, L. «The end of end-to-end: preserving the architecture of the Internet in the broadband era», *UCLA Law Review* 48, 2001, pp. 925 y ss.

(16) Por ejemplo, D. Clark y M. Blumenthal, «The end-to-end argument and application design: the role of trus», *Federal Communications Law Journal*, vol. 63, n.º 2, 2011 pp. 357 y ss.

(17) D. Arjonés Giráldez, «Un principio jurídico de neutralidad aplicado a la regualción del servicio de banda ancha. Análisis de la neutralidad de la red desde la perspectiva de su arquitectura por capas», *REDA* núm. 155, pp. 319 y ss., defiende que el problema se resolvería diferenciando los distintos ámbito de negocio y mercado y estableciendo una separación de actividades para impedir la integración vertical de las empresas, promoviendo en cada «capa» la máxima competencia; en el mismo sentido, «La neutralidad de la red desde la perspectiva de su arquitectura por capas. ¿De transportistas públicos a gestores de contenidos?» en A. Cerrillo, M. Peguera, I. Peña y M. Vilasau (coord.), *Neutralidad de la red y otros retos para el futuro de Internet*, Actas del VII Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya, Barcelona, 11-12 de julio de 2011, Ed. Huygens, 2011, pp. 53 y ss.

Estos sistemas de gestión pueden ir identificando y abriendo el contenido de cada capa como si de distintos sobres de cartas en papel se tratara con el fin de encauzar el tráfico. Unas inspecciones que no han de ser íntegras ni exhaustivas si no quieren calificarse de intromisiones ilegítimas en la intimidad.

Entrar en tales propuestas técnicas me resulta algo ajeno a estas páginas. Lo que sí resalto es que cualesquiera prácticas de gestión que se adopten deberán satisfacer unas mínimas exigencias jurídicas para que puedan ser admitidas porque, en todo caso, han de respetarse los derechos y libertades fundamentales. En especial, la protección a la intimidad y la defensa del secreto de las comunicaciones.

Ha de garantizarse pues una gestión que no afecte a los derechos fundamentales.

Más abajo atenderé de nuevo a la calidad del servicio y a la gestión del tráfico formulando mis propuestas. Conviene ahora conocer otros aspectos.

2.3 **Quejas y reclamaciones**

Cualquier internauta puede formular quejas y reclamaciones ante restricciones, bloqueos, retrasos, demoras, interrupciones y demás molestias graves y permanentes que padezca ante la empresa con la que se ha contratado el servicio de acceso a Internet. Muchos preceptos lo recuerdan: los artículos 47 de la Ley de telecomunicaciones, 26 de la Carta de derechos de los usuarios de comunicaciones electrónicas, así como la Orden ministerial de 12 de abril de 2007 (18). Si la mediación de la Administración no satisface, podrán ejercitarse las correspondientes acciones judiciales al tratarse de disputas enmarcadas en un contrato privado entre particulares. Demandas que también pueden presentarse por asociaciones de defensa de los consumidores, en virtud de la posible acción de cesación incorporada al Derecho español desde la Ley 39/2002, de 28 de octubre.

La neutralidad también puede ser exigida por las empresas que ofrecen servicios y contenidos a través de Internet y advierten cómo es bloqueado o se dificulta el acceso a sus páginas. Estas reclamaciones han de ser dirigidas ante la Comisión nacional de los mercados y la competencia, por lo que se podrán perseguir las denuncias por fijación de condiciones de servicio, conductas colusorias que impliquen un control en la distribu-

(18) *Vid.* L. Arroyo Jiménez y A. I. Mendoza Losana, «Los usuarios de las telecomunicaciones» en la obra dirigida por T. de la Quadra *Regulación económica. IV. Telecomunicaciones*, cit. en especial pp. 286 y ss.; J. M. Serrano Cañas, «La protección de los usuarios de los servicios de telecomunicación electrónicatelefonía fija-móvil e internet» en *Derecho (privado) de los consumidores*/coord. por Luis María Miranda Serrano, Javier Pagador López, 2012, pp. 389 y ss.; A. Carrasco Pereda, *Estudios sobre telecomunicaciones y Derecho del consumo*, Aranzadi, Pamplona, 2005.

ción de contenidos en Internet, abusos de posición dominante, en fin, todas aquellas actuaciones que incidan en el desenvolvimiento del mercado de empresas de Internet (arts. 1 y 2 de la Ley de defensa de la competencia, núm. 15/2007, de 3 de julio) (19).

En consecuencia, existen técnicas de defensa. Sin embargo, a mi juicio, no resultan del todo suficientes porque asegurar la neutralidad de la Red no implica únicamente que se garanticen unas mínimas condiciones de calidad en el servicio de acceso a Internet. No hay que atender únicamente a las condiciones que establezcan las empresas operadoras y a las posibilidades de los usuarios de cambiar el contrato. La neutralidad de la Red no gira de manera exclusiva sobre las prácticas de negocio, sobre las cláusulas mercantiles en los contratos con los usuarios, sobre la defensa de la competencia para facilitar la incorporación de nuevos empresarios, de nuevas iniciativas. Advertir sólo esa faz cuando se habla de neutralidad de la Red supone prescindir de la trascendencia que oculta la verdadera cara de la moneda: responder a la libertad de los usuarios y no incorporar elementos que discriminen a unos u otros ciudadanos y empresarios.

Pasado un año de la entrada en vigor del Reglamento europeo, tanto el Gobierno de España, como el Organismo europeo que acoge a todas las autoridades competentes en este ámbito (ORECE), han publicado informes sobre su aplicación y, con relación a la neutralidad de la Red, han afirmado que las quejas y reclamaciones presentadas por los usuarios son escasas, por lo que entienden que los problemas «no son significativos» (20). No obstante, algunos organismos reguladores de los Estados miembros sí han adoptado decisiones suspendiendo determinadas prácticas de las empresas –como las denominadas *zero rating,* que deberíamos traducir como «tasa cero»– al considerar que originaban unas desproporcionadas discriminaciones en la gestión del tráfico de datos (21).

En fin, afirmar que en la actualidad los usuarios estemos satisfechos porque nuestras pautas de conducta quedan complacidas por la zona en la que navegamos no ha de conducir a que nos instalemos en una situación de despreocupada confianza. Por el contrario, habría que permane-

(19) Sobre el procedimiento y las facultades de la Comisión existe, como es sabido, muchos e ilustrativos estudios. Me remito a los mismos. En todo caso, recogen precisas consideraciones y abundante bibliografía los estudios recogidos en la obra colectiva dirigida por J. M. Sala Arquer, *Comentario a la Ley de defensa de la competencia*, Aranzadi, Pamplona, 2012.

(20) Me refiero al Informe del ORECE 17/240, de 7 de diciembre, así como al Informe de la Secretaría de Estado para la información y la sociedad digital, sobre «la supervisión en España de la normativa europea en materia de acceso a una Internet abierta (neutralidad de la Red)», de 14 de julio de 2017. Ambos están, lógicamente, accesibles a través de Internet en las sedes electrónicas correspondientes.

(21) Tal ha sido el caso de Bélgica, Eslovenia, Hungría, Los Países Bajos y Suecia como recoge el informe elaborado por la consultora Cullen Internacional en marzo de 2017 (disponible en su página web). En España, sin embargo, no se ha adoptado decisión alguna sobre estas prácticas que empiezan a ofertar algunas empresas de telecomunicaciones.

cer vigilantes y en estado de alerta. Ha de impedirse que las empresas canalicen en unos pocos cauces algunas aguas de Internet y, siguiendo con el símil, los ciudadanos nos acostumbremos a chapotear en esas aguas embalsadas sin posibilidad de conocer otros mares y experiencias. Ese es el gran riesgo (22).

De ahí que insista en los intrínsecos fundamentos sobre los que se asienta una firme defensa de la neutralidad.

3. LA NECESIDAD DE INSISTIR EN LO IMPORTANTE

La razón esencial para exigir una adecuada actitud neutral en el tráfico por las redes radica en reconocer que Internet se ha convertido en la actualidad en un medio común donde los ciudadanos manifestamos nuestra personalidad. El despliegue tecnológico en Internet no sólo ha impulsado negocios u ordenado tantos aspectos sociales de gestión de infraestructuras. A través de Internet los ciudadanos «nos vivimos», nos expresamos y desarrollamos. Eso tiene una trascendencia capital porque conduce a la necesidad de que la Red respete la libertad y los derechos fundamentales, esencia de nuestra civilización (23).

Derechos como la intimidad, la libertad de expresión y comunicación están directamente afectados por la forma de entender la neutralidad de la Red. Admitir determinadas intrusiones en la gestión del tráfico de Internet, en la comprobación y selección de los datos lesiona tales derechos fundamentales y, por ello, deben rechazarse con contundencia. Del respeto y protección de estos derechos depende el libre desarrollo de la personalidad base del orden social que posibilita las ventajas de una sociedad abierta y libre.

Con anterioridad ya recordé la Declaración de las Naciones Unidas de 1 de junio de 2011 (24). En la misma, se subraya la importancia de la liber-

(22) Alertó hace tiempo sobre estas amenazas J. L. Zittrain, *The future of the Internet and how to stop it*, 2008 (disponible en http://futureoftheInternet.org) y recientemente el organismo regulador francés ARCEP ha publicado un informe en el que llama la atención sobre los peligros de cierre de espacios que se están generalizando a través de los terminales móviles y las aplicaciones, *Les terminaux, maillon faible de l'ouverture d'Internet*, febrero 2018.

(23) Sobre las conquistas que ha superado la lucha por la libertad de expresión es muy recomendable la lectura del libro de S. Muñoz Machado, *Los itinerarios de la libertad de palabra*, Ed. Crítica, Barcelona, 2013, que también acoge los problemas derivados de la comunicación a través de Internet. Recuerdo, además, los sugerentes trabajos publicados en la obra colectiva dir. por L. Corredoira y L. Cotino, *Libertad de expresión e información en Internet. Amenazas y protección de los derechos personales*, CEPC, Madrid, 2013; el interesante artículo de M. L. Fernández Esteban, «La regulación de la libertad de expresión en Internet en Estados Unidos y en la Unión Europea», *Revista de estudios políticos*, núm. 103/1999, pp. 149 y ss.; en fin, también C. Marsan, «The net as a public space: is net-neutrality necessary to preserva on-line freedom of expression?», en A. Cerrillo, M. Peguera, I. Peña y M. Vilasau (coord.), *Neutralidad de la red y otros retos para el futuro de Internet*, cit. pp. 79 y ss.

(24) La cita correcta y completa es larga: Declaración conjunta por el Relator especial de las Naciones Unidas (ONU) para la libertad de opinión y de expresión, la Representante para la libertad de los medios de comunicación de la organización para la seguridad y la cooperación en Europa

tad de expresión y se insiste en que son contrarias al Orden internacional algunas quiebras de la neutralidad de la Red. Tal sería el caso de bloqueos en el uso de Internet, que sólo podrían realizarse siguiendo estándares internacionales para la protección de otros derechos preferentes; y se equipara el filtrado de contenidos a una forma de censura no admisible.

En similar sentido, desde el Consejo de Europa se pretende promover una regulación que garantice los derechos fundamentales en Internet. En concreto, el Consejo de Ministros de telecomunicaciones firmó una Declaración sobre neutralidad de la Red en la que se resalta el necesario respeto a la vida privada, a la libertad de expresión, de información y difusión del conocimiento, a la protección de los usuarios para utilizar los instrumentos y herramientas que sean de su elección, sin perjuicio de admitir que las empresas realicen una mínima gestión del tráfico (septiembre de 2010). A la misma han seguido estudios y propuestas para concretar ese posible marco común de neutralidad (25). Junto a estas declaraciones ha sido el Tribunal europeo de Derechos humanos quien con contundencia ha declarado que impedir el acceso a Internet supone una violación de las libertades de expresión e información (26). En su sentencia de 18 de diciembre de 2012 (caso Ahmet Yildirim) (27), al resolver sobre el bloqueo a la página web de un acusado declaró que: «*Internet es en la actualidad el principal medio de la gente para ejercer su derecho a la libertad de expresión y de información: se encuen-*

(OSCE), la Relatora especial de la Organización de Estados Americanos (OEA) para la libertad de expresión y la Relatora especial sobre libertad de expresión y acceso a la información de la Comisión africana de Derechos humanos y de los pueblos (CADHP).

(25) Una interesante propuesta recogen L. BELLI y M. VAN BERGEN en «Protecting human rights through Network Neutrality: furthering internet users' interest, modernising human rights and safeguarding the Open Internet», dentro del encuentro promovido por el Consejo de Ministros de los medios y la sociedad de la información celebrado en Estrasburgo en diciembre de 2013 (referencia CDMSI, 2013, MISC 19E) y disponible en www.coe.int.

(26) Es una línea doctrinal constante de este Tribunal que la libertad de expresión se extiende tanto al contenido de la información como *«a los medios de transmisión o recepción, ya que cualquier restricción impuesta... interfiere necesariamente en el derecho a recibir y proporcional información»* (sentencia de 22 de mayo de 1990, caso Autronic). Entre esos medios ha de ocupar ahora un lugar prioritario Internet.

(27) Interesa conocer el conflicto que se inicia porque un juez penal de Turquía había acordado en junio de 2009 el bloqueo de un sitio web cuyo titular había sido acusado de insultar la memoria de Atatürk. Con posterioridad, la autoridad turca competente en telecomunicaciones solicitó que se ampliara el bloqueo a todo el servicio «Google sites», en el que se alojan como es conocido muchas páginas web. Entre ellas, la del denunciante que llega a Estrasburgo. Recurre porque esas medidas impedían el acceso a su propia página. Medidas que subsistían incluso mientras se sustanciaba el proceso ante ese Tribunal de derechos humanos en 2012, a pesar de que las iniciales actuaciones contra el difamador habían cesado por haber sido imposible localizarle. El Tribunal europeo declaró la violación del Convenio de Roma: no se había sustanciado ningún proceso contra el recurrente, ni contra el servidor Google; ni se había analizado por el Tribunal penal la proporcionalidad de la medida, ni si había otras alternativas para perseguir las difamaciones. A los efectos que aquí me interesan, resulta relevante este pronunciamiento porque el Tribunal reconoce que el acceso a Internet es un derecho instrumental de la libertad de expresión. Aun no tratándose de una prohibición total, de una restricción absoluta de acceder a Internet, esa medida generó una importante limitación que bloqueó el acceso a la página web del demandante.

tran herramientas esenciales de participación en actividades y debates relativos a cuestiones políticas o de interés público... Este hecho es suficiente para que el Tribunal concluya que la medida en cuestión constituye una "injerencia de las autoridades públicas" en el derecho del interesado a la libertad de expresión, de la que forma parte la libertad de recibir y de comunicar informaciones o ideas». Esta doctrina se reitera en otro importante pronunciamiento que tiene como fecha el 1 de diciembre de 2015 y que atendió los recursos contra el corte general al servicio de YouTube (28). En fin, este Tribunal se ha pronunciado igualmente sobre la procedencia de algunas restricciones al uso de Internet de los reclusos (así, las sentencias de 19 de enero de 2016 y 17 de enero de 2017).

Y junto a estas libertades públicas, amparar la neutralidad es defender la igualdad de oportunidades de los ciudadanos y también de las empresas (29). Constituye la igualdad el núcleo esencial de la alegato de la neutralidad de la Red. Los datos que transitan por la Red no deben ser discriminados de manera arbitraria por quien gestiona el tráfico.

En consecuencia, las autoridades públicas han de garantizar el derecho de acceso a una Internet abierta y neutral. Para ello pueden imponer las correspondientes obligaciones de servicio a las empresas privadas. Una obligaciones que garanticen el adecuado respeto a los derechos fundamentales. Es bien conocida la historia de la conquista de esa progresiva modulación de las relaciones privadas con el fin de salvaguardar el contenido esencial de los derechos fundamentales y arbitrar el equilibrio de

(28) Se trata del caso Cengiz y otros contra Turquía. En resumen: en un proceso penal se acordó el bloqueo general del citado servicio y algunos ciudadanos, contra los que no se actuaba, pretendieron presentar alegaciones por sufrir tal restricción. El Tribunal penal las inadmitió al no ser parte directa en ese proceso penal y hubo quien recurrió al Tribunal Constitucional que sí declaró que la legislación no amparaba un bloqueo general y estimó que se había producido una violación a los derechos de libertad de información y comunicación. Pero, además, tres profesores de Facultades de Derecho de distintas Universidades recurrieron ante el Tribunal europeo de Derechos Humanos y pretendieron una condena específica por violación del Convenio de Roma. Durante años había estado bloqueado el acceso a YouTube y alegaban que constituía una fuente de conocimiento para sus estudios y clases por los vídeos de muchos Organismos internacionales, además uno de ellos también tenían cuenta en ese servidor para difundir sus conferencias. Recordando su doctrina, en especial la citada sentencia Ahmet Yildirim, el Tribunal de Estrasburgo declaró la violación del Convenio porque ni estaba amparado legalmente un bloqueo general, ni se habían considerado los efectos indirectos, ni se había facilitado a los demandantes un suficiente grado de protección de sus derechos fundamentales.

(29) Resulta innecesario reiterar las decenas de pronunciamientos del Tribunal Constitucional que insisten es esta básica idea y que se repite con similares expresiones desde las primeras sentencias, entre las que cabe recordar la núm. 22, de 2 de julio de 1981. Son muchos también los estudios doctrinales que han profundizado en el análisis de este principio. Sirva la cita de los trabajos de I. DE OTTO, «El principio de igualdad en la Constitución española» en *Igualdad, desigualdad y equidad en España y México*, Instituto de Cooperación Iberoamericana, Madrid, 1985, pp. 345 y ss.; J. SUAY RINCÓN, *El principio de igualdad en la justicia constitucional*, IEAL, Madrid, 1985; o el libro colectivo *El principio de igualdad*, Dykinson, Madrid, 2000.

intereses afectados. De ahí que no me detenga ahora en la misma y me remita a los estudios publicados (30).

4. CON LA MIRADA EN LOS PRÓXIMOS PASOS

4.1 **Propuestas relativas a la calidad del servicio y a la gestión del tráfico**

Como hemos visto, la regulación actual pivota en garantizar una buena calidad del servicio a los usuarios confiando en la adecuada gestión del tráfico por las operadoras. Sin duda, sucesivos avances tecnológicos permitirán incorporar nuevos modos de gestión que anuncien un mejor tráfico y podrá plantearse que las empresas, conocedoras de sus capacidades e infraestructuras gestionen la disponibilidad no utilizada. La introducción de otras posibles técnicas que, sin duda aparecerán porque es imposible predecir el desarrollo de las investigaciones, deberá ser objeto de singular y prudente análisis. Por ejemplo, abrir la espita para una total catalogación y de ahí ofrecer precios distintos podría debilitar la igualdad de trato y generar discriminaciones. Más si establecen ya la prioridad a determinados usuarios o a grandes empresarios, o si se limitara el uso del ancho de banda para reservarlo a futuros usuarios. Toda técnica debe ser analizada de manera individual, en cada caso concreto, porque, en principio, supone la eventual reducción del ámbito del principio de neutralidad. Son riesgos potenciales pero, insisto, cualquier limitación en el desarrollo de Internet puede tener daños irreversibles de ahí la necesidad de resaltar el principio de precaución que se ha extendido en otros ámbitos como la protección ambiental o la seguridad ciudadana.

Los avances tecnológicos que disfrutamos se han impulsado precisamente al estar inicialmente garantizada la igualdad y la libertad en Internet. Por ello, ha de mantenerse con carácter general la prohibición de cualquier discriminación irrazonable en la gestión del tráfico (31).

---

(30) De la extensísima relación de monografías y trabajos que tanto en España como en otros países se ha preocupado de esta cuestión recojo la referencia a muy pocas obras, a partir de las cuales, cualquier lector interesado puede seguir tirando del hilo que le conducirá a otros muchos libros y artículos de gran interés. Me remito a las obras de F. Sosa Wagner, *Juristas y enseñanzas alemanas (1945-1975). Con lecciones para la España actual*, Marcial Pons, Madrid, 2013; P. Cruz Villalón, *Derechos fundamentales y Derecho privado*, Academia sevillana del Notariado, tomo extra 1, 1988, pp. 97 y ss.; T. de la Quadra Salcedo, *El recurso de amparo y los derechos fundamentales en relaciones entre particulares*, Madrid, 1981 así como su minucioso trabajo «Incidencia o existencia de los derechos fundamentales en el Derecho privado» dentro de la obra colectiva dir. J. E. Soriano, *Por el Derecho y la libertad. Libro homenaje al Prof. J.A. Santamaría Pastor*, Iustel, Madrid, 2014, pp. 121 y ss; J. García Torres y A. Jiménez Blanco, *Derechos fundamentales y relaciones entre particulares*, Civitas, Madrid, 1986; J.M. Bilbao Ubillos, *La eficacia de los derechos fundamentales frente a particulares*, CEPC, Madrid, 1997, en fin, R. Sarazá Jimena, *La protección jurisdiccional de los derechos fundamentales en las relaciones entre particulares*, Tirant-Lo Blanch, Valencia, 2011.

(31) En este sentido también se pronuncia T. Wu, *Net neutrality*, cit, pp. 167 y ss. en las que incluso formula una iniciativa de ley de neutralidad de la red.

Las decisiones sobre nuevas técnicas de gestión habrán de superar una rigurosa evaluación de las diversas posibilidades que se presenten y sus efectos. Han de tenerse en cuenta todas las infraestructuras y, así, como nos han demostrado algunas empresas operadoras, la propia organización en red de los servicios ha facilitado la descarga o desvío del tráfico (*offloading*) para evitar congestiones a través de múltiples redes, como ocurre con las comunicaciones móviles que van saltando a través de otras redes wifi o wimax.

Además, si esa gestión del tráfico origina alguna aparente desventaja, la misma debe quedar sobradamente satisfecha con los beneficios que ofrezca. Las prácticas que catalogan el tráfico y atienden a los paquetes que entran en las redes para evitar su congestión o limitan su salida, sólo tendrán justificación si los datos que se retrasan no hacen degradar el servicio y se consigue una óptima transmisión de aquellos que no admiten ningún retraso. Se puede admitir una pequeña demora en la entrega de un mensaje de texto, pero no en la retransmisión de un concierto o una conversación en el que de una inmediata respuesta dependen otras decisiones.

Esas técnicas que consideran los paquetes en su inicio y organizan su salida pueden admitirse siempre que también se hagan con cierto ritmo, sin degradar lo que se considera una comunicación normal (32).

Y lo más importante: en ningún caso esa gestión puede afectar al contenido esencial de los derechos fundamentales y las libertades públicas. En especial, el derecho a la intimidad, a la libre expresión, a la igualdad de oportunidades. La inspección profunda de las capas, el filtrado de códigos o expresiones, no deberían desvelar en modo alguno la intimidad personal, el carácter confidencial y reservado de las comunicaciones, ni censurar la libertad de expresión e información. Es este punto, el asunto central que deben atender las técnicas de gestión del tráfico.

Ya lo he señalado. Las transmisiones se realizan a través de un complejo sistema de interconexiones de datos que se integran por múltiples capas de información: de identificación de los dispositivos, protocolos de navegación, programas utilizados... Conocer algunas de estas capas resulta indispensable para impulsar el tráfico de datos. Recordando el símil que

(32) El grupo internacional que trabaja en la ingeniería y estructura de Internet, que promueve las propuestas de estándares, *Internet engineering task force* (IETF), ha desarrollado dos protocolos diferentes que permiten, por un lado, advertir una reserva de fuentes (rsvp) y, por otro, servicios diferenciados (diffserv) que utilizan diversas estrategias de colas para ir adaptando el tráfico a las expectativas de los usuarios. B. ZELNICK y E. ZELNICK *The illusion of net neutrality. Policial alarmism, regulatory creep and the real threat to Internet freedom*, Hoover Institution press Publication, 2013, p. 158, se remite a los detalles técnicos del manual «Internetworking Technology Handbook», así como la documentación facilitada por Cisco. Menciona algunas de estas técnicas, Luis M. GONZÁLEZ DE LA GARZA, *El nuevo marco jurídico de las telecomunicaciones en Europa. Redes sociales especializadas, neutralidad de la red y dividendo digital*, La Ley, Madrid, 2011, en la nota 794 de la p. 767.

ya he utilizado de las capas como sobres de cartas: ningún cartero se dirige a ciegas al destinatario sin haber leído su nombre en un sobre de correos. Pero ese control no le permite leer el contenido para advertir el interés en su entrega.

El control de algunas capas permite evitar virus o los mensajes no deseados. Un filtrado que puede ser respetuoso con la privacidad, del mismo modo que lo son, en cierta medida, los controles de seguridad en las oficinas de correos u, otro ejemplo, en los aeropuertos, como los arcos detectores de metales. Otras inspecciones que penetren en el contenido de las capas pueden ya incidir en el ámbito reservado a la intimidad y confidencialidad. Así, revelar los sitios web visitados, los ficheros que se descargan, la identidad de los destinatarios de un mensaje, su contenido... Tales sistemas de gestión que realizan una inspección profunda no deben ser admitidos.

Conviene recordar que el Tribunal de Justicia de la Unión europea, en su sentencia de 8 de abril de 2014 (asuntos acumulados C-293/12 y C-594/12), declaró inválida la Directiva de 2006/24, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones por considerar que no satisfacía la mínima protección de la vida privada ni la protección de datos. Y es que imponía unas obligaciones generales a las empresas que permitían conocer, entre otros aspectos, los hábitos de los ciudadanos, sus relaciones sociales, sus comunicaciones, su tráfico en Internet... La falta de precisión de los fines perseguidos, de los supuestos concretos en los que debían conservarse esa información y, sobre todo, la carencia de proporcionalidad de la regulación condujo a esa declaración de incompatibilidad con el Derecho europeo, en especial, con la Carta de derechos fundamentales (33).

Ese juicio sobre las previsiones de la Directiva nos puede dar una cabal idea del cuidado que ha de tenerse en la gestión del tráfico para que tampoco pueda considerarse incompatible con la protección de datos y el respeto a la vida privada y a la confidencialidad de las comunicaciones. Por ello hay que estar muy vigilante para garantizar el efectivo cumplimiento de la normativa de protección de datos, pues son muchos los peli-

(33) Son muy sustanciosas las consideraciones del escrito de Conclusiones del Abogado general P. Cruz Villalón, que tienen fecha de 12 de diciembre de 2013. Conviene atender a este ámbito porque presentará relevantes conflictos. Así, el 31 de julio de 2014 una juez de apelación norteamericana (de la Corte de Distrito sur para Nueva York) ha ratificado la condena a una empresa de servicios a entregar los datos de un usuario, aún estando localizados en Irlanda, sin seguir el procedimiento establecido en el Tratado de asistencia legal.

gros que pueden derivar de la evolución de las técnicas de gestión y los medios de inspección masiva de las comunicaciones (34).

Es cierto que ese tráfico deberá permitir que una autoridad judicial acuerde su intervención; o que puedan discriminarse los programas o servicios generales que se hayan fijado en el contrato (como ocurre, con la protección de los menores). Pero junto a ello, hay que recordar que esas cláusulas contractuales han de ser muy cuidadosas con la protección de las comunicaciones porque afectan a varios usuarios y, además, porque el consentimiento siempre ha de garantizar otras alternativas: bien con otras empresas operadoras u otras modalidades de contratos con la misma empresa. Resulta inadmisible que se pierdan oportunidades de contratos o de herramientas si no se «aceptan» unas condiciones impuestas de manera unilateral y sin otra alternativa.

La valoración será distinta si la gestión del tráfico ha sido solicitada por el propio usuario. Del mismo modo que admitimos la suscripción de contratos diversos, con cláusulas específicas para el control paterno, también es posible que el usuario adquiera instrumentos que incorporen determinados criterios de gestión para controlar las conexiones como la seguridad en las redes inalámbricas.

En fin, para advertir si existe o no discriminación, si hay razones suficientes para una gestión de la Red, resulta imprescindible el conocimiento de la situación, esto es, de los datos del tráfico, los problemas de congestión, las condiciones de los contratos... Para defender la neutralidad es necesaria la difusión de información por las compañías operadoras, unas mínimas reglas de transparencia, así como una mayor educación de los usuarios en todos estos conceptos y sus consecuencias.

4.2 **Una defensa contundente: su reconocimiento constitucional**

Consignar una mención explícita del derecho de acceso a una Internet neutral y abierta dentro del catálogo de derechos fundamentales facilitaría su defensa y evitaría los riesgos que una mera consideración mercantil puede traer.

Y es que, de no mantenerse la neutralidad, las empresas que prestan el servicio de acceso a Internet tendrían la puerta abierta para discriminar sobre las condiciones de utilización de los servicios. Podrían establecer criterios de preferencia, prioridad, de ahí exigir pagos y cuotas diversas, ora a los usuarios, pero sobre todo a las empresas de servicios. Una situación que partiría el mercado en dos. Los economistas que ana-

(34) Aspecto en el que insistió el Supervisor europeo de protección de datos en su Informe sobre la neutralidad de la red, la gestión del tráfico y la protección de la intimidad y los datos personales (de 7 de octubre de 2011, publicado en el DOCE 2012/C 34/01).

lizan la realidad según lo que denominan «la teoría de los juegos» han insistido en que se pondría rápidamente un alto precio al tráfico por Internet (35).

Ello conduciría a establecer vínculos entre algunas empresas para obtener mayores ventajas, favoreciendo su tráfico, así como la consolidación de grandes grupos empresariales que beneficiarían a sus filiales. Lo que, a su vez, conduciría a la reducción de nuevas empresas pues la entrada en ese mercado sería muy difícil ante las situaciones que se consolidarían. La incursión de iniciativas o emprendedores, tan comunes en los mares de Internet, disminuiría de manera contundente.

Tal situación supondría una reducción drástica de la innovación y de la investigación. Hay menos iniciativa cuando el negocio está consolidado (36). Esta consecuencia haría perder el alma a Internet, su inicial espíritu y la razón de por qué se ha desarrollado y evolucionado como lo ha hecho, a través de las libres y abiertas iniciativas de muchos empresarios o emprendedores, grandes o pequeños (37).

Un horizonte ciertamente perturbador el que resumen los especialistas al insistir en esa restricción y reducción del tráfico de algunos datos, en la degradación de servicios, en la expansión de nuevas iniciativas e, incluso, en la división de Internet. Pero, sobre todo, un control del tráfico de Internet incidiría de manera directa en la forma de actuar de los ciudadanos. La conciencia de sabernos vigilados devaluaría nuestra privacidad, reprimiría nuestra expresividad, lo que tendría consecuencias en la formación de nuestra personalidad (38). Ello repercutiría en la calidad de la sociedad democrática.

Defiendo, por ello, la neutralidad, la libre elección para navegar por Internet, como hace siglos hubo una defensa de la libertad de navegación por los mares. Resulta oportuno recordar la obra de los juristas de la Escuela salmantina, en especial, Fernando Vázquez de Menchaca, que argumentaron sobre los bienes comunes e inspiraron la obra de Hugo Groccio

---

(35) Son muchos los trabajos que analizan estos aspectos. Sirva la mera remisión de los siguientes: B. VAN SCHEWICH, «Towards an economic framework for network neutrality regulation», *Journal on Telecommunications and High Technology Law*, vol. 5/2007, pp. 329 y ss.; N. Ecoomides, Economics of the Internet, NET Institut, enero 2007 pp. 6 y ss.

(36) *Vid.* H. CHENG y H. GUO, «The debate on net neutrality: a policy perspective», insisten en estos aspectos; y H. Nadal, «Sin neutralidad en la red: ¿dónde la lógica universal de la innovación?, en A. CERRILLO, M. PEGUERA, I. PEÑA y M. VILASAU (coord.), *Neutralidad de la red y otros retos para el futuro de Internet*, *cit.* pp. 95 y ss.

(37) Entre otros muchos, insiste T. WU en «Network Neutrality, broadband discrimination», cit., en especial página 146, en los logros de Internet a través de esa creación evolutiva, darwiniana de la red, que ha multiplicado la innovación y la meritocracia. Resulta también indispensable la lectura de J. L. ZITTRAIN, *The future of the Internet and how to stop it*, 2008 (disponible en http://futureoftheInternet.org).

(38) Alertan de muchas consecuencias tóxicas y nocivas E. MOROZOV, *La locura del solucionismo tecnológico*, Katz, Madrid, 2015; y E. PARISER, *El filtro burbuja. Cómo la Red decide lo que leemos y lo que pensamos*, Taurus, 2017.

sobre la libertad de mares. La neutralidad es muy similar a esa libertad de navegación por los mares. Por ello, quizás como esa libertad de navegación conozca de futuras mermas pues son varias las amenazas existentes.

¿Por qué? Porque así como en el mar son los Estados ribereños y las grandes compañías que se consolidan quienes arbitran el tráfico en los mares, así en la navegación por Internet algunos Estados quieren bloquear y controlar el tráfico. Y, sobre todo, grandes empresas de telecomunicaciones están queriendo influir sobre el acceso a específicos contenidos y servicios. Son los nuevos y poderosos señores feudales y dueños de los mares que pretenden establecer sus reglas y encauzar el tráfico.

Es cierto que no sabemos qué nos deparará el futuro en este mundo que galopa veloz. Un ejemplo: tras anunciarse la votación de la Comisión federal americana revocando los derechos amparados por la neutralidad, a los pocos días se difundió una aplicación para que los usuarios pudieran conocer si su empresa respeta o no la neutralidad.

Pero, a pesar de tantos vientos de cambios, de tantas tendencias que se suceden, hemos de ser firmes en anudar la defensa de la neutralidad con la libertad y la igualdad para navegar por Internet. No está sólo en juego la competencia en el mercado. Están en juego los derechos y libertades fundamentales. No defender la neutralidad podría generar el descenso por la pendiente de admitir la desigualdad y perder nuestro espacio de intimidad. La lucha de la humanidad ha sido y sigue siendo la lucha por la igualdad porque es expresión del respeto a la dignidad humana. Esto es lo que funda el Derecho como nos recordó brillantemente Stefano Rodotá (39).

Hay, por consiguiente, una urgencia por proclamar la necesidad de una sociedad abierta, de una sociedad libre. Y así como en el pasado los juristas han aprestado sus técnicas y conocimientos para garantizar esas conquistas al hilo de los grandes avances técnicos que se han vivido a lo largo del siglo XX, procede ahora que los juristas contemporáneos procedamos de análoga forma. Esta es la contribución que se espera de nosotros y por tanto el desafío que como profesionales del Derecho estamos obligados a afrontar.

(39) S. Rodotá, *El derecho a tener derechos*, Ed. Trotta, Madrid, 2014.

CAPÍTULO 24

LA CONFIANZA EN LA SOCIEDAD DIGITAL: LA FUNCIÓN DE LOS INTERMEDIARIOS Y LOS SISTEMAS REPUTACIONALES

Teresa Rodríguez de las Heras Ballell
Profesora Titular de Derecho Mercantil, Universidad Carlos III de Madrid

1. EL VALOR DE LA CONFIANZA EN UNA SOCIEDAD DIGITAL

La confianza es el catalizador de la interacción social y de las relaciones de cooperación e intercambio en el mercado. La percepción de ciertos factores de credibilidad teje así el entramado de confianza en el que se construyen y desarrollan las relaciones sociales y económicas. En la sociedad digital, su carácter descentralizado, su dimensión global, las dificultades de identificación, la ineficiencia de los mecanismos de supervisión y ejecución, debilitan el efecto de previsibilidad de los modelos tradicionales de generación de confianza, que se convierte en el activo más escaso del mundo digital.

El objetivo es analizar los instrumentos de generación y retención de confianza en las relaciones que se entablan y desarrollan en la sociedad digital. Para ello, se propone, en primer lugar, una definición de confianza como un concepto multidimensional que se proyecta sobre el sistema, la relación o la comunidad (2.). Las dimensiones de la confianza –sistémica, específica y agregada– permitirán identificar y construir los diversos modelos de generación de confianza (3.). Primero, los modelos centralizados que permiten retomar la figura de los intermediarios como generadores, gestores y distribuidores de confianza. Segundo, los modelos descentralizados a través de sistemas reputacionales, de revisión y opinión que emulan los mecanismos sociales de control en las comunidades digitales. A partir de esta clasificación, se propone un marco normativo para los servicios de confianza (4.) en una sociedad digital «omnimétrica» (víctima de la cuantificación), tendente a la descentralización (con modelos y tecnologías colaborativos), y marcada por una automatización creciente y expansiva de tareas, procesos y decisiones (mediante algoritmos y aplicaciones de inteligencia artificial).

2. LA CONFIANZA: CONCEPTO, FUNCIÓN Y DIMENSIONES

La confianza es un concepto amplio y multiforme que las diferentes disciplinas científicas contemplan desde diversas perspectivas (1). Por ello, no es fácil articular un concepto de confianza que sea operativo en contextos diferentes y resulta aún más complejo tratar de formularlo como un concepto jurídico. Si bien es claro que las raíces de la confianza se hunden en los modernos mercados de la información, la abundancia de información, sin embargo, no sólo deriva en la «pobreza de la atención», sino que afecta también a los pilares de la credibilidad. De ahí que estudios recientes revelen que la información exacta no es siempre suficiente

(1) O'Neill, Brian, «Trust in the information society», *Computer Law & Security Review*, num. 28, 2012, pp. 551-559.

para desmentir o corregir errores, de modo que hay que considerar otros factores que aseguren que más que informar se logre persuadir (2). En definitiva, la confianza no sólo depende de que toda la información correcta y relevante esté disponible, sino que viene determinada esencialmente por cómo se accede a ella, cómo se percibe, y cómo se procesa para generar una percepción de credibilidad.

Esta constatación nos permite articular un concepto propio de confianza que se compone de dos piezas. Primero, una pieza objetiva que abunda en la veracidad, la corrección, la suficiencia y la disponibilidad de la información necesaria para adoptar una decisión racional. Segundo, una pieza subjetiva que determina la percepción de credibilidad sobre la que se asienta la confianza. Esta percepción se refuerza positivamente con factores e indicios de credibilidad basados en la reputación, la experiencia, la popularidad, la atribución de funciones reconocidas. La sociedad digital ha dificultado la constatación y verificación de la dimensión objetiva, a la vez que ha multiplicado los factores e indicios susceptibles de reforzar la percepción de credibilidad y ha alterado sus efectos. Más aún, el componente subjetivo de la percepción ha ganado tal protagonismo en la determinación de la confianza que ha desplazado a un segundo lugar, casi irrelevante, el componente objetivo. Ante la dificultad de verificar la veracidad y corrección de la información, y como resultado de un progresivo deterioro de las referencias de autoridad y fiabilidad, la sociedad digital se recrea en factores de credibilidad basados en la popularidad, la viralidad, la relevancia, o la visibilidad, frente a criterios objetivos de veracidad y corrección cada vez más imperceptibles.

A partir de este concepto de confianza, podremos abordar en esta sección, de un lado (2.1), la relación entre la confianza y la información que alimenta su componente objetivo, y, de otro lado (2.2), los factores e indicios determinantes de la percepción de credibilidad como componente subjetivo. Tras este marco teórico, elaboramos una teoría sobre las tres dimensiones de la confianza (2.3) que nos permitirá identificar los diversos modelos de generación de confianza en la sociedad digital que analizamos en la sección siguiente (3.).

(2) Como constata un interesante estudio liderado por Kelly Garrett en *The Ohio State University, The Promise and Peril of Real-Time Corrections to Political Misperceptions*. Junto con Brian Weeks publica el artículo disponible en http://rkellygarrett.com/wp-content/uploads/2014/05/Garrett-and-Weeks-Promise-and-peril-of-real-time-corrections.pdf (última consulta, 11/5/2018), que cuestiona la eficacia de los dispositivos y programas que advierten instantáneamente a los usuarios de informaciones falsas publicadas en la Red o datos controvertidos.

2.1 **Información y confianza en la toma de decisiones en el mercado: el componente objetivo de la confianza**

La información ha sido siempre un elemento esencial para la interacción social y el desenvolvimiento de relaciones comerciales, de intercambio y cooperación, al atenuar las asimetrías informativas, reducir los riesgos y facilitar la toma de decisiones. En particular, la información precisa y confiable ha gozado de un gran valor y ha sido altamente apreciada por los operadores económicos; especialmente la información que no se ha hecho pública y que otorgaría así, hipotéticamente, algún tipo de ventaja o privilegio frente al resto de participantes en el mercado. La disponibilidad y el fácil acceso a la información se ha convertido, de hecho, en una condición necesaria para que algunos mercados funcionen de manera eficiente, sobrevivan en condiciones de estabilidad y rentabilidad razonable o incluso existan. Más aún, junto a esta función accesoria y facilitadora, la información se ha convertido en el activo principal de modelos de negocios en imparable expansión en el «mercado de la información» (3).

En las economías modernas, los entornos negociales, veteados por el entramado de los medios de comunicación y la tecnología digital, muestran hoy un grado de complejidad apreciablemente superior en la composición y el alcance de los mercados, la condición de los intercambios y la naturaleza de los operadores. En este contexto económico, las relaciones que tienen lugar en el mercado digital han acentuado además las asimetrías, la complejidad y la incertidumbre que entorpecen las decisiones, desincentivan las transacciones, y generan riesgos. Su estructura abierta, la descentralización y el fácil acceso al mercado –dadas las casi inexistentes barreras de entrada para la provisión de contenidos– limitan extraordinariamente la capacidad de evaluar el grado de *reliability* de la información, es decir, de valorar de manera eficiente –si los costes que ello implica no superan los beneficios obtenidos de esta tarea de control y evaluación– si los contenidos, bien como activos en sí mismos o bien como referencias a criterios y condiciones de la transacción, del objeto de intercambio o de la contraparte, son dignos de confianza.

La incertidumbre agudiza la percepción del riesgo que afecta a su vez a la toma de decisiones. Todas las decisiones de contenido económico están determinadas, en gran medida, por la evaluación del riesgo. Esta valoración del riesgo está principalmente basada en la información que

(3) Sobre el relevante papel de la información en los mercados y la función de la confianza para la protección de la seguridad del tráfico, extensamente, Alba Fernández, Manuel y Rodríguez de las Heras Ballell, Teresa, «Las agencias de rating como terceros de confianza: responsabilidad civil extracontractual y protección de la seguridad del tráfico», *Revista de Derecho Bancario y Bursátil*, núm. 120, octubre-diciembre 2010, pp. 141-177.

puede adquirirse sobre los diferentes elementos de la transacción y su interpretación. La información, abundante y ampliamente disponible en los mercados modernos y, de forma abrumadora, en el mercado digital, habría de servir para la generación y el reforzamiento de la confianza, cuyo efecto es, a su vez, reducir el riesgo y así facilitar el tráfico (4). Sin embargo, en estos mercados sobreinformados hay que garantizar la accesibilidad efectiva a la información, su visibilidad y, sobre todo, su credibilidad. Y, en efecto, en el mercado digital, la confianza es hoy el activo más escaso.

Por ello, la generación y la retención de la confianza son esenciales para favorecer el funcionamiento adecuado del mercado digital, estimular las relaciones de cooperación e intercambio e incluso, en el medio plazo, asegurar su subsistencia y viabilidad (5). La confianza reduce la complejidad y permite a las personas lidiar con la incertidumbre y la complejidad del mundo actual porque reduce las alternativas y permite así centrar la atención sólo en ciertas opciones disponibles (6), facilitando la toma de decisiones. La confianza es, por tanto, un mecanismo de reducción de la incertidumbre en organizaciones complejas con circunstancias impredecibles (7). No es ciertamente la única herramienta para la contención de la incertidumbre y la gestión de la complejidad. Las normas, en todas sus manifestaciones y desde las diversas fuentes de producción y control –la ley, el mercado, las normas sociales– cumplen esta función de forma principal y altamente efectiva. Sin embargo, la confianza refuerza este papel y adquiere mayor protagonismo en contextos transaccionales o de interacción social donde la efectividad de las normas puede encontrarse debilitada. En la sociedad digital, la menor predictibilidad sobre la ley aplicable o sobre la efectividad de las decisiones en la resolución de conflictos, la incertidumbre en la identificación de las partes, o la operativa descentralizada de la Red convierten la confianza en el mecanismo más importante

(4) Frankel, Tamar, «Trusting and Non-Trusting on the Internet», *Boston University Law Review*, num. 81, 2001, pp. 457-458, en referencia a las relaciones comerciales entabladas a través de Internet.

(5) La imposibilidad de identificar y evaluar proveedores y contenidos dignos de confianza podría acarrear el «*breakdown*» del mercado digital. Los intermediarios, como defenderemos más adelante en el texto y en relación con otras funciones y medios, contribuyen a relanzar la eficiencia y operatividad del mercado digital dando valor a las transacciones electrónicas a través de cinco medios posibles: la búsqueda de información, la selección de información relevante, la gestión de los derechos de propiedad industrial e intelectual, la autenticación de la información y el procesamiento de datos. Kannan, P. K., *et alii*, «The Internet Information Market: The Emerging Role of Intermediaries», en, Michael J. Shaw *et alii* (eds.), *Handbook on Electronic Commerce*, Springer, Heidelberg, 2000, pp. 569-590, en pp. 573-578.

(6) Luhman, Niklas, «Familiarity, confidence, trust: problems and alternatives», en D. G. Gambetta (ed.), *Trust*, Basil Blackwell, New York, 1988, pp. 94-107.

(7) En la literatura sobre el concepto y la función de la confianza en el comportamiento social, en particular, Fukuyama, Francis, *Trust: the social virtues and the creation of prosperity*, The Free Press, New York, 1995; Lewis, J. David, Weigert, Andrew, «Trust as a social reality», *Social Forces*, num. 63(4), 1985, pp. 967-985; Luhman, Niklas, «Familiarity, confidence, trust:…», *op. cit.*

para reducir la complejidad de las interacciones sociales y las transacciones comerciales.

Todos los esfuerzos regulatorios, los modelos de negocios y estrategias comerciales, y los avances tecnológicos han de dirigirse a la creación y la retención de la confianza. Sorprendentemente, el incremento espectacular de información accesible que ha significado la expansión de los medios electrónicos ha invertido el proceso que hacía derivar racionalmente de una mayor información disponible decisiones más eficientes. Sólo la información accesible, visible y precisa, pero sobre todo fiable, actúa como facilitadora de los intercambios y como estímulo de las relaciones sociales de cooperación. Cuanto más confiamos en que las cosas y las personas implicadas en la transacción son como esperamos, más impulsados nos sentimos a celebrar la transacción prevista, y a exponernos a las consecuencias que de ello deriven (8). Si entendemos riesgo como la probabilidad de que las cosas tomen un curso diferente al esperado, la confianza es, por tanto, uno de los vectores de la evaluación del riesgo y en tal sentido la confianza actúa como un elemento que contribuye a estimular el comercio y, en general, las relaciones. En la medida en que la confianza, entendida como la creencia razonable de que las cosas y las personas son lo que parecen, está a su vez intensamente determinada por la información que podemos obtener por cualquier medio, la información se convierte en uno de los ingredientes catalizadores del tráfico comercial y de las relaciones de cooperación.

La información determina así el nivel de confianza. De este modo, la falta de información conducirá normalmente a una falta de confianza, que no necesariamente desconfianza y, desde el punto de una decisión racional, un incentivo a no contratar o, al menos, una tendencia a no cooperar por aversión al riesgo. Así, se presume que el prejuicio de una oportunidad perdida producirá siempre un daño menor que una confianza excesiva y erróneamente ubicada que conducirá seguramente a una decisión que ocasione pérdidas (9). De igual modo, la calidad de la información relevante determina la eficiencia y la estabilidad de las relaciones comerciales. Disponer de información completa, exacta y veraz significará normalmente ubicar correctamente la confianza o la desconfianza, y por tanto determinará un proceso de toma de decisiones eficiente. En el medio y largo plazo, la confianza bien ubicada disminuye además los costes de transacción y de verificación (10). Así mismo, la información falsa, inexacta, sesgada o parcial conducirá normalmen-

(8) Hill, Claire A.; O'Hara, Erin Ann, «A Cognitive Theory of Trust», *Washington University Law Review*, num. 84, 2006, pp. 1717-1796, en p. 1724.

(9) Hardin, Russell, «Distrust», *B. U. L. Rev.*, num. 81, 2001, pp. 495-522, en p. 496; Hill, Claire A.; O'Hara, Erin Ann, «A Cognitive Theory…», *op. cit.*, p. 1737.

(10) Frankel, Tamar, «Trusting and Non-Trusting …», *op. cit.*, p. 460.

te a una confianza o desconfianza excesiva y erróneamente ubicada, y, por tanto, a una ineficiente toma de decisiones que implica pérdida de oportunidades o frustración de expectativas, conflictos y pérdidas potenciales.

2.2 **Factores e indicios de credibilidad: el componente subjetivo de la confianza**

Si la información, veraz y relevante, alimenta el componente objetivo de la confianza, la percepción de credibilidad, marcada por factores e indicios reveladores de la confiabilidad, soporta el componente subjetivo cada vez más decisivo en la consolidación de la confianza en la sociedad digital.

La experiencia es esencialmente el vector de la confianza. Depositamos nuestra confianza en función de nuestras experiencias previas (11) en transacciones sucesivas (12). Pero, en el primer contacto, cuando el intercambio o la relación se entabla por primera vez y no disponemos de experiencias pasadas, la confianza ha de basarse en otros factores y se buscan indicios de confiabilidad. La reputación (13) es el indicio de confiabilidad principal cuando carecemos de experiencias pasadas (14). En definitiva, la reputación es, en realidad, el reflejo de las experiencias de otros.

---

(11) En este sentido, hasta el momento, la atención se ha centrado esencialmente en valorar la confianza en la Red como medida de fiabilidad del entorno, de modo que se califica la Red como una «tecnología de experiencia» («experience technology») que significa que a medida que los usuarios adquieren mayor experiencia en el espacio digital ganan mayor confianza en las transacciones y la interacción social que desarrollan en este entorno. Dutton, W. H.; Shepherd, A., *Trust in the Internet: the social dynamics of an experience technology*, Oxford Internet Institute, Oxford, 2003.

(12) Que respondería de forma amplia a lo que Luhman define como *familiarity* (familiaridad), Luhmann, Niklas, «Familiarity, confidence, trust:…», *op. cit.*, en su esquema conceptual familiaridad-credibilidad-confianza.

(13) Bajo el instrumental conceptual de Luhman que distingue entre familiaridad, basada básicamente en el conocimiento que resulta de experiencias pasadas, y confianza, que refleja las expectativas razonables sobre el comportamiento futuro, el estudio empírico de Gefe, David, «E-commerce: the role of familiarity and trust», *Omega*, num. 28, 2000, pp. 725-737 confirma la importancia de ambos factores en el comportamiento de compra de los usuarios en el comercio electrónico (librerías online).

(14) A su vez, el recurso a un intermediario está condicionado por una serie de variables directas e indirectas que determinan el grado de adopción de sus servicios. Además de la confianza (*trust*), la necesidad de experiencia o habilidad que requiere su uso (*expertise*) son los factores más determinantes. A través de un estudio econométrico, Chircu, Davis y Kauffman han confirmado que confianza y experiencia son variables relevantes para determinar el grado de intervención de los intermediarios en el marco de las transacciones electrónicas. Chircu, Alina M. *et alii*, «The Role of Trust and Expertise in the Adoption of Electronic Commerce Intermediaries», *MISRC Working Paper*, disponible en http://misrc.umn.edu/workingpapers/fullpapers/2000/0008_030100.pdf. (última consulta, 27/02/2018). De ahí se explica que los nuevos intermediarios recurran a estrategias de fidelización y trasladen sus factores reputacionales del entorno tradicional al contexto electrónico, ante la amenaza de «reintermediación» de los intermediarios tradicionales que conservan el potencial de su conocimiento especializado.

La reputación además puede venir reforzada por el papel que la ley, las normas sociales o el mercado hayan atribuido al sujeto en el que depositamos la confianza que se hace confiable por razón de su cargo o posición. En ocasiones, esta asignación de determinadas funciones de control, supervisión o prescripción se convierte, en ciertos mercados, en el motivo más determinante de la confianza. Por ello, en estos casos, en los que la reputación puede no venir respaldada siempre por experiencias sucesivas ni por una profesionalidad constatada, es esencial incorporar incentivos adecuados para que el comportamiento del sujeto a quien se atribuye esta confiabilidad adopte las medidas más adecuadas para asegurar la fiabilidad de su actuación. A tales efectos, el establecimiento de estándares para procedimentalizar la diligencia, el recurso a códigos de conducta o un sistema sólido, efectivo y predecible de responsabilidad coadyuvan en la consecución de este objetivo.

Tomando estos criterios de experiencia, reputación y «rol asignado» como vectores de la confianza, en la sociedad digital se han venido desarrollando fórmulas, estructuras y estrategias diversas y muy interesantes que tratan de generar confianza con base reputacional (intermediarios reputacionales), crear entornos confiables para el desarrollo de transacciones económicas o relaciones sociales (mercados electrónicos o redes sociales) mediante el ofrecimiento de un espacio de negociación o convivencia social sujeto a normas comunes, supervisión y control mutuo o jerárquico, o facilitar la toma de decisiones en contextos donde mayor información no proporciona mayor certeza en la decisión mediante sistemas centralizados o descentralizados de prescripción y recomendación [sistemas de recomendación (15), prescriptores]. Todas ellas representan actividades de intermediación que corresponden a lo que hemos denominado (16) el tercer estrato de la intermediación en la Red, centrado en generar, retener y reforzar la credibilidad.

2.3 **Las dimensiones de la confianza**

La confianza como catalizador de la interacción social y de las relaciones de cooperación e intercambio presenta varias dimensiones que tienen que ver con el tipo y la procedencia de la información que se incorpora en

(15) Un estudio de las implicaciones jurídicas de los denominados *recommender systems*, Rodríguez de las Heras Ballell, Teresa, «Legal Aspects of Recommender Systems in the Web 2.0: Trust, Liability and Social Networking», en Jose Pazos Arias *et alii* (eds.), *Recommender Systems for the Social Web*, Series «Intelligent Systems Reference Library» vol. 32, Springer-Verlag, New York, 2012, pp. 43-62.

(16) Rodríguez de las Heras Ballell, Teresa, «Intermediación en la Red y responsabilidad civil. Sobre la aplicación de las reglas generales de la responsabilidad a las actividades de intermediación en la Red», *Revista Española de Seguros*, núm. 142, 2010, pp. 217-259; y «La responsabilidad de los prestadores de servicios de intermediación y los estratos de la intermediación en la Red», *Revista Derecho y Tecnología*, núm. 11, 2010, pp. 69-96.

el juicio sobre el grado de confiabilidad en cada situación. Nuestra propuesta (17) es distinguir entre tres dimensiones de la confianza: «confianza sistémica», «confianza específica» y «confianza agregada».

En primer lugar, la «confianza sistémica» depende básicamente de las condiciones del mercado, es decir, del entorno transaccional o del contexto relacional (18). Por ejemplo, de la información disponible y de los esfuerzos de supervisión realizados por las autoridades competentes y, en su caso, por entidades a las que se atribuyen facultades de supervisión o prevención *(gatekeepers)* que verifican el cumplimiento de los requisitos normativos y la exactitud, veracidad y fiabilidad de la información que se suministra. La «confianza sistémica» es, de hecho, una condición *sine qua non* para contratar en un mercado específico o para interactuar en un determinado contexto social (una comunidad digital). El entorno nos aporta indicios de confiabilidad que refuerzan nuestra disposición a confiar para entablar una relación social o económica con otros participantes.

En segundo lugar, en relación con una transacción determinada, sin embargo, la evaluación del riesgo y la predisposición a entablar una relación requieren la confianza en que los elementos específicamente implicados en la transacción o en la interacción son y se comportarán como esperamos. Este tipo de confianza y su nivel adecuado dependen de la información disponible sobre los particulares elementos de la relación a los que no se refiere y que no dependen de las circunstancias del mercado y del contexto general. En ocasiones, para obtener información sobre los elementos específicos de la transacción se ha de recurrir a terceros que ponen a disposición del público la información. Las entidades o personas cuya información induce el suficiente nivel de confianza específica son entonces identificadas como terceros de confianza. El recurso a los terceros de confianza es especialmente intenso cuando el coste de recopilar, procesar y verificar la información necesaria es excesivo o simplemente inasumible (19). Mientras que la confianza sistémica puede ser condición necesaria para la decisión de contratar, esta clase de «confianza específica» normalmente será condición suficiente para tal decisión siempre que el resto de las variables de la estimación del riesgo así lo determinen también (20). Ambas dimensiones de la confianza se complementan y, en cier-

(17) Ya planteamos esta propuesta con el profesor Manuel Alba en Alba Fernández, Manuel y Rodríguez de las Heras Ballell, Teresa, «Las agencias de rating como terceros de confianza…», *op. cit.*

(18) El sistema electrónico o transaccional que gobierna la relación de intercambio o cooperación, Anderson, D. Scott, «What Trust is in These Times? Examining the Foundation of Online Trust», *Emory Law Journal*, num. 54, 2005, pp. 1441-1474, en p. 1442.

(19) Frankel, Tamar, «Trusting and Non-Trusting…», *op. cit.*, pp 465-466.

(20) Una diferente, aunque parcialmente coincidente en los términos, taxonomía de los diferentes tipos de confianza en relaciones de cooperación puede verse en Hill, Claire A., O'Hara,

ta medida, se suplen mutuamente, pues si la confianza sistémica es baja o inexistente, se exigirá mayor información sobre todos los elementos involucrados en la transacción específica para obtener indicios de confiabilidad que el entorno no proporciona. En estos casos, el ámbito y la importancia decisoria de la confianza específica crece.

En tercer lugar, lo que hemos denominado «confianza agregada» reflejaría una especie de respuesta comunitaria o de autorregulación para crear confianza sistémica cuando el mercado o el entorno social carece de herramientas formales que avalen los criterios de confiabilidad. Es una reacción del propio mercado para generar entornos confiables mediante acciones colectivas de los operadores, al margen de medidas regulatorias, con la finalidad de preservar e incrementar la calidad y fiabilidad de los servicios y la percepción que el público pueda tener de la industria en general (códigos de conducta generados y adoptados por la propia industria), de la confiabilidad de la información (fenómenos de redacción y revisión colectiva y descentralizada mediante técnicas wiki), o de los credenciales de los usuarios para interactuar (sistemas reputacionales, mecanismos de denuncia y notificación).

3. MODELOS DE GENERACIÓN DE CONFIANZA EN UNA SOCIEDAD DIGITAL

3.1 **La confianza en una sociedad omnimétrica**

La sociedad digital ha transferido a la confianza una de sus vulnerabilidades más críticas: la tiranía de la cuantificación. A medida que la revolución digital reducía drásticamente los costes de cuantificar, contar, ordenar, y clasificar, la sociedad digital ha ido quedando cada vez más expuesta a la tiranía de la cuantificación (21). Listas, rankings, ratings, números, y porcentajes parecen ofrecer hoy los instrumentos más seguros y efectivos para comprender un mundo complejo y altamente incierto. Ciertamente, la cuantificación ayuda en la toma de decisiones. Pero la obsesión por reducir toda variable, todo comportamiento humano, toda argumentación a la medida de los números ha intensificado una confianza cie-

---

Erin Ann, «A Cognitive Theory…», *op. cit.*, pp. 1740 y ss. Las autoras distinguen dos tipos de confianza interpersonal, «confianza específica» y «confianza residual» o «general», ambas de las cuales se refieren a la confianza que nos inspiran las personas. Bajo este enfoque, la «confianza específica» es la relativa a la creencia de que una persona se comportará de acuerdo con nuestras predicciones en una situación concreta, en función de la valoración realizada y la información reunida y procesada específicamente para tal situación. Por su parte, la «confianza residual» o «general» es la relativa al grado de confianza en que una persona se comportará de acuerdo con nuestras predicciones sobre la base de un juicio más general y emocional (y menos específico y consciente) sobre la fiabilidad de dicha persona (experiencias previas, ciertos prejuicios sociales, raciales, o de género, etc.).

(21) Frey, Bruno S., «Omnimetrics and Awards», *CESifo Working Paper*, núm. 6582, 2017, en p. 3.

ga en el valor de la cuantificación para ordenar el mundo, para medir la calidad, para cuantificar la fiabilidad, en definitiva, para objetivar cualquier atributo y medir, sin amenaza de subjetivismo, cualquier aspecto de la sociedad. La sociedad digital es una «sociedad omnimétrica», donde todo se debe medir y sólo lo que se puede medir importa. El dominio de la cuantificación, como triunfo del *dataísmo,* sugiere objetividad, evoca neutralidad, y facilita la decisión mediante una simple comparación de atributos según su orden y su prioridad.

La percepción de esta penetrante cuantificación del mundo en la sociedad digital es esencial para entender las nuevas coordenadas de la confianza. En una sociedad omnimétrica, la percepción de la credibilidad se asocia a criterios de popularidad, de viralidad, de relevancia. Así, la veracidad de la información queda relegada si no viene apoyada, amplificada, y reforzada por índices de popularidad y relevancia. El efecto perverso de este dominio de la cuantificación es que la popularidad ha llegado a reemplazar la veracidad. En definitiva, en nuestro concepto de confianza, el componente subjetivo de la percepción ha anulado el componente objetivo de la veracidad. Por ello, no puede combatirse de forma efectiva la falsedad de la información si no se cuenta con el efecto amplificador de la popularidad.

La prueba más visible y alarmante de esta vulnerabilidad de la sociedad omnimétrica es el preocupante fenómeno de desinformación que refleja el crecimiento incontrolado de las conocidas como «noticias falsas» *(fake news).* Un problema que ha alcanzado una relevancia extraordinaria en la escena política internacional y que ha despertado una profunda preocupación al constatar sus efectos desestabilizadores para nuestras sociedades. La gravedad de esta situación refleja, de un lado, el desplome del papel de los terceros de confianza y las referencias de autoridad, y se ve exacerbada, de otro, por un movimiento expansivo hacia los sistemas descentralizados de confianza *(peer-determined truth)*.

Es en este contexto convulso en el que han de analizarse los modelos de generación de confianza en la sociedad digital. Primero, la recuperación del valor de los intermediarios como generadores de confianza (3.2). Segundo, el desarrollo de mecanismos descentralizados de confianza y sistemas reputacionales (3.3).

3.2 **Los estratos de la intermediación digital y la generación de confianza específica**

La percepción inicial de que la Red implicaría esencialmente la desaparición de los intermediarios se ha visto progresivamente desmentida por un continuo proceso de reintermediación de la sociedad digital. Si bien la reducción de los costes de transacción, de búsqueda, de compara-

ción, de seguimiento, que la tecnología digital facilita eliminó de forma drástica el valor de la intermediación, al facilitar la interacción directa, las necesidades de la nueva sociedad digital, cada vez más sofisticada y compleja, reclamaron pronto nuevas funciones de intermediación y nuevos intermediarios. Tras una primera etapa de desintermediación, la reintermediación es una respuesta a las necesidades que el nuevo entorno va progresivamente reclamando que sean adecuadamente satisfechas (22).

Nuestra propuesta es que el intenso y extenso proceso de reintermediación responde a la emergencia progresiva de nuevas necesidades que definen las demandas de la interacción social en el espacio digital. Para entender este proceso de reintermediación, se ha formulado la tesis de los *estratos de la intermediación en la Red*. Primero, los intermediarios han venido a cubrir la necesidad básica de accesibilidad proporcionando disponibilidad y acceso efectivo a servicios y contenidos digitales. Es el primer estrato de la intermediación. Segundo, cuando la accesibilidad está garantizada, emerge una nueva necesidad, lograr la visibilidad. Estar en la Red no significa siquiera ser accesible si no hay visibilidad. En una sociedad sobreinformada, abierta y plana, el centro de gravedad de la comunicación reposa en el usuario quien busca, selecciona, interactúa y decide. Frente a los esquemas unidireccionales de los medios tradicionales de comunicación de masas, la accesibilidad depende de la visibilidad. En una sociedad digital donde la atención es el recurso más escaso, las estrategias de visibilidad son clave para captar y retener la atención. Los intermediarios digitales que promueven, facilitan y refuerzan la necesitada visibilidad conforman el segundo estrato de la intermediación. Tercero, emerge entonces la necesidad más acuciante de nuestra sociedad digital, la credibilidad. La intervención de los intermediarios como terceros de confianza representa el tercer estrato de la intermediación digital. La creciente prestación de servicios de confianza (23) junto a la transformación de la economía digital en una economía de plataformas es el reflejo de esta función primordial de los nuevos intermediarios. Pues, los operadores de las plataformas actúan como intermediarios de confianza que gestionan un entorno autorregulado, supervisado, previsible, fiable. Las plataformas son así «oasis de confianza» en una Red abierta, anónima, incierta, anárquica. Las plataformas logran conformar comunidades digitales sujetas a unas reglas de acceso, bajo unas normas comunes, con mecanismos de

(22) Una exposición muy interesante de las posibles funciones de los intermediarios en Bailey, Joseph P. & Bakos, Yannis, «An Exploratory Study of the Emerging Role of Electronic Intermediaries», *International Journal of Electronic Commerce*, vol. 1, núm. 3, 1997, pp. 7-20.

(23) Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, OJ L 257, 28.8.2014, pp. 73-114.

denuncia y supervisión, e incluso sistemas de resolución interna de conflictos. Esta previsibilidad confiere a la pertenencia, a la comunicación y a la actuación en la plataforma un nivel de confianza que la Red abierta no puede otorgar.

La intervención de los intermediarios en la sociedad digital como creadores de confianza articula fundamentalmente una estrategia centralizada que refuerza y explota factores positivos de credibilidad basados en la reputación, la experiencia y el conocimiento, la especialización, el reconocimiento legal de funciones, la profesionalidad, la responsabilidad o simplemente la capacidad de asumir el riesgo *(deep pocket).* En este sentido, operan básicamente los mismos controles reputacionales y de confiabilidad que se aplican tradicionalmente en la interacción social. Así, por ejemplo, mercados electrónicos como eBay resultarán atractivos si demuestran contar con políticas adecuadas y sistemas de supervisión efectivos; las plataformas de financiación participativa *(crowdfunding)* contarán con la fiabilidad que la propia legislación les confiere al exigirles el control y la verificación de cierta información proporcionada en la plataforma; la transparencia y el buen funcionamiento de los sistemas de denuncia en Tripadvisor serán indicios decisivos de la credibilidad de sus servicios; o, finalmente, la decisión de Facebook de contar con revisores profesionales *(fact checkers* y *trusted flaggers)* para verificar la veracidad de los contenidos y detectar noticias falsas incrementará la percepción de credibilidad.

3.3 **Estructuras descentralizadas y sistemas reputacionales**

En su etapa más reciente de evolución, la sociedad digital presenta rasgos y características propios de una segunda generación. En efecto, en los últimos años, han convergido diversos movimientos sociales, tendencias económicas y soluciones tecnológicas que han impulsado la redefinición de modelos, comportamientos, prácticas y estructuras organizativas. La descentralización ha invadido la sociedad digital en todas sus dimensiones. De un lado, con la emergencia y la apabullante expansión de las tecnologías *blockchain* o *distributed ledgers,* que anuncian una total transformación de los servicios financieros, los medios de pago, los sistemas registrales, los mecanismos de identificación, o el sector asegurador, bajo esquemas descentralizados. De otro lado, con la popularidad creciente de modelos sociales y económicos de cooperación, intercambio o interacción basados en esquemas entre iguales *(peer-to-peer),* generadores de una confianza distribuida e inspirados por la razón económica de compartir. Estas tendencias se han concretado en el floreciente sector de la economía colaborativa en sus múltiples formas, en la consolidación como modelo de financiación alternativa del *crowdfunding* (financiación parti-

cipativa), en el creciente recurso de los usuarios a sistemas de recomendación basados la opinión de otros usuarios, y en la amplia penetración de los mecanismos reputacionales, de revisión o de opinión. Estos modelos son una respuesta a un deterioro progresivo de los referentes de autoridad, a una pérdida de confianza en el control centralizado, y una inclinación generalizada a valorar como neutral y respetar como imparcial la opinión, la recomendación o la actuación del igual *(peer-determined truth, like-minded people opinion).* La concurrencia de estos factores, tecnológicos, sociales y de negocio, ha dado forma, en nuestra opinión, a una segunda generación de la sociedad digital.

En esta sociedad digital de segunda generación conviven modelos centralizados y descentralizados de generación de confianza. Los intermediarios y las plataformas pugnan por consolidar su función de terceros de confianza junto con modelos de confianza distribuida, mecanismos reputacionales o sistemas de opinión. Más aún, ambas estrategias y soluciones se entretejen y combinan hábilmente para conformar un ecosistema variado y complejo. Así, de hecho, los modelos de economía colaborativa o de *crowdfunding* operan en plataformas centralizadas gestionadas por un operador que desempeña funciones de regulación, supervisión o resolución de disputas, los mercados electrónicos incorporan sistemas reputacionales y de recomendación descentralizados, y las redes sociales y los agregadores de noticias combinan el recurso a voces autorizadas *(fact checkers, trusted flaggers)* y a sistemas de denuncia de usuarios *(report systems)* para combatir la desinformación y mejorar la percepción de credibilidad.

En la conformación de estos modelos descentralizados y de reputación se observan también los rasgos propios de una sociedad omnimétrica. El valor de la opinión se lo confiere el número, la popularidad, la relevancia en términos cuantitativos. Así funcionan esencialmente los sistemas reputacionales y de opinión. El mayor número de opiniones le da mayor credibilidad al rating concedido, el posicionamiento en la primera posición del ranking por el público se percibe como más imparcial y fiable que la opinión de un crítico, la reputación de un usuario depende de la opinión de los otros que interactúan con él frente a méritos, referencias o acreditaciones de terceros, la viralidad de una noticia (repetida, reenviada, compartida, *retuiteada)* le otorga visibilidad y mayor credibilidad frente a opiniones expertas o rectificaciones públicas que se observan con sospecha y desconfianza.

Los modelos reputacionales, de confianza distribuida, y descentralizados que describimos impactan sobre dos dimensiones de la confianza. De un lado, se presentan como un exponente claro y evidente de generadores de confianza agregada. De otro lado, sin embargo, también operan en la

dimensión de la confianza sistemática. En efecto, reemplazan o refuerzan los sistemas tradicionales de confianza sistemática, como el marco normativo o institucional. En definitiva, un sistema descentralizado trata de crear un «sistema» propio capaz de generar confianza y los mecanismos reputacionales en una plataforma sustituyen los modelos sociales de interacción y confianza y eluden la necesidad de contar con sistemas normativos, institucionales o de confianza centralizados.

4. UN MARCO NORMATIVO PARA LOS SERVICIOS DE CONFIANZA EN LA SOCIEDAD DIGITAL

4.1 **Sobre el paradigma de la responsabilidad de los intermediarios digitales**

El régimen de responsabilidad de los prestadores de servicios de intermediación constituye uno de los ejes principales del marco normativo global del comercio electrónico. La Unión Europea, inspirada en el precedente legislativo estadounidense de «puerto seguro» *(safe harbour)* –esencialmente, la *Section 512 of the Digital Millennium Copyright Act*– (24), incorpora en la Directiva de Comercio Electrónico (25) (arts. 12 a 15) las disposiciones que articulan el paradigma básico de la responsabilidad de los intermediarios electrónicos. De un lado, la prohibición de imponer a los intermediarios una obligación general de supervisar o realizar activamente búsqueda de hechos o circunstancias que puedan revelar actividades ilícitas. De otro lado, un sistema de responsabilidad subjetiva basada en el conocimiento efectivo que será el factor que active la obligación del intermediario de actuar con prontitud para retirar o impedir el acceso a los contenidos o los servicios. Bajo ambos parámetros se define la esfera de responsabilidad de los prestadores de servicios de transmisión, copia temporal (*caching*), almacenamiento de datos y, en algunas legislaciones, (26) de búsqueda y de provisión de enlaces. En definitiva, el régimen de «puerto seguro» se configura conforme a una visión instrumental, altamente técnica, y esencialmente neutral de los prestadores de servicios de intermediación.

El modelo de responsabilidad resultante de este paradigma logra así, como ha reconocido la jurisprudencia (27), un razonable equilibrio entre

(24) The *Digital Millennium Copyright Act*, 1998, 17 USC § 512 (United States of America) (en adelante, DMCA), Pub. L. No. 105-304, 112 Stat. 2860 (Oct. 28, 1998).

(25) Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior, OJ L 178, 17.7.2000, pp. 1-16.

(26) Artículo 17 de la Ley española 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico, publicada en el *BOE* de 12 de julio de 2002.

(27) TJUE 2012, 85, C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) contra Netlog NV*; TJUE 2010, 159, casos acumulados C-236/08 a C-238/08 *Google*

la libertad de información, la protección de los derechos en juego, y la libertad de empresa de los intermediarios en el desarrollo de su negocio. A pesar de la aparente solidez de este paradigma central, se perciben, sin embargo, signos de cambios que parecen someter a consideración el paradigma actual y abrir un debate sobre la conveniencia de un cambio. Primero, la transformación de la economía digital en una economía de plataformas (28) que coloca en el centro del debate a unos nuevos protagonistas, los operadores de plataformas, cuyo estatuto jurídico encaja con dificultad en el binomio tradicional prestadores de servicios e intermediarios (29). Segundo, la tendencia marcada por una reciente línea jurisprudencial en diversas jurisdicciones que parece apuntar hacia un distanciamiento progresivo del paradigma actual mediante la imposición a los intermediarios de obligaciones activas de supervisión para la prevención de actividades ilegales. A pesar de que esta línea no es consistente y contrasta con otras decisiones jurisprudenciales que reconocen y refuerzan el régimen actual de responsabilidad (30), cada vez es más visible la narrativa jurisprudencial que alerta de la alarmante amenaza que la tecnología digital (31) representa para ciertos derechos como argumento para proponer un incremento de la responsabilidad de los intermediarios como compensación (32). Tercero, la propuesta de acciones legislativas, en el marco de la estrategia de un Mercado Único Digital para Europa, en particular (33), que introducen obligaciones de supervisión, control o filtrado

---

France SARL and Google Inc. contra Louis Vuitton Malletier SA, C-236/08, *Google France SARL contra Viaticum SA and Luteciel SARL* (C-237/08) y *Google France SARL contra Centre national de recherche en relations humaines (CNRRH) SARL and Others* (C-238/08).

(28) Rodríguez de las Heras Ballell, Teresa, «The Legal Anatomy of Electronic Platforms: A Prior Study to Assess the Need of a Law of Platforms in the EU», *The Italian Law Journal*, num. 1/3, 2017, pp. 149-176.

(29) Rodríguez de las Heras Ballell, Teresa, «Rules for Electronic Platforms: the role of platforms and intermediaries in digital economy. A Case for Harmonization», *Proceedings of the UNCITRAL Congress*, *Modernizing International Trade Law to Support Innovation and Sustainable Development* to celebrate the 50th Annual Session of UNCITRAL, 4-6 julio 2017, vol. 4, United Nations, Viena, 2017, pp. 146-155.

(30) Rodríguez M. Belén c/Google y otro s/ daños y perjuicios, R.522. XLIX. (Corte Suprema, 29 octubre 2014) (Argentina); Reti Televisive Italiane S.p. A. (RTI) v. Yahoo! Italia S.r.l. (Yahoo!) *et al*, N RG 3821/2011 (Corte de Apelación de Milán, 7 enero 2015); Mediaset Premium S.p.a. v. Telecom Italia S.p.a. *et al*. (Tribunal de Milán, 27 julio 2016); TF1 v. DailyMotion (Cour d'Appel Paris, 2 diciembre 2014).

(31) Frosio, Giancarlo F., «The Death of 'No Monitoring Obligations': A Story of Untameable Monsters», *Journal of Intellectual Property, Information Technology and E-Commerce Law*, núm. 8(3), 2017, pp. 199-215.

(32) Google Brazil v Dafra, Special Appeal N.º 1306157/SP (Superior Court of Justice, 4th Panel, 24 marzo 2014), https://cyberlaw.stanford.edu/page/wilmap-brazil; Universal v Corley, 273 F.3d 429, 60 U. S. P. Q.2d 1953, 1968 (2nd Cir. 2001); TEDH *Delfi AS v. Estonia* N 64569/09 (ECHR, 16 June 2015) § 110.

(33) En Estados Unidos, sobre este asunto *Joint Supplemental Comments of American Federation of Musicians* et al *to U. S. Copyright Office, In the Matter of Section 512 Study: Notice and Request for Public Comment*, Docket N.º 2015-7 (28 febrero 2017). En la Unión Europea, Propuesta de Directiva del Parlamento Europeo y del Consejo sobre los derechos de autor en el mercado único digital, COM(2016) 593 final, 14.9.2016, Artículo 13; Propuesta de Directiva del Parlamento Europeo y del Consejo, COM(2016) 287 final, por la que se modifica la Directiva 2010/13/

de los intermediarios en algunas áreas y promueven e incentivan la adopción de mecanismos voluntarios de prevención y protección. Estos signos de cambio parecen dirigirse hacia un nuevo paradigma de mayor responsabilización de los intermediarios en la prevención de actos ilícitos y la protección de derechos (34).

La decisión de abandonar el paradigma actual requiere un debate profundo, meditado y global. Sus resultados son altamente inciertos. De un lado, en cuanto a los modelos de responsabilidad alternativos, que aún no están definidos. De otro lado, en cuanto a las consecuencias futuras de un cambio de paradigma para la sociedad digital.

El recurso al régimen de responsabilidad de los intermediarios como solución jurídica para mejorar la confianza en la sociedad digital está cargado de incertidumbres y de riesgos potenciales que deben, al menos, reconocerse, ponderarse y, en su caso, mitigarse en todo lo posible. Una mayor responsabilidad de los intermediarios puede conducir a una pérdida de neutralidad, un celo excesivo en el control y el acceso, una retirada preventiva de contenidos sospechosos para limitar la exposición al riesgo, una selección arbitraria o discriminatoria de usuarios, contenidos o actividades, y definitivamente un posicionamiento ideológico de las plataformas en el filtro y la selección de usuarios, procedencias, temáticas, opiniones. Esto derivaría, frente al objetivo último esperado de la prevención, en el fomento de una hábil estrategia de, lo que denominamos, «platform shopping».

4.2 **Una política de transparencia para los sistemas reputacionales**

Los sistemas reputacionales, tal y como los hemos descrito, se perciben como mecanismos esencialmente descentralizados. Son los usuarios los que emiten su juicio valorativo sobre otros usuarios, sus experiencias, o los productos, servicios o contenidos, y es, por tanto, la comunidad la que controla la generación de reputación y la que sanciona reputacionalmente la desviación de las normas sociales. Sin embargo, en una plataforma los sistemas reputacionales tienen una importante dimensión centralizada. Es el operador el que diseña el sistema, define los procesos, lo configura como de revisión, rating, u opinión, establece las condiciones, y sobre todo procesa, selecciona y presenta el resultado conforme a unas decisiones de estructura, permanencia, popularidad, prioridad, e incluso

---

UE, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual, a la vista de la evolución de las realidades del mercado, Artículo 6.

(34) Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *Lucha contra el contenido ilícito en línea. Hacia una mayor responsabilización de las plataformas en línea*, COM(2017) 555 final, 28.9.2017.

retribución (pago por posicionamiento). El desconocimiento de estos criterios puede generar una errónea percepción, una inadecuada valoración, y, por tanto, una respuesta inconsciente y desinformada. Por ejemplo, si las opiniones son retribuidas, si se eliminan trascurrido un periodo de tiempo, si se ordenan temporalmente y no por relevancia, si se seleccionan o se publican automáticamente, si se verifican los datos fácticos por el operador, si para emitir un rating es preciso contar con un número mínimo de calificaciones, si se ponderan conforme algún criterio, son decisiones de diseño críticas para la fiabilidad del mecanismo reputacional y esenciales para asegurar que las señales lanzadas al mercado son correctas e interpretadas correctamente.

Las opciones de política legislativa en este punto son varias. Primera, sencillamente optar por no acometer ninguna acción legislativa y dejar la configuración de los sistemas de reputación a la autonomía de la voluntad, la creatividad empresarial y la competencia en el mercado. Segundo, imponer un deber de transparencia para asegurar exclusivamente que las normas y criterios de diseño, construcción y publicación son conocidas por los usuarios para adoptar sus decisiones libremente. Tercero, recurrir al establecimiento de estándares (35) sobre las modalidades de recogida, procesamiento, agregación y publicación que aseguren la fiabilidad, la diligencia y la transparencia del sistema. Esta última opción legislativa puede, a su vez, adoptar diversos niveles de intensidad. Bien que los estándares sean recomendados o bien que sean de obligado cumplimiento y, en tal caso, estos estándares pueden establecer un modelo único o permitir el diseño de diversos modelos capaces de cumplir estos estándares generales. En nuestra opinión, la opción de estándares obligatorios que definen un modelo único es la menos deseable y adecuada. A su vez, la definición precipitada de estándares, aun voluntarios y flexibles, puede producir una consolidación demasiado temprana de las opciones en el mercado y estancar la innovación empresarial. Por ello, parece que la opción por una política general de transparencia que imponga a los intermediarios y operadores de las plataformas la obligación de desvelar la información relevante sobre el funcionamiento de los sistemas reputacionales sería la más conveniente, como etapa previa, de prospección del mercado y ponderación de alternativas, a una eventual regulación de estándares.

4.3 **Automatización y confianza: el derecho de explicación**

La creciente y expansiva automatización de procesos, tareas y decisiones en la sociedad digital incorpora otro factor perturbador en la genera-

(35) ISO/FDIS 20488: *Online consumer reviews-Principles and requirements for their collection, moderation and publication*, https://www.iso.org/standard/68193.html.

ción de confianza. Intermediarios y plataformas aplican de forma regular y sistemática algoritmos para automatizar búsquedas, procesos de selección, ordenación de rankings, cálculo de precios, valores o tiempos, toma de decisiones, acceso a determinados contenidos, determinación de la elegibilidad para ciertos servicios, fiabilidad de un mensaje, detección de infracciones, sistemas de recomendación, personalización, u opinión. Estas decisiones automáticas permiten la gestión eficiente de operaciones, contenidos, consultas, y tareas a gran escala, eliminando la intervención humana y personalizada en cada decisión.

La automatización masiva basada en algoritmos y sujeta a un creciente y cada vez más amplio autoaprendizaje plantea tres cuestiones controvertidas. Primera, la opacidad de las precondiciones conforme a las que se programa el proceso de toma de decisiones y los criterios bajo los que opera el sistema automatizado. El desconocimiento de las condiciones que determinan la selección, la concesión, la clasificación, la prioridad genera una situación de desprotección y vulnerabilidad que despierta una alarmante preocupación ante una sociedad opaca o «caja negra» *(black box society)* (36) dominada por máquinas sin control humano. Segunda, la consistencia y regularidad *(procedural regulatority)* (37) de los resultados que el sistema automatizado va determinando por efecto del autoaprendizaje y que se separa progresivamente de las condiciones previas. La complejidad operativa y de diseño de un sistema algorítmico para la ejecución de procesos automáticos puede conducir a resultados imprevisibles o inesperados. De modo que ni la adecuada determinación de las condiciones previas ni el argumento habitual de la transparencia son suficientes (38) si no se garantiza la consistencia en la operativa del proceso automatizado que confiera previsibilidad a los resultados. La transparencia puede ser inadecuada por razones de confidencialidad, insuficiente por la dependencia de factores imprevisibles, inadecuada por la complejidad de los procesos, o simplemente inútil porque deviene obsoleta inmediatamente por efecto del autoaprendizaje. Tercera, el inadecuado diseño del proceso puede favorecer que se incorporen, interpreten o procesen ciertos factores (raza, género, ideología, procedencia, idioma) que impliquen un tratamiento arbitrario o conduzcan a unos resultados discriminatorios. Ante estas situaciones se alzan voces que advierten del riesgo de una manipulación algorítmica del mercado (39) y la sociedad digital. Los modelos de

(36) Pasquale, Frank, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge-London, 2015.

(37) Kroll, Joshua A., *et alii*, «Accountable Algorithms», *University of Pennsylvania Law Review*, num. 165, 2017, pp. 634-706, en pp. 656 y ss.

(38) *Ibidem.*

(39) Calo, Ryan, «Digital Market Manipulation», *George Washington Law Review*, núm. 82, 2014, pp. 995-1051.

autoaprendizaje basados en la experiencia implican esencialmente que el programa extrae reglas de las experiencias pasadas y las aplica a las futuras (40) pudiendo replicar prejuicios implícitos, perpetuar discriminaciones existentes que el sistema interpreta como regularidades (41) o agravar los efectos de una distorsión estadística. La automatización agrava los efectos en la medida que los aplica a gran escala y los amplifica y refuerza de forma continua y sistemática sin control específico de cada resultado y sin intervención humana.

La mera transparencia del diseño, las condiciones y la lógica del proceso es una condición necesaria pero no parece suficiente para asentar la confianza en las decisiones adoptadas y los resultados obtenidos. Con base en el Reglamento General de Protección de Datos (42) (en adelante, RGPD), este derecho general a ser informado se transforma en un «derecho de explicación». Un derecho cualificado o reforzado que supera los umbrales mínimos y pasivos de la transparencia *ex ante* (general y abstracta de la lógica del proceso) para centrarse en la explicación *ex post* de la decisión específica y conforme a los parámetros y datos concretos. Este derecho de explicación que anuncia de forma más amplia el Considerando 71 RGPD, queda progresivamente sujeto a limitaciones en el articulado (en particular, pero no sólo, Artículo 22). Por ello, sin mayores precisiones y sin el refuerzo de acciones legislativas específicas, se duda (43) del impacto general que pueda tener el derecho de explicación para generar confianza en las decisiones automatizadas, mitigar el riesgo de discriminación o arbitrariedad, o aumentar la seguridad jurídica.

4.4 **Algoritmos confiables... y responsables: el derecho a intervención humana**

En una sociedad digital de imparable automatización para lidiar eficazmente con lo «grande» y lo «pequeño» en la Red, es decir, con la producción masiva de decisiones personalizadas a gran escala y de forma inmediata, nos debemos preguntar si la confianza sistémica, específica y agregada bastará para afianzar la confianza en los algoritmos que parecen, cada vez más, piezas centrales de la vida en la sociedad digital.

---

(40) Dwork, Cynthia *et al*ii, «Fairness Through Awareness», 2012 *Proceedings 3rd Innovations Theoretical Computer Science Conf*erence, 2012, pp. 214-226.

(41) Barocas Solon; Selbst, Andrew D., «Big Data's Disparate Impact», *California Law Review*, num. 104, 2016, pp. 671-732, en p. 677.

(42) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), OJ L 119, 4.5.2016, pp. 1-88.

(43) Goodman Bryce; Flaxman, Seth, «European Union regulations on algorithmic decision making and a "right to explanation"», versión de 31 de agosto de 2016. URL https://arxiv.org/abs/1606.08813.

La construcción de esta confianza algorítmica plantea los siguientes dilemas. En primer lugar, si la atribución de los efectos jurídicos y la responsabilidad de los procesos automáticos puede articularse satisfactoria y suficientemente con las reglas generales de la representación (44), de acuerdo con las reglas de la responsabilidad como situaciones propias de la esfera de riesgo, o conforme a las pautas de la responsabilidad por productos defectuosos. En qué medida podemos resolver con los esquemas actuales la acelerada tendencia hacia una mayor independencia y quizá imprevisibilidad de las decisiones y las acciones automáticas bajo sistemas de inteligencia artificial cada vez más complejos y sofisticados (45). En segundo lugar, cómo asegurar el control, la fiabilidad y la consistencia de las decisiones adoptadas automáticamente. En este sentido, a partir del RGPD pueden perfilarse algunas pautas para definir un marco de confianza, si pudieran generalizarse como parámetros de credibilidad de los algoritmos más allá de las fronteras de la protección de datos.

Con este esfuerzo de abstracción, generalización y extrapolación, comienza a perfilarse un conjunto de principios, estándares y reglas que podrían conformar el marco de la confianza para una sociedad de algoritmos y creciente automatización. Primero, asegurar la conformidad de las condiciones previas de todo proceso automático con el orden público y el marco constitucional. Segundo, incrementar la transparencia de la lógica y el diseño del proceso automático. Tercero, promover el sometimiento a auditorías externas para asegurar la regularidad y consistencia de los procesos y resultados y detectar desviaciones o reiteraciones que generen situaciones de manipulación, arbitrariedad o discriminación. Cuarto, plantear la concesión de un derecho de explicación de la evaluación, clasificación o decisión en una situación concreta a petición del afectado. Quinto, valorar la posibilidad de que el afectado por una decisión automática pueda objetar el resultado y solicitar intervención humana conforme a las reglas, requisitos o condiciones aplicables en cada caso. El recurso final a la intervención humana como cláusula de cierre del sistema abre, sin embargo, otros interrogantes. De un lado, si este derecho se puede ejercitar en cualquier momento y de forma sistemática, lo que haría la automatización prácticamente inútil e inefectiva, generaría los costes que pretendían evitarse con el proceso automático, y podría paralizar, de ser masiva, la actividad automatizada. De otro lado, la confianza en la intervención humana como garantía de imparcialidad, corrección y equidad sólo se verifi-

(44) Scholz, Lauren Henry, «Algorithmic Contracts», *Stanford Technology Law Review*, num. 20, 2017, pp. 101-139.

(45) Parlamento Europeo, *European Civil Law Rules in Robotics*, *Study for the JURI Committee*, PE 571.379, 2016.

ca si las condiciones y requisitos son claros, conocidos previamente, y de aplicación directa. En definitiva, la cuestión que se plantea es si la intervención humana se requiere para que modifique la decisión automática, que habría que probar como errónea, o simplemente para que informe, explique y supla el proceso de decisión del algoritmo con los mismos criterios, la misma ponderación y el mismo resultado.

CAPÍTULO 25

GOBERNANZA DE INTERNET Y DERECHOS DIGITALES

Zoraida Frías
Profesora ayudante de la ETSI Telecomunicación
de la Universidad Politécnica de Madrid
Directora de la Oficina Técnica del Foro de Gobernanza de Internet
en España (IGF Spain) y miembro de su grupo asesor

Jorge Pérez
Catedrático de la ETSI Telecomunicación de la Universidad Politécnica de Madrid
Director del Observatorio Nacional de Telecomunicaciones (ONTSI)
Coordinador del Foro de Gobernanza de Internet en España (IGF Spain)

Christoph Steck
Director de Public Policy e Internet de Telefónica
Miembro del MAG (Grupo Asesor Multistakeholder) del Foro de Gobernanza (IGF)
Copresidente de OMAC (Comité de Miembros Organizativos) de Internet Society
Vicepresidente del Comité de Economía Digital de BIAC (OCDE)

RESUMEN

La irrupción de Internet ha dado lugar a una red de naturaleza global que ha generado nuevas estructuras para su gobernanza. A pesar de que Internet sea percibida con frecuencia como un recurso público mundial, su modelo de gestión ha estado siempre alejado de las tradicionales fórmulas multilaterales. A diferencia de las telecomunicaciones, el modelo de gobernanza de Internet responde a unos principios de soberanía compartida que permiten la participación de, además de los gobiernos, la comunidad técnica, la sociedad civil, la academia y el sector privado. La gobernanza de Internet ha desarrollado caminos diferentes en el plano técnico y en el social, en el que se incluyen los derechos digitales. Este capítulo analiza la gestación del ecosistema de gobernanza de Internet en sus dimensiones técnica y social, así como su evolución hacia estructuras globales

que mantienen una red única pero que generan conflictos de derechos por su naturaleza transnacional.

Palabras clave: gobernanza de Internet, modelo *multistakeholder,* globalización, Internet, derechos digitales.

1. INTRODUCCIÓN

Internet, como máximo exponente de los avances en la globalización económica y política, ha desarrollado un modelo de gobierno particular. Este modelo ha resultado capaz de lidiar con los conflictos que inevitablemente surgen ante un proceso disruptivo y de mantener a su vez una estructura técnica compleja funcionando adecuadamente en todo el mundo.

A pesar de que Internet sea a menudo percibida como un bien público mundial, sus recursos críticos están en manos de organizaciones internacionales en un modelo en el que el sector privado ha adquirido un papel clave como impulsor de la innovación y como agente creador de valor en la Red. Estas organizaciones mantienen una serie de procesos abiertos a la partición pública, basados en la transparencia y en el consenso generalizado entre distintos grupos de interés.

Este modelo organizativo, denominado *multistakeholder*, se define como una forma de gobernanza y de toma de decisiones basada en la cooperación entre distintos grupos de interés para encontrar soluciones a sus problemas u objetivos comunes (Peake, 2017). Estos grupos de interés son habitualmente el sector privado, la sociedad civil, los gobiernos, la academia y la comunidad técnica. El modelo *multistakeholder* o de múltiples partes interesadas ha resultado muy exitoso para la gestión de los recursos críticos de Internet, y está experimentando importantes avances en la gobernanza de las cuestiones más sociales, incluyendo la garantía de los derechos digitales.

La forma en la que ha evolucionado la gobernanza de los recursos críticos de Internet contrasta con el modelo de gobierno tradicional de las infraestructuras de telecomunicación que la soportan. Estas diferencias encuentran su causa en el distinto contexto histórico en el que se han desarrollado uno y otro sector. Durante la segunda mitad del siglo XIX y el comienzo del siglo XX, la telegrafía, primero y la telefonía, después, experimentaron un rápido proceso de expansión entre la población. Ante la utilidad e interés de las nuevas formas de comunicación, los Estados intentaron poner los medios necesarios para garantizar el despliegue de infraestructuras y para mantener un servicio adecuado. El desarrollo de redes y servicios tuvo una fuerte componente estatal y los servicios de telecomunicación pasaron a ser de esa titularidad (Pérez, 2008). La interconexión de las distintas redes telefónicas que se proyectaban dentro de las fronteras nacionales era gestionada por los propios Estados, que promovieron la creación de organismos multilaterales que hicieran más sencillos los acuerdos (Pérez, 2008). Así nació en 1865 la Unión Telegráfica Internacional, que cambió su nombre a Unión Internacional de Telecomunicaciones (UIT) en 1934.

Internet, por el contrario, surge en un contexto radicalmente diferente. El desarrollo de los supercomputadores durante la década de los sesenta que sucedió a la invención del transistor en 1947, había creado máquinas con una capacidad de cálculo desconocida hasta la fecha (Severance, 2015). Sin embargo, las redes telefónicas del momento, diseñadas para las comunicaciones de voz, no eran adecuadas para la transmisión de datos y la conexión remota a las nuevas instalaciones de cómputo. El desarrollo de nuevos protocolos de comunicación que facilitaban las conexiones entre máquinas de cualquier fabricante hizo posible la gestación de lo que luego se convertiría en la red de redes. Esta naturaleza abierta de Internet ha constituido su principal clave de éxito, facilitando la innovación y transformando la red científica que se desarrolla en Estados Unidos en la década de 1980, la *National Science Foundation Net*, en la red mundial que hoy conocemos como Internet.

En el ecosistema de gobernanza de Internet pueden distinguirse dos planos bien diferenciados: la gobernanza técnica y lo que podemos denominar gobernanza social. La Figura 1 ilustra cómo se articulan los distintos grupos de interés en torno a uno y otro plano. Como puede apreciarse, mientras la gobernanza técnica tiene una estructura muy definida que gira alrededor de las llamadas funciones IANA (1) y en la que las organizaciones participan en un área específica (nombres, números, estándares o infraestructura), la gobernanza social está formada por un compendio de instituciones que participan en el ecosistema en el ámbito de sus competencias o soberanía.

(1) Las funciones IANA son la gestión de las direcciones IP, los nombres de dominio y los parámetros de los protocolos que mantienen una red única en todo el mundo.

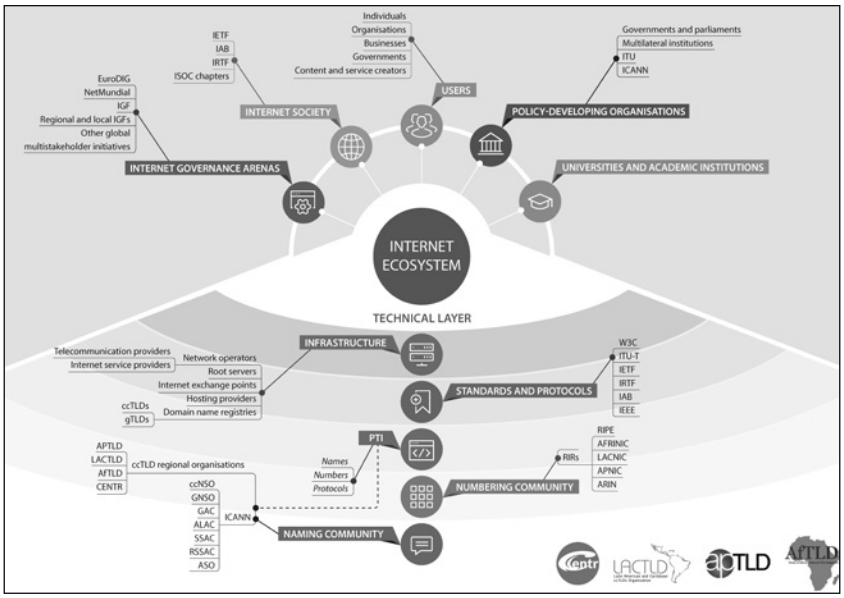


Figura 1. Ecosistema de gobernanza de Internet. Fuente: CENTR

Este capítulo analiza la gestación y evolución del ecosistema de gobernanza de Internet, tanto en su dimensión técnica como social, así como las implicaciones para la garantía de los derechos digitales. La sección 2 se centra en el desarrollo de la gobernanza de Internet más allá de los recursos críticos y describe la creación del Foro de Gobernanza de Internet. Las secciones 3 y 4 analizan el proceso de globalización del ecosistema de gobernanza en los planos técnico y social, respectivamente. Finalmente, la sección 5 señala algunas conclusiones del estudio comparativo del desarrollo de ambas partes del ecosistema y apunta a los desafíos que suponen para la garantía de los derechos de los ciudadanos en el ciberespacio común que constituye Internet.

2. DE LA GOBERNANZA TÉCNICA A LA GOBERNANZA SOCIAL

A pesar de la naturaleza abierta y descentralizada de Internet, es necesaria una gestión centralizada y coordinada de sus recursos críticos para mantener una red única a nivel global. Esta gestión atañe a las direcciones IP, que identifican de manera única a cada máquina conectada a la Red, a los nombres de dominio (las direcciones web) y a los parámetros de los protocolos que permiten las comunicaciones. Estos tres recursos son conocidos como las funciones IANA.

Estos recursos críticos han estado desde hace tiempo gestionados por ICANN, una entidad privada sin ánimo de lucro, bajo la supervisión del Gobierno de Estados Unidos, quien se reservó un estatus privilegiado tras la privatización de la NSFNet y la creación de esta organización. Otros gobiernos han intentado contrarrestar el poder de Estados Unidos en la Red, especialmente a medida que Internet se ha convertido en un elemento central en la vida de los ciudadanos. Los esfuerzos de estos gobiernos se han canalizado a través de Naciones Unidas desde principios de la década de los 2000, en particular a través de la UIT, que venía realizando las labores de estandarización y coordinación en los sistemas de telecomunicaciones, y de su Consejo Económico y Social (ECOSOC).

La creación de un Foro Anual de Gobernanza de Internet para el debate de estas cuestiones fue entendida como una solución de compromiso y, si bien con una función exclusivamente asesora, ha resultado una fórmula exitosa en la tarea de avanzar en los conflictos que inevitablemente surgen debido a la naturaleza extraterritorial de Internet. Las siguientes secciones analizan la gestación del ecosistema técnico y social de gobernanza de Internet.

2.1 **La creación de ICANN**

En los albores de Internet, la labor de coordinar el uso de las direcciones IP era realizada por un estudiante de la Universidad de California, Jon Postel, que registraba y anotaba manualmente cada nueva máquina que se conectaba a la Red. A medida que Internet fue adquiriendo mayores dimensiones, especialmente tras el éxito de la *World Wide Web*, se hizo imprescindible la creación de sistemas de gestión más escalables y globales. En 1998, se constituyó la Internet Corporation for Assigned Names and Numbers (ICANN), una entidad privada sin ánimo de lucro, que aún en la actualidad continúa realizando las tareas de coordinación de la asignación y adjudicación de identificadores que deben ser únicos, como las direcciones IP y los nombres de dominio.

ICANN ha sido la organización que ha abanderado el modelo *multistakeholder* que gobierna la toma de decisiones de estos identificadores únicos que mantienen una Internet única, abierta y segura. Aunque el modelo *mutistakeholder* no está exento de debilidades, como pueden ser las barreras económicas para ciertos grupos de interés o la legitimidad de algunos procesos, ICANN ha conseguido desarrollar una organización adaptada a los retos del siglo XXI, en el que el mundo es cada vez más global y más heterogéneo al mismo tiempo.

ICANN se constituye en 1998 a imagen y semejanza de otras organizaciones primigenias de Internet relacionadas con su desarrollo técnico, como el Internet Engineering Task Force (IETF), una comunidad cuya misión principal consiste en el desarrollo de estándares técnicos que me-

joren la arquitectura de Internet y su funcionamiento. Estas organizaciones se caracterizan por una estructura ágil, en la que el consenso aproximado (*rough consensus*) constituye la principal forma de toma de decisiones, sino la única. En concreto, el IETF es muy conocido por su modo de funcionamiento para crear especificaciones técnicas, a través de peticiones de comentarios o Requests for Comments (RFCs). Cualquier persona interesada en cambiar un estándar de Internet podía (y puede) publicar su propuesta y lanzar una RFC para recibir comentarios del resto de la comunidad. Los mecanismos de aprobación de una RFC nunca se han reglado, sino que las decisiones de incorporar cambios al estándar se basaban en el consenso aproximado de todos los participantes.

Desde sus inicios, ICANN fue plenamente consciente de que su misión fundamental era eminentemente técnica, pero que su papel trascendía estas cuestiones y tenía implicaciones en otras áreas, como las políticas de Internet o la competencia en el mercado de nombres de dominio. Por ello, además de un funcionamiento basado en el consenso aproximado, ICANN adoptó una estructura organizativa en torno a los distintos grupos de interés que conviven en Internet, que son tratados en pie de igualdad.

ICANN se organiza en torno a diferentes Organizaciones de Apoyo (SO, Supporting Organizations), cuya misión es elaborar políticas que la Junta Directiva (el Board) tiene la potestad última de adoptar, aconsejada por los Comités Asesores (AC, Advisory Committees). Para que este modelo multistakeholder funcione eficazmente, ICANN necesita alentar la participación, infundir confianza, facilitar el acceso a la información y contar con sólidos mecanismos de análisis y disputa (Olmos, 2015).

A diferencia del modelo que históricamente ha gobernado el sector de las telecomunicaciones, en la gestión de la infraestructura de Internet los gobiernos participan como un grupo de interés más dentro de la comunidad. El Comité Asesor Gubernamental (GAC) está compuesto por representantes designados por los gobiernos y las organizaciones gubernamentales. El GAC desempeña una labor muy importante asesorando a la Junta Directiva en cuestiones en las que se intersectan las actividades y políticas de ICANN y las leyes nacionales o los tratados internacionales. Los miembros del GAC eligen a un miembro sin derecho a voto de la Junta Directiva de ICANN, que representa sus intereses y actúa como coordinador.

2.2 **La creación del Foro de Gobernanza de Internet (IGF)**

Desde principios del siglo XXI, cuando Internet alcanza ya una amplia adopción y comienza a convertirse en un elemento relevante para la actividad diaria de muchos ciudadanos y organizaciones, los gobiernos comenzaron a adquirir mayor consciencia sobre su importancia. El primer esfuerzo de los gobiernos de todo el mundo por aumentar su control sobre

Internet quedó retratado en la celebración de la Cumbre Mundial de la Sociedad de la Información (*WSIS*, *World Summit on the Information Society*), auspiciada por Naciones Unidas en dos fases, en 2003 y 2005, celebradas respectivamente en Ginebra y Túnez. La WSIS supuso un primer un impulso para los interrogantes que surgían en torno a la gobernanza de una red cada vez más global, tanto en cuestiones técnicas como socioeconómicas, en las que los derechos de los ciudadanos en el nuevo ciberespacio común comienzan a ocupar un lugar destacado.

Durante la primera fase, surgieron dos visiones claramente enfrentadas acerca del modelo idóneo para la gobernanza de la infraestructura técnica: los partidarios de mantener ICANN como la organización responsable de los recursos críticos, como había venido ocurriendo desde su creación en 1998, y los que preferían una trasferencia progresiva de estas competencias hacia un organismo de la ONU, como la UIT. Además, en este encuentro comienzan a trascender los debates de tipo más social que cuestionaban el papel de la regulación y las políticas públicas relativas a Internet y su influencia en el desarrollo de la Sociedad de la Información.

Dos años después, en la segunda fase, comenzó a vislumbrarse cierto consenso sobre el papel relevante que deberían tener todos los gobiernos para garantizar la estabilidad y seguridad de una red global única y la protección de los derechos de sus ciudadanos. La WSIS culminó con el acuerdo de celebrar todos los años, al amparo de Naciones Unidas, un foro de gobernanza de Internet (IGF, por sus siglas en inglés, *Internet Governance Forum*) que reuniera a los distintos grupos de interés y que sirviera como espacio abierto y descentralizado para el debate sobre políticas que favorecieran la sostenibilidad y solidez de Internet.

La llamada Agenda de Túnez define la Gobernanza de Internet como «el desarrollo y la aplicación por los gobiernos, el sector privado y la sociedad civil, en las funciones que les competen respectivamente, de principios, normas, reglas, procedimientos de adopción de decisiones y programas comunes que configuran la evolución y utilización de Internet.» (World Summit on the Information Society, 2005)

La creación del Foro de Gobernanza de Internet fue un resultado muy exitoso de la Cumbre Mundial de la Sociedad de la Información, y ha sido considerado una solución de compromiso entre las dos visiones enfrentadas que existían inicialmente. El mandato inicial encomendado a la ONU fue de 10 años, que se renovó en 2015 durante otros diez años (United Nations, 2015).

La agenda para el primer IGF celebrado en Atenas (IGF Secretariat, 2006) se elaboró en torno a cuatro áreas temáticas que englobaban de alguna manera una «visión amplia» de la gobernanza de Internet: el acce-

so, la seguridad, la apertura y la diversidad. Superadas las principales barreras técnicas, los debates fueron evolucionando para incluir cuestiones concernientes a unos nuevos «derechos digitales» como la reducción de la brecha digital, la inclusión en Internet, o a derechos reconocidos que debían ser especialmente protegidos con las nuevas tecnologías, como la protección de los menores, la propiedad intelectual, la privacidad, etc. Así, el debate fue extendiéndose más allá de los recursos críticos de Internet a otras cuestiones de interés general en las que el modelo *multistakeholder* podría satisfacer la voluntad de todas las partes de participar en la toma de decisiones.

Estas cinco áreas temáticas han ayudado a estructurar históricamente el programa del IGF, aunque han ido sufriendo algunas variaciones cada año (2), ya que los temas particulares de las sesiones son elegidos por la comunidad *multistakeholder*, que participa en el proceso de decisión.

3. LA GLOBALIZACIÓN DE LA GOBERNANZA TÉCNICA: LA TRANSICIÓN DE LAS FUNCIONES DE IANA

La gestión centralizada de los identificadores únicos de Internet (las funciones IANA), en manos de ICANN, es lo que ha conseguido que, a pesar de la expansión geográfica, haya podido mantenerse una red global y única. Como se mencionó anteriormente, Estados Unidos ha tenido históricamente un papel protagonista en la gestión de sus recursos críticos, reservándose una función supervisora a través de un contrato entre ICANN y el Departamento de Comercio (DoC), que se ha ido renovando con el tiempo.

A pesar de que la función del Gobierno de Estados Unidos ha sido puramente supervisora y nunca ha emprendido acciones sobre el control de los recursos críticos de Internet, el vestigial poder de supervisión del Gobierno de Estados Unidos resultaba incómodo para una comunidad cada vez más internacional. A medida que evolucionaba el propio ecosistema de gobernanza de Internet, aumentaron las voces que reclamaban el fin de la relación contractual existente entre ICANN y el Gobierno de Estados Unidos, aunque no estuviera teniendo consecuencias en la práctica. De alguna forma, el simbolismo de que un único gobierno controlara uno de los pocos puntos críticos de Internet encubría el hecho de que el sistema funcionara bien (Olmos, 2015).

(2) Las grandes áreas de debate del IGF de 2017 en Ginebra (el último celebrado en el momento en el que se escriben estas líneas) fueron: i) acceso, inclusión y diversidad; ii) recursos críticos de Internet; iii) ciberseguridad; iv) economía digital, trabajo digital, comercio y desarrollo sostenible, v) género y juventud, vi) derechos humanos en la red; vii) cooperación y gobernanza y vii) nuevas tecnologías y temas emergentes (IoT, Blockchain, VR, Big data, Fakenews).

No obstante, la cuestión de cómo crear una verdadera estructura internacional que pudiera eliminar el histórico papel supervisor del Gobierno de Estados Unidos ha protagonizado acalorados debates durante mucho tiempo. La idea de sustituir al Gobierno de Estados Unidos por una estructura multilateral en el marco de las Naciones Unidas, es decir, la sustitución de un gobierno por muchos gobiernos, ha creado también fuertes rechazos entre la comunidad.

Si bien el gobierno de Estados Unidos siempre tuvo claro que su papel supervisor de las funciones IANA sería temporal, las revelaciones del exagente de la CIA, Edward Snowden, sin duda aceleraron el proceso de transición. En 2014, el Gobierno de Estados Unidos anunció su intención de renunciar a la custodia de las funciones de IANA, siempre y cuando se encontrara un mecanismo que sirviera de reemplazo (NTIA, 2014) y que: i) apoyara el modelo multistakeholder, ii) mantuviera la seguridad, estabilidad y resiliencia del sistema de nombres de dominio, satisficiera las necesidades y expectativas de los clientes y socios de los servicios de IANA, y iii) mantuviera la naturaleza abierta de Internet.

Tras el anuncio, ICANN inició dos procesos que, si bien independientes, han estado fuertemente relacionados (Olmos, 2015). El primero es la búsqueda de un mecanismo que sirviera de reemplazo a la supervisión del Gobierno de Estados Unidos. El segundo, una mejora de la rendición de cuentas de ICANN, que, sin duda, sería importante a su vez para el éxito de la transición de la custodia de las funciones de IANA.

El último contrato entre ICANN y el DoC que reguló la gestión de las funciones de IANA fue firmado en 2012 y expiraba el 30 de septiembre de 2015, aunque la dilación del proceso de transición requirió que fuera ampliado durante un año más. El 8 de abril de 2014, ICANN lanzó el proceso multistakeholder para desarrollar una propuesta que presentar a la NTIA en tiempo y forma. La solución adoptada ha consistido en la creación de una nueva entidad legal filial de ICANN, la *Public Technical Identifiers* (PTI), que tiene como objetivo gestionar las funciones de IANA.

En el desarrollo de la propuesta de transición de la custodia de las funciones IANA, la comunidad global *multistakeholder* consideró específicamente una potencial captura de los procesos de ICANN por uno o varios de los grupos de interés, incluidos los gobiernos. Los nuevos mecanismos de toma de decisiones evitan que un grupo de interés particular pueda influir de manera deshonesta sobre ICANN. Tal y como ocurría antes de la transición, los gobiernos continúan su labor como asesores de la Junta Directiva a través del Comité Asesor Gubernamental (GAC) en el curso habitual de las actividades de ICANN, que puede ser rechazado por la Junta Directiva.

La creación de la PTI ha supuesto el fin a la relación contractual entre el gobierno de Estados Unidos y ICANN, dando lugar a un entidad plenamente independiente y global para la gobernanza técnica de Internet.

4. LA GLOBALIZACIÓN DE LA GOBERNANZA SOCIAL: WCIT Y NETMUNDIAL

En el plano social, el éxito del IGF sirvió durante algún tiempo para canalizar el debate sobre los derechos digitales y la confrontación de los mismos que causa la naturaleza extraterritorial de Internet. Sin embargo, a partir de 2012, varios acontecimientos pondrían de manifiesto que, aunque el IGF podía ser considerado una buena plataforma de debate, carecía de capacidad para generar resultados tangibles. En este momento surgieron varios intentos de discutido éxito para cubrir esta carencia, en particular la Conferencia Mundial de Telecomunicaciones Internacionales (*WCIT, World Conference on International Telecommunications*) y Netmundial.

La WCIT se celebró en diciembre de 2012 en Dubái, bajo el auspicio de Naciones Unidas. En ella se daban cita gobiernos de todos los países para debatir una revisión del Reglamento de Telecomunicaciones Internacionales (*ITR, International Telecommunications Regulation*), que, datando de 1988 y con carácter de tratado internacional, regula la explotación de servicios internacionales de telecomunicaciones. Hasta la fecha, el tráfico Internet había quedado fuera de este tratado, que se aplicaba exclusivamente a la telefonía. A pesar de que la UIT había insistido en que la gobernanza de Internet no era el principal objetivo de la WCIT, fue en torno a ésta donde se centró la mayor parte del debate. La petición explícita de países como Rusia o China de ampliar la jurisdicción del ITR al tráfico de Internet generó una gran fractura con la mayoría de los países de Occidente, que consideraban que tales propuestas vulneraban claramente los derechos de sus ciudadanos. Además, existían notables diferencias en las visiones respecto a la ciberseguridad y a la protección de las infraestructuras críticas nacionales. Esto provocó que, a diferencia del amplio consenso conseguido en 1988, donde el RTI fue aprobado por los 178 países asistentes, el nuevo reglamento fuera firmado solamente por 89. El resto consideró que traspasaba las líneas rojas que permitirían seguir manteniendo una Internet abierta. A pesar de que las Actas Finales de la Conferencia estaban lejos de las pretensiones de China o Rusia, el resultado es que desde 2015 están coexistiendo dos tratados internacionales.

Por otro lado, las revelaciones del ex agente de la CIA Edward Snowden sobre los programas de espionaje del Gobierno de Estados Unidos en junio de 2013 sirvieron para impulsar de manera definitiva un proceso que

ya estaban siendo reclamado por una comunidad internacional *mulstistakeholder* cada vez más madura, y que consideraba que estas prácticas habían transgredido los límites razonables del equilibrio entre la privacidad y la seguridad.

Las revelaciones relacionadas con la NSA tuvieron un efecto especialmente intenso en el plano político internacional, al conocerse que afectaban también a importantes líderes como las presidentes de Brasil y Alemania, países que instaron a la elaboración de un marco común básico sobre Internet que recogiera los principios fundamentales que todas las instituciones y organizaciones el ecosistema Internet deberían seguir y aplicar en el ejercicio de sus funciones. Además, el gobierno de Brasil aceleró por la vía constitucional de urgencia la aprobación del Marco Civil de Internet –un conjunto de principios reguladores básicos en torno a la neutralidad de red y los derechos de los ciudadanos brasileños en el uso de Internet–, que se encontraba en tramitación.

Adicionalmente, durante la 68.ª Asamblea General, la presidente de Brasil, Dilma Roussef, instó a Naciones Unidas a que comenzara a regular el papel de los gobiernos en torno a la gobernanza de Internet. El 9 de octubre y tras una reunión celebrada entre la propia Roussef y Fadi Chehadé, entonces CEO de ICANN (3), el gobierno de Brasil anunciaba la convocatoria de una Cumbre Global Multistakeholder sobre gobernanza de Internet (llamada NETmundial) para el primer semestre de 2014. Esta cumbre tenía como objetivo la toma de decisiones sobre los temas más candentes y una coalición *multistakeholder* sirvió como soporte para garantizar que se celebrara en un formato inclusivo en el que todas las partes interesadas se trataran en pie de igualdad.

NETmundial significó el esfuerzo de Brasil por adecuar sus preocupaciones fundamentales como Estado acerca de Internet a los contenidos y el formato típico del modelo de cooperación *multistakeholder*. La Cumbre reclamó, además, el papel de todos los Estados sobre los recursos críticos, y elaboró una «Declaración Multisectorial de Sao Paulo», que recogía tanto una serie de principios fundamentales en Internet, como una hoja de ruta para el futuro de su gobernanza.

A pesar del carácter no vinculante del documento y la poca concreción de la hoja de ruta elaborada, NETmundial fue valorada de forma positiva. Se ha reconocido ampliamente el esfuerzo de la comunidad internacional *multistakeholder* por alcanzar resultados tangibles en torno en los aspectos socioeconómicos de Internet, cuestión que no estaba en la misión del IGF.

(3) La comunidad técnica había mostrado también públicamente su malestar y disconformidad en relación con las prácticas de vigilancia masiva en la que se denominó Declaración de Montevideo.

Los principios de gobernanza de Internet recogidos en la Declaración Multisectorial de SaoPaulo de Netmundial parten de la necesidad de equiparar el reconocimiento de los derechos *online* y *offline*, de acuerdo a las obligaciones legales existentes en materia de derechos humanos, incluyendo el Pacto Internacional de Derechos Económicos, Sociales y Culturales (ICESCR, *International Convenant on Economic, Social and Cultural Rights*) y la Convención Internacional sobre los Derechos de las Personas con Discapacidad (CRPD, *Convention on the Rights of Persons with Disabilities*). Los principios incluyeron: i) los derechos humanos (libertad de expresión, libertad de asociación, derecho a la privacidad, accesibilidad, derecho a la información y derecho al desarrollo), ii) la necesidad de implementar las limitaciones a la responsabilidad de los intermediarios en armonía con el crecimiento económico, la innovación y la libre circulación de información, iii) la promoción de la diversidad cultural y lingüística, iv) la protección de una Internet única, v) la protección de la seguridad, estabilidad y resiliencia de Internet y de su arquitectura abierta y distribuida, y vi) la facilidad para la innovación y la creatividad.

Netmundial despertó mucha expectación y muchos percibieron que podría generar una Carta Magna de Internet, inspirada en el Marco Civil. Por otro lado, a pesar del carácter *multistakeholder*, implementado a través de diversos Comités (4), la organización de NETmundial sufrió varias críticas en relación con su falta de transparencia en cuanto a la concesión de participación presencial, al procesado de las contribuciones aportadas y a la redacción del documento final, que se hizo a puerta cerrada. De una u otra forma, Netmundial sentó el primer precedente en la redacción de un documento global que constituyera una suerte de carta universal de derechos digitales y algunos vieron en él un documento análogo a la Declaración Universal de Derechos Humanos, que, sin ser vinculante sentó un precedente para la inclusión de una serie de derechos en los marcos legales nacionales.

5. DESAFÍOS PARA LA GOBERNANZA SOCIAL DE INTERNET Y LA PROTECCIÓN DE LOS DERECHOS DIGITALES

Internet, concebida como una red que permitía la interconexión de máquinas con distinto hardware y software, ha generado un ecosistema

(4) La cumbre se articuló en torno a cuatro comités: i) el Comité Multisectorial de Alto Nivel, presidido por el ministro de comunicaciones de Brasil y encargado de supervisar la estrategia general de la reunión y promover la participación de la comunidad internacional, ii) el Comité Multisectorial Ejecutivo, responsable de la agenda y el formato de la reunión, iii) el Comité de Logística y Organización, y iv) el Comité Asesor Gubernamental, abierto a todos los representantes gubernamentales interesados.

que ha experimentado un rápido crecimiento, en el plano técnico y en el social.

A pesar de las no pocas complicaciones que han surgido a medida que Internet se ha ido expandido geográficamente y se ha convertido en uno de los ejes fundamentales para la vida de los ciudadanos y la actividad de las empresas, el modelo de gobernanza técnica ha conseguido mantener una red global, abierta y segura.

Esto ha supuesto una importante disrupción en un sistema de organización política en torno al concepto de soberanía nacional. Este sistema, establecido hace casi 400 años y ha definido la forma de operar en otros sectores transnacionales y con una fuerte componente tecnológica, como el de las telecomunicaciones. Sin embargo, el ecosistema Internet ha desarrollado nuevas estructuras organizativas para la gestión de unos recursos que son, por definición, globales. La reciente creación de una nueva entidad, la PTI, para la gestión de las funciones de IANA al margen de cualquier gobierno, incluyendo al de Estados Unidos, supone un gran éxito en la creación de organizaciones globales capaces de lidiar de manera efectiva con la naturaleza extraterritorial de Internet.

Sin embargo, la gobernanza socioeconómica de Internet, que afecta principalmente a los derechos digitales de los ciudadanos, se encuentra actualmente mucho más fragmentada y lejos de encontrar una solución que permita abordar los desafíos de la acelerada globalización que propicia Internet. Hasta la fecha, los mecanismos de gobernanza no han encontrado una fórmula para la armonización legal o la salvaguarda de los derechos de los ciudadanos *online*, si bien las funciones asesoras están sólidamente constituidas a través de organizaciones como el Foro de Gobernanza de Internet. De hecho, es notable el aumento de iniciativas IGF nacionales y regionales (conocidas como NRIs, *National and Regional Initiatives*) que actúan como catalizadoras de los debates en sus respectivas comunidades, replicando el modelo *bottom-up* y *multistakholder* de la iniciativa global.

En la actualidad, el IGF se debate en la necesidad de producir resultados más tangibles que permitan avanzar en la protección de los derechos digitales en Internet, para lo que se han creado grupos específicos como el Grupo de Trabajo para el Programa de Trabajo Multianual Estratégico del IGF (IGF Secretariat, 2017). Las propuestas iniciales van en la dirección de generar recomendaciones en forma de documentos consensuados y validados tras un proceso similar a una votación. Las recomendaciones adquirirían el rango de propuestas consensuadas por la comunidad *multistakeholder* del IGF para su posterior utilización como referencia para gobiernos, empresas, etc.

Este cambio de orientación del IGF no deja de estar exento de inconvenientes, en la medida en que supondría un cambio drástico para sus dinámicas actuales: el IGF es un foro en el que se debate de manera abierta, inclusiva, en igualdad de condiciones y transparente la gobernanza socioeconómica de Internet, y su efecto en personas, gobiernos y empresas, permitiendo conocer un amplio abanico de perspectivas. El cambio de orientación podría convertir las sesiones en arduos procesos de negociación de los textos a aprobar, perdiéndose la frescura, transparencia y autenticidad de los debates. La capacidad de identificación de problemas en el ámbito de la gobernanza socioeconómica es precisamente el gran activo del IGF. Una labor de promoción más activa y eficiente de los aspectos destacados de las sesiones relevantes del IGF podría ser por sí mismo un resultado tangible que podrían aprovechar otros procesos de gobernanza de Internet, continuando así con la labor iniciada en el IGF.

Netmundial, a pesar de su reconocido éxito, no ha conseguido consolidar una estructura *mulstitakeholder* global para proteger los derechos de los ciudadanos en la Red, y más allá de esta Cumbre, los avances posteriores han sido escasos. Existen, no obstante, algunas iniciativas en marcha, que dan cuenta de la necesidad latente de seguir progresando en esa dirección. Entre ellas se encuentra la *Internet & Jurisdiction Policy Network* (Internet & Jurisdiction Policy Network, 2012), que tiene como objetivo consolidar una red de colaboración *multistakeholder* que facilite una verdadera cooperación transnacional y aborde los problemas relacionados con la naturaleza transfronteriza de Internet, conservando su naturaleza global a la vez que protegiendo los derechos humanos, y permite el desarrollo de la economía digital. La gran mayoría de las transacciones y del flujo de datos en Internet atañen a la jurisdicción de varios Estados dependiendo de la localización de los usuarios, servidores, plataformas de Internet u operadores técnicos involucrados. La determinación de las leyes de qué Estado aplican a las transacciones en Internet no es unívoca, y tiene importantes repercusiones en los derechos de las personas y empresas, así como en la propia soberanía de los Estados.

No todos los procesos de gobernanza de Internet se producen a través de mecanismos *multistakeholder*. En algunos casos son los Estados los que tiene la responsabilidad y obligación de definir y aplicar los principios de gobernanza. Este puede ser el caso del ciberterrorismo o de los acuerdos de libre comercio. No obstante, dada la amplia dimensión y complejidad de estos problemas, los Estados pueden en todo caso beneficiarse de los procesos de gobernanza de Internet, como fuente de inspiración y generación de propuestas. La cooperación público-privada a escala global es ya una realidad, y se está sumando a los esfuerzos por encontrar nuevos modelos de gobernanza, como en el acuerdo alcanzado entre Australia,

Canadá, Nueva Zelanda, Reino Unido y Estados Unidos de América (*Five Country Ministerial Joint Communiqué, 2017*) en la Reunión Ministerial de Ottawa de 2017 que incorporó a empresas privadas (Google, Facebook, Microsoft y Twitter) en la elaboración del acuerdo para la lucha contra el ciberterrorismo.

También las empresas están adoptando un papel más activo acordando estándares y principios con un claro impacto en la gobernanza de Internet. Una muestra relevante de este tipo de iniciativas es la reciente firma entre ocho compañías globales del acuerdo de ciberseguridad *Charter of Trust for a Secure Digital World (2018)* en la Conferencia de Múnich de Seguridad. Las empresas firmantes se comprometen a unir fuerzas para promover los principios acordados con tres objetivos fundamentales: proteger los datos de individuos y empresas, prevenir el daño a personas, negocios e infraestructuras, y establecer bases para la confianza en el mundo digital.

Los procesos que influyen y definen la de gobernanza de Internet están en continua evolución, no sólo por la aparición de nuevos modelos liderados por diversos agentes, sino también por la propia evolución tecnológica, motivo de una necesaria cooperación transnacional sostenida.

Para esta deseada cooperación transnacional que permita la salvaguarda de los derechos de los ciudadanos en la Red, parece aconsejable una mayor exploración de los mecanismos de autorregulación y corregulación con una fuerte base *multistakeholder*. Para ello, la gobernanza social de Internet puede inspirarse más que nunca en la trayectoria de la gobernanza técnica, que ha conseguido articular un modelo efectivo para la gestión de los recursos críticos en torno a tres pilares: i) abordando la problemática de la rendición de cuentas con la creación de una nueva comunidad global empoderada, ii) infundiendo confianza mediante una mayor transparencia, y iii) cuidando la inclusividad, tratando a todos los agentes que participan en el ecosistema en pie de igualdad, y iv) poniendo a las personas en el centro de la motivación para todos los procesos.

BIBLIOGRAFÍA

Access Now, Article19, Center for Democracy & Technology, Human Rights Watch, Open Technology Institute, Public Knowledge, & Ranking Digital Rights. (2016). *Civil society statement of support for IANA transition*

Charter of Trust for a Secure Digital World. (2018). Conferencia de Seguridad de Munich. http://www.charter-of-trust.com/

Cross-Community Working Group on Accountability. (2016). *Supplemental final proposal on work stream 1 recommendations.*

Five Country Ministerial Joint Communiqué. (2017) https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/fv-cntry-mnstrl-2017/fv-cntry-mnstrl-2017-en.pdf

IANA Stewardship Transition Coordination Group. (2016). *Proposal to transition the stewardship of the IANA functions from the US commerce department's NTIA to the global multistakeholder community*.

ICANN. (2013). *Beginner's guide to participating in ICANN.*

ICANN. (2015a). Bylaws for internet corporation for assigned names and numbers. Retrieved from https://www.icann.org/resources/pages/governance/bylaws-en

ICANN. (2015b). Comité de nominaciones. Pautas 2015. Retrieved from https://www.icann.org/resources/pages/2015-guidelines-2014-12-11-es

ICANN. (2016). Post-transition IANA. Retrieved from https://www.icann.org/en/stewardship-implementation/post-transition-iana

ICANN. (2018). La comunidad empoderada. Acciones en curso, próximas acciones y reuniones y foros Retrieved from https://www.icann.org/es/ec

IGF Secretariat. (2006). First IGF meeting: Athens, Greece. Retrieved from http://www.intgovforum.org/multilingual/content/first-igf-meeting-athens-greece

IGF Secretariat. (2007). Second IGF meeting: Rio de Janeiro, brazil. Retrieved from http://www.intgovforum.org/multilingual/content/second-igf-meeting-rio-de-janeiro-brazil

IGF Secretariat (2017). WG on IGF multi-year strategic work programme https://www.intgovforum.org/multilingual/filedepot_download/4931/652

Internet & Jurisdiction Policy Network (2012). A global multi-stakeholder Dialogue Process. Annual Report. Retrieved from https://www.internetjurisdiction.net/uploads/pdfs/Annual-Reports/Internet-Jurisdiction-2012-Report.pdf

Microsoft, Amazon, Google, Dell, Facebook, Cloudflare,... SIIA. (2016). An open letter to congress from U. S. business. Retrieved from https://blogs.intel.com/policy/files/2016/04/Business-Open-Letter-supporting-IANA-Transition-VersionV.pdf

National Science Foundation. (2003). A brief history of NSF and the internet. Retrieved from https://www.nsf.gov/news/news_summ.jsp?cntn_id=103050

NTIA. (2014). NTIA announces intent to transition key internet domain name functions. Retrieved from https://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

NTIA. (2016a). NTIA finds IANA stewardship transition proposal meets criteria to complete privatization. Retrieved from https://www.ntia.doc.gov/press-release/2016/iana-stewardship-transition-proposal-meets-criteria-complete-privatization

NTIA. (2016b). Q and A on IANA stewardship transition. Retrieved from https://www.ntia.doc.gov/other-publication/2016/q-and-iana-stewardship-transition-0

NTIA. (2016c). Reviewing the IANA transition proposal. Retrieved from https://www.ntia.doc.gov/blog/2016/reviewing-iana-transition-proposal

Olmos, A. (2015). Recursos críticos. Avances destacados en la gobernanza de internet. In A. Olmos (Ed.), *La gobernanza de internet en España 2015.* (pp. 48-58). Madrid: Fundetel.

Peake, A. The mulstistakeholder approach to internet governance.

Pérez, J. (2008). *La gobernanza de internet. Contribución al debate mundial sobre la gestión y el control de la red.* Madrid: Ariel.

PTI Board. (2016). Approved board resolutions. Retrieved from https://pti.icann.org/approved-board-resolutions-28-sep-2016

Severance, C. (2015). In University of Michigan (Ed.), *Internet history, technology and security*. Coursera course.

United Nations (2015). *Messaged from Mr. Wu Hongbo Under-Secretary-General for economic and social affairs issued on the adoption of WSIS+10 outcome document*.

World Summit on the Information Society. (2005). *Tunis agenda for the information society*. Tunis: International Telecommunication Union.

VI

SEGURIDAD Y CIBERDEFENSA

CAPÍTULO 26

SEGURIDAD PÚBLICA EN EL MUNDO DIGITAL

OFELIA TEJERINA RODRÍGUEZ
Dra. Derecho Constitucional por la UCM. Abogada.
Prof. Máster ICADE y Prof. Asociada URJC

1. CONCEPTO CONSTITUCIONAL DE LA «SEGURIDAD PÚBLICA»

El bien jurídico de la *seguridad pública* está garantizado por el artículo 149.1.29.ª de la Constitución Española. Se establece que es el Estado quien tiene competencias exclusivas para ordenar y regular esta materia, eso sí, sin perjuicio de la oportunidad que se confiere a las Comunidades Autónomas para la creación de policías conforme dispongan sus Estatutos.

Pero es expresamente en el artículo 104 de la CE donde se establece que «proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana» será tarea de las Fuerzas y Cuerpos de Seguridad, en lo que constituye un verdadero servicio público, y diferente en todo caso del concepto *orden público*.

El Tribunal Constitucional ha señalado en numerosas ocasiones (1) que «no toda seguridad de personas y bienes, ni toda normativa encami-

(1) Por todas: STC 59/1985, de 6 de mayo. F. J.º 2.º *BOE* núm. 134, de 5 de junio.

nada a conseguirla o a preservar su mantenimiento puede englobarse en el título competencial de *seguridad pública,* pues si así fuera, la práctica totalidad de las normas del ordenamiento serían normas de seguridad pública, y por ende competencia del Estado, cuando es claro que se trata de un concepto más estricto, en el que hay que situar de modo predominante las organizaciones y los medios instrumentales, en especial los cuerpos de seguridad a que se refiere el artículo 104 de la Constitución». Entiende que el concepto de *orden público* es menos preciso (2), y que puede incluir, por ejemplo, cuestiones como las referentes a la salubridad, mientras que la *seguridad pública* «se centra en la actividad dirigida a la protección de personas y bienes (seguridad en sentido estricto) y al mantenimiento de la tranquilidad u orden ciudadano, que son finalidades inseparables y mutuamente condicionadas».

En consecuencia, el objetivo de la *seguridad pública* es constituirse como tarea principal de las Fuerzas y Cuerpos de Seguridad, en el sentido de «proteger el libre ejercicio de los derechos y libertades y garantizar la seguridad ciudadana». Y tal y como pide el artículo 104.2 de la CE, en Ley Orgánica 2/1986, de 13 marzo, de Fuerzas y Cuerpos de Seguridad, respondería sobre los criterios y límites de sus funciones en su conjunto, sus estatutos y principios básicos de actuación, ya dependan del Gobierno de la nación o de las policías autonómicas y locales.

Esta Ley reconoce en la Exposición de Motivos que la seguridad pública es una competencia «difícil de parcelar», que no permite establecer delimitaciones o definiciones con el rigor y precisión de otras materias, y que es así porque «las normas ordenadoras de la seguridad pública no contemplan realidades físicas tangibles, sino eventos meramente previstos para el futuro, respecto a los cuales se ignora el momento, el lugar, la importancia y, en general, las circunstancias y condiciones de aparición».

Dice también que las Fuerzas y Cuerpos de Seguridad deben actuar respetando siempre el principio de cooperación recíproca y de coordinación orgánica entre ellas, así como los principios de jerarquía y subordinación a la autoridad; respetando la Constitución, especialmente los criterios orientativos que establecen para su actuación los principios constitucionales de legalidad y adecuación al ordenamiento jurídico, de responsabilidad por sus actos, de adecuación entre fines y medios, de secreto profesional, de neutralidad política, de imparcialidad y evitación de cualquier actuación arbitraria o discriminatoria, del respeto a la igualdad ante la Ley, así como al honor y dignidad de la persona. Están al servicio perma-

(2) Ello no quita para que, en aras de la protección ciudadana, ante una crisis sanitaria se deban tomar medidas propias de la seguridad pública. STC 33/1982, de 8 de junio. Conflicto de competencia positivo número 17/1982. F. J.º 3.º *BOE* supl. al núm. 153.

nente de la comunidad (3), en todas sus esferas de convivencia, sobre todo cuando se trata de la protección del libre ejercicio de los derechos y libertades objeto del título I de la CE, todo ello incluyendo, por supuesto, el entorno digital.

2. CONCEPTO DE «SEGURIDAD CIUDADANA» Y ENTORNO DIGITAL

En la Exposición de Motivos de la LO 4/2015, de 30 de marzo, de protección de la seguridad ciudadana se explica que la CE asumió los conceptos de seguridad ciudadana (art. 104.1) y de seguridad pública (art. 149.1.29.ª) casi como sinónimos. Posteriormente, la doctrina y la jurisprudencia los han ido interpretando conjuntamente y entendiendo que abarcan toda actividad «dirigida a la protección de personas y bienes, y al mantenimiento de la tranquilidad ciudadana». También la LO 2/1986, de 13 de marzo, se refería a ambos como conceptos que se pueden utilizar indistintamente. En el artículo 1 dice que «el mantenimiento de la seguridad pública se ejercerá por las distintas Administraciones Públicas a través de las Fuerzas y Cuerpos de Seguridad», y en el artículo 11 les atribuye varias funciones, como por ejemplo «mantener y restablecer, en su caso, el orden y seguridad ciudadana». De manera que podemos afirmar que la confusión de conceptos ha sido legalmente diseñada por ambas normas. Si además consultamos la definición que da la RAE de *seguridad ciudadana:* «situación de tranquilidad pública y de libre ejercicio de los derechos individuales, cuya protección efectiva se encomienda a las fuerzas de orden público», vemos que también encaja con el sentido jurídico que hemos expuesto y que, en definitiva, lo que trata de garantizar es una sensación particular de seguridad del individuo en el ejercicio de sus libertades en el grupo. En términos amplios podemos considerar que se refiere tanto a lo que le suceda en el territorio físico nacional, como a su condición hoy de «ciudadano digital», en la convivencia social que se establece a través de la tecnología.

El último informe del Parlamento Europeo «sobre la democracia digital en la Unión Europea: posibilidades y retos» (2016-2017) (4), se recordaba a los Estados miembros que la iniciativa ciudadana europea es un derecho político de los ciudadanos, y que es «una herramienta única e innovadora para definir la agenda política en aras de una democracia participativa en

(3) *Esta es la razón que determina el particular relieve con que la Ley resalta la promesa o juramento de acatar y cumplir la Constitución, por parte de los miembros de todos los Cuerpos y Fuerzas de Seguridad, que no constituye un mero trámite o formalismo, sino un requisito esencial, constitutivo de la condición policial y al mismo tiempo símbolo o emblema de su alta misión.* Exposición de Motivos de la Ley 2/1986, de 13 marzo, de Fuerzas y Cuerpos de Seguridad.

(4) «Informe sobre la democracia digital en la Unión Europea: posibilidades y retos» del Parlamento Europeo» [2016/2008 (INI)]. Comisión de Asuntos Constitucionales. Parlamento Europeo (22/02/2017). Ponente: Ramón Jáuregui Atondo.

la Unión Europea, que permite a los ciudadanos ser parte activa en los proyectos y procesos que les atañen, y cuyo potencial debe, sin duda, explotarse al máximo y mejorarse de forma significativa». Esta iniciativa no podría hoy ser viable si no se entendiera incluida en el entorno digital. Dice por ello también que «el refuerzo de la legitimidad democrática de las instituciones debe ser uno de los objetivos prioritarios de la UE», y que no se puede hablar de democracia ni de seguridad sin «potenciar el empleo de las nuevas tecnologías en la vida institucional y política». Es preciso pues proteger los derechos de los ciudadanos también en este escenario digital, fomentar su participación en los procesos de toma de decisiones y generar confianza mediante la superación de la brecha digital, de manera que se pueda garantizar un acceso generalizado y seguro a la tecnología, «y propiciar una mayor seguridad en la utilización de Internet».

Si ponemos estas reflexiones en relación directa con el artículo 104 y con los derechos recogidos en el Título I de nuestra CE, vemos que la seguridad ciudadana en el contexto digital también conecta como uno de los elementos esenciales del Estado de Derecho. Sin duda es para los ciudadanos una garantía más de sus libertades el que puedan ser efectivamente ejercidas en todos los ámbitos en que se desenvuelve su vida, pues Internet es parte de la realidad y es herramienta para el correcto desarrollo de nuestra naturaleza como personas. La necesidad de esta protección es indiscutible, pero tan peligroso sería no tenerlo en cuenta, como permitir que se convirtiera en una carta blanca para la actuación policial en las redes.

Las normas que procuren la protección de los individuos en el entorno digital y que determinen la intervención de las Fuerzas y Cuerpos de Seguridad deben definirse con pleno respeto a los límites constitucionalmente establecidos, máxime si están en juego derechos fundamentales. No por el hecho de interactuar en un medio diferente, no físico, podemos interpretar que los ciudadanos dejan de ser personas titulares de derechos con plena capacidad de obrar.

Ciertamente el lema «no hay leyes para Internet» ha traído de cabeza al legislador en los últimos 15 años. Y por alguna exótica razón, además ha infundido una prisa irreflexiva, también en los gobernantes y juzgadores, por crear todo tipo de reglas que les permitían de forma más o menos efectiva la posibilidad de controlar las conexiones digitales y los contenidos que circulan a través, tratando de demostrar que eran perfectamente capaces de atajar todo tipo de riesgos online (5).

(5) Por ejemplo: «La Policía podrá instalar un troyano en el ordenador de un sospechoso» (8/12/2015). Disponible en: https://elpais.com/tecnologia/2015/12/04/actualidad/1449259283_679909.html También: «Identificar a los usuarios en las redes sociales, una medida muy difícil de legislar» (29/11/2017). Disponible en: http://www.abc.es/tecnologia/redes/abci-identificar-usuarios-redes-sociales-medida-dificil-legislar-201711292159_noticia.html

Tan importante es infundir esa sensación de tranquilidad, que ya se está trabajando, por ejemplo, en la creación de una ciberreserva de voluntarios que dependerá del Gobierno y que «colaborará en la detección de riesgos y la notificación de incidencias» (6). Algo que si no se trata con el debido respeto, puede resultar en lo que el famoso criptógrafo americano Bruce Schneier (7) lleva años denunciando, lo que él llama «El teatro de la seguridad».

Este ingeniero considera que parte de las estrategias de seguridad que se plantean por los gobiernos de medio mundo son solo diseñadas para hacer sentir más segura a la gente. Entiende que se crean normas y se adoptan medidas de seguridad inútiles al fin que se persigue, que no solo no protegen a los ciudadanos sino que en algunos casos pueden ser incluso realmente peligrosas para sus intereses. Por ejemplo, en enero de 2007, publicaba en su blog, un post dedicado precisamente a «El elogio del teatro de la seguridad», en el que analizaba las medidas de seguridad que se habían implantado un hospital para evitar el secuestro de niños. Todos los bebés tenían etiquetas RFID en las pulseras colocadas en sus tobillos, y había además sensores en las puertas de la sala de maternidad, de manera que la alarma se activaba si pasaba un bebé por ese lugar. Sin embargo, las estadísticas (8) de sustracción de bebés habían descendido muchísimo en las últimas décadas, y si se calculaba la probabilidad matemática de que el gasto en esas medidas fuese proporcionalmente útil a la evitación de secuestros, veríamos que tales medidas de seguridad en realidad solo habrían activado para tranquilizar a las madres. Algo de cara a la galería, una medida de puro marketing (vender calidad) muy costosa: «la seguridad es a la vez una realidad y un sentimiento. La realidad de la seguridad es matemática, está basada en la probabilidad de diferentes riesgos y la efectividad de diferentes contramedidas. Conocemos las tasas de sustracción de bebés y que las pulseras las reducirían. También sabemos el coste de las pulseras y, por tanto, podemos calcular si son una medida de seguridad rentable o no. Pero la seguridad también es un sentimiento, basado en reacciones psicológicas individuales a los riesgos y las contramedidas. Y las dos cosas son diferentes: puede estar seguro aunque no se sienta seguro, y puede sentirse seguro aunque no esté realmente seguro».

Entiende la psicología de la seguridad como un sentimiento del todo subjetivo y recuerda cómo gran parte de los programas de seguridad implementados después del 11 de septiembre de 2001 (y de posteriores

(6) «Un ejército de ingenieros, abogados y filósofos para defender España de los ciberataques» (18.01.2018). Disponible en:
http://www.elmundo.es/papel/futuro/2018/01/18/5a5f9577268e3e8c1d8b4618.html
(7) Página web personal de Bruce Schneier https://www.schneier.com/
(8) *La probabilidad es de 1 en 375.000*. «En elogio del teatro de seguridad». Disponible en:
https://www.schneier.com/essays/archives/2007/01/in_praise_of_securit.html

atentados terroristas), no tenían la capacidad de protección que se negociaba con la sociedad. Por ejemplo, no resultaban suficientes para mejorar la seguridad en los puestos de control, pero sí sería para tranquilizar a los pasajeros de un vuelo ver a cientos de agentes repartidos por todo el aeropuerto, aunque ni siquiera llevaban sus armas cargadas. Hace también referencia al coste de ese teatro, no solo en lo material, que podría ser invertido en cosas mucho más necesarias o útiles para el ser humano, sino también de la oportunidad, sobre lo que dejamos de hacer por «respetar» esas medidas de seguridad. Pensemos por ejemplo en el contexto de las comunicaciones en Internet, en esas medidas gubernamentales de control de contenidos o de acceso remoto a ordenadores personales, que en su momento se pretendía que fueran ejecutadas por las autoridades policiales sin una autorización judicial que determinase su alcance concreto, justificándolo con argumentos de «rapidez» y supuesta eficiencia para la detención de sospechosos. Pero si quienes ejecutan esas medidas no tienen competencias para delimitar la actuación frente a posibles vulneraciones de derechos fundamentales, lo más probable es que terminen conculcándolos por la presión de obtener resultados lo más rápido posible en la investigación. Y el fin no justifica los medios. Está demostrado que las prisas y las situaciones que crean alarma social nos llevan a adoptar malas decisiones en cuanto a la capacidad del Estado para vigilar y proporcionar seguridad a los ciudadanos. Obviamente el mundo digital requiere inmediatez en las intervenciones para hacer que cesen eventuales ataques, pero no por ello, se justifican las medidas que ignoren los principios de necesidad, idoneidad y proporcionalidad sobre el fin perseguido.

3. PRINCIPALES AMENAZAS Y RETOS

En España, la Ley Orgánica 4/2015, de 30 de marzo, de seguridad ciudadana, se aprobó por la necesidad de actualizar la forma en que debían protegerse los derechos de los ciudadanos (9), observando que «la libertad y seguridad constituyen un binomio clave para el buen funcionamiento de una sociedad democrática avanzada, siendo la seguridad un instrumento al servicio de la garantía de derechos y libertados y no un fin en sí mismo. Por tanto cualquier incidencia o limitación en el ejercicio de las

(9) Exposición de Motivos: « (…) varios factores aconsejan acometer su sustitución por un nuevo texto. La perspectiva que el transcurso del tiempo ofrece de las virtudes y carencias de las normas jurídicas, los cambios sociales operados en nuestro país, las nuevas formas de poner en riesgo la seguridad y la tranquilidad ciudadanas, los nuevos contenidos que las demandas sociales incluyen en este concepto, la imperiosa necesidad de actualización del régimen sancionador o la conveniencia de incorporar la jurisprudencia constitucional en esta materia justifican sobradamente un cambio legislativo. Libertad y seguridad constituyen un binomio clave para el buen funcionamiento de una sociedad democrática avanzada, siendo la seguridad un instrumento al servicio de la garantía de derechos y libertados y no un fin en sí mismo».

libertades ciudadanas por razones de seguridad debe ampararse en el principio de legalidad y en el de proporcionalidad en una triple dimensión: un juicio de idoneidad de la limitación (para la consecución del objetivo propuesto), un juicio de necesidad de la misma (entendido como inexistencia de otra medida menos intensa para la consecución del mismo fin) y un juicio de proporcionalidad en sentido estricto de dicha limitación (por derivarse de ella un beneficio para el interés público que justifica un cierto sacrificio del ejercicio del derecho). Son estas consideraciones las que han inspirado la redacción de esta Ley, en un intento de hacer compatibles los derechos y libertades de los ciudadanos con la injerencia estrictamente indispensable en los mismos para garantizar su seguridad, sin la cual su disfrute no sería ni real ni efectivo».

Ese era su espíritu, supuestamente, porque al final resulta que ha sido conocida como «Ley mordaza» por la forma en que afectaba, en sentido negativo, al entorno digital, y especialmente a la libertad de expresión.

Entre sus disposiciones se hace referencia a circunstancias tales como la responsabilidad por la organización de protestas o manifestaciones, imponiendo sanciones a quienes, aun no habiendo suscrito o presentado una comunicación de convocatoria, pudiera deducirse su participación directa «por publicaciones o declaraciones de convocatoria de las mismas, por las manifestaciones orales o escritas que en ellas se difundan» (…) «o por cualesquiera otros hechos pueda determinarse razonablemente que son directores de aquellas» (art. 30.3 de la LO 4/2015, de 30 de marzo). Esto se ha interpretado por los medios de comunicación y socialmente como la sanción de meras consignas que puedan llegar a incitar a alguien a manifestarse o a secundar una convocatoria de protestas hecha por terceros, sobre todo cuando se difundan por Internet.

Además, se sanciona la captación y difusión de «datos personales o imágenes no autorizadas de autoridades policiales en el ejercicio de sus funciones», por cuanto pueda ponerse en peligro «la seguridad personal o familiar de los agentes, de las instalaciones protegidas o en riesgo el éxito de una operación, con respeto al derecho fundamental a la información» (art. 36.23 de la LO 4/2015, de 30 de marzo). Los detractores lo interpretan como un límite a la libertad de expresión de los particulares, pues en caso de estar observando conductas impropias de las funciones de seguridad pública, no podrían captar esas imágenes o pruebas de lo que estuviera sucediendo.

Tales disposiciones no fueron bien recibidas por la comunidad internauta, hasta el punto de que la conocida comunidad activista «Ano-

nymus» respondió a su entrada en vigor revelando de manera totalmente injustificada información personal de miles de agentes de policía (10).

Hoy, la actualización legal de estas cuestiones lleva más de un año bloqueada en el Congreso, pero plantea por ejemplo la eliminación de esas sanciones para quienes participen en manifestaciones o quienes utilicen imágenes de agentes de las policías.

Otra desacertada innovación en materia de seguridad ciudadana en el entorno digital, fue la de los artículos 573.2 y 575.2 del Código Penal, que convirtieron en delitos de terrorismo los delitos informáticos tipificados en los arts. 197 bis, 197 ter y 264 a 264 quater del Código Penal «cuando tengan como objetivo subvertir el orden constitucional, o suprimir o desestabilizar gravemente el funcionamiento de las instituciones políticas, alterar gravemente la paz pública, desestabilizar gravemente el funcionamiento de una organización internacional o provocar un estado de terror en la población o en una parte de ella, y correlativamente». Cuestiones éstas interpretables de muy diferentes maneras según el contexto en que se produzcan los hechos, lo que provoca gran inseguridad jurídica a la hora de aplicarlo. También convirtió en delito el acceder «de manera habitual a uno o varios servicios de comunicación accesibles al público en línea o contenidos accesibles a través de internet o de un servicio de comunicaciones electrónicas cuyos contenidos estén dirigidos o resulten idóneos para incitar a la incorporación a una organización o grupo terrorista, o a colaborar con cualquiera de ellos o en sus fines».

En ambos casos pasa de recoger una cuestión de seguridad pública, a algo con características más propias del ámbito de la seguridad del Estado. Y lo que es más grave, especialmente en el segundo supuesto, se convirtió en delito una conducta que en principio es un mero indicio que debería llevaría a teorizar sobre sospechas (acceder a contenidos online). Convierte un indicio en prueba de un delito, pudiendo restringir la presunción de inocencia de forma desproporcionada, también al ignorar el principio de mínima intervención del Derecho Penal.

Otro caso en el que se traspasaría el criterio de idoneidad que exige toda medida de seguridad pública es la tipificación de alguno de los delitos contra la propiedad intelectual, imponiendo en muchos casos sanciones de privación de libertad, aun cuando no es posible determinar siquiera el dolo del presunto responsable. Es el caso del artículo 270.2 del Código Penal, cuando dice que se castigará a quien «con ánimo de obtener un beneficio económico directo o indirecto, y en perjuicio de tercero, facilite de modo activo y no neutral y sin limitarse a un tratamiento meramente

(10) «Anonymous difunde datos personales de 5.400 policías nacionales en protesta por la Ley Mordaza» (1.06.2016). Disponble en: http://www.europapress.es/nacional/noticia-anonymous-difunde-datos-personales-5400-policias-nacionales-protesta-ley-mordaza-20160601155336.html

técnico, el acceso o la localización en internet de obras o prestaciones objeto de propiedad intelectual sin la autorización de los titulares de los correspondientes derechos o de sus cesionarios, en particular ofreciendo listados ordenados y clasificados de enlaces a las obras y contenidos referidos anteriormente, aunque dichos enlaces hubieran sido facilitados inicialmente por los destinatarios de sus servicios». Es difícil imaginar cómo se puede demostrar la intencionalidad de conseguir algo indirectamente, y más cuando se trata de contenidos alojados tras un enlace, cuyo autor o editor pueden cambiar en cuestión de segundos.

Previsiones regulatorias más pacíficas son las relativas a otro tipo de amenazas como las estafas informáticas *(fhishing y scam)* previstas en el artículo 248 del CP, los daños informáticos de los artículos 263 y 264, el acoso *online (stalking)* del artículo 172 ter., los delitos contra la indemnidad sexual de menores *(grooming)* tipificados en el artículo 183 ter., o los delitos contra la intimidad, también cometidos mediante el uso de la tecnología, del artículo 197, todos ellos código normativo.

Por otra parte, no se aprecian grandes debates sobre la regulación del uso de la videovigilancia por el sector público, al menos de momento. En este caso, los derechos fundamentales afectados son límite preciso para su utilización. Tal vez sea por tratarse de un uso de la tecnología de mayor tradición, o bien porque simplemente tiene menos repercusión, en el sentido de que no es habitual la difusión no autorizada de informaciones así captadas a través de las redes, y no se ha visto comprometida su utilidad. En España, se produjo en 1993 un suceso clave que puso de manifiesto para la opinión pública la importancia de la instalación de dispositivos de videovigilancia con motivos de seguridad pública. Ese año, durante las fiestas de Bilbao se produjo el linchamiento de un ertzaintza en la calle, hecho este que fue captado por cámaras de videovigilancia y cuyas imágenes sirvieron de prueba definitiva para condenar a los agresores (11). Esta circunstancia forjó una corriente de opinión a favor de estos sistemas que llevó al Congreso de los Diputados a replantear su idoneidad para la prevención y detección de delitos. Se aprobó entonces la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos. El debate se centraba concretamente en «la prevención de actos delictivos, la protección de las personas y la conservación y custodia de bienes que se encuentren en situación de peligro, y especialmente cuando las actuaciones perseguidas suceden en espacios abiertos al público, lleva a los miembros de las Fuerzas y Cuerpos de Seguridad al empleo de medios técnicos cada vez más sofisticados», y la norma llegó porque «con estos medios, y en particular

(11) Sentencia de la Audiencia provincial de Bilbao, de 10 de enero de 1997.

mediante el uso de sistemas de grabación de imágenes y sonidos y su posterior tratamiento, se incrementa sustancialmente el nivel de protección de los bienes y libertades de las personas». Era pues el momento oportuno para «proceder a la regulación del uso de los medios de grabación de imágenes y sonidos que vienen siendo utilizados por las Fuerzas y Cuerpos de Seguridad, introduciendo las garantías que son precisas para que el ejercicio de los derechos y libertades reconocidos en la Constitución sea máximo y no pueda verse perturbado con un exceso de celo en la defensa de la seguridad pública» (12). Tras esta norma, otro momento importante lo marcó la Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras. En él se señalaron las pautas y distinciones necesarias, a nivel administrativo, para la utilización de estos sistemas con fines privados o públicos, considerando que la instalación de videocámaras en las vías públicas (captando la vía pública) sólo estaría permitida cuando fuera realizada por las Fuerzas y Cuerpos de Seguridad (13), sobre lo que la Agencia carecería de competencia alguna para autorizarlo. Eso sin perjuicio de que les fuera aplicable lo especialmente previsto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, como ocurre en el caso de instalaciones de seguridad instaladas por empresas privadas en edificios de la Administración Pública.

En Europa, cabe mencionar las Directrices del Supervisor Europeo de Protección de Datos (14) publicadas en marzo de 2010, para la utilización de videovigilancia por instituciones y organismos europeos, ya que establece los principios a tener en cuenta para evaluar la necesidad de recurrir a este tipo de sistemas de seguridad, y ofrecen orientación sobre cómo utilizarlos minimizando el impacto sobre la privacidad y otros derechos fundamentales. Cuando fueron aprobadas, Giovanni Buttarelli, entonces asistente del SEPD, señaló que «los derechos fundamentales y la seguridad no tienen que ser mutuamente excluyentes: si se utiliza un enfoque pragmático basado en los principios de selectividad y proporcionalidad, los sistemas de videovigilancia pueden satisfacer las necesidades de seguridad mientras respeten también nuestra privacidad». En todo caso, el Supervisor promueve, y más ahora con la entrada en vigor del Regla-

(12) Exposición de Motivos de la Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

(13) Artículo 22 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad Ciudadana. *Uso de videocámaras*: *La autoridad gubernativa y, en su caso, las Fuerzas y Cuerpos de Seguridad podrán proceder a la grabación de personas, lugares u objetos mediante cámaras de videovigilancia fijas o móviles legalmente autorizadas, de acuerdo con la legislación vigente en la materia.*

(14) Informe disponible en inglés es: https://edps.europa.eu/sites/edp/files/publication/10-03-17_video-surveillance_guidelines_en.pdf

mento General de Protección de Datos de la Unión Europea, ya sea en el sector público o el privado, la realización de evaluaciones de impacto así como una especial diligencia en supuestos como la vigilancia encubierta o los sistemas de vigilancia dinámicos preventivos. La protección de datos no debe verse como una carga regulatoria, sino que debe formar parte de una cultura organizacional y una buena gobernanza, donde la administración de cada institución tome las decisiones basándose en el asesoramiento de sus oficiales de protección de datos y consultas abiertas todas las partes interesadas. El RGPD precisamente trae el principio denominado de «accountability» o de responsabilidad proactiva.

Nadie concibe hoy que la ciudad pueda llenarse esquina a esquina de cámaras de videovigilancia, y si a llegase plantearse, nadie permitiría que se legitimara sin más la posibilidad de utilizar las imágenes así captadas para otro fin que no fuera el de la seguridad pública.

Por último, importante es también la preocupación de los Gobiernos por la represión de los *delitos de odio* en el entorno digital. Este término fue acuñado para ciertas conductas tipificadas en el Código Penal que contienen un elemento motivador hacia la violencia por odio y discriminación, y que están reguladas en el Título XXI. Capítulo IV, Secc. 1 del Código Penal, dedicado a «los delitos cometidos con ocasión del ejercicio de los derechos fundamentales y de las libertades públicas garantizados por la Constitución». Estos delitos se codificaron para reprimir aquellas conductas que incitasen a la «hostilidad, discriminación o violencia contra un grupo, una parte del mismo o contra una persona determinada por razón de su pertenencia a aquél», y ello si fuera por «motivos racistas, antisemitas u otros referentes a la ideología, religión o creencias, situación familiar, la pertenencia de sus miembros a una etnia, raza o nación, su origen nacional, su sexo, orientación o identidad sexual, por razones de género, enfermedad o discapacidad».

Con la última reforma, en 2015, las condenas imponibles a estos supuestos se agravaron para los casos en que «los hechos se hubieran llevado a cabo a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información», haciéndose accesible a un gran número de personas (art. 510.3 del CP), y cuando «los hechos, a la vista de sus circunstancias, resulten idóneos para alterar la paz pública o crear un grave sentimiento de inseguridad o temor entre los integrantes del grupo, se impondrá la pena en su mitad superior, que podrá elevarse hasta la superior en grado» (art. 510.4 del CP). Se entendió que la agresión a los derechos de las personas era mucho más complicada y perniciosa si se producía a través de este medio, y más aún si afecta a la seguridad pública.

El problema con el que se está encontrando la justicia a la hora de interpretar este precepto, es el de configurar un criterio actualizado sobre la distinción entre el mal gusto y la lesión a la dignidad u honor de una persona o grupo, y en ocasiones se obvia que hay diferencia entre una y otra conducta (especialmente en consideración al principio de intervención mínima del derecho penal) simplemente «para dar ejemplo». Recientemente se ha conocido una sentencia del Tribunal Supremo que ha anulado la condena impuesta a una tuitera, por la Audiencia Nacional (15), al considerar que había cometido un delito de humillación a las víctimas de terrorismo. El TS determinó que los comentarios que esta mujer había vertido en Twitter eran simplemente chistes de mal gusto que repetían algo «muy trillado y agotado» y que los mensajes «no contienen ningún comentario ácido contra la víctima del atentado ni expresan frases o comentarios hirientes, lacerantes o ultrajantes contra su persona o cualquier aspecto concreto de su vida pública o privada» (16).

En este caso la libertad de expresión en las redes ha quedado salvaguardada, y ha sido conforme a criterios tradicionales, sobre lo que es o no ofensivo en un comentario y cuándo eso es susceptible de crear un riesgo de alteración grave del orden público o de terrorismo. Pero en general no se aprecia tanta mesura. Cuando se trata de imponer restricciones al uso de Internet, con restricciones de derechos fundamentales de los ciudadanos incluidas, parece que juzgadores y legislador se olvidan de cuestiones básicas de su funcionamiento y su utilidad, tratando de dar respuestas ágiles, ejemplificativas y aparentemente efectivas, pero no siempre acertadas.

Véase también el caso de la imposición de responsabilidades a los proveedores de servicios por los contenidos que otros editan en Internet, cuando resultan contrarios a las leyes, el empeño en obligarles a censurar lo que le pidan los ciudadanos sin más criterio que el suyo propio de lo que es o no un interés legítimo, de lo moralmente aceptable o reprobable en un momento concreto, con el evidente riesgo de interferir en el libre ejercicio de la libertad de expresión e información. Y es que no se acaba de comprender que, y ya lo señalaba la Directiva 2002/22/CE [Directiva sobre servicio universal (17)], no se debe exigir a los proveedores «que controlen la información transmitida a través de sus redes ni que inter-

(15) «La Audiencia Nacional condena a Cassandra Vera, la tuitera que hizo chistes de la muerte de Carrero Blanco» (30.03.2017). Disponible en:
https://politica.elpais.com/politica/2017/03/29/actualidad/1490788774_203770.html

(16) Nota de prensa del CGPJ «El Tribunal Supremo absuelve a la tuitera Cassandra del delito de humillación a las víctimas por sus chistes sobre Carrero Blanco» (1.03.2018). Disponible en: http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Sala-de-Prensa/Notas-de-prensa/El-Tribunal-Supremo-absuelve-a-la-tuitera-Cassandra-del-delito-de-humillacion-a-las-victimas-por-sus-chistes-sobre-Carrero-Blanco

(17) Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009.

pongan acciones judiciales contra sus clientes con motivo de dicha información, ni responsabiliza a los proveedores de dicha información». Y que «la responsabilidad por acciones punitivas o el enjuiciamiento penal es competencia de la legislación nacional, dentro del respeto de los derechos y las libertades fundamentales, incluido el derecho a las garantías procesales», así como que «corresponde a los Estados miembros, y no a los proveedores de redes o servicios de comunicaciones electrónicas, decidir de conformidad con los procedimientos adecuados si los contenidos, las aplicaciones o los servicios son lícitos o nocivos».

Por último, respecto a los retos a los que se enfrenta la seguridad pública, citar la utilización de dispositivos automáticos programados mediante secuencias de algoritmos que no siempre tienen en cuenta los límites constitucionalmente establecidos (o simplemente no logran aprenderlos). Drones, coches autónomos o robots a los que se recurrirá simplemente porque llama más la atención su posible utilidad para la persecución del delincuente que los daños que puedan causar tratando de poner remedio a un riesgo.

No por más cercana a la ciencia ficción resulta más útil la tecnología, o menos peligrosa.

4. ESTRATEGIAS DE SEGURIDAD PARA LA PROTECCIÓN DE LOS CIUDADANOS EN LA UE Y LA SEGURIDAD NACIONAL

En el contexto digital la UE ha definido un espacio de justicia, libertad y seguridad que solo puede ser realizado, o así debería ser, implementando políticas y/o programas de actuación que manifiesten pleno respeto a los derechos fundamentales de los ciudadanos (especialmente, en lo que afectan a su intimidad o la libertad de información, y por extensión, a su dignidad).

Por ejemplo, cuando en la investigación de los delitos es necesario proceder al intercambio de información genética, o acceder a bases de datos de pasajeros de vuelos nacionales e internacionales (PNR, pero también *body* escáneres), datos de procesados o personas con antecedentes penales, datos de videovigilancia efectuada por instituciones públicas o gubernamentales, de interceptación de comunicaciones, etc., la norma general impide cualquier intervención que invada la esfera individual del artículo 8 de la Carta Europea de los Derechos Fundamentales (CEDH) sobre el derecho al respeto a la vida privada y familiar (18). Esta Carta no forma parte del Tratado de Lisboa, pero el artículo 6, apartado 1, del TUE, le atribuye un carác-

(18) Artículo 8 CEDH: «1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional,

ter «jurídicamente vinculante», como a cualquier otro Tratado, de manera que el respeto a los derechos que recoge es un principio general del Derecho de la UE que lógicamente, también afecta a las políticas de investigación de la delincuencia en Internet de los Estados Miembros. Y se debe entender que es así, no sólo para los delitos de terrorismo o seguridad nacional, sino también para investigar asuntos que atañen a aspectos más propios de la seguridad ciudadana como las estafas informáticas, el blanqueo de capitales, los ciberataques a empresas o la protección de la infancia y la juventud en las redes.

El concepto de seguridad nacional tiene su marco regulatorio definido por la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, como un espacio mucho más amplio que el de la seguridad pública o ciudadana. Entiende su Preámbulo que es «un espacio de actuación pública nuevo, enfocado a la armonización de objetivos, recursos y políticas ya existentes en materia de seguridad», que es específicamente «la acción del Estado dirigida a proteger la libertad y el bienestar de sus ciudadanos, a garantizar la defensa de España y sus principios y valores constitucionales, así como a contribuir junto a nuestros socios y aliados a la seguridad internacional en cumplimiento de los compromisos asumidos; concepto que, hasta la fecha, no había sido objeto de una regulación normativa integral». Respecto a las materias que abarca, señala expresamente que nos enfrentamos a situaciones de elevada complejidad «que desbordan las fronteras de categorías tradicionales», como defensa, seguridad pública, acción exterior e inteligencia, y otras más actuales como «el ciberespacio». Busca la protección del superior interés nacional, también en este contexto de la Sociedad de la Información. Por estas razones el Real Decreto 1008/2017, de 1 de diciembre, que aprobó la última Estrategia de Seguridad Nacional (19), mencionaba que entre sus principales preocupaciones están las amenazas y vulnerabilidades propias del ciberespacio, incluyéndolo como un objetivo más de acción estratégica (20). Habla de la necesidad de impulsar la dimensión de seguridad en el desarrollo tecnológico, considerando que su progreso está asociado a una mayor exposición a nuevas amenazas: «la hiperconectividad actual agudiza algunas de las vulnerabilidades del sistema de seguridad y exige una mejor protección de las redes y sistemas, así como de la

---

la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

(19) Disponible en: https://www.boe.es/boe/dias/2017/12/21/pdfs/BOE-A-2017-15181.pdf.

(20) «(…) las ciberamenazas han incrementado en número e impacto, como fue el caso del ciberataque de mayo de 2017 WannaCry, de escala global y afección directa a empresas, servicios e intereses nacionales. Este incremento se ha de relacionar con la prevalencia de las conocidas como acciones híbridas. Se trata de acciones combinadas que pueden incluir, junto al uso de métodos militares tradicionales, ciberataques, operaciones de manipulación de la información, o elementos de presión económica, que se han manifestado especialmente en procesos electorales. La finalidad última que se persigue es la desestabilización, el fomento de movimientos subversivos y la polarización de la opinión pública.»

privacidad y los derechos digitales del ciudadano. España debe adaptarse a esta transformación permanente con un mayor esfuerzo de digitalización y tecnificación del Estado y la sociedad, basado en un sistema educativo y de formación adaptado a la nueva realidad.»

Las amenazas que en el contexto digital puede llegar a afectar de forma más directa a la estabilidad política propia de la democracia y la seguridad nacional, van desde el poder manipulador de las *fake news,* a los ataques informáticos contra servicios esenciales del Estado, el hackeo de procesos electorales y la revelación de información confidencial en materia de defensa. Son retos regulatorios aún pendientes sobre el uso de las tecnologías y sobre la gestión de contenidos digitales que preocupan hoy a los Gobiernos. Por ejemplo, respecto al espionaje, la referida Estrategia de Seguridad entiende que «es una amenaza de primer orden para la seguridad, que se ha adaptado rápidamente a las posibilidades que ofrece la tecnología moderna. En este sentido, el ciberespacio juega hoy un papel más relevante a nivel de espionaje y es utilizado por Estados, grupos o individuos que usan sofisticados programas que proporcionan acceso a ingentes volúmenes de información y datos sensibles».

Respecto a ataques informáticos con intereses económicos, no solo se producen desde el sector privado, sino que algunos Estados persiguen sus propios fines, «persiguen la expansión de sus intereses geopolíticos a través de acciones de carácter ofensivo y subversivo, como de organizaciones terroristas, grupos de crimen organizado y actores individuales» y hay que estar también preparados para ello.

El anonimato es otro elemento que tiene en cuenta entre sus preocupaciones, que los delincuentes lo aprovechan para «conseguir sus fines a un mínimo coste y asumiendo un riesgo menor dada la dificultad de atribución» del daño una vez comprometidos los sistemas. Dice que ataques ransomware y de denegación de servicios, el hackeo de dispositivos móviles y sistemas industriales, los ciberataques contra las infraestructuras críticas, las acciones de desinformación, la propaganda o financiación terrorista y las actividades de crimen organizado «impactan en la Seguridad Nacional, amplificando la complejidad y la incertidumbre, y también pone en riesgo la propia privacidad de los ciudadanos».

Sin embargo nada dice sobre el problema que supone la falta de recursos materiales y de formación especializada para llevar a cabo estas operaciones de seguridad de manera efectiva. Además, si bien combatir estas amenazas o reparar el daño una vez producido exigen un importante esfuerzo presupuestario, lo cierto es que no hay aún una conciencia generalizada de que en muchas ocasiones dichas amenazas, o mejor dicho, el daño, ha sido resultado de un fallo humano que podría haberse evitado adoptando medidas de prevención bastante elementales. Reconocer esto

abiertamente no es una estrategia de imagen que interese ni a las entidades privadas ni a la Administración Pública, pero deberían considerar que hacerlo tiene un impactante resultado de concienciación y educación en ciberseguridad, con efectos muy beneficiosos más allá de la alarma social que se pudiera crear en un primer momento (21) (véase por ejemplo, el caso «wannacry», que aunque se trató de controlar la información que se daba al público, desde el minuto uno hubo reportes de los empleados de la propia empresa atacada, pero apenas se mencionó que el origen del ataque fue la apertura de un correo electrónico de origen desconocido infectado).

Recientemente la Agencia para los Derechos Fundamentales (FRA), ha publicado un informe (22) a petición del Parlamento Europeo, sobre una investigación a fondo del impacto de la vigilancia por los servicios de inteligencia en los derechos fundamentales. En este interesante documento se pone de manifiesto que con el impacto del terrorismo, los ciberataques y las sofisticadas redes criminales transfronterizas, el trabajo de los servicios de inteligencia se ha vuelto más urgente, complejo e internacional, y reconoce que este trabajo puede interferir fuertemente con los derechos fundamentales, especialmente en la intimidad y la protección de datos, algo que va en contra de cualquier concepto de seguridad ciudadana. Pretendiendo proteger, desprotegen, de manera que habrá que establecer mecanismos de control que puedan frenar un potencial de abuso.

En el contexto de la Política Común de Seguridad y Defensa de la UE (PESD), el Informe sobre la Aplicación de la ESS de 11 de diciembre de 2008, dedicaba entonces un apartado a la cibersegurdiad (23) señalando que «veinte años después de la guerra fría, Europa debe enfrentar amenazas y retos de gran complejidad», y en relación con la Estrategia Europea de Seguridad (EES) del Consejo Europeo, de diciembre de 2003, recogía entre los retos mundiales y principales amenazas, que «las economías modernas dependen en gran medida de las infraestructuras vitales como los transportes, las comunicaciones y el suministro de energía, e

(21) Este es uno de los objetivos, por ejemplo, del RGPD al regular específicamente la obligatoria notificación de las brechas de seguridad en materia de protección de datos. La previsión de estrategias de seguridad para «garantizar un uso seguro de las redes y los sistemas de información y comunicación a través del fortalecimiento de las capacidades de prevención, detección y respuesta a los ciberataques, potenciando y adoptando medidas específicas para contribuir a un ciberespacio seguro y fiable», parece una declaración de intenciones muy loable pero insuficiente, a pesar de que expresamente se promueva reforzar «el alcance y mantenimiento de los conocimientos, habilidades, experiencia, así como capacidades tecnológicas y profesionales que necesita España para sustentar los objetivos de la ciberseguridad».

(22) «Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU - Volume II: field perspectives and legal update». European Union Agency for Fundamental Rights. October 2017. Disponible en: http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega

(23) Informe disponible en: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/ES/reports/104637.pdf.

igualmente de internet. La Estrategia de la UE para una sociedad de la información segura en Europa, adoptada en 2006, hace referencia a la delincuencia basada en internet. Sin embargo, los ataques contra sistemas de TI privadas o gubernamentales en los Estados miembros de la UE han dado una nueva dimensión a este problema, en calidad de posible nueva arma económica, política y militar. Se debe seguir trabajando en este campo para estudiar un planteamiento general de la UE, concienciar a las personas e intensificar la cooperación internacional».

En este escenario la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA), en sus funciones de ayuda a la elaboración de políticas y legislación sobre seguridad de las redes y de la información, realizó un estudio (24) identificando los cinco aspectos clave a tener en cuenta hoy sobre esta materia: estrategias coherentes en todos los Estados miembros y de coordinación dentro de las directrices del PESD, actualización del panorama legislativo, desarrollo de habilidades cibernéticas y promoción de la cibercultura. Distingue ocho tipos de ciberamenazas, por su origen o impacto: ataques físicos a servidores e infraestructuras de soporte a la Sociedad de la Información; desastres naturales; pérdidas de información y activos involuntarios; fallos o mal funcionamiento; cortes de suministro; espionaje, interceptación o hacking; otras actividades fraudulentas o abusos, y problemas legales.

Para combatir todo ello, además de recursos materiales, se pone énfasis en la necesidad de contar con profesionales cualificados que puedan ayudar tanto a la prevención como a la reparación del daño, en caso de que se produzca. No se puede ignorar que la seguridad absoluta no existe, tampoco en el contexto digital.

El ciberespacio es un escenario marcado por componentes tecnológicos, por la accesibilidad y la velocidad en la transmisión de datos, pero también por el incremento de las agresiones procedentes de intereses económicos privados así como de servicios de inteligencia extranjeros contra intereses nacionales, fenómenos para los que resulta imprescindible la mejora de las capacidades tecnológicas de un país, para poder garantizar una respuesta eficaz que dará seguridad a los ciudadanos.

5. CONCLUSIONES

Según la Estrategia Nacional de Seguridad, de diciembre de 2017, es preciso continuar impulsando el aspecto de la seguridad en el desarrollo tecnológico, porque la sociedad depende en gran medida de ello. La

(24) «Cybersecurity in the EU Common Security and Defence Policy (CSDP). Challenges and risks for the EU». Parlamento Europeo. Disponible en:

http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf

automatización de tareas transforma los sistemas de producción y gestión, y ha rebajado su coste sin vuelta atrás. Pero también lo ha hecho con la elaboración, almacenamiento, acceso y difusión de archivos de datos, de informaciones de todo tipo, razón por la cual, entre las medidas necesarias de formación o desarrollo seguro de tecnología, es importante fomentar que incorporen aspectos de seguridad desde su concepción «además de paliar las vulnerabilidades existentes y asegurar sistemas protegidos, bien configurados y gestionados». La seguridad por diseño, la privacidad por diseño, y la ética por diseño, algo de lo que ya se empieza a oír hablar como «Responsabilidad Social Tecnológica».

Otro aspecto a tener en cuenta es la gobernanza de las tecnologías emergentes «ya sea relacionada con la revolución de los datos, dados los ingentes volúmenes de datos que se generan y que son susceptibles de explotación, o con la inteligencia artificial, la robotización y computerización o la biogenética».

Sea como fuere, el Estado debe preservar la capacidad tecnológica de la comunidad y proporcionar herramientas útiles a las estrategias de seguridad pública, aspirando incluso al desarrollo de industrias tecnológicas propias para evitar la dependencia de países terceros en este sentido. Hasta ese punto es necesaria la intervención de los poderes públicos, para ofrecer a los ciudadanos las máximas garantías de seguridad y de protección de sus derechos y libertades, también en el contexto tecnológico y digital.

Por la complejidad de los retos y amenazas a los que nos estamos enfrentando es importante que las políticas de seguridad pública estén provistas de una capacidad de respuesta adecuada, que permita la máxima eficacia en la obtención de resultados con los recursos disponibles. La Constitución confía la garantía de la seguridad ciudadana a las Fuerzas y Cuerpos de Seguridad, siendo éstos los órganos responsables principalmente (no en exclusiva) de acometer estas tareas, con un conjunto muy plural y diversificado de actuaciones configuradas al amparo del libre ejercicio de los derechos y libertades de las personas.

La seguridad pública debe ser entendida como la actividad dirigida a proteger personas y bienes, al mantener en definitiva la tranquilidad de los ciudadanos. En el contexto digital, las amenazas se traducen en ataques informáticos a infraestructuras y servicios esenciales, el espionaje, la manipulación de información, los delitos económicos online, los daños informáticos, la interceptación de comunicaciones, la videovigilancia y cualesquiera otros sistemas de control de movimientos de las personas, etc. Y pueden tener un alcance más propio del concepto «seguridad pública», que de la «seguridad nacional», según el caso.

La Sociedad de la Información debe pues enfrentarse a amenazas propias de su naturaleza tecnológica y a la necesaria optimización de los recursos para lograr combatirlos sin invadir los derechos fundamentales de quienes, al fin y al cabo, son los destinatarios de dicha protección. Las Smart Cities, la inteligencia artificial y el Internet de las Cosas pondrán más riesgos sobre este escenario. Pero si bien es lógico que se vayan actualizando las legislaciones conforme los retos de seguridad lo exijan, no lo es menos que dejarse llevar por la inmediatez como criterio principal de actuación, no va a garantizar el resultado menos lesivo. Las fórmulas para atajar el problema no pueden basarse sin más en el hecho de que exista tecnología que permita repeler las acciones delictivas, sino que se debe ponderar si es tanta la utilidad que proporcionará a efectos de seguridad (Teoría del teatro de la seguridad), más aún, si no será peor el remedio que la enfermedad, cuando se conculquen derechos fundamentales de forma irreversible o de muy difícil reparación.

Los días 19 y 20 de octubre de 2017, el Consejo Europeo planteó la necesidad de una estrategia común de la ciberseguridad en la UE. En sus conclusiones señalaba que «el mundo digital se basa en la confianza, y que esta solo puede lograrse si, en todas las políticas digitales, garantizamos una seguridad más proactiva desde su concepción, proporcionamos una certificación adecuada de seguridad de los productos y servicios y aumentamos nuestra capacidad para prevenir, disuadir, detectar y responder a los ciberataques», y recuerda la necesidad de «concienciarse de la urgencia de hacer frente a las nuevas tendencias, lo que comprende cuestiones como la inteligencia artificial y las tecnologías de cadena de bloques, garantizando al mismo tiempo un elevado nivel de protección de los datos, así como los derechos digitales y las normas éticas». Los Estados miembros tienen claro en todo caso que es suya la responsabilidad de consolidar sus propias estrategias de seguridad en el ciberespacio y de responder a los ataques con los recursos necesarios para prevenir, detectar y responder ante las crisis, y con el respeto de los derechos de los ciudadanos (25).

(25) Conclusiones disponibles en: http://www.consilium.europa.eu/es/policies/cyber-security/, e Informe «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE (Comisión Europea)» (13.09.2017). Disponible en:

http://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cybersecurity_ec.pdf

CAPÍTULO 27
EL DERECHO A LA CIBERSEGURIDAD

Carlos Galán, PhD
Licenciado y Doctor en Informática. Licenciado en Derecho.
Abogado. Profesor de la Universidad Carlos III de Madrid
Presidente de la Agencia de Tecnología Legal

1. DERECHOS HUMANOS: ¿NUMERUS CLAUSUS?

Tradicionalmente, las disciplinas jurídicas más cercanas a la esencia del ser humano (el Derecho Natural, la Filosofía del Derecho, el Derecho Político, especialmente) han venido construyendo un consistente entramado de derechos humanos en torno al más representativo –e inmaterial, probablemente– de todos ellos: la dignidad de la persona.

Tales derechos, denominados *fundamentales* por constituir el fundamento de los restantes, han cimentado el sistema jurídico occidental de los últimos siglos. «Soy un hombre; nada de lo humano me es ajeno.» ponía Terencio en boca de uno de sus personajes, ciento cincuenta años a. C. Es seguramente esta misma idea la que subyace en las manifestaciones y reivindicaciones de derechos desde finales del siglo xviii.

Avanzando hasta la era contemporánea, la Declaración Universal de Derechos Humanos de 1948 enuncia, en su primera línea, la libertad, la justicia y la paz como base para el reconocimiento de la dignidad del hom-

bre. Estos elementos esenciales de la condición humana se van transfigurando en el texto, párrafo a párrafo, adoptando diferentes formas: libertad de palabra y de creencia; igualdad de derechos; no discriminación por razón de raza, color, sexo, idioma, religión, opinión política, origen nacional o social, posición económica, nacimiento o cualquier otra condición; derecho a la vida y a la seguridad personal, abolición de la esclavitud, la servidumbre, las torturas o penas crueles, inhumanas o degradantes; reconocimiento a la personalidad, igualdad ante la ley y derecho a la protección jurisdiccional, sin que quepa la detención ilegal, la prisión o el destierro; derecho a la presunción de inocencia; derecho a la intimidad, sin que quepa injerencia en la vida privada, familia, domicilio o correspondencia; derecho a la libertad de circulación y residencia; derecho al asilo, a la nacionalidad, a la formación de una familia, a la propiedad, etc.

Todos estos derechos, modelados por el tiempo, han sido reinterpretados por los ordenamientos jurídicos de los países democráticos de todo el mundo, y la Constitución Española de 1978 no es una excepción.

Efectivamente, nuestra Carta Fundamental, consagra la Sección 1.ª del Capítulo II de su Título I a enunciar los que denomina «Derechos fundamentales y libertades públicas», dedicando los artículos 15 a 29 a su explícito reconocimiento. Uno tras otro, nuestra Constitución desgrana los que constituyen requisitos existenciales de los destinatarios de la norma: igualdad, derecho a la vida y a la integridad física y moral, a la libertad ideológica, religiosa y de culto, a la libertad y seguridad, al honor, a la intimidad y a la propia imagen, a la libertad de residencia y circulación, a la libertad de expresión, al derecho de reunión, asociación o a participar en asuntos, funciones y cargos públicos, al derecho a la tutela judicial efectiva, al derecho a la educación, a la libertad de sindicación y al derecho a la huelga y al derecho de petición.

No obstante lo anterior –o precisamente debido a ello–, y entrado ya el siglo XXI debemos formularnos un par de preguntas: ¿Son estos los únicos derechos posibles? ¿Cabe algún otro?

2. LA SOCIEDAD DE LA INFORMACIÓN Y SUS RIESGOS

Atendiendo a los datos publicados por Internet World Stats, la población mundial, a 30 de junio de 2017, era de 7.519 millones de personas, de las cuales, 3.885 millones eran usuarios de Internet. En otras palabras: más de la mitad de la población mundial (el 51,7%) es usuaria de Internet (1).

(1) Internet World Stats: *Internet Usage Statistics*, June 30, 2017. (www.internetworldstats.com/stats.htm, último acceso 03.02.2018). El índice señalado de penetración por habitante se corresponde con la media global. Los datos por regiones mundiales son, de mayor a menor: América del Norte (88,1%), Europa (80,2%), Oceanía (69,6%), América Latina y Caribe (62,4%),

Como hemos señalado en otros trabajos (2), constituye un lugar común insistir en la dependencia de las sociedades occidentales de sus sistemas de información, públicos o privados. La actividad cotidiana de los ciudadanos, de los profesionales, de las empresas, de las entidades públicas, del Estado, en suma, depende de que ese conjunto de herramientas tecnológicas a las que hemos denominado *sistemas de información* (computadores y redes de comunicaciones, esencialmente), permanezcan operativos y en condiciones de prestar los servicios que de ellos se esperan.

Efectivamente, en España, en la actualidad, servicios esenciales tales como la energía, los transportes, las finanzas, la sanidad, el comercio, la Defensa y la seguridad, el ocio e, incluso, el procedimiento administrativo, se desarrollan o se gestionan, de forma mayoritaria, por medios electrónicos, y lo harán todavía más en el futuro (3). La importancia de garantizar la continuidad operativa de los sistemas que soportan estos servicios esenciales ha quedado claramente reflejada en la regulación sobre Protección de Infraestructuras Críticas, contemplando doce sectores estratégicos de especial atención: Administración Pública, Espacio, Industria nuclear, Industria Química, Instalaciones de Investigación, Agua, Energía, Salud, Tecnologías de la Información y las Comunicaciones, Transporte, Alimentación y Sistema financiero y tributario (4).

Por tanto, habiendo emprendido este camino sin retorno, la llamada «digitalización de la sociedad» exige garantizar que las herramientas tecnológicas utilizadas tienen la capacidad de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas prestan o hacen accesibles: lo que se ha denominado *resiliencia* (5).

La necesidad de asegurar el normal funcionamiento de los sistemas de información se desprende del hecho de que –como así vienen señalando

---

Oriente Medio (58,7%), Asia (46,7%) y África (31,2%). España posee un índice de penetración por habitante del 87,1%, por encima de la media europea citada.

(2) Galán Pascual, C. «Ciberseguridad pública: el marco integrador de la Estrategia de Ciberseguridad Nacional», en *Los retos del Estado y la Administración en el Siglo xxi.* Libro homenaje al profesor Tomás de la Quadra-Salcedo Fernández del Castillo (Tirant lo Blanch, 2017)

(3) Buena prueba de ello lo constituyen la Ley 39/2015, de Procedimiento Administrativo Común de las Administraciones Públicas y la Ley 40/2015, de Régimen Jurídico del Sector Público, ambas de 1 de octubre, que confieren al uso de los mecanismos electrónicos en las relaciones de las entidades públicas con los ciudadanos y de estas entre sí, respectivamente, el medio prioritario y habitual.

(4) Anexo de la Ley 8/2011, de 28 de abril, por la que se establecen las medidas de protección de las infraestructuras críticas, en desarrollo de la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección.

(5) Como así recoge el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la administración electrónica.

diferentes informes y estudios periódicos (6)–, la realidad diaria evidencia el volumen y la virulencia de los ciberataques contra la seguridad de tales sistemas, muy especialmente aquellos de los que son víctimas los gobiernos, el sector público y las empresas poseedoras de patrimonio tecnológico de todo el mundo, advirtiéndose un incremento inusitado de las acciones de **ciberespionaje** llevadas a cabo por los propios estados, con la pretensión de obtener información valiosa o sensible desde los puntos de vista político, estratégico o económico.

Por otro lado, la universalización de los medios electrónicos en la actividad habitual de las sociedades avanzadas representa un enorme estímulo para ciertos sujetos y organizaciones delincuenciales, que ven con satisfacción cómo la «superficie de ataque» se ensancha, al tiempo que lo hacen los beneficios derivados de su comportamiento delictivo. La comisión de tales acciones en el ciberespacio, cuando revisten las características del delito, es lo que se ha denominado **ciberdelincuencia,** habiéndose desarrollado en los últimos años un nuevo modelo de negocio: el Ciberdelito como Servicio (*Crime-as-a-service*).

Aunque ciberespionaje y ciberdelincuencia han venido siendo las más significativas amenazas de los últimos años y, en su consecuencia, constituyendo la mayor preocupación de los gobiernos, los servicios de inteligencia y los cuerpos policiales de todo el mundo, no podemos olvidar que el activismo antisocial desarrollado en Internet –lo que se ha denominado **hacktivismo**–, junto con la potencial amenaza del **ciberterrorismo,** siguen constituyendo una fuente enorme de inquietud para las organizaciones públicas y privadas de los países más desarrollados.

Además de lo anterior, ha surgido recientemente una nueva amenaza: el **ciberyihadismo,** que, aunando métodos, procedimientos y herramientas del terrorismo, el hacktivismo y la ciberguerra, constituye ya una realidad y supone uno de los mayores riesgos con los que habrán de enfrentarse las sociedades occidentales en los próximos años. Las importantes vías de financiación de estos grupos –al socaire de ISIS o Daesh– hacen que ya no constituya un problema insalvable para los atacantes la adquisición de los conocimientos y las herramientas precisas para el desarrollo de ciberataques o la contratación de los elementos humanos requeridos para su perpetración.

(6) Publicados en nuestro país, entre otros, por el Centro Criptológico Nacional (CCN) –organismo gubernamental nacional adscrito al Centro Nacional de Inteligencia (CNI) y competencialmente responsable de velar por la ciberseguridad de los sistemas de información de las entidades públicas y aquellos otros que tratan información clasificada–, el Instituto Nacional de Ciberseguridad (INCIBE) –organismo encuadrado en las competencias del Ministerio de Energía, Turismo y Agenda Digital en relación con la ciberseguridad de empresas y ciudadanos, el Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) –organismo encuadrado en el Ministerio del Interior en relación con la protección de las Infraestructuras Críticas, o el Mando Conjunto de Ciberdefensa (MCCD), encuadrado en el Ministerio de Defensa.

Finalmente, la persistencia de distintos conflictos armados en todo el mundo, en los que se han visto involucrados no sólo los ejércitos convencionales sino también unidades paramilitares y tropas adoctrinadas a través de fanatismos y radicalismos de raíz religiosa, han propiciado que las acciones que hemos denominado como **ciberguerra** se hagan especialmente presentes. Estos últimos años han dejado claro que las redes y los sistemas informáticos constituyen un nuevo espacio para la confrontación militar.

3. LA SEGURIDAD EN LOS TEXTOS POLÍTICOS Y ESTRATÉGICOS ESPAÑOLES

Consciente de la necesidad de garantizar el desenvolvimiento seguro de las organizaciones españolas –públicas o privadas–, sus profesionales y sus ciudadanos, y siguiendo el camino emprendido por las instituciones europeas y buena parte de sus estados miembro, el estado español publicó en 2013 la Estrategia de Seguridad Nacional (ESN-2013), texto político que manifestaba con claridad la posición y compromiso de España. Su primer párrafo señalaba aquella necesidad: «La seguridad es un fundamento esencial para el desarrollo y el progreso de una sociedad libre. Por eso, resulta imprescindible un entendimiento básico y generalizado de la importancia de la seguridad como garantía de bienestar de los ciudadanos y de la estabilidad del propio Estado».

Recientemente, se ha renovado este compromiso con la seguridad, mediante la publicación del Real Decreto 1008/2017, de 1 de diciembre, por el que se aprueba la Estrategia de Seguridad Nacional 2017 (ESN-2017). Sus líneas iniciales no dejan lugar a dudas:

> *La Estrategia de Seguridad Nacional es el marco de referencia para la política de Seguridad Nacional, una política de Estado que parte de una concepción amplia de la seguridad. La Estrategia actual profundiza en algunos de los conceptos y líneas de acción definidos en 2013 y avanza en la adaptación de dicha Política ante nuevos desarrollos de un entorno de seguridad en cambio constante.*
>
> …
>
> *España se enfrenta a una serie de amenazas y desafíos, tanto internos como externos, incluyendo el reto demográfico, su limitada interconexión energética o problemas de cohesión territorial. Los desafíos a la legalidad y al interés general de España requieren una respuesta desde el Estado de Derecho con objeto de garantizar los derechos y libertades de todos los ciudadanos.*
>
> *Asimismo, en plena revolución tecnológica, España, como país interconectado e interdependiente, se debe adaptar a esta transformación y aprovechar sus oportunidades de progreso, a la vez que aborda los*

nuevos desafíos que comporta la hiperconectividad. En este sentido, es importante fomentar la concienciación sobre las principales amenazas y desafíos actuales, a través de una adecuada cultura de Seguridad Nacional.

No desaprovecha la oportunidad la ESN-2017 para señalar los riesgos de operar en el ciberespacio cuando añade, un poco más allá:

De manera notable, el desarrollo tecnológico está asociado a una mayor exposición a nuevas amenazas, especialmente las asociadas al ciberespacio. La hiperconectividad actual agudiza algunas de las vulnerabilidades del sistema de seguridad y exige una mejor protección de las redes y sistemas, así como de la privacidad y los derechos digitales del ciudadano. España debe adaptarse a esta transformación permanente con un mayor esfuerzo de digitalización y tecnificación del Estado y la sociedad, basado en un sistema educativo y de formación adaptado a la nueva realidad.

Más allá de las líneas de acción estratégicas que en materia de ciberseguridad recoge la ESN-2017, el señalamiento de los intereses nacionales, los objetivos perseguidos y las líneas de acción para alcanzarlos se explicitan en la vigente Estrategia de Ciberseguridad Nacional (ECSN), texto hecho público el 5 de diciembre de 2013 a instancias del Consejo de Seguridad Nacional, y cuyo propósito es: «Fijar las directrices generales del uso seguro del ciberespacio, impulsando una visión integradora cuya aplicación ayude a garantizar a nuestra nación su seguridad y progreso, a través de la adecuada coordinación y cooperación de todas las Administraciones Públicas entre ellas, con el sector privado y con los ciudadanos. Todo ello dentro del máximo respeto a los principios recogidos en la Constitución; en las disposiciones de la Carta de Naciones Unidas, relativas al mantenimiento de la paz y seguridad internacional; en coherencia con la Estrategia de Seguridad Nacional y con iniciativas desarrolladas en el marco europeo, internacional y regional».

Como hemos mencionado en otros trabajos (7), la ECSN señala seis objetivos sectoriales y ocho líneas de acción para alcanzarlos. Unos y otras persiguen: «Lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, y respuesta a los ciberataques».

Los cuadros siguientes muestran los Objetivos de la ECSN y sus Líneas de Acción.

(7) Galán Cordero, C. y Galán Pascual, C. «La ciberseguridad pública como garantía del ejercicio de derechos». *Revista Derecho y Sociedad*, núm. 47, PUCP, 2016.

Objetivo Global: ***Política de Ciberseguridad***	Lograr que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección, y respuesta a los ciberataques.
Objetivo I: ***Administraciones Públicas***	Garantizar que los Sistemas de Información y Telecomunicaciones que utilizan las Administraciones Públicas poseen el adecuado nivel de ciberseguridad y resiliencia.
Objetivo II: ***Sector privado e Infraestructuras Críticas***	Impulsar la seguridad y resiliencia de los Sistemas de Información y Telecomunicaciones usados por el sector empresarial en general y los operadores de Infraestructuras Críticas en particular.
Objetivo III: ***Ámbito judicial y policial***	Potenciar las capacidades de prevención, detección, re- acción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio.
Objetivo IV: ***Sensibilización***	Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio.
Objetivo V: ***Capacitación***	Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad.
Objetivo VI: ***Ámbito Internacional***	Contribuir a la mejora de la ciberseguridad en el ámbito internacional.

Objetivos de la Estrategia de Ciberseguridad Nacional de 2013

LÍNEA DE ACCIÓN 1 ***Capacidad de prevención, detección, respuesta y recuperación ante las ciberamenazas***	Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional.
LÍNEA DE ACCIÓN 2 ***Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Administraciones Públicas***	Garantizar la implantación del Esquema Nacional de Seguridad, reforzar las capacidades de detección y mejorar la defensa de los sistemas clasificados.
LÍNEA DE ACCIÓN 3 ***Seguridad de los Sistemas de Información y Telecomunicaciones que soportan las Infraestructuras Críticas***	Impulsar la implantación de la normativa sobre Protección de Infraestructuras Críticas y de las capacidades necesarias para la protección de los servicios esenciales.
LÍNEA DE ACCIÓN 4 ***Capacidad de investigación y persecución del ciberterrorismo y la ciberdelincuencia***	Potenciar las capacidades para detectar, investigar y perseguir las actividades terroristas y delictivas en el ciberespacio, sobre la base de un marco jurídico y operativo eficaz.

LÍNEA DE ACCIÓN 5 ***Seguridad y resiliencia de las TIC en el sector privado***	Impulsar la seguridad y la resiliencia de las infraestructuras, redes, productos y servicios empleando instrumentos de cooperación público-privada.
LÍNEA DE ACCIÓN 6 ***Conocimientos, Competencias e I+D+i***	Promover la capacitación de profesionales, impulsar el desarrollo industrial y reforzar el sistema de I+D+i en materia de ciberseguridad.
LÍNEA DE ACCIÓN 7 ***Cultura de ciberseguridad***	Concienciar a los ciudadanos, profesionales y empresas de la importancia de la ciberseguridad y del uso responsable de las nuevas tecnologías y de los servicios de la Sociedad de la Información.
LÍNEA DE ACCIÓN 8 ***Compromiso Internacional***	Promover un ciberespacio internacional seguro y confiable, en apoyo a los intereses nacionales.

Líneas de Acción de la Estrategia de Ciberseguridad Nacional de 2013

4. LA SEGURIDAD Y LA CIBERSEGURIDAD EN EL ORDENAMIENTO JURÍDICO

El término «seguridad», obedeciendo a su carácter polisémico y multidisciplinar, aparece en infinidad de textos políticos, estratégicos y jurídicos, de dispares objetivos y alcances, presentándose siempre como un deseo, una pretensión… cuando no como derecho.

Así aparece, por ejemplo y ciñendo nuestro discurso al ámbito español, en el artículo 17 (Derecho a la libertad y a la seguridad) de nuestra Constitución, cuando afirma: «Toda persona tiene derecho a la libertad y a la seguridad. Nadie puede ser privado de su libertad, sino con la observancia de lo establecido en este artículo y en los casos y en la forma previstos en la ley.», concretándose parcialmente en el artículo 51 (Defensa de los consumidores y usuarios), cuando señala: «1. Los poderes públicos garantizarán la defensa de los consumidores y usuarios, protegiendo, mediante procedimientos eficaces, la seguridad, la salud y los legítimos intereses económicos de los mismos.»

Aunque sin mencionarlo explícitamente, el amplio concepto de «seguridad» se esconde también en los artículos 18 (derecho a la intimidad y al tratamiento informatizado de datos), 24 (tutela efectiva de jueces y tribunales), 39 (protección social, económica y jurídica de la familia) de nuestra Carta Magna. Es precisamente el citado artículo 18 –cuya literalidad refiere la pretensión de adecuación e idoneidad de la informática en los tratamientos de los datos personales–, al que debe atribuirse jurídicamen-

te un primer acercamiento nacional al término «ciberseguridad» del que más tarde hablaremos.

Como era previsible, más amplio y detallado es el desarrollo que se hace del concepto en estudio en la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. Ya en su preámbulo puede leerse: «La seguridad constituye la base sobre la cual una sociedad puede desarrollarse, preservar su libertad y la prosperidad de sus ciudadanos, y garantizar la estabilidad y buen funcionamiento de sus instituciones.»

Es en este texto en el que, de forma explícita, se referencia un nuevo ámbito de aplicación de la seguridad: **el ciberespacio.** Efectivamente, sigue diciendo el Preámbulo: «Por otro lado, la realidad demuestra que los desafíos para la Seguridad Nacional que afectan a la sociedad revisten en ocasiones una elevada complejidad, que desborda las fronteras de categorías tradicionales como la defensa, la seguridad pública, la acción exterior y la inteligencia, así como de otras más recientemente incorporadas a la preocupación por la seguridad, como el medio ambiente, la energía, los transportes, el ciberespacio y la estabilidad económica.»

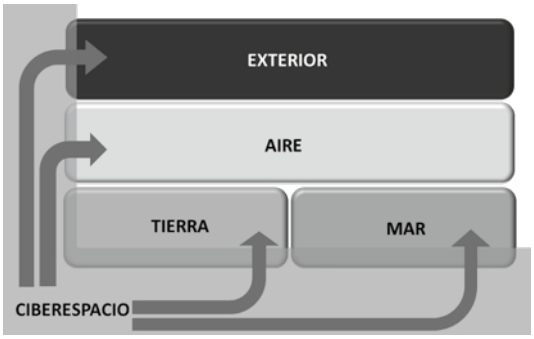
La consideración del ciberespacio como un componente de primer orden en la construcción y mantenimiento de la seguridad se pone claramente de manifiesto en el artículo 10 (Ámbitos de especial interés de la Seguridad Nacional) del citado cuerpo legal, cuando afirma: «Se considerarán ámbitos de especial interés de la Seguridad Nacional aquellos que requieren una atención específica por resultar básicos para preservar los derechos y libertades, así como el bienestar de los ciudadanos, y para garantizar el suministro de los servicios y recursos esenciales. A los efectos de esta ley, serán, entre otros, la ciberseguridad, la seguridad económica y financiera, la seguridad marítima, la seguridad del espacio aéreo y ultraterrestre, la seguridad energética, la seguridad sanitaria y la preservación del medio ambiente.»

Efectivamente, como acertadamente señala Robles Carrillo, M.: «El ciberespacio no solo es una realidad diferente, sino que también es una realidad capacitada para alterar la naturaleza y el funcionamiento de la realidad no virtual» (8). El ciberespacio (realidad artificial) constituye un escenario táctico, estratégico y operativo diferente de los espacios terrestre, marítimo, aéreo y exterior (realidades naturales), que ha sido calificado por la doctrina, como uno de los *Global Commons* (9).

---

(8) Robles Carrillo, M. «El Ciberespacio y la Ciberseguridad: consideraciones sobre la necesidad de un modelo jurídico». Instituto Español de Estudios Estratégicos, núm. 124/2015.

(9) Gómez de Ágreda, A., «Global Commons en la era de la incertidumbre», *Boletín de Información del CESEDEN*, n.º 317, 2010.



La influencia del ciberespacio en los Global Commons naturales

Examinando la cuestión desde el punto de vista sectorial, la (ciber) seguridad, en su condición de **bien público** (como lo es la seguridad ciudadana o la seguridad nacional) (10), constituye también una obligación para las competencias y actuaciones del Sector Público. Así lo recoge el artículo 3 (Principios generales) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, cuando prescribe: «2. Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados.», exigencia que se concreta parcialmente en su artículo 38 (Sede electrónica), cuando, en relación con los requisitos que debe poseer toda sede electrónica administrativa, exige expresamente, la conformidad con los principios de «transparencia, publicidad, responsabilidad, calidad, seguridad, disponibilidad, accesibilidad, neutralidad e interoperabilidad.» Hacemos notar al lector la aparición en este precepto del término **«disponibilidad»** que, como más adelante se verá, resulta crucial para el objetivo perseguido por este trabajo.

Sigue la citada norma considerando la (ciber)seguridad en distintos preceptos: artículos 44 (Intercambio electrónico de datos en entornos cerrados de comunicación), 46 (Archivo electrónico de documentos), 155 (Transmisiones de datos entre Administraciones Públicas), 156 (Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad), 157 (Reutilización de

(10) Véase: Asllani, A., White, Ch. S. y Ettkin, L., «Viewing Cybersecurity As A Public Good: The Role Of Governments, Businesses, And Individuals», *Journal of Legal, Ethical and Regulatory Issues*, vol. 16, n.º 1, 2013.

sistemas y aplicaciones de propiedad de la Administración), 158 (Transferencia de tecnología entre Administraciones), entre otros.

Por su parte, la seguridad jurídica perseguida por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, fundamento esencial de la actividad administrativa, también sustenta su desarrollo en la ciberseguridad, tal y como señala su artículo 13 (Derechos de las personas en sus relaciones con las Administraciones Públicas), cuando recoge, entre otros derechos: «h) A la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.», exigencia contenida asimismo en el artículo 16 (Registros), 17 (Archivo de documentos) y 31 (Cómputo de plazos en los registros), entre otros.

No es ajena la actividad legislativa europea a la problemática de la ciberseguridad, muy al contrario. Significativos son los textos jurídicos emanados de las instituciones europeas que tratan esta cuestión y evidencian –una vez más– la necesidad de garantizar la ciberseguridad de los sistemas de información europeos para el adecuado desarrollo político, económico y social de los estados, poniendo especial énfasis en los sistemas de información que gestionan sectores estratégicos o esenciales, cuya pérdida, deterioro o indisponibilidad, conllevaría un enorme impacto negativo para sus sociedades o colectivos destinatarios.

Así se expresa la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. Esta norma, que al tiempo de redactar estas líneas está siendo transpuesta al ordenamiento jurídico nacional, contempla la exigencia de la aplicación de medidas de seguridad a los **operadores de servicios esenciales** de siete sectores (energía, transporte, banca, infraestructuras de los mercados financieros, sector sanitario, suministro y distribución de agua potable e infraestructura digital), sectores a los que se les unirán otros en la futura norma nacional (las AA. PP., por ejemplo), así como a los **proveedores de servicios digitales** relacionados con los mercados en línea, motores de búsqueda en línea y servicios de computación en la nube.

No obstante, con anterioridad a esta importante regulación, la Unión Europea ya dejaba clara su preocupación por la seguridad física y lógica de las denominadas Infraestructuras Críticas, publicando la Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, de la que ha traído causa la Ley 8/2011, de 28 de abril, de Medidas para la Protección de las Infraestructuras Críticas.

No debemos olvidar en esta necesariamente incompleta enumeración, y prescindiendo de la todavía vigente normativa nacional en materia de protección de datos, al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) y, en su consecuencia, a la nueva ley orgánica nacional de protección de datos que se publicará complementariamente, cuyo primer borrador ya ha sido difundido al tiempo de redactar estos párrafos.

Aunque la codificación de los derechos a la privacidad y a la protección de datos viene a regular significativos aspectos de la seguridad de la información (la confidencialidad y, en menor medida, la integridad de los datos tratados), derechos elevados incluso a la categoría de fundamentales (art. 18 de la Constitución), no tratan sin embargo todos los elementos en cuestión, olvidando componentes que consideramos cruciales, entre ellos: **la disponibilidad de los sistemas de información.** Más adelante insistiremos sobre ello.

Por último, y constituyendo probablemente la norma nacional que, de modo integral y con mayor detalle ha tratado la seguridad de la información, no debemos olvidar el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (ENS).

El ENS, como anuncia el artículo 156 de la Ley 40/2015, de 1 de octubre –norma de la que hereda por novación ámbito subjetivo de aplicación–, tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos, estando constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada, debiendo ser aplicado a los sistemas de información de las entidades de su ámbito de aplicación para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestionen en el ejercicio de sus competencias.

5. LAS DIMENSIONES DE LA CIBERSEGURIDAD

Como hemos señalado, la seguridad de la información, tal y como la define el ENS, es la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Así pues, la seguridad de estos sistemas (la ciberseguridad) es un concepto poliédrico que puede estudiarse desde diferentes puntos de vista, atendiendo precisamente a las garantías exigibles a la información tratada o los servicios que deben ser especialmente preservados.

La figura siguiente muestra un esquema de tales principios o **dimensiones** de la ciberseguridad.

Dimensiones de la seguridad

El ENS –siguiendo la metodología MAGERIT de análisis y gestión de riesgos (11)– define cinco dimensiones de seguridad: Confidencialidad, Integridad, Autenticidad, Trazabilidad y Disponibilidad, a las que nosotros hemos añadido una más, de carácter genérico: Conformidad Legal.

El cuadro siguiente muestra las definiciones de estas dimensiones, así como su aplicabilidad a la información tratada o a los servicios prestados por los sistemas de información de que se trate.

DIMENSIÓN	DEFINICIÓN	APLICABILIDAD
Confidencialidad	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.	Información
Integridad	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.	Información
Autenticidad	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.	Información y Servicios

(11) Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#. Wj5K7LpFxdg

DIMENSIÓN	DEFINICIÓN	APLICABILIDAD
Trazabilidad	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.	Información y Servicios
Disponibilidad	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.	Información y Servicios
Conformidad Legal	Propiedad o característica de las herramientas, soluciones o servicios que sustentan las operaciones, para mantenerse permanentemente alineados con lo dispuesto en la legislación nacional e internacional que resulte de aplicación.	Servicios

Dimensiones de la Seguridad de la Información

6. DEL DERECHO DE ACCESO AL DERECHO A LA CIBERSEGURIDAD

Significativos trabajos han analizado la posibilidad de incluir el acceso a Internet como un derecho (prescindamos, por el momento, de adjetivo alguno) de las personas, en tanto que individuos inmersos en la denominada Sociedad de la Información, realidad que, como hemos señalado, ya no es posible soslayar.

Efectivamente, como acertadamente señala Barrio Andrés (12), y aun cuando no parece existir un consenso suficiente, los últimos años han venido siendo testigos de la conceptuación doctrinal del derecho de acceso a Internet como derecho fundamental (13). La argumentación dada para sustentar tan significativa adscripción ha sido, con sus matices, siempre la misma: ya no es posible concebir una adecuada implicación del hombre en su entorno político, social o económico, al margen de Internet y de las posibilidades que ofrece. Esta adscripción ha sido igualmente tratada y aceptada en la Declaración Conjunta sobre Libertad de Expresión e Internet (14).

Naturalmente, el derecho de acceso a Internet debe concretarse un poco más, exigiéndose, como requisitos para su adecuado ejercicio, la garantía del mantenimiento de la velocidad y la capacidad de tal acceso (15).

(12) Barrio Andrés, M. «El acceso a Internet como elemento cardinal del servicio universal de telecomunicaciones», en *Los Retos del Estado y la Administración en el Siglo xxi – Libro Homenaje al Profesor Tomás de la Quadra-Salcedo Fernández del Castillo*. Ed. Tirant lo Blanch. 2017

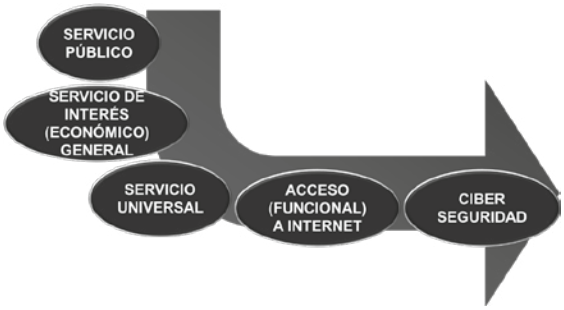
(13) Véase, por ejemplo: De Hert, P., «Internet (access) as a new fundamental night. Inflating the current rights framenork?» *European Journal of Law and Technology*, Vol. 3, 2012.

(14) Organization for Security and Co-operation in Europe (OSCE), 1 junio 2011.

(15) Este concepto de «Acceso funcional a Internet» fue puesto de manifiesto en la Directiva 2002/22/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa al servicio

Siendo sin duda importante esta aproximación, nos parece, sin embargo, insuficiente.

Si, como es sabido, casi cualquier actividad que podamos desarrollar en Internet está sustentada en uno o varios sistemas de información (ordenadores y redes de comunicaciones, hardware y software) de diferentes prestadores de servicios, de poco serviría la garantía de un acceso (incluso, *funcional,* expresado en términos de capacidad y velocidad adecuadas y suficientes) a Internet si el sistema de información del prestador del servicio en cuestión no dispusiera de las debidas garantías de seguridad, expresadas en función de las dimensiones definidas con anterioridad: confidencialidad, integridad y disponibilidad, especialmente.



Recorrido de los derechos tecnológicos

7. CONCLUSIONES

Así pues, admitiendo que Internet constituye un elemento esencial para el desarrollo del ser humano y para garantizar el disfrute efectivo de derechos tales como la libertad de expresión, el derecho a la educación, la atención a la salud y el trabajo o el derecho de reunión y asociación –como apunta el documento de la OSCE antes citado–, no debemos limitar nuestras aspiraciones al mero reconocimiento de un pretendido «derecho de acceso» que, llegado el caso y por lo dicho, podría resultar inútil a la postre. Debemos dar un paso más allá: es necesario asegurar que los servicios accedidos, cuando se encuentren sustentados en sistemas de información, gocen de las adecuadas garantías de seguridad y resiliencia.

Habiendo concretado la ciberseguridad a través de sus dimensiones constituyentes (integridad, confidencialidad, autenticidad, trazabilidad y disponibilidad), el legislador, consciente de la problemática asociada a

universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal).

cada una de ellas, ha venido regulando la garantía de su observancia, aunque con diferente grado de intensidad –y acierto, habría que decir–. Así, las dimensiones *integridad, autenticidad y trazabilidad* han sido significativamente reguladas por la legislación nacional (Ley 59/2003, de 19 de diciembre, de Firma Electrónica, entre otras) y europea (por todas, el Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE), en lo tocante a la identificación electrónica de personas físicas y jurídicas y la prestación de servicios de confianza (16).

Por su parte, las dimensiones *confidencialidad* (y, parcialmente, *integridad*) han constituido el leitmotiv de las regulaciones en materia de Privacidad y Protección de Datos (por todas, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE-Reglamento general de protección de datos).

Finalmente, la dimensión *disponibilidad* constituye el eje central de los principios del Real Decreto 3/2010 (Esquema Nacional de Seguridad), cuyo ámbito de aplicación se extiende a las entidades del Sector Público, la Ley 8/2011 (Medidas de Protección de Infraestructuras Críticas) y la ley nacional que finalmente trasponga la Directiva (UE) 2016/1148, de aplicación a los operadores de servicios esenciales y proveedores de servicios digitales.

Así pues, creemos que con todo lo dicho –y su necesaria brevedad–, debe quedar claro que, pese a constituir un eslabón necesario, el derecho de acceso a internet no puede erigirse en un derecho humano finalista. Más aún, como hemos señalado, el acceso a internet debe ir necesariamente acompañado de un derecho a la ciberseguridad que lo haga plenamente efectivo.

Es, por consiguiente, labor esencial de los poderes públicos, articulados a través del Consejo Nacional de Ciberseguridad (17), hacer efectivo tal derecho, construyendo y abonando una regulación coherente e inte-

(16) Al tiempo de redactar estas líneas, se encuentra en fase de redacción final una nueva norma nacional en materia de identificación electrónica y servicios de confianza que, trayendo casusa del Reglamento 910/2014, derogará a la mencionada Ley 59/2003.

(17) El Consejo de Ciberseguridad Nacional es un órgano colegiado de apoyo al Consejo de Seguridad Nacional en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, en el marco de la Ley 50/1997, de 27 de noviembre, del Gobierno, habiéndose creado por Acuerdo del Consejo de Seguridad Nacional del 5 de diciembre de 2013, modificado por Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad.

gradora, articulando una esencial –y muchas veces olvidada– cooperación público-privada, diseñando programas de I+D+i, formativos y de concienciación realistas y garantizando la cooperación internacional con nuestros socios y aliados. Aprovechemos el reto de la actualización de la Estrategia de Ciberseguridad Nacional para seguir insistiendo en el camino correcto.

Cualquier otro acercamiento –creemos– no daría adecuada respuesta a la siempre tozuda realidad.

CAPÍTULO 28

DE LA CIBERDEFENSA A LAS ARMAS AUTÓNOMAS LETALES

ANTONIO SEGURA SERRANO
Profesor Titular de Derecho Internacional Público
Universidad de Granada

1. INTRODUCCIÓN

La ciberseguridad global es un desafío para las sociedades modernas, ya que existe una maraña de ciberamenazas a las que se debe hacer frente de forma incremental dedicando un cada vez más importante conjunto de recursos humanos y materiales (1). Entre esas amenazas está la ciberguerra. Aunque aún no se ha materializado un ataque armado a través del ciberespacio o, al menos, no se ha invocado formalmente una violación del principio de prohibición del uso de la fuerza por parte de ningún Estado (2), es evidente que los Estados deben poner en marcha estrategias de ciberdefensa que les permitan estar preparados para actuar frente a las acciones ofensivas que se materialicen a través del ciberespacio. España ya ha adoptado una iniciativa clara en este sentido dentro de la Estrategia

(1) SEGURA SERRANO, A. y GORDO GARCÍA, F. (eds.): *Ciberseguridad global: oportunidades y compromisos en el uso del ciberespacio*, Editorial Universidad de Granada, Granada, 2013.
(2) SEGURA SERRANO, A.: «Ciberseguridad y Derecho Internacional», *Revista Española de Derecho Internacional*, vol. LXIX, n.º 2, 2017, p. 294.

de Seguridad Nacional, en el marco de su nítida actitud de cooperación europea e internacional dentro de este ámbito (3).

Desde un punto de vista conceptual, la ciberdefensa se configura como el conjunto de ciber-capacidades que un Estado pone en marcha para hacer frente a los posibles ataques externos que tienen su origen en la actividad de otros Estados. Por tanto, desde el punto de vista jurídico se trataría de extrapolar al plano del ciberespacio todo el andamiaje construido en torno a la legítima defensa regulada en la actualidad en el artículo 51 de la Carta de la ONU. Aunque este cuerpo normativo se creó para regular las relaciones entre Estados, es cierto que recientemente se plantea con cada vez más insistencia si resulta posible su aplicación a los entes no estatales, como los grupos terroristas.

No existe aún un cuerpo normativo creado expresamente para regular las actividades estatales relativas a la ciberdefensa. En efecto, la única alternativa hoy día es la consistente en aplicar el Derecho internacional y, en concreto, el derecho que regula el uso de la fuerza y los conflictos armados, a las actividades que se llevan a cabo en el ciberespacio. Esto es precisamente lo que se ha hecho a través del proyecto conocido como Manual de Tallin, por el que un conjunto de expertos ha tratado de recopilar en el mismo las reglas que resultarían de la adaptación del Derecho internacional actual a su aplicación en el ciberespacio (4).

Una de las características que presenta el ciberespacio en materia de defensa es la creciente dependencia del desarrollo de capacidades en inteligencia artificial. Lo que cabe esperar en este ámbito es una mayor utilización de complejos tipos de software que permitan reaccionar al sistema defensivo de forma autónoma o casi autónoma. En ese sentido, la ciberdefensa presenta hoy día una problemática muy similar a la que se plantea con relación a las armas autónomas letales (5), en inglés, *lethal autonomous weapons,* o también conocidos como los *killer robots,* y la posible respuesta legal ante ambos fenómenos debería ser compatible (6).

---

(3) Segura Serrano, A.: «Estrategia española de ciberseguridad: análisis comparado», en J. Roldán Barbero (dir.), *La seguridad nacional de España: Un enfoque geoestratégico*, Tirant, Valencia, 2017, pp. 521-553.

(4) Schmitt, M. N. (ed.): *Tallin Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013.

(5) United Nations Institute for Disarmament Research: *The Weaponization of Increasingly Autonomous Technologies: Autonomous Weapons Systems and Cyber Operations*, UNIDIR Resources n.º 7, Geneva, 2017, p. 5; véase Guarino, A.: «Autonomous Intelligent Agents in Cyber Offence», en K. Podins, J. Stinissen, M. Maybaum (eds.), *5th International Conference on Cyber Conflict*, NATO CCD COE Publications, 2013, p. 379, que señala «*Autonomous intelligent agents can be purely software, or integrated into a physical system ('robots')–the difference lies mainly in the environment in which the agent operates: while purely software agents live in what we call 'cyberspace', robots can sense and interact with the same physical environment that we live in. … [T]he similarities between software agents and robots are relevant, given that even in a robot the embedded software … is at the heart of its behaviour and capabilities*».

(6) Messinger, E.: «Is It Possible to Ban Autonomous Weapons in Cyberwar?», *Just Security*, en https://www.justsecurity.org/19119/ban-autonomous-weapons-cyberwar/.

Las armas autónomas letales han sido objeto de atención creciente en los últimos años por parte de la comunidad internacional. En este sentido, existen dos bandos claramente enfrentados, unos a favor y otros en contra del desarrollo y despliegue de este tipo de armas. Inicialmente, el Relator Especial de la ONU en materia de ejecuciones extrajudiciales, sumarias o arbitrarias, Phillip Alston (7), ya advirtió sobre el hecho de que un incremento en la autonomía de las armas provocaría una importante dificultad a la hora de aplicar los marcos jurídico-internacionales existentes sobre responsabilidad estatal e individual. Por estas razones, el siguiente Relator Especial de la ONU en esta misma materia, Christof Heyns, ha hecho un «llamamiento a hacer una pausa que permita examinar la cuestión a nivel internacional de manera seria y racional» (8). Por el contrario, hay una buena parte de la doctrina, principalmente la vinculada con el ejército estadounidense, que se ha mostrado favorable a estas armas, por las ventajas estratégicas y militares que presentan (9). No obstante, el debate sobre estas armas se ha propagado a nivel internacional propiamente tras la publicación de un informe de *Human Rights Watch* en el que se pide la prohibición absoluta de estas armas autónomas letales (10). De forma casi coetánea, el gobierno de Estados Unidos ponía de manifiesto su posición respecto del desarrollo de estas armas (11).

El informe de *Human Rights Watch* ha propulsado la puesta en marcha de una campaña global por la abolición de estas armas denominada *Stop Killer Robots* (12). A partir de aquí, Organizaciones Internacionales (13),

(7) United Nations, General Assembly: Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston, A/HRC/14/24/Add.6, 28 May 2010; Naciones Unidas, Asamblea General: Informe provisional del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias, Philip Alston, A/65/321, 23 de agosto de 2010.

(8) Naciones Unidas, Asamblea General: Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias, A/HRC/23/47, 9 de abril 2013, apartado 33.

(9) Schmitt, M. N. y Thurnher, J. S., «*Out of the Loop*: Autonomous Weapons Systems and the Law of Armed Conflict», *Harvard National Security Journal*, Vol. 4, 2013, pp. 231-281; Sassòli, M.: «Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified», *International Law Studies*, *Naval War College*, Vol. 90, 2014, p. 310; Boothby, W. H.: *Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors*, TMC Asser Press, 2014, pp. 104-7.

(10) Human Rights Watch and International Human Rights Clinic (Harvard Law School): *Losing Humanity. The Case against Killer Robots*, 19 November 2012.

(11) United States, Department of Defense: Directive, Number 3000.09, Autonomy in Weapon Systems, November 21, 2012.

(12) Stop Killer Robots: «Urgent Action Needed to Ban Fully Autonomous Weapons. Non-governmental organizations convene to launch Campaign to Stop Killer Robots», 23 April 2013, en http://stopkillerrobots.org/wp-content/uploads/2013/04/KRC_LaunchStatement_23Apr2013.pdf.

(13) Parlamento Europeo: *Resolución del Parlamento Europeo sobre el uso de drones armados*, 2014/2567(RSP)), 25 de febrero de 2014, párrafo H(2)(d), en http://justsecurity.org/wp-content/uploads/2014/02/European-Parliament-Resolution-Drones.pdf.

otras ONGs (14), movimientos de la sociedad civil (15), y gobiernos se han ido sumando a la movilización general, a favor o en contra, de estas armas (16). Finalmente, ha sido en el marco de la Convención de Naciones Unidas sobre Ciertas Armas Convencionales en donde se ha concretado la puesta en marcha de un diálogo para el tratamiento de esta cuestión. Tras las reuniones informales habidas en los años 2014-2016 (17), los Estados parte en esta Convención han decidido establecer un Grupo de Expertos Gubernamentales de carácter abierto, con el objetivo de explorar las posibles recomendaciones y opciones en relación con las armas autónomas letales (18). El establecimiento de este Grupo de Expertos supone la confirmación oficial de la importancia que ha adquirido esta cuestión en el plano internacional, así como el compromiso más o menos implícito de los Estados parte en la Convención de avanzar, aunque con prudencia, hacia la regulación internacional de esta materia. Este Grupo se ha reunido en Ginebra en noviembre de 2017 y ha adoptado un primer informe que recoge conclusiones y recomendaciones (19). Está previsto que se vuelva a reunir en abril de 2018 para continuar con su trabajo (20).

2. DEFINICIÓN DE ARMAS AUTÓNOMAS LETALES

La definición de lo que constituye un arma autónoma letal es una de las cuestiones problemáticas más sugestivas que se han planteado en tor-

---

(14) Véase la petición de prohibición por parte de la ONG denominada Article 36 realizada ya en 2012, Article 36: *Ban autonomous armed robots*, March 5, 2012, en http://www.article36.org/statements/ban-autonomous-armed-robots/.

(15) Esta movilización de la sociedad civil ha tenido varios momentos álgidos. Por un lado, en una Carta Abierta de 2015, un grupo de expertos muy cualificado en el ámbito de la robótica y la inteligencia artificial, liderado por Stephen Hawking, ya se hace eco de las cuestiones jurídicas y éticas más importantes en relación con las armas autónomas letales, Future of Life Institute: *Research Priorities for Robust and Beneficial Artificial Intelligence*, 28 July 2015, en https://futureoflife.org/ai-open-letter/. Por otro lado, en otra Carta Abierta de 2017, firmada por los fundadores y directores ejecutivos de empresas del ámbito de la robótica y la inteligencia artificial, liderada por Elon Musk, se pide a los Estados que forman de la Convención sobre Ciertas Armas Convencionales que eviten una carrera de armamentos en este ámbito, véase Future of Life Institute: *An Open Letter to the United Nations Convention on Certain Conventional Weapons*, 21 August 2107, en https://futureoflife.org/autonomous-weapons-open-letter-2017/; Por último, el *International Committee for Robot Arms Control* ya había emitido un llamamiento en favor de esta prohibición en 2009: https://www.icrac.net/statements/.

(16) Véase la cronología de eventos y posiciones de distintas organizaciones elaborada por Stop Killer Robots: *Chronology*, https://www.stopkillerrobots.org/chronology/.

(17) Véase los documentos CCW/MSP/2014/3, CCW/MSP/2015/3, y CCW/CONF. V/2, respectivamente.

(18) Fifth Review Conference of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects: Final Document of the Fifth Review Conference, CCW/CONF. V/10, 23 December 2016, p. 9.

(19) Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects: Report of the 2017 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS), CCW/GGE.1/2017/CRP.1, 20 November 2017.

(20) Reaching Critical Will: *2018 CCW Group of Governmental Experts on lethal autonomous weapon systems*, en http://www.reachingcriticalwill.org/disarmament-fora/ccw/2018/laws.

no al debate sobre estas armas. Para intentar acotar progresivamente dicha definición, sería importante recordar las ventajas y los inconvenientes que se han identificado en torno al uso de estas armas. En cuanto a las primeras, se ha señalado que estas armas presentan la ventaja estratégica de la velocidad en el acopio y procesamiento de la información; la flexibilidad, rapidez y precisión en la toma de decisiones y en la elección del objetivo; la posibilidad de asumir tareas aburridas, sucias y peligrosas; la ausencia de emociones o interés propio que pueden conducir en general a resultados menos dañinos (21); así como la reducción de los riesgos para el personal militar, en el entendido de que se salvaguardarían vidas humanas al reemplazar a los soldados de carne y hueso (22). En cuanto a las amenazas que presentan estas armas, se ha sostenido que esta tecnología podría proliferar y ser objeto de abuso; que estas armas pueden ser imperfectas y funcionar mal; que pueden dar lugar a una lucha asimétrica e injusta si una parte las posee y la otra no; y, por último, la ausencia de emociones humanas, como la compasión o la misericordia (23).

A partir de ahí surge una variedad de aproximaciones que determina la ausencia de un entendimiento común sobre lo que es un arma autónoma letal (24). Desde un punto de vista sustancial, existe una diferencia radical de enfoque entre, por un lado, quienes entienden que las armas autónomas permiten hacer la guerra cada vez de forma más moral y conforme a Derecho, por lo que el advenimiento de estas armas es inevitable y cualquier intento de prohibirlas será inútil (25). Por otro lado, están quienes, planteándose de forma problemática la expansión de las tecnologías y racionalidades militarizadas, discrepan sobre la inevitabilidad de estas armas, y están a favor de una prohibición preventiva como modo de controlar los futuros desarrollos tecnológicos en este ámbito (26). Por esa razón, el Grupo de Expertos Gubernamentales se ha planteado como uno

(21) Boothby, W. H.: *Conflict Law: The Influence of New Weapons Technology, Human Rights and Emerging Actors*, *op. cit.*, pp. 104-7; Sassòli, M.: «Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified», *loc. cit.*, p. 310.

(22) International Committee of the Red Cross: *Autonomous weapons systems: technical, military, legal and humanitarian aspects*, Geneva, 2014, p. 9.

(23) Weizmann, N.: *Autonomous Weapon Systems under International Law*, Geneva Academy of International Humanitarian Law and Human Rights, 2014, pp. 4-5.

(24) Brehm, M.: *Defending the Boundary – Constraints and Requirements on the Use of Autonomous Weapons Systems under International Humanitarian and Human Rights Law*, Geneva Academy of International Humanitarian Law and Human Rights, Academy Briefing N.º 9, 2017, p. 13.

(25) Anderson, K. y Waxman, M.: *Law and Ethics for Autonomous Weapon Systems – Why a Ban Won't Work and How the Laws of War Can*, Hoover Institution, Stanford University, p. 2.

(26) Sharkey, N. E.: «The Evitability of Autonomous Robot Warfare», *International Review of the Red Cross*, n.º 94, 2012, p. 787; Zawieska, K.: «An ethical perspective on autonomous weapons systems», en UNODA, *Perspectives on Lethal Autonomous Weapons*, UNODA Ocassional Papers, núm. 30, 2017, p. 51.

de sus objetivos el relativo a la caracterización de estas armas con el fin de promover ese entendimiento común (27).

En relación con la cuestión definicional, es posible en teoría operar con tres enfoques distintos: el enfoque tecnológico, el humano y el funcionalista (28). No obstante, en la práctica se han identificado dos construcciones básicas, y opuestas, de autonomía con relación a las armas autónomas, que giran en torno a las propuestas realizadas desde los gobiernos del Reino Unido y de Estados Unidos, respectivamente (29). Por un lado, el Ministerio de Defensa del Reino Unido publicó un documento en 2011 en donde se establecen unos requisitos relativamente exigentes para poder conceptuar un arma como autónoma, en concreto, que el arma tenga el más alto nivel de intencionalidad y que sea capaz de decidir su propio curso de acción (30). Estas exigentes características se derivan también de un documento de la OTAN, que atribuye a estas armas autónomas capacidad de conciencia (verdadera inteligencia artificial) y determinación propia (fruto del auto-aprendizaje) (31). Estos niveles de inteligencia artificial no se encuentran desarrollados en el momento actual, por lo que se dibujan en escenarios más bien futuros que, incluso, podrían no concretarse (32).

Por otro lado, Estados Unidos ha optado por una caracterización amplia de estas armas, que se definen como aquellas «que, una vez activadas, pueden seleccionar y comprometer objetivos sin intervención ulterior de un operador humano» (33). *Human Rights Watch* ha definido estas armas utilizando casi las mismas palabras, etiquetándolas como *human-out-of-the-loop weapons* (34). Y el Comité Internacional de la Cruz Roja ha utilizado una caracterización que puede asimilarse igualmente a las anteriores,

---

(27) Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects: Report of the 2017 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS), *cit.*, p. 4.

(28) United Nations Institute for Disarmament Research: *The Weaponization of Increasingly Autonomous Technologies: Concerns, Characteristics and Definitional Approaches*, UNIDIR Resources n.º 6, Geneva, 2017, p. 19.

(29) Amoroso, D.: «*Jus in bello* and *jus ad bellum* arguments against autonomy in weapons systems: A re-appraisal», *Questions in International Law, Zoom-in*, n.º 43, 2017, p. 8.

(30) United Kingdom, Ministry of Defence, *The UK Approach to Unmanned Aircraft Systems*, Joint Doctrine Note 2/11, 30 March 2011, p. 14, que ha sido objeto de actualización en United Kingdom: Ministry of Defence: *Unmanned Aircraft Systems*, Joint Doctrine Publication 0-30.2, August 2017, p. 13.

(31) Joint Air Power Competence Center (NATO): *Future Unmanned System Technologies. Legal and Ethical Implications of Increasing Automation*, Kalkar, November 2016, p. 9.

(32) United Kingdom: Statement to the Informal Meeting of Experts on Lethal Autonomous Weapons Systems, 11-15 April 2016, p. 2.

(33) United States, Department of Defense: Directive, Number 3000.09, Autonomy in Weapon Systems, *cit.*, pp. 13-14.

(34) Aquí se incluyen aquellos sistemas considerados *human-on-the-loop weapons*, es decir, un operador humano podría anular el sistema, pero en la realidad la supervisión humana es muy limitada por diversas razones, Human Rights Watch and International Human Rights Clinic (Harvard Law School): *Losing Humanity. The Case against Killer Robots*, *op. cit.*, pp. 1-2.

en la medida en que considera a las armas autónomas como «cualquier sistema de armas con autonomía en sus funciones críticas. Es decir, un sistema de armas que puede seleccionar (es decir, buscar o detectar, identificar, rastrear, seleccionar) y atacar (es decir, usar la fuerza en contra, neutralizar, dañar o destruir) objetivos sin intervención humana» (35).

Una definición tan amplia y funcional como ésta presenta dos ventajas. Por un lado, permite incluir en la misma una serie de armas que ya existen en la actualidad (36), por tanto, convierte en reales a las armas autónomas letales, lo que contrasta con la posición de quienes, tanto en contra como a favor de estas armas, consideran que estamos todavía en una etapa muy prematura y que dichas armas forman parte aún de la ciencia ficción (37). Entre los ejemplos de armas actuales que se acomodan a esta definición omnicomprensiva se encuentran las utilizadas de manera defensiva contra misiles o cohetes, tales como el Phalanx, de Estados Unidos; el Iron Dome, de Israel; el Goalkeeper, de los Países Bajos; o el MANTIS, de Alemania. Otros sistemas defensivos son los utilizados por los vehículos con protección activa, como el AMAP-ADS de Alemania, o el LEDS-150 de Sudáfrica. Otros sistemas tienen el carácter de centinela anti-personas, como el aEgis y súper aEgis, desarrollado por Corea del Sur. Finalmente, otros sistemas de perfil ofensivo son los misiles y torpedos, como el AIM-120 de Estados Unidos y el Brimstone del Reino Unido, así como los denominados «merodeadores», tales como el sistema Harpy de Israel, o el TARES de Alemania (38). Por otro lado, esta amplia definición permite afrontar desde ya las cuestiones de tipo ético y jurídico que dichas armas generan, sin tener que esperar a un momento ulterior en que estas armas previsiblemente alcanzarán un mayor estadio de desarrollo (39).

Como ha señalado el Presidente del Grupo de Expertos Gubernamentales, el uso de la tecnología para hacer la guerra no es nada nuevo. Lo que resulta novedoso es la pérdida del control humano (40). En efecto, en la cuestión definicional se ha introducido un nuevo concepto, como es el

(35) International Committee of the Red Cross: *Autonomous Weapon Systems - Implications of Increasing Autonomy in the Critical Functions of Weapons*, Expert Meeting, 15-16 March 2016, p. 8.

(36) Crootof, R.: «The Killer Robots Are Here: Legal And Policy Implications», *Cardozo Law Review*, Vol. 36, 2015, p. 1863.

(37) Véase, respectivamente, Human Rights Watch and International Human Rights Clinic (Harvard Law School): *Losing Humanity. The Case against Killer Robots*, *op. cit.*, p. 3; Schmitt, M. N. y Thurnher, J. S., «*Out of the Loop*: Autonomous Weapons Systems and the Law of Armed Conflict», *loc. cit.*, p. 234.

(38) International Committee of the Red Cross: «Background Paper», *Autonomous Weapon Systems - Implications of Increasing Autonomy in the Critical Functions of Weapons*, Expert Meeting, 15-16 March 2016, pp. 72 y ss.

(39) Amoroso, D.: «*Jus in bello* and *jus ad bellum* arguments against autonomy in weapons systems: A re-appraisal», *loc. cit.*, pp. 10-11.

(40) Gill A. S.: «Introduction», en United Nations Office for Disarmament Affairs: *Perspectives on Lethal Autonomous Weapons*, UNODA Ocassional Papers, núm. 30, New York, 2017, p. 1.

«control humano significativo». Esta idea fue lanzada por la ONG «Article 36» en 2013 (41), y ha sido asumida por la campaña internacional a favor de la prohibición de las armas autónomas (42). Pero, además, este concepto ha empezado a ganar tracción en los debates negociadores en torno a la regulación de estas armas (43), hasta el punto de que el Grupo de Expertos Gubernamentales, sin hacer suyos expresamente estos términos, sí ha asumido la labor relativa a clarificar el «elemento humano» en el uso de la fuerza letal, así como la interacción «hombre-máquina en el desarrollo, despliegue y uso de las tecnologías emergentes en el área de las armas autónomas letales» (44). Esta nueva aproximación podría conseguir evitar las dificultades que giran en torno al concepto de autonomía, en el sentido de que ya no haría falta clarificar qué armas pueden calificarse como autónomas, y la cuestión relevante sería que los operadores humanos deben ejercer un control significativo sobre todas ellas (45). No obstante, no cabe engañarse sobre las posibilidades reales de este nuevo concepto cuando se trata de poner fin al debate relativo a la definición de las armas autónomas. Los contrarios a la prohibición de estas armas ya han señalado, no sin razón, que el problema ahora se traslada a la determinación de cuándo se produce dicho control significativo, sobre el que no hay consenso y que habría que definir (46).

3. LA CUESTIÓN HUMANITARIA

El problema más importante que las armas autónomas letales han planteado desde el punto de vista jurídico-internacional es su capacidad para cumplir con las normas humanitarias, fundamentalmente, el principio de distinción y el principio de proporcionalidad. En efecto, una de las reglas del Derecho internacional humanitario es la que obliga a las partes de un conflicto armado a distinguir entre personas y objetos civiles, por

(41) Article 36: *Killer Robots: UK Government Policy on Fully Autonomous Weapons*, April 2013, p. 1, en http://www.article36.org/wp-content/uploads/2013/04/Policy_Paper1.pdf.

(42) Stop Killer Robots: *Call to Action*, en https://www.stopkillerrobots.org/call-to-action/.

(43) United Nations Institute for Disarmament Research: *The Weaponization of Increasingly Autonomous Technologies: Considering How Meaningful Human Control Might Move the Discussion Forward*, UNIDIR Resources n.º 2, Geneva, 2014, en http://www.unidir.org/files/publications/pdfs/considering-how-meaningful-human-control-might-move-the-discussion-forward-en-615.pdf; Fifth Review Conference of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects, Report of the 2016 Informal Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), CCW/CONF. V/2, 10 June 2016.

(44) Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects: Report of the 2017 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS), *cit.*, p. 4.

(45) Amoroso, D.: «*Jus in bello* and *jus ad bellum* arguments against autonomy in weapons systems: A re-appraisal», *loc. cit.*, p. 12.

(46) Crootof, R.: «A Meaningful Floor for 'Meaningful Human Control'», *Temple International and Comparative Law Journal*, vol. 30, 2016, p. 54.

una parte, y combatientes u objetivos militares, por otra. De manera similar, en el marco del principio de necesidad militar, resulta obligado identificar a las personas *hors de combat* (47) y, por otra parte, se exige el respeto de la regla sobre precauciones en el ataque (48). Quienes proponen la prohibición de las armas autónomas entienden que estas armas difícilmente pueden operar en el pleno respeto del principio de distinción, habida cuenta que carecen de las capacidades sofisticadas de reconocimiento y el sentido común (49) que se exigen en los ambientes de combate contemporáneo, caracterizados por la existencia de conflictos asimétricos y batallas urbanas (50), en donde es necesario realizar análisis de tipo contextual (51). Se defiende, pues, que estas armas son incapaces de cumplir con este principio, en especial en lo relativo a la determinación del momento en que los civiles han podido perder su protección frente a ataques, debido a la asunción de «funciones continuas de combate» o «la participación directa en las hostilidades» (52). Por el contrario, los defensores de estas armas creen que, aun teniendo en cuenta las dificultades para conseguir que las mismas puedan cumplir con el principio de distinción, ello afectaría a sus posibles usos, pero no a su legalidad *per se* (53). Por lo tanto, serían perfectamente legítimas en zonas despobladas sin peligro para los civiles, tales como los desiertos, en el combate aéreo o en el altamar (54).

Respecto del principio de proporcionalidad, como es sabido, exige que la afectación incidental de objetivos de carácter civil, en términos de pérdidas de vidas humanas o daños a bienes civiles, que pueda resultar de un ataque no sea excesiva en relación con la ventaja militar concreta y directa que se ha previsto. Para los opuestos al desarrollo de estas armas se trata, por tanto, de un test básicamente subjetivo que la jurisprudencia internacional ha caracterizado como fundamentado en el principio de la

(47) Sparrow, R.: «Twenty Seconds to Comply: Autonomous Weapon Systems and the Recognition of Surrender, *International Law Studies*, US Naval War College, vol. 91, 2015, p. 699.

(48) Weizmann, N.: *Autonomous Weapon Systems under International Law*, *op. cit.*, p. 15.

(49) Skarkey, N. E.: «The Evitability of Autonomous Robot Warfare», *loc. cit.* pp. 788-789; Grut, C.: «The Challenge of Autonomous Lethal Robotics to International Humanitarian Law», *Journal of Conflict and Security Law*, Vol. 18, 2013, pp. 11-12.

(50) Human Rights Watch and International Human Rights Clinic (Harvard Law School): *Losing Humanity. The Case against Killer Robots*, *op. cit.*, pp. 30 y 34, respectivamente, sobre la distinción y la necesidad militar.

(51) Wagner, M.: «The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapons Systems», *Vanderbilt Journal of Transnational Law*, vol. 47, 2014, p. 1392.

(52) Sobre la dificultad de aplicar estos conceptos, véase International Committee of the Red Cross: *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law*, Geneva, 2009, pp. 33-34.

(53) Schmitt, M. N.: «Autonomous Weapon Systems and International Humanitarian Law: A Reply to the Critics», *Harvard National Security Journal Features*, 2013, p. 11.

(54) Anderson, K., Reisner, D., y Waxman, M.: «Adapting the Law of Armed Conflict to Autonomous Weapon Systems,» *International Law Studies*, US Naval War College, vol. 90, 2014, p. 406.

razonabilidad y que requiere mucho más que un mero análisis de datos cuantitativos (55). Estamos, pues, ante una decisión de naturaleza evaluativa, que exige comparar nociones disimilares, en un tipo de análisis contextual, no reducible a fórmula alguna, que las armas autónomas no pueden realizar por ahora (56). Aunque las armas autónomas puedan hacer estimaciones sobre daños colaterales, lo cierto es que ese tipo de análisis sólo ofrecerá datos en relación con la cantidad de daño, pero no resolverá la cuestión de cuándo estamos ante un daño colateral excesivo (57). Entre otras razones porque esa evaluación debe hacerse con anterioridad y debe seguir siendo válida a lo largo del proceso de despliegue del arma, en el marco de situaciones dinámicas y muy cambiantes (58). Los partidarios de estas armas entienden que ya existen sistemas, como el *collateral damage estimate methodology* (CDEM), que realizan cálculos de proporcionalidad, lo que demuestra que estas armas autónomas ya cumplirían con esta exigencia humanitaria (59). Además, aunque el estadio actual de las armas autónomas no permite realizar evaluaciones completas de proporcionalidad debido a que éste debe incorporar un elevado elemento contextual, no obstante, no debe esperarse de las máquinas más de lo que se exige a los seres humanos, en el sentido de que el objetivo debe ser realizar análisis no perfectos, sino razonables, de proporcionalidad (60). Por otra parte, estos partidarios sostienen que, a la espera de que las armas autónomas puedan realizar evaluaciones completas de proporcionalidad en un futuro próximo (61), estas armas podrían utilizarse para propósitos específicos y ambientes operacionales concretos, como aquellos en donde hay pocos seres humanos o bienes civiles, o incluso en batallas de máquina contra máquina (62).

Por último, además de las normas sobre distinción y proporcionalidad, existe otra regla en Derecho internacional humanitario que se ha conver-

(55) Human Rights Watch and International Human Rights Clinic (Harvard Law School): *Losing Humanity. The Case against Killer Robots*, *op. cit.*, p. 33; Skarkey, N. E.: «The Evitability of Autonomous Robot Warfare», *loc. cit.*, pp. 789-790.

(56) Grut, C.: «The Challenge of Autonomous Lethal Robotics to International Humanitarian Law», *loc. cit.*, pp. 12-13; Boothby, B.: «Autonomous Attack - Opportunity or Spectre?», *Yearbook of International Humanitarian Law*, vol. 16, 2015, p. 83.

(57) Wagner, M.: «The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapons Systems», *loc. cit.*, p. 1398.

(58) Weizmann, N.: *Autonomous Weapon Systems under International Law*, *op. cit.*, p. 15.

(59) Crootof, R.: «The Killer Robots Are Here: Legal and Policy Implications», *loc. cit.*, p. 1877; Kastan, B.: «Autonomous Weapons Systems: A Coming Legal 'Singularity?'», *Journal of Law, Technology and Policy*, 2013, p. 62.

(60) Schmitt, M. N. y Thurnher, J. S., «*Out of the Loop*: Autonomous Weapons Systems and the Law of Armed Conflict», *loc. cit.*, pp. 254-257.

(61) Para una crítica de esta posición, a la que se tilda de «ejercicio imaginativo de ciencia ficción», véase Bhuta, N., Beck, S., y Geiss, R.: «Present Futures: concluding reflections and open questions on autonomous weapons systems», en Bhuta, N. *et al.* (eds.): *Autonomous Weapons Systems*, Cambridge University Press, 2016, p. 352.

(62) Anderson, K. y Waxman, M.: *Law and Ethics for Autonomous Weapon Systems – Why a Ban Won't Work and How the Laws of War Can*, *op. cit.*, 2013, p. 13.

tido en una piedra angular en relación con la consideración de la juridicidad de estas armas autónomas, la denominada como Cláusula Martens. Se trata de un principio con carácter consuetudinario que ha quedado reflejado en el Protocolo Adicional I a los Convenios de Ginebra en el sentido de que, en ausencia de regulación específica, «las personas civiles y los combatientes quedan bajo la protección y el imperio de los principios del Derecho de gentes derivados de los usos establecidos, de los principios de humanidad y de los dictados de la conciencia pública». Por una parte, derivado de esta Cláusula Martens, se encuentra el principio de humanidad que ha adquirido así relevancia jurídica como límite en el despliegue de las armas autónomas, con diversas manifestaciones. Por un lado, siguiendo al Relator Especial Christof Heyns, la dignidad humana entendida en el sentido de la tradición kantiana se pone en entredicho cuando se excluye al ser humano de la adopción de decisiones relativas al empleo de la fuerza letal. En otras palabras, del Derecho internacional se deriva la premisa de que sólo los seres humanos pueden adoptar la decisión de usar la fuerza contra otros seres humanos. Incluso si una máquina pudiera cumplir con los requisitos humanitarios anteriormente mencionados de distinción y proporcionalidad, seguiría siendo ilegítimo que un arma autónoma pudiera adoptar tal decisión: *«[d]eath by algorithm means that people are treated simply as targets and not as complete and unique human beings, who may by virtue of this status deserve to meet a different fate»* (63). Además, el principio de humanidad choca directamente con la falta de emociones y capacidad para la compasión de la que adolecen las armas autónomas (64). Por otra parte, se ha aducido que, para que una decisión sobre la supresión de la vida de un ser humano cumpla con este principio de humanidad es necesario que el propio razonamiento humano se encuentre involucrado. En otras palabras, como sucede con el principio del proceso debido en el ámbito de la justicia, debe existir un proceso deliberativo realizado por un ser humano o, si es realizado por una máquina, sujeta a revisión humana, antes de que se alcance cualquier decisión sobre el uso de la fuerza letal (65).

Quienes defienden el despliegue de las armas autónomas replican que lo realmente importante es si las armas autónomas cumplen con las exigencias del Derecho internacional humanitario, ya que éste último no exi-

(63) Heyns, C.: «Autonomous weapons systems: living a dignified life and dying a dignified death», en Bhuta, N. *et al.* (eds.): *Autonomous Weapons Systems*, Cambridge University Press, 2016, pp. 10-11.

(64) Human Rights Watch and International Human Rights Clinic (Harvard Law School): *Losing Humanity. The Case against Killer Robots*, *op. cit.*, pp. 36, 38.

(65) Asaro, P.: «On Banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making», *International Review of the Red Cross*, vol. 94, 2012, pp. 700-702.

ge promover el amor, la compasión o la empatía humana (66). Por otro lado, la mera posibilidad de que haya misericordia o compasión por parte de un mando humano no cambia la situación si luego esa posibilidad no se materializa, de modo que resulta indiferente que las armas estén o no controladas por un ser humano (67). Como se ha afirmado, quizá no debe confundirse la dignidad humana con la idea de moralidad, por más que la delegación de ciertos tipos de actividad o razonamiento humano a las máquinas pueda generar ansiedad (68).

El otro límite derivado de la Cláusula Martens es el relativo a los dictados de la conciencia pública, aunque no está claro cómo se puede identificar esta conciencia pública ni qué valor jurídico se puede atribuir a la misma (69). Los defensores de las armas autónomas niegan relevancia jurídica alguna a esta cláusula, en la medida en que sólo cabe recurrir a la misma cuando hay una ausencia de regulación específica, situación que no se produce en realidad ya que el Derecho de los conflictos armados resulta perfectamente aplicable a las armas autónomas (70). Frente a esta conclusión, los que se oponen al desarrollo de estas armas recuerdan el valor atribuido a la Cláusula Martens por el Tribunal Internacional de Justicia como «medio efectivo para hacer frente a la rápida evolución de la tecnología militar» (71). Incluso si no puede considerarse como una fuente formal del Derecho internacional humanitario, entienden que este concepto entronca con la emergencia de una corriente global a favor de la prohibición de estas armas autónomas, que puede servir como un argumento adicional de peso para forzar a los Estados a negociar un Protocolo que materialice esta prohibición (72).

4. ATRIBUCIÓN DE LA RESPONSABILIDAD

Otra de las cuestiones más problemáticas que plantea el despliegue de las armas autónomas letales es el relativo a la atribución de responsabilidad en caso de que se produzca una vulneración de las normas del Dere-

(66) Sassòli, M.: «Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified», *loc. cit.*, p. 318.

(67) Birnbacher, D.: «Are autonomous weapons systems a threat to human dignity?», en Bhuta, N. *et al.* (eds.): *Autonomous Weapons Systems*, Cambridge University Press, 2016, p. 120-121.

(68) Bhuta, N., Beck, S., y Geiss, R.: «Present Futures: concluding reflections and open questions on autonomous weapons systems», *loc. cit.*, p. 355.

(69) Cassese, A.: «The Martens Clause: Half a Loaf or Simply Pie in the Sky?», *European Journal of International Law*, Vol. 11, 2000, pp. 187 y ss.; Meron, T.: «The Martens Clause, Principles of Humanity, and Dictates of Public Conscience», *American Journal of International Law*, Vol. 94, 2000, pp. 78 y ss.

(70) Schmitt, M. N. y Thurnher, J. S., «*Out of the Loop*: Autonomous Weapons Systems and the Law of Armed Conflict», *loc. cit.*, pp. 275-276.

(71) International Court of Justice: Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, *I. C. J. Reports 1996*, párrafo 78.

(72) Amoroso, D.: «*Jus in bello* and *jus ad bellum* arguments against autonomy in weapons systems: A re-appraisal», *loc. cit.*, pp. 25-28.

cho internacional humanitario, o del Derecho internacional de los derechos humanos, que, en el peor de los casos, puede determinar la comisión de un crimen internacional. Como es sabido, el objetivo de la atribución de responsabilidad en Derecho internacional penal consiste en la disuasión respecto de futuras vulneraciones de la norma, o sea, se persigue el efecto de prevención general, así como en la rendición de cuentas, que aspira a conseguir una cierta compensación a favor de las víctimas (73). Sin embargo, las armas autónomas no pueden ser consideradas responsables directas en la medida en que todo crimen requiere de dos elementos, en primer lugar, la comisión de un hecho punible *(actus reus)* y, en segundo lugar, el dolo o la intencionalidad *(mens rea),* imposible de concretar en el caso de estas armas. Pero, además, los tribunales penales internacionales sólo ejercen jurisdicción sobre las personas físicas (74). En efecto, las armas autónomas no pueden ser consideradas responsables por carecer de discernimiento moral. Se plantea así el problema jurídico nuclear de quién puede ser considerado responsable en caso de vulneración de las normas internacionales antes mencionadas (75). En el supuesto de no poder identificar a un responsable, se estaría generando potencialmente un vacío legal de tremendas consecuencias para el sistema jurídico internacional.

En principio, existe un grupo de personas que pueden en todo caso relacionarse con la producción y el despliegue de un arma autónoma y sobre las que podría recaer esta responsabilidad (76). Entre estas personas estarían los programadores del *software,* los fabricantes y vendedores del *hardware,* los dirigentes políticos, los jefes militares, los operadores que desplegaron el arma autónoma o que la supervisaron en el momento de realizar la operación, sin excluir a los militares responsables de su compra o de su revisión jurídica (en el sentido del art. 36 del Protocolo Adicional I a los Convenios de Ginebra) (77). El problema es que no se puede

(73) Naciones Unidas, Asamblea General, Consejo de Derechos Humanos: *Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias*, Christof Heyns, cit., p. 16; Human Rights Watch and International Human Rights Clinic (Harvard Law School): *Mind the Gap – The Lack of Accountability for Killer Robots*, 2015, p. 13.

(74) Véase, por ejemplo, el artículo 25 del Estatuto de Roma de la Corte Penal Internacional, en el que se estipula que «la Corte tendrá competencia respecto de las personas naturales».

(75) Beard, J. M.: «Autonomous Weapons and Human Responsibilities», *Georgetown Journal of International Law*, vol. 45, 2014, p. 642; Cass, K.: «Autonomous Weapons and Accountability,» *Loyola of Los Angeles Law Review*, vol. 48, 2015, p. 1054.

(76) Por tanto, para los autores que defienden esta posición no habría vacío legal en cuanto a la responsabilidad criminal individual, véase Schmitt, M. N. y Thurnher, J. S., «*Out of the Loop*: Autonomous Weapons Systems and the Law of Armed Conflict», *loc. cit.*, p. 277; Sassòli, M.: «Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified», *loc. cit.*, pp. 323-324.

(77) Naciones Unidas, Asamblea General, Consejo de Derechos Humanos: *Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias*, Christof Heyns, *cit.*, p. 16; Wagner, M.: «The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapons Systems», *loc. cit.*, pp. 1404-1407; Jain 321.

atribuir responsabilidad directa individual a ninguna de estas personas por la ausencia del elemento de la intencionalidad (78). Si se trata de armas que funcionan con autonomía, aunque sólo sea parcialmente, no es posible establecer un vínculo directo entre el acto criminal y las personas anteriormente mencionadas, en la medida en que los actos de estas armas autónomas resultan impredecibles, a no ser que el programador o el operador, por ejemplo, hubiesen actuado con la intención de cometer un crimen internacional (79).

La alternativa a una responsabilidad directa es la responsabilidad indirecta o de mando (80) que se ha definido como la responsabilidad que tiene lugar cuando un militar superior en la cadena de mando no toma las medidas necesarias y razonables para prevenir o castigar los actos criminales de un subordinado sobre quien el superior tiene control efectivo, una vez que el superior sabe o tiene razones para saber de los actos delictivos (81). No obstante, esta alternativa relativa a la responsabilidad de mando no parece tampoco aplicable, en la medida en que el elemento de la intencionalidad no puede concretarse respecto de un comportamiento impredecible de las armas autónomas, además de que el tiempo de reacción del que dispone el superior jerárquico en el marco de la velocidad de procesamiento de estas armas en realidad no permitiría un control efectivo (82). Por esa razón, se han propuesto alternativas que invitan a rebajar las exigencias de la responsabilidad de mando. La primera alternativa consiste en la aceptación de la responsabilidad de mando en los casos en que existe lo que se denomina como imprudencia opaca *(opaque recklessness),* en donde se penaliza simplemente una conducta arriesgada, cuando el sujeto no se da cuenta o ignora conscientemente las razones específicas del riesgo. Igualmente, se podría utilizar el concepto de responsabilidad por negligencia, en donde, añadiendo más flexibilidad aún, sería suficiente con la creación de un riesgo de forma inadvertida (83).

---

(78) *Contra* Sassòli, M.: «Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified», *loc. cit.*, p. 324.

(79) Crootof, R.: «War Torts: Accountability for Autonomous Weapons», *University of Pennsylvania Law Review*, vol. 164, 2016, p. 1376-1377; Grut, C.: «The Challenge of Autonomous Lethal Robotics to International Humanitarian Law», *loc. cit.*, p. 16; Wagner, M.: «The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapons Systems», *loc. cit.*, pp. 1403-1407; Stewart, D. M.: «New Technology and the Law of Armed Conflict», *International Law Studies*, US Naval War College, vol. 87, 2011, p. 290.

(80) Esta responsabilidad de mando, de los jefes o del superior jerárquico, está recogida en los arts. 86 y 87 del Protocolo Adicional I a los Convenios de Ginebra, así como en el artículo 28 del Estatuto de Roma de la Corte Penal Internacional.

(81) International Criminal Tribunal for the Former Yugoslavia: *Prosecutor v. Delalić*, Case N.º IT-96-21-T, Judgment (Trial Chamber), November 16, 1998, para. 346.

(82) Human Rights Watch and International Human Rights Clinic (Harvard Law School): *Mind the Gap – The Lack of Accountability for Killer Robots*, *op. cit.*, pp. 22-24; Crootof, R.: «War Torts: Accountability for Autonomous Weapons», *loc. cit.*, pp. 1379-1380.

(83) Jain. N.: «Autonomous weapons systems: new frameworks for individual responsibility», en Bhuta, N. *et al.* (eds.): *Autonomous Weapons Systems*, Cambridge University Press, 2016, pp. 317-318.

Otra alternativa consiste en extender la responsabilidad de mando a un estadio anterior, el relativo a la decisión adoptada por los militares responsables de las compras públicas (84).

Sin embargo, estas alternativas, aun teniendo el mérito de identificar a un sujeto responsable de la comisión de un hecho punible en el plano internacional, presentan el mismo inconveniente y es el de no resolver el vacío jurídico respecto de la responsabilidad criminal individual. En efecto, una cosa es evitar la impunidad y otra cosa es buscar chivos expiatorios a través de las personas físicas más próximas al despliegue de las armas autónomas (85). Además, la introducción del concepto de negligencia en el Derecho penal internacional no es necesariamente positiva, ya que puede conducir a una hípercriminalización (86). Por tanto, el verdadero problema reside en la imposibilidad de atribuir una auténtica responsabilidad criminal, de tipo causal, en el caso de la comisión de un hecho punible por parte de un arma autónoma, puesto que la extensión de la responsabilidad, de tipo indirecto, al mando o al programador no elimina ese vacío (87).

Una fórmula completamente distinta sería la que consiste en el recurso a la responsabilidad de tipo civil, en concreto, por la elaboración de productos defectuosos (88). En este caso, los posibles responsables serían los programadores y los fabricantes (89). El problema es que, en el sector de la defensa, difícilmente los fabricantes son declarados responsables por defectos de diseño, sobre todo cuando esos defectos son notificados con antelación (90). Además, ello obligaría a las víctimas a asumir la carga de poner en marcha reclamaciones frente a los fabricantes de armas autónomas, con el agravante de que estas víctimas pueden carecer de los recursos necesarios para ello o encontrarse geográficamente muy distantes (91). Otra alternativa sería recurrir a la responsabilidad civil del Esta-

(84) Corn, G. S.: «Autonomous weapons systems: managing the inevitability of 'taking the man out of the loop'», en Bhuta, N. *et al.* (eds.): *Autonomous Weapons Systems*, Cambridge University Press, 2016, pp. 233-234.

(85) Liu, H.-Y.: «Refining responsibility: differentiating two types of responsibility issues raised by autonomous weapons systems», en Bhuta, N. *et al.* (eds.): *Autonomous Weapons Systems*, Cambridge University Press, 2016, p. 341.

(86) En otras palabras, *«[I]f an individual could be held criminally liable for negligent actions in war and if her commander would be indirectly liable for negligence, every commander would be a war criminal»* y, a la inversa, *«if everyone is a criminal, no one is»*, Crootof, R.: «War Torts: Accountability for Autonomous Weapons», *loc. cit.*, pp. 1383-1385.

(87) Liu, H.-Y.: «Refining responsibility: differentiating two types of responsibility issues raised by autonomous weapons systems», *loc. cit.*, pp. 336-341.

(88) Khrisnan, A.: *Killer Robots – Legality and Ethicality of Autonomous Weapons*, Ashgate, Farnham, 2009, pp. 103-104; Singer, P. W.: *Wired for war: the robotics revolution and conflict in the twenty-first century*, Penguin Press, New York, 2009, p. 410.

(89) Naciones Unidas, Asamblea General, Consejo de Derechos Humanos: *Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias*, Christof Heyns, cit., p. 16.

(90) Beard, J. M.: «Autonomous Weapons and Human Responsibilities,» *loc. cit.*, p. 647.

(91) Human Rights Watch and International Human Rights Clinic (Harvard Law School): *Losing Humanity. The Case against Killer Robots, op. cit.*, p. 44.

do, lo que tampoco conduciría a resultados satisfactorios, ya que se suele respetar la doctrina de la inmunidad soberana del Estado (92).

Por último, cabría acudir a la responsabilidad internacional del Estado como opción para articular algún sistema efectivo de asunción del daño causado por parte de un arma autónoma. Este es el sistema preferido por aquellos que amparan el desarrollo de las armas autónomas (93). Sus defensores arguyen que es la opción preferible desde un punto de vista normativo, ya que puede generar el incentivo necesario para que los Estados desplieguen armas autónomas que sean compatibles con el Derecho internacional, pero también desde un punto de vista moral, ya que el Estado es teóricamente el responsable final de la puesta en marcha y el despliegue de estas armas (94). Sin embargo, la responsabilidad internacional del Estado como mecanismo para articular una compensación en caso de vulneración grave de las normas internacionales no permite ofrecer una respuesta satisfactoria, en los mismos términos en que lo hace la responsabilidad criminal individual. Por esa razón, el Grupo de Expertos ha concluido que, junto con la responsabilidad estatal, los Estados deben asegurar la responsabilidad por las acciones letales de acuerdo con el Derecho internacional humanitario (95).

5. REFLEXIONES FINALES

Este trabajo se ha centrado en el análisis de la problemática que plantean las armas autónomas letales desde el punto de vista del Derecho internacional humanitario, dejando de lado otras cuestiones, como las posibles violaciones del Derecho internacional de los derechos humanos [en el caso de su despliegue para el mantenimiento del orden público interno (96)], o las consecuencias que pueden generar en el plano del mantenimiento de la paz y la seguridad internacionales (97).

---

(92) Human Rights Watch and International Human Rights Clinic (Harvard Law School): *Mind the Gap – The Lack of Accountability for Killer Robots*, *op. cit.*, pp. 27-29; Para un panorama sobre la responsabilidad civil del Estado en Estados Unidos, véase Kastan, B.: «Autonomous Weapons Systems: A Coming Legal 'Singularity?'», pp. 69 y ss.

(93) Anderson, K. y Waxman, M.: *Law and Ethics for Autonomous Weapon Systems – Why a Ban Won't Work and How the Laws of War Can*, *op. cit.*, 2013, p. 17; Hammond, D. N.: «Autonomous Weapons and the Problem of State Accountability», *Chicago Journal of International Law*, vol. 15, 2015, p. 668 y ss.; Crootof, R.: «War Torts: Accountability for Autonomous Weapons», *loc. cit.*, pp. 1389 y ss.

(94) Hammond, D. N.: «Autonomous Weapons and the Problem of State Accountability», *loc. cit.*, pp. 669-670.

(95) Group of Governmental Experts of the High Contracting Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects: Report of the 2017 Group of Governmental Experts on Lethal Autonomous Weapons Systems (LAWS), cit., p. 4.

(96) Heyns, C.: «Human Rights and the use of Autonomous Weapons Systems (AWS) During Domestic Law Enforcement», *Human Rights Quarterly*, vol. 38, 2016, pp. 350-378.

(97) Se ha sostenido que el despliegue de estas armas puede facilitar, incluso «normalizar», los conflictos armados, incrementando la potencialidad de la violación de las normas sobre el *ius*

Resulta difícil predecir cuál será el curso que seguirán los acontecimientos en el marco de las armas autónomas letales y qué opciones de política normativa prevalecerán en el plano internacional, que pueden ir desde un tratado internacional de prohibición hasta la no adopción de regla alguna, pasando por la elaboración de normas de *soft-law* en forma de códigos de conducta o manuales de mejores prácticas (98). No obstante, hay algunos elementos que se pueden destacar de cara al futuro inmediato en este ámbito. En primer lugar, parece claro que las armas autónomas letales van a ser objeto de un creciente desarrollo por parte de Estados avanzados tecnológicamente, particularmente los Estados Unidos, que no van a renunciar fácilmente a las ventajas estratégicas que esperan de ellas (99). No obstante, esta inevitabilidad respecto del desarrollo incremental en el futuro de dichas armas ha sido rechazada por los autores que defienden su prohibición, en la medida en que la consideran como una conclusión anticipada (100), una especie de profecía auto-cumplida a la que hay que hacer frente.

En segundo lugar, también resulta evidente que los mencionados Estados no van a tomar la iniciativa respecto de la regulación de los aspectos jurídicos y éticos que giran en torno a esta tecnología, particularmente los relativos al respeto del Derecho internacional humanitario, los derechos humanos, así como la responsabilidad criminal individual y la responsabilidad estatal (101). Esta estrategia consistente en dilatar cualquier proceso regulador en el plano internacional se ha constatado ya, por otro lado, en un ámbito no muy lejano como es el del ciberespacio (102).

En tercer lugar, aunque es difícil aventurar el resultado de los debates que se están produciendo en torno a la regulación de estas armas en el marco de la Convención sobre Ciertas Armas Convencionales, cabe esperar que la estrategia de los Estados más interesados en el desarrollo de esta tecnología haga muy difícil, aunque no imposible, el éxito de cualquier propuesta relativa a su prohibición. Incluso si esta prohibición se hiciera una realidad, es previsible que Estados Unidos y otros Estados interesados, como Israel o el Reino Unido, no ratifiquen el correspondien-

---

ad bellum, véase Alston, P.: «Lethal Robotic Technologies: The Implications for Human Rights and International Humanitarian Law», *Journal of Law, Information and Science*, Vol. 21, 2011/2012, p. 55; Naciones Unidas, Asamblea General, Consejo de Derechos Humanos: *Informe del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias*, Christof Heyns, cit., p. 12.

(98) Sobre estas opciones, véase Marchant, G. E. *et al.*: «International Governance of Autonomous Military Robots», *The Columbia Science and Technology Law Review*, vol. 12, 2011, p. 272.

(99) Anderson, K. y Waxman, M.: *Law and Ethics for Autonomous Weapon Systems-Why a Ban Won't Work and How the Laws of War Can*, *op. cit.*, p. 5.

(100) Asaro, P.: «On Banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making», *loc. cit.*, pp. 704-706.

(101) Alston, P.: «Lethal Robotic Technologies: The Implications for Human Rights and International Humanitarian Law», *loc. cit.*, p. 59.

(102) Segura Serrano, A.: «Ciberseguridad y Derecho Internacional», *loc. cit.*, p. 298.

te acuerdo internacional. No obstante, hay ejemplos de tratados internacionales, como el relativo a las minas antipersona de 1997 o el relativo a las bombas de racimo de 2008, que, no habiendo sido ratificados por Estados tales como los Estados Unidos, Rusia o China, han resultado exitosos y podrían convertirse en Derecho consuetudinario de obligado cumplimiento para todos los Estados (103). Sin embargo, está por ver que este derrotero sea el que finalmente se concrete en relación con las armas autónomas, ya que la ventaja militar que ofrecen puede ser un incentivo difícil de esquivar para las potencias militares.

Otras alternativas intermedias se pueden materializar, en el sentido de que, entre la prohibición total y la ausencia de regulación, pueden encontrarse fórmulas a medio camino que permitan una regulación incremental con el objetivo último de la limitación en su uso y despliegue. Como se ha indicado, existen marcos internacionales que pueden servir de guía en la articulación de incipientes mecanismos de control internacional. Este es el caso del Derecho internacional del medio ambiente en materia de actividad transfronteriza peligrosa, en donde se aplican los principios de diligencia debida, identificación y control del riesgo, e intercambio de la información. Igualmente, se puede recurrir como marco de actuación al mecanismo sobre revisión de armas nuevas previsto en el artículo 36 del Protocolo Adicional I de los Convenios de Ginebra (104). En cualquier caso, lo que se necesitará con seguridad es incrementar la transparencia en este ámbito de las armas autónomas, en donde se practica naturalmente el secreto militar, como mejor medio para facilitar el debate y hacer frente de manera coordinada a los riesgos derivados de las armas autónomas letales (105).

(103) Sharkey, N. E.: «The Evitability of Autonomous Robot Warfare», *loc. cit.*, p. 798.

(104) Bhuta, N. y Pantazopoulos, S.-E.: «Autonomy and uncertainty: increasingly autonomous weapons systems and the international legal regulation of risk», en Bhuta, N. *et al.* (eds.): *Autonomous Weapons Systems*, Cambridge University Press, 2016, pp. 290 y ss.

(105) Knuckey, S.: «Autonomous weapons systems and transparency: towards an international dialogue», en Bhuta, N. *et al.* (eds.): *Autonomous Weapons Systems*, Cambridge University Press, 2016, pp. 175 y ss.

VII

TRABAJO Y MERCADO LABORAL EN UN MUNDO DIGITAL

CAPÍTULO 29

EL FUTURO DEL TRABAJO Y EL EMPLEO EN LA ERA DE LA DIGITALIZACIÓN Y LA ROBÓTICA

JESÚS R. MERCADER UGUINA
Catedrático Derecho del Trabajo y Seguridad Social
de la Universidad Carlos III de Madrid

I. UN NUEVO ESCENARIO: LA DISRUPCIÓN TECNOLÓGICA

El cambio tecnológico que estamos viviendo anuncia una transformación disruptiva en los modos y formas de entender en un futuro próximo la idea de trabajo (1). Estamos en una época caracterizada por una acele-

(1) Para una reflexión de conjunto sobre todos estos problemas nos permitimos remitir a J. R MERCADER UGUINA, *El futuro del trabajo en la era de la digitalización y la robótica*, Valencia, Tirant lo Blanch, 2017 e, igualmente, a *Disrupción tecnológica, robótica y nuevas formas de trabajo*,

ración que nació, precisamente, con la incorporación de la máquina como elemento esencial del sistema productivo y cuya evolución se ha caracterizado por un desarrollo progresivo en el que cada proceso tecnológico ha sido más potente y veloz que el anterior: el «turbocapitalismo» (2). La especialidad de esta transformación en relación con los procesos anteriores, la virulencia y velocidad con la que esos cambios se instalan ahora en nuestros sistemas productivos carece, por completo, de precedentes.

El actual cambio, revolución o como quiera que lo califiquemos, ha venido siendo considerado como una verdadera «disrupción». El concepto de lo disruptivo merece nuestra atención. Schumpeter utilizó el término «destrucción creativa» (3) que representa la idea de que los sistemas progresan creando nuevas estructuras destruyendo las existentes. Este proceso permanente de innovación obedece a que la maquinaria del capitalismo no puede ser estacionaria sino que, como una mutación, revoluciona desde su mismo interior las viejas estructuras, creando otras nuevas de manera incesante. Otros señalan que lo disruptivo representa la actuación de la tecnología que viene a interrumpir el statu quo, a alterar la forma en que la gente vive y trabaja, reorganizar el valor y crear productos y servicios enteramente nuevos, pero también señalan que «la tecnología a menudo suplanta las viejas maneras de hacer las cosas (4). Lo disruptivo es, pues, la tecnología que altera el status quo existente e innova radicalmente la realidad productiva.

II. TRABAJO Y *PLATFORM ECONOMY*

La «on-demand economy» representa la última ola de una nueva economía. Rental platforms, craft platforms o financing platforms y gig platforms se están desarrollando en todos los países de forma creciente. Quién no ha oído hablar o ha utilizado Airbnb para proveerse de un alojamiento, de BlaBlaCar para compartir viaje o de Deliveroo para que le traigan comida desde un restaurante. La que se ha denominado *platform economy* se articula en páginas web o apps cuyo objetivo declarado es el contacto directo entre clientes y prestadores de servicio. Una conexión en la que, se ha dicho, «todo el mundo sale ganando», al nacer al mundo económico nuevos servicios y también nuevos consumidores (5).

Diálogos Jurídicos. Anuario de la Facultad de Derecho de la Universidad de Oviedo, 2017, n.º 2, pp. 83-106.

(2) L. Concheiro, *Contra el tiempo. Filosofía práctica del instante*, Barcelona, Anagrama, 2016, pp. 26 y 29.

(3) J. A. Schumpeter, *Capitalismo, socialismo y democracia*, Barcelona, Folio, 1984, pp. 117-124.

(4) Mckinsey Global Institute, *Disruptive Technologies: Advances that will transform Life, Business, and the Global Economy*, May, McKinsey & Company, 2013.

(5) J. Tirole, *La economía del bien común*, Barcelona, Taurus, 2017, pp. 443-444.

Este modelo de negocio se instala en sectores tradicionales de actividad sólidamente consolidados (transporte, limpieza, delivery, etc.) pero transforma de manera radical sus formas y modos de actividad. El desarrollo técnico permite una conexión más fluida y transparente a través de modos de pago automático, la trazabilidad de todas las fases de prestación de los servicios, o, en fin, la tarificación de los servicios en función de las puntas de demanda. Pero este conjunto de transformaciones tiene un profundo efecto en la forma de prestar los servicios. Las formas tradicionales y los conceptos que han sustentado la idea de trabajo se ponen en cuestión. Varios factores llevan a ese resultado (6).

Las plataformas informáticas basan su actuación en algoritmos y, a través de los mismos, efectúan asignaciones de actividades a los profesionales incluidos dentro de la plataforma. El programa se encarga de elaborar una planificación perfecta que permite la asignación más eficiente. En otras palabras, el sistema informático procede a la asignación de tareas asignando el servicio al profesional que en cada momento concreto reúna los requerimientos profesionales y geográficos mejor adaptados a las necesidades del cliente. En resumen, el jefe parece que termina siendo un algoritmo.

Un segundo factor diferencial de la actividad de estas plataformas es la transparencia de sus operaciones en la medida en que toda la información relacionada con cada transacción queda registrada. Con ello se garantiza la visibilidad de la actividad económica y productiva y la mejora los procesos de recaudación y control administrativo a efectos fiscales y de Seguridad Social. De esta opinión es el Parlamento Europeo que en su informe *The Situation of Workers in The Collaborative Economy* subraya que «el intercambio de información con plataformas permite determinar los ingresos de los trabajadores y así mejorar la declaración de impuestos».

Un rasgo que se añade al anterior es el de la trazabilidad de las operaciones. Ello genera un alto nivel de la confianza que se genera entre los proveedores de servicios y quienes los reciben. La verificación de identidades y los sistemas de reputación y evaluación contribuyen a ello. La reputación colectiva de la empresa con el control del comportamiento de sus asalariados deja paso a la reputación individual.

Un tercer rasgo que caracteriza la prestación de servicios en estas plataformas es el de la plena voluntariedad en el tiempo y lugar de prestación de servicios. La plataforma expone el servicio de reparto ofertado y los

(6) Sobre los problemas laborales y posibles propuestas de reforma en esta materia nos remitimos a nuestros estudios, *El nuevo modelo de trabajo autónomo en la prestación de servicios a través de plataformas digitales*, Diario La Ley, Sección Ciberderecho, 11 de julio de 2017 y, más recientemente, *La prestación de servicios en plataformas profesionales: nuevos indicios para una nueva realidad*», Todoli Signes, A., Hernández Bejarano, M. (Dir.), *Trabajo en plataformas digitales: innovación, Derecho y mercado*, Pamplona, Aranzadi/Thomson Reuters, 2018, pp. 155-176.

repartidores compiten para aceptar dicho servicio. La decisión de prestar el servicio depende en exclusiva del prestador de servicios. No hay trabajos en exclusiva. Lo propio de estas actividades es la prestación de servicios para una pluralidad de empresas, incluso dentro propio sector de actividad.

Finalmente, el trabajo se desarrolla a través de «microtareas» en la medida en que dichas prestaciones se concentran en tiempos muy limitados y que, por tanto, dan lugar a micropagos y, en última, instancia a *microworkers.* Una situación criticada y que ha sido bautizada por Robert Reich como «economía del reparto de los restos». La precariedad laboral adopta nuevas formas si bien, en algunos casos, el tiempo de prestación de servicios puede dar lugar a compensaciones económicas elevadas. En todo caso, ello supone un reto para el sindicalismo tradicional que debe salir de su zona de confort y buscar respuestas para estos nuevos intereses colectivos.

El debate sobre la laboralidad o no de esta nueva forma de prestación de servicios se encuentra en plena ebullición: ¿Nos dirigimos hacia una generalización del trabajador autónomo? En el caso de Uber los pronunciamientos existentes ha declarado, rotundamente, su laboralidad (caso O'Connor v. Uber Technologies de 11 de marzo de 2015 del Tribunal de Distrito de los Estados Unidos para el Distrito del Norte de California o sentencia del Employment Tribunal of London 26 de octubre de 2016, Aslam v. Uber). Sin embargo, en las Sentencias de la Cour d´appel de Paris de fecha 20 de abril de 2017, que resuelve sobre la demanda de un repartidor de la plataforma, Take Eat Easy y en la posterior de 9 de noviembre de 2017 en relación con Deliveroo, el Tribunal concluye que no es posible considerar que existe una relación laboral. En la misma dirección apunta la Sentencia del Tribunal del Lavoro di Torino de 11 de abril de 2018 en el Asunto Foodora.

El primer pronunciamiento de la jurisdicción social en esta materia ha sido la Sentencia del Juzgado de lo Social n.º 6 de Valencia de 1 de junio de 2018 (Proc. 633/17), que estima parcialmente la demanda de un repartidor que fue despedido por Roofood Spain, S.L. (denominación social de Deliveroo) y considera existente una relación laboral. El referido pronunciamiento entiende irrelevante que repartidor tenga licencia fiscal como autónomo, que aporte la bicicleta y el móvil para prestar su trabajo, que tenga la posibilidad de buscar un sustituto para realizar los repartos o, en fin, que tuviera libertad para fijar las franjas horarias en que quiere trabajar. El juzgado afirma que se dan los presupuestos que definen la existencia de una relación laboral en la medida en que «era la empresa la que decidía la zona en la que el trabajador debía desempeñar sus funciones. En cuanto al horario, siendo cierto que el trabajador ofertaba a la empresa

las franjas horarias en las que quería trabajar, también lo es que esas franjas tenían que estar dentro del horario previamente establecido por la demandada, y que era ésta quien finalmente decidía en qué horario iba a desempeñar sus funciones el trabajador cada semana, siendo que en ocasiones este quedaba reducido a una parte del solicitado por el trabajador. Respecto al servicio de reparto, la empresa daba instrucciones concretas a los repartidores sobre la forma en que este se tenía que llevar a cabo, fijando tiempos y normas de comportamiento que estos debían cumplir. Consta, asimismo, que al inicio del turno asignado los trabajadores debían acudir al lugar fijado por la empresa, centroide, para que esta les asignara servicios a través de la plataforma, debiendo retornar a esta cada vez que finalizaban un servicio. Además, la empresa tenía en todo momento geolocalizado al trabajador, a quien podía pedir explicaciones en cualquier momento sobre el servicio, llevando un control de tiempos de cada reparto, siendo la empresa la que decidía en cada momento sobre los repartos a realizar y la efectiva asignación de los mismos». Entiende por tanto que «se dan las notas características de la relación laboral de ajeneidad y dependencia, ya que la prestación de servicios del demandante, a favor de Deliveroo, presenta rasgos que solo son concebibles en el trabajo dependiente y por cuenta ajena».

Las anteriores realidades plantean desde una perspectiva estrictamente jurídica el problema técnico de si las nociones de dependencia y ajenidad son categorías susceptibles de acoger las nuevas formas de trabajo. La duda que emerge en la dogmática laboral de la sociedad postindustrial es la relativa a la adecuación de las referidas nociones a los nuevos modelos de producción. En esta nueva era se produce una neta mutación en la morfología del concepto clásico de trabajador. Autonomía, coordinación, participación son los rasgos diferenciadores de este momento frente a las clásicas de dependencia, subordinación y conflicto. Los valores cambian y también lo hacen los conceptos jurídicos sobre los que las realidades se asientan. En el trasfondo de la anterior idea está, en muchos casos, la marcada proximidad sociológica e, incluso, jurídica entre el trabajo por cuenta ajena y otras prestaciones susceptibles de ser encuadradas dentro del Derecho Civil o del Mercantil.

Todo ello requiere reflexiones profundas y, sobre todo, capacidad de adaptación al cambio. Me parece especialmente lúcida la reflexión que realiza Jean Tirole en su obra *La economía del bien común:* «Es necesario, pues, recapitular sobre los fundamentos del derecho laboral. Estamos tan habituados a recurrir a la legislación laboral que hemos olvidado su motivación fundamental: el bienestar del trabajador. Hay que garantizar una neutralidad competitiva entre las diferentes formas de organización, no se deben trucar los dados en favor del trabajador asalariado o del autoempre-

sario. Si hay algo seguro es que se tiene que reconsiderar nuestra legislación y el contexto laboral en un mundo en rápida mutación tecnológica».

III. LA CONSOLIDACIÓN DE LA EMPRESA «PANÓPTICA»

Los cambios tecnológicos no solo están incidiendo en la creación y reformulación de las formas tradicionales del trabajo por cuenta ajena sino que poseen una incidencia real e inmediata en el desarrollo de la actividad laboral de nuestros días y contribuyen también al uso de herramientas jurídicas adaptadas a las situaciones de conflicto sobre las que se proyectan. Ciertamente, la idea de la empresa panóptica se hace cada vez más fuerte y los mecanismos de control y seguimiento empresarial adquieren nuevos contenidos y también nuevas dimensiones (7).

La incorporación de técnicas de control tecnológicamente avanzadas convierten esta sociedad en una nueva sociedad transparente que no puede prescindir de un trabajo, también, «transparente». La sombra del Big Brother orwelliano de su 1984 ha sido vista cerniéndose amenazadora sobre nuestra sociedad tecnologizada; un mundo que hasta hace bien poco moraba, tan sólo, en el onírico entorno de la imaginación literaria. El control a través de sistemas de videovigilancia, microfónicos y telefónicos, el rastreo a través de sistemas de geolocalización; los controles biométricos; el control informático de los niveles de productividad de los trabajadores en tiempo real; el seguimiento de los correos electrónicos y de las navegaciones por internet; el impacto de las redes sociales o, en fin, la enorme proyección que sobre lo laboral comienzan a tener las técnicas del Big Data, conforman una realidad en permanente transformación en la que la vigilancia empresarial se ha convertido en algo más impersonal, pero no por ello menos invasivo (8).

En este contexto, el debate sobre la dignidad personal y los derechos de la persona alcanza un lugar fundamental en la medida en que se convierten en el contrapeso necesario de un escenario tan limitativo de la autonomía de la persona. Esta nueva dimensión se conecta con el proceso de individualización que vive nuestro sistema de relaciones laborales. La función del contrato de trabajo observa, en los últimos tiempos, un resurgimiento sobre nuevos fundamentos quizá menos ajustados a los modos tradicionales de concebir la actuación de la autonomía de la voluntad en

(7) La concepción panóptica de la empresa se apunta en el trabajo de R. Whitaker, *El fin de la privacidad. Cómo la vigilancia total se está convirtiendo en realidad*, Barcelona, Paidos, 1999. Su proyección en la realidad laboral puede verse en J. R. Mercader Uguina, *Derechos fundamentales de los trabajadores y nuevas tecnologías: ¿hacia una empresa panóptica?*, RL, 2001, n.º 10, pp. 11 a 31.

(8) F. J. Cavico, *Invasion of privacy in the private employment sector: tortious and ethical aspects*. Houston Law Review, 1993, v. 30, pp. 1263-1346, espec. pp. 1284-1292, que realiza una sugerente reflexión sobre los fundamentos kantianos y utilitaristas que sirven de base a los razonamientos en esta materia.

este sector del ordenamiento jurídico. Este proceso representa «una revalorización del perfil subjetivo en el contrato de trabajo» (9), que conecta de forma directa e inmediata con la revalorización de los derechos fundamentales en su seno. La transformación tecnológica tiene como una de sus consecuencias el acentuar la importancia de los derechos personalísimos en la esfera individual.

IV. LA ERA DEL BIG DATA Y LOS EFECTOS SOBRE LAS RELACIONES LABORALES

En la actual economía de los datos personales, nuestra información, fotos, contenidos y comentarios se han convertido en la pieza clave sobre la que pivotan las empresas de Internet, y, en especial, las redes sociales. Las tecnologías Big Data están conduciendo además a la consideración del dato como materia prima capital de la sociedad de la información y del conocimiento. La evolución tecnológica permite reelaborar gran cantidad de datos simples, de forma que, combinados entre sí, pueden contribuir a definir el perfil íntimo de una persona, no sólo a través de la recogida directa de datos, sino mediante la recopilación de noticias fragmentarias y aparentemente inocuas que, unidas, nos pueden dar bastante información sobre un individuo o grupo de individuos.

Son precisamente estas las razones de la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Tal y como se expone en un en su Considerando [6]: «La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales».

(9) G. Vardaro, *Tecnica, tecnologia e ideologia della tecnica nel Diritto del Lavoro*, PD, 1986, n.º 1, p. 124.

Existen características de la relación laboral que dan trascendencia al tratamiento de datos y que convierten a la misma en especialmente sensible a los peligros derivados de las anteriores realidades: su perdurabilidad, que hace importante la conservación de datos; su carácter personal, que hace más complejo el tipo de datos a considerar; la diversidad de escenarios para los que pueden ser relevantes; y, en fin, el número de trabajadores tan elevado a los que se requiere información. Los complejos problemas que se plantean en materia laboral con el tratamiento de datos se amplifican en un momento de hiperdatificación del lugar del trabajo, donde la empresa es un emisor constante de datos (10).

Es, por ello, particularmente relevante tener en cuenta, como han venido recomendado los órganos consultivos internacionales en materia de protección de datos, que la legislación sobre protección de datos no debe aplicarse de forma independiente del Derecho del Trabajo y las prácticas laborales y que éstos, a su vez, no pueden aplicarse aisladamente, sin tener en cuenta la legislación sobre protección de datos. Esta interacción es necesaria y valiosa y debe contribuir al desarrollo de soluciones que protejan adecuadamente los intereses de los trabajadores.

El manejo del Big Data puede afectar con especial virulencia a lo laboral en todos y cada uno de los aspectos de su relación. Los grandes datos ya están afectando el intercambio de trabajo haciendo coincidir a los candidatos calificados con oportunidades de empleo y alineando la educación y el desarrollo de habilidades con las necesidades de la economía. La educación, la experiencia laboral y los intereses pueden conectarse para compilar un «perfil de calificaciones» preciso, que puede alinearse con las habilidades y experiencia que los empleadores necesitan. A medida que evolucione esta capacidad, mejorará, presuntamente, la eficacia con la que se hace coincidir a los solicitantes de empleo con los puestos de trabajo.

En todo caso, los riesgos del desarrollo de estas nuevas fórmulas se proyectan como oscuras sombras en el ámbito empresarial, reformulando la clásica consideración del «trabajador transparente», al permitirse, si cabe, una mayor capacidad de transmisión de datos y de combinación de los mismos a través del uso de los ficheros de datos, con el peligro añadido de la descontextualización de la información, lo que creará un clima psicosociológico de control y transparencia, esto es, la conciencia en los trabajadores de poder ser conocidos en todos sus aspectos.

(10) Monográficamente remitimos a nuestra reciente obra, *Protección de datos en las relaciones laborales*, Madrid, Francis Lefebvre, 2018.

V. LOS RIESGOS ASOCIADOS AL DESARROLLO DE LA INDUSTRIA DIGITAL

Los riesgos de lo que se ha llamado la «cuarta revolución industrial» son cada vez más evidentes. Esta realidad que viene marcada por la transformación del espacio de trabajo, por la intermediación tecnológica, y en las que la robótica y las aplicaciones de inteligencia artificial se convierten en un instrumento fundamental de la producción, la incertidumbre asociada a los riesgos se encuentra cada vez más presente. Retos que van desde la transformación del modelo normativo hasta las incógnitas que lleva consigo el desarrollo tecnológico (11).

El vínculo físico entre el lugar de trabajo y las labores que deben realizarse se hace cada vez más vago gracias a la expansión de las tecnologías de la información. Estos cambios no afectan a la relación laboral en sí misma, aunque pueden difuminar las diferencias entre trabajadores asalariados y autónomos, pero plantean problemas específicos, por ejemplo, en el caso de los teletrabajadores: el empresario es responsable de su salud y su seguridad, independientemente del lugar donde se realiza el trabajo. Se hace necesario, pues, adoptar medidas para prevenir los riesgos y realizar controles en el caso de trabajadores móviles o que trabajan en sus domicilios. El teletrabajo se incorpora a la actividad empresarial con su acervo de posibilidades pero también aparece acompañado de riesgos desconocidos: singularmente, el aislamiento, junto con formas singulares de fatiga muscular y física, lo que convierte a esta forma de organización en una materia necesitada de reflexión y análisis.

A ello se unen los efectos de un uso constante de las nuevas tecnologías, que llevan consigo el conocido «tecnoestrés». El concepto de tecnoestrés está directamente relacionado con los efectos psicosociales negativos del uso de las TIC. Fue acuñado por primera vez por el psiquiatra norteamericano Craig Brod en 1984 en su libro «Technostress: The Human Cost of the Computer Revolution». Lo define como: «una enfermedad de adaptación causada por la falta de habilidad para tratar con las nuevas tecnologías del ordenador de manera saludable (Como señala la NTP 730: *Tecnoestrés: concepto, medida e intervención psicosocial*). Fórmulas como la desconexión laboral están en este camino. El Acuerdo Marco sobre estrés laboral (2004) que lo define como «un estado que viene acompañado de quejas o disfunciones físicas, psicológicas o sociales y que resulta del sentimiento de incapacidad de los individuos para cumplir

(11) Más extensamente sobre la amplia problemática que plantea esta materia, J. R. Mercader Uguina, *Nuevos riesgos y nuevas soluciones, la prevención en el siglo xxi*, Teoría y Derecho, 2018 (en prensa).

los requisitos o expectativas depositados en ellos», puede ser una buena senda a recorrer.

También la aparición de nuevos materiales, como es el caso de las nanopartículas, supone un reto a la hora de realizar las evaluaciones de riesgos y aplicar medidas de prevención y control dadas las lagunas de conocimiento aún existentes. Las propiedades de estas novedosas nanopartículas y nanoestructuras son todavía, en gran parte, desconocidas. La nanotecnología nos exige reflexionar sobre la aplicación de los anteriores principios. La nanociencia y sus aplicaciones (nanotecnología) es un áreas de la ciencia de los materiales que aborda el estudio de objetos (una nanopartícula, NP) en escala nanométrica (orden de escala de centenares de nanometros, nm, 1 nm = 10^{-9}).

La OIT ha llamado la atención acerca del enorme desfase entre el conocimiento en las aplicaciones de la nanotecnología y el de su impacto en la salud, brecha que la Agencia Europea para la Seguridad y Salud en el Trabajo (EU-OSHA) cuantifica en 20 años, en su informe de 2013 titulado «Prioridades para la investigación sobre seguridad y salud laboral en Europa: 2013-2020». En 2009 el Comité Científico de los Riesgos Sanitarios Emergentes y Recientemente Identificados afirmaba: «se han demostrado los peligros que diversos nanomateriales fabricados entrañan para la salud y el medio ambiente. Los peligros identificados indican que los nanomateriales tienen efectos tóxicos potenciales en el ser humano y el medio ambiente. Sin embargo, es preciso señalar que no todos los nanomateriales inducen efectos tóxicos» (Galera, 2015).

Otro ejemplo de los riesgos que trae de la mano la industria 4.0 es el de las Impresoras 3D. Las mismas permiten un trabajo «sin moldes», personalizado y basado en el negocio «long tail». La misma impresora puede fabricar varios modelos de un mismo producto e, incluso, productos distintos realizados con un mismo material (por ejemplo, una pieza de un coche o de un grifo) durante el mismo periodo de tiempo o ciclo de producción. En el futuro, diversas clases de materiales se utilizarán en una impresora 3D, como plástico, aluminio, acero inoxidable, aleaciones de cerámica o incluso más avanzados. Según un estudio del Instituto de Tecnología de Illinois, cuando la impresora 3D trabaja con este material emite 20 mil millones de micro-partículas por minuto, que se depositan en los pulmones o el torrente sanguíneo y plantean riesgos para la salud, especialmente, para los enfermos de asma.

Este conjunto de realidades exige de una profunda adecuación de la forma en la que la empresa debe abordar estos futuros riesgos.

VI. EL CAMBIO TECNOLÓGICO Y LA NECESIDAD DE REPENSAR LA ACCIÓN COLECTIVA

Por otro lado, esta nueva realidad exige nuevos sistemas de representación: redes de información sindical o periódicos electrónicos. La «nueva cultura ciudadana de la comunicación» extiende a ámbito sindical un nuevo «*digital activism*». Como han recordado varios pronunciamientos judiciales, «la introducción en las empresas de medios de comunicación electrónicos en paralelo a los tradicionales o en sustitución de los mismos ha derivado en frecuentes litigios sobre los derechos de los trabajadores en estos nuevos contextos de organización. Las primeras respuestas judiciales a tales conflictos mostraron cierta incertidumbre en cuanto al conocimiento del verdadero alcance de las modificaciones que esa nueva forma de relación produce en el entorno laboral» (12). En la actualidad, tras la doctrina fijada por el Tribunal Constitucional, se han asentado unos principios básicos en esta materia que «se fundamentan en la ponderación del reconocimiento del derecho a la acción sindical en el entorno de comunicación electrónica, pero siempre ponderando los intereses en juego con los que exige la organización empresarial y el coste que el ejercicio de dicho derecho puede tener para la empresa».

El derecho fundamental de huelga también queda sujeto a restricciones tecnológicas. Como decía Sun Tzu: «El arte de la guerra no tiene una forma constante, lo mismo que el agua no tiene contornos». La relativa independencia, en determinados sectores industriales y de servicios, del funcionamiento del proceso productivo respecto del trabajo de una parte significativa de la plantilla, permite que muy pocos trabajadores puedan poner en marcha la producción con independencia de la mayoría de la plantilla de la empresa. Nuevas formas de «esquirolaje virtual» están en camino: huelgas en retransmisiones televisivas, en programas radiofónicos en los que se utilizan grabaciones efectuadas con anterioridad y son transmitidas sin intervención de persona alguna, o huelgas de teletrabajadores, pudieran ser un buen caldo de cultivo. Hace unos años, durante las negociaciones para la renovación del convenio colectivo interno de IBM Italia decidió organizar la primera protesta virtual de la historia en Second Life, con la ayuda de UNI. Ya no es infrecuente el uso de «youtube» para las reivindicaciones laborales. En los tiempos actuales aparecen fórmulas renovadas como el Netstrike o sentada virtual, una protesta pacífica en internet que consiste en que el mayor número de personas de varios países interactuén en un mismo sitio web de forma coordinada, lo que hace que el servicio de la página se vuelva lento, se sature la red y la página quede inutilizada por algunos momentos. El FloodNet es una aplicación

(12) Como resume la SAN de 10 de octubre de 2014 (R.º 207/2014).

de Java que consiste en hacer una protesta o sentada virtual como la de Netstrike, sólo que de forma automática recargando una página web varias veces a cada minuto (13).

VII. EL IMPACTO DE LA ROBÓTICA EN EL EMPLEO

Una de las cuestiones más complejas a las que deberá enfrentarse el futuro del trabajo es la relativa al impacto de los veloces procesos de robotización y de su impacto en unos debilitados mercados de trabajo marcados por la precariedad laboral y los altos índices de desempleo. La robótica tiene el potencial necesario para transformar las vidas y las prácticas laborales. Su impacto será cada vez mayor, a medida que se multipliquen las interacciones entre los robots y las personas. Aunque no existe un consenso sobre los efectos que ello tendrá sobre el empleo y nuestros futuros mercados de trabajo, lo que sí es indiscutible es que su impacto será muy importante. Son muchas las dudas que se plantean como consecuencia de ello: ¿Soportará nuestro modelo de trabajo la disrupción digital? ¿Cómo deben distribuirse los beneficios de la robótica? ¿La renta básica universal dejará de ser una posibilidad y pasará a ser una obligación? ¿Debemos seguir inventando? Son preguntas que lejos de resultar ciencia ficción ya esperan respuestas.

1. **¿Se cumplirá la profecía de Keynes?**

El 10 de junio de 1930, J. M. Keynes dictó en la Residencia de Estudiantes de Madrid la conferencia: «*Posible situación económica de nuestros nietos*»: Predijo que, como consecuencia del incremento de la productividad, nuestra jornada laboral no se extendería más allá de las 15 horas semanales a partir de 2030: se abría así un período de felicidad para los seres humanos. En 2030, «cada trabajador dispondría de maquinaria suficiente como para hacer de él un superhombre en comparación con su abuelo cien años antes» (14). No se equivocaba… Con los datos de la contabilidad nacional, si dividimos el total de horas trabajadas en España el 2015 por la población entre 16 y 64 años, el promedio es de 19,96 horas semanales cuando fueron 22,51 el 2008 (15). Dicha profecía ni remotamente tuvo en cuenta el impacto de la robotización ni tampoco los efectos de un mundo sin trabajo.

---

(13) De interés en relación con todas estas nuevas fórmulas es el trabajo de A. Rota, *La acción sindical en la sociedad altamente tecnológica. Una reflexión sobre el contexto italiano*, RTSS (CEF), 2018, n.º 420, pp. 77-99.

(14) Como resume R. Heilbroner, *Los filósofos terrenales*, Madrid, Alianza Editorial, 2015, p. 427.

(15) L. Torrens, E. Gonzalez De Molina, *La garantía del tiempo libre: desempleo, robotización y reducción de la jornada laboral*, en http://www.sinpermiso.info/.

La literatura más antigua acerca de la automatización puede dar algunas pistas sobre cómo los robots afectarán a los puestos de trabajo en el futuro. Algunos autores argumentan que los llamados puestos de trabajo de cualificación media son los que encuentran un riesgo mayor de desaparición. Estos trabajos, que han incluido históricamente contables, oficinistas, y ciertos trabajadores de las líneas de montaje, son relativamente fáciles de convertir en rutina. Esto dará lugar a que los trabajadores menos cualificados se encuentren abocados a desarrollar actividades con un más bajo nivel de competencias, lo que se traducirá, en el medio y largo plazo, en menores salarios y en unas mayores posibilidades de perder su empleo. Por el contrario, empleos altamente cualificados que implican las capacidades de resolución de situaciones, la intuición y la creatividad, y tareas que se realizan «en persona» y que precisan de ciertas destrezas y habilidades de comunicación social flexible para una mejor prestación de servicios (atención, trato, etc.), son más difíciles de convertir en rutina. Algunos autores señalan que los robots y la informatización no han sido capaces históricamente de replicar o automatizar estas tareas.

Los grandes volúmenes de datos y aprendizaje automático harán que sea posible automatizar muchas tareas que eran difíciles de automatizar en el pasado. En un estudio específico sobre los robots y los puestos de trabajo se demostró que en las industrias con niveles altos de densidad de robots los trabajadores de baja calificación trabajaban un número menor de horas (16). Si bien la robótica puede afectar a los sectores industriales de la economía de manera diferente, también es probable que afecte a las ocupaciones dentro de estos sectores de forma diferente.

¿Son los robots de almacén y los superordenadores los precursores de una ola tecnológica de progreso que finalmente va a barrer los seres humanos fuera de la economía? El «fantasma de la inutilidad nos acecha» (17).

Schumpeter señalaba con acierto que la innovación y la tecnología juegan un papel primordial como motores del crecimiento económico (18). Clásicamente, la innovación se asocia a la tecnología y aunque la innovación va mucho más allá, lo cierto es que en estos momentos el progreso tecnológico posee un indudable protagonismo. Desde una perspectiva económica, la innovación puede proyectarse sobre los productos o sobre los procesos operativos o comerciales o, incluso, podemos hablar de innovaciones organizativas. Los estudios empíricos indican en general que la

(16) G. Graetz, G. Michaels, *Robots at Work*, Centre for Economic Performance Discussion Paper No. 1335, London School of Economics, 2015.

(17) R. Sennet, *La cultura del nuevo capitalismo*, Barcelona, Anagrama, 2006, p. 81.

(18) Un detenido análisis de las ideas de desarrollo e innovación en el pensamiento de Schumpeter puede hallarse en X. Vence Deza, *Economía de la innovación y del cambio tecnológico*, Madrid, Siglo XXI, 1995, pp. 106-143.

innovación en productos genera empleo mientras que la innovación en procesos destruye empleo.

La industrialización –siendo un proceso de innovación de proceso– ha generado en los países más avanzados un aumento importante de la productividad y, por ende, ha permitido en estos países un nivel de vida antes impensable. Pero este aumento de productividad ha conllevado de forma ineludible un efecto negativo sobre la cantidad de empleo en los sectores donde se aplican estas innovaciones de proceso. El economista Vassily Leontief afirmó que «el papel de los seres humanos como factores más importantes de la producción queda disminuido de la misma forma que inicialmente el papel de los caballos en la industria agrícola, para luego ser eliminados por la introducción de los tractores» (19). Por ello, concluía, que «alegar que los trabajadores desplazados por las máquinas encontrarán necesariamente empleo en la construcción de dichas máquinas no es mucho más sensato que considerar que los caballos desplazados por los vehículos mecánicos pueden ser empleados directa o indirectamente en distintos sectores de la industria automotriz».

La anterior dinámica ha generado dos líneas de pensamiento. En un primer grupo se encontrarían los tecnoptimistas que considerarían la robotización como un «gran bluff» (20). Para ellos, el resultado neto entre destrucción de empleo y creación de nuevos empleos de las tres revoluciones industriales pasadas es que al tiempo que creció la productividad creció el empleo. El progreso técnico ha provocado un cambio estructural masivo: en 1900 el 41% de empleo en EE.UU. y el 63,6% en España estaba en la agricultura. Cien años más tarde estos porcentajes habían caído al 2% y al 6,9% respectivamente. Sin embargo, con menos empleo la producción es mucho mayor gracias a las máquinas y al progreso técnico. El efecto final durante buena parte del siglo XX fue un aumento de la productividad y de los salarios reales, sobre todo, tras la segunda revolución industrial, sin que aumentara el desempleo. Al contrario, la evidencia para muchos países es que cuanto más rápido crece la productividad tendencialmente menor es la tasa de desempleo como, por ejemplo, en EE.UU. o España en los años 60 y 70.

Lo más probable es que esto siga sucediendo, es decir que la economía dinámicamente genere nuevos empleos y nuevas necesidades a medida que hay exceso de trabajadores en algunos segmentos. Además, muchos empleos simplemente nunca se automatizarán: bomberos, fisioterapeutas, ortodoncistas y se crearán otros nuevos: científico de datos, programado-

(19) En la cita de J. Rifkin, *El fin del trabajo. Nuevas tecnologías contra puestos de trabajo: el nacimiento de una nueva era*, Barcelona, Paidos, 1998, p. 26.

(20) En la calificación de L. Torrens, E. Gonzalez de Molina, *La garantía del tiempo libre: desempleo, robotización y reducción de la jornada laboral*, en http://www.sinpermiso.info/.

res, diversos perfiles del campo de la ciberseguridad, consultor de sistemas de *big data*, desarrolladores, etc. De este modo se afirma que cada trabajo creado en sectores high-tech genera 4,9 empleos en sectores de bienes no comercializables y que el futuro contiene ocupaciones que nos parecerán tan extrañas como muchas de las actuales a nuestros abuelos. Así el Conseil d'Orientation pour l'Emploi ha señalado que las estimaciones de los riesgos de la automatización y digitalización no tienen en cuenta que los empleos actuales van a cambiar, ni la creación de empleo directa e indirecta derivada del cambio tecnológico La «gig economy» puede mejorar los emparejamientos laborales y la eficiencia del mercado de trabajo.

Nuestra falta de imaginación es en gran parte responsable del pesimismo actual. En suma, lo que ha hecho el progreso técnico no ha sido reducir el empleo, sino cambiar su composición (21), pero la gran cuestión es si estos nuevos puestos de trabajo se crean con la suficiente rapidez para reemplazar los puestos de trabajo perdidos. Por ello, un segundo grupo lo integrarían los tecnopesimistas, para quienes si bien históricamente la incorporación de la máquina ha sustituido más que destruido el empleo, el cambio al que nos enfrentamos esta vez sí va en serio y puede producir una destrucción masiva de puestos de trabajo.

Tanto Jeremy Rifkin como Martin Ford dan cifras escalofriantes: están en riesgo 90 de 124 millones de empleos a escala global; el desempleo tecnológico en los países industrializados podría llegar hasta el 75%. Otros informes también se sitúan en esta línea, en algunas industrias llegarán hasta un 40% de robotización. Se ganará en productividad de manera impresionante y el concepto de competitividad cambiará. El Foro Económico Mundial sobre el futuro del trabajo advierte de que, entre los años 2015 y 2020, la digitalización de la industria puede conllevar la desaparición de 7,1 millones de puestos de trabajo y la creación de 2,1 millones de nuevos empleos. Los expertos de CaixaBank Research pronostican que «un 43% de los puestos de trabajo actuales en España tienen un riesgo elevado de ser automatizados a medio plazo». A medida que la economía lentamente se reactiva, este componente de desempleo tecnológico puede pesar más de la cuenta: muchos puestos de trabajo que se destruyeron ya no volverán jamás; serán sustituidos por máquinas más eficientes. El informe *A future that works* elaborado por Mckinsey Global Institute alcanza unas soluciones más moderadas pero que, no por ello, generan menos incertidumbre. Dicho informe estima, en términos generales, que el 49% de las actividades que son remuneradas en la economía global tienen el potencial de ser automatizadas si se adaptan las tecnologías probadas en la actualidad. Aunque menos del 5% de las profesiones pueden ser total-

(21) S. Bentolila y J. F. Jimeno, ¿Nos van a quitar las máquinas de trabajar?, en nadaesgratis.es/

mente automatizadas, cerca del 60% tienen por lo menos un 30% de actividades automatizables.

La incorporación de nuevos procesos tecnológicos lleva no solo a una pérdida de empleo sino que también produce un segundo efecto: la «polarización de la ocupación» (22). Esto es, la pérdida progresiva de puestos de trabajo en los sectores con salarios medios. Una de las principales teorías para explicarlo viene, precisamente, de la mano de la incorporación de las nuevas tecnologías. Las mismas han disminuido la demanda de trabajadores que realizan tareas rutinarias que pueden ser mecanizadas fácilmente, a la vez que ha incrementado la demanda relativa de los puestos de trabajo que mantienen una cierta ventaja sobre la tecnología, ya sea porque precisan de mayor creatividad o porque requieren habilidades manuales o interpersonales. Pero la polarización podría llegar más lejos e incluir a sectores altamente cualificados. Buen ejemplo es el robot Watson. Este sistema de tecnología cognitiva que ha construido IBM permite que el robot pueda entender y responder preguntas complejas, planteadas en lenguaje natural, con suficiente precisión y velocidad para competir contra algunos de los humanos con más conocimientos del mundo (23). Además, se adapta al individuo que lo usa, con capacidad de relación y razonamiento y también de aprender de la experiencia. Watson pudiera convertirse en un sustituto a largo plazo de los abogados y a medio y corto plazo en una eficaz herramienta de control del razonamiento jurídico. La idea puede resumirse pragmáticamente: «*Every minute you spend on legal research is time you can't bill for*» (24).

En esta misma línea, el diario *El País* (25) informaba que la aseguradora japonesa Fukoku Mutual Life ha reemplazado a 34 empleados de oficinas, los denominados de cuello blanco, por un sistema de inteligencia artificial basado en el IBM Watson Explorer, capaz de calcular los pagos a los asegurados. El software instalado leerá decenas de miles de certificados médicos, duración de las estancias en el hospital, las historias médicas y cualquier procedimiento quirúrgico antes de calcular los pagos sin perjuicio de que las sumas no se pagarán hasta que sean aprobadas por un miembro del personal. Añade la noticia que «este no es un caso aislado. Según un informe del Instituto de Investigación Nomura de 2015, cerca de la mitad de los trabajos en Japón podrán ser realizados por robots en 2035».

---

(22) Al respecto, CES, *Informe sobre competencias profesionales y empleabilidad*, Madrid, CES, 2015, p. 24-30.

(23) https://www.unocero.com/2016/05/17/la-super-computadora-watson-se-convierte-en-abogado/

(24) http://www.rossintelligence.com/

(25) *El País* 5 de enero de 2017 en un artículo titulado «La robótica también sustituye a los empleados de cuello blanco».

En todo caso, tenemos ya la oportunidad de calcular la probabilidad de automatización de nuestras actividades a día de hoy. La página web *Will robots take my job?,* lo permite. Para saber si un puesto de trabajo corre peligro, el usuario tiene que escribir el nombre de su profesión y seleccionarla en una lista de trabajos relacionados.

Seamos tecno-pesimistas o tecno-optimistas el ser humano deberá diferenciarse de un robot en las tareas tanto personales como intelectuales que desarrolla. La cualificación profesional resulta, en este escenario, un factor fundamental que puede actuar como barrera o desincentivo al desempleo. Pero también las habilidades personales que separan al individuo de la máquina. De enorme interés son los resultados del «*Informe ADECCO sobre el futuro del trabajo en España*» (2016) (26). De acuerdo con el mismo, los expertos en recursos humanos encuestados, entre los que se encuentran responsables de Recursos Humanos de diferentes compañías nacionales e internacionales, creen que las cualidades que deberán reunir los trabajadores en 2025 estarán enfocadas a habilidades transversales que compartan todos los perfiles, independientemente de rangos o de formación concreta. Los criterios de selección del personal más relevantes serán, principalmente, las habilidades personales y las actitudes, les seguirán las competencias transversales resultando cada vez menos relevante la formación académica y la experiencia previa.

Como brillantemente ha resumido Edmund S. Phelps, Premio Nobel de Economía, en su reflexión «*Educar para el dinamismo económico*»: «El mercado laboral no solo necesita competencias técnicas, sino que requiere un número cada vez mayor de soft skills, como capacidad de pensar de modo imaginativo, de elaborar soluciones creativas para desafíos complejos y de adaptarse a circunstancias cambiantes y a nuevas relaciones».

2. «Cuando teníamos las respuestas, nos cambiaron las preguntas»

Las soluciones para abordar estas nuevas necesidades son diversas pero para plantear respuestas efectivas es necesario partir de una visión real de la situación. En relación con el mercado de trabajo, se vierten con cierto desenfado algunas afirmaciones cuestionables desde la perspectiva económica: «El progreso tecnológico destruye empleo, si las máquinas hacen el trabajo, habrá menos trabajadores ocupados». «Solo reduciendo la jornada de trabajo, mejorarán las oportunidades de empleo de los parados».

(26) http://www.adecco.es/

Detrás de las anteriores afirmaciones está la denominada falacia de la cantidad fija de trabajo (*lump of labour fallacy*) (27). Las falacias constituyen argumentos incorrectos, defectuosos y engañosos, es decir, argumentos de los que ya Aristóteles aseguraba que solo tienen la «apariencia» de tales. Pero es, precisamente, su condición de «argumentos aparentes» lo que los convierte en temibles fuentes de confusión. La idea de que la cantidad de trabajo está determinada exógenamente constituye una de las falacias más conocidas en Economía y, sin embargo, más repetidas en muchas de las propuestas de políticas de empleo. Otro nombre para la falacia en cuestión es «falacia de suma cero». En la teoría de juegos, un juego suma cero es aquel en el cual la suma del bien ganable de todos los jugadores permanece constante. En otras palabras, todo lo que un jugador gana, es perdido por otro u otros jugadores. El error es creer que la cantidad de trabajo es fija, como un pastel y que, por tanto, de lo que se trata es de repartir bien el pastel para que haya para todos. El error estriba en que no hay tal cosa como una cantidad de trabajo establecida de antemano y los empleos son creados por la inversión en función de la productividad. Si fuera así, bastaría con reducir por ley las horas de trabajo para acabar totalmente con el paro (28). Implantar medidas como los fines de semana de tres días se convierte, en una solución a corto plazo, en algo esencial para que la vida sea viable en unas condiciones económicas diferentes (29), pero probablemente los problemas en el futuro lleven consigo retos más profundos.

Hacen falta más respuestas pero lo cierto es que las preguntas también han cambiado. En suma, como resumió Jorge Eduardo Adoum: «Cuando teníamos las respuestas nos cambiaron las preguntas».

2.1 Debemos dejar de inventar o inventar más despacio: ¿Hacia «empresas tecnológicamente responsables»?

En este contexto, la respuesta social a estos cambios nos puede retrotraer a las que se dieron durante la primera de las revoluciones industriales: la reacción luddita. Este movimiento rechazaba el porvenir, a través de la destrucción de las fábricas que consideraba prisiones y del rechazo del trabajo asalariado que presentían como una nueva forma de esclavitud, sin plantear alternativas. Este modo de pensar escenifica lo que ha

(27) P. Schwartz. *Las reducciones forzadas de la oferta de mano de obra para combatir el paro*, Cuadernos de Ciencias Económicas y Empresariales, 1979, n.º 5, págs. 199-230. En el blog «*Nada es gratis*» la entrada, *Aprendiendo a sumar (I): La falacia de la cantidad fija de trabajo.*

(28) Para una reflexión de conjunto sobre estas ideas nos remitimos a J. R. Mercader Uguina, *Se busca… El mercado de trabajo en España*, Barcelona, Debate, 2014, en concreto el apartado: ¿Trabajar menos para trabajar todos?

(29) Como proponen, N. Srnicek, A. Williams, *Inventing the Future: Postcapitalism and a World without Work*, London, Verso, 2015.

calificado el filósofo francés Onfray como la política del rebelde (30). Los «espectros de Ludd» (31) adquieren nuevos perfiles en la actual sociedad tecnológica pues la negación de la evidencia sigue y seguirá constituyendo una reacción propia del género humano, incluso, en la era de lo posthumano (32).

Las nuevas tecnologías están provocando en la actualidad una alteración del mercado de trabajo pero una reacción luddita no lo evitará. Por el contrario, el entorno en el que se produzca este cambio y cómo reaccionen los actores influirán en el alcance y la manera en que se materialice este potencial de crecimiento, sobre todo a corto plazo. Por ello, no siendo factible tal rotunda acción, ¿no sería mejor que las empresas fueran responsables al controlar la creciente incorporación del cambio tecnológico? Las grandes corporaciones son sensibles a los efectos que puede producir en el medio y largo plazo el desarrollo de la tecnología y, en particular, de la robótica. Pensar en un modelo de desarrollo de empresas tecnológicamente responsables puede abrir nuevos caminos de reflexión.

2.2 ¿Regreso al artesanado?

El «trabajo» y el «trabajador» de la era de la técnica adquieren una morfología singular. Las nuevas tecnologías transforman la percepción del trabajo y pueden contribuir a la transformación de los modos de prestación de servicios. Su singularidad pone en cuestión los moldes clásicos de definición no solo de las fórmulas tradicionales de trabajo por cuenta ajena sino, incluso, las de trabajo autónomo tradicional. Se hace necesario reformular su concepción tradicional. En este contexto, el regreso al artesanado marca una senda en esa dirección.

La lucha del artesano con las máquinas se remonta a las páginas de la Enciclopedia de Diderot. La artesanía es, pues, la resistencia silente de la creación humana pues todas las habilidades, incluso las más abstractas, empiezan como prácticas corporales; la comprensión técnica se desarrolla a través del poder de la imaginación (33). En una época de transformación tecnológica, la vuelta a la creación paciente del ser humano, a la individualización de las creaciones y a la huida de la rutina de la producción en masa puede ser una respuesta al desafío de la robotización. Buena muestra de esta tendencia viene de la mano de la progresiva expansión de las impresoras 3D cuyas características y forma de producción podrían dar lugar a

(30) M. Onfray, *La política del rebelde. Tratado de resistencia e insumisión*, Madrid, Anagrama, 2011, p. 282, quien no duda en afirmar que: «en estos tiempos sombríos harían falta el espíritu y la acción de nuevos ludditas, cuya voluntad de fuego furioso suscribiría yo de muy buen grado…».

(31) J. Van Daal, *La cólera de Ludd*, Logroño, Pepitas de Calabaza, 2015, pp. 291.

(32) Como la ha calificado, R. Braidotti, *Lo posthumano*, Barcelona, Gedisa, 2015.

(33) R. Sennet, *El artesano*, Barcelona, Anagrama, 2009.

la formación de un nuevo artesanado. Las mismas permiten un trabajo «sin moldes», personalizado y basado en el negocio «long tail» (34).

2.3 ¿Tienen que cotizar los robots a la Seguridad Social?

El diario El País del día 17 de octubre de 2016, nos sorprendía en su página 47 con un titular inquietante pero enormemente sugerente: ¿Tienen que cotizar los robots a la Seguridad Social? La pregunta es inteligente por dos motivos. Por un lado, pone sobre la mesa un camino de salida a la crisis de nuestro sistema de Seguridad Social, por otro, plantea la forma y modo de reparto de los beneficios potenciales que pueden producir los incrementos espectaculares de productividad y riqueza que puede generar en el futuro próximo la revolución robótica. Pero si los robots crean los problemas, ¿podrían ayudar a resolverlos?

Se hace necesario, por lo tanto comenzar a construir y a reflexionar sobre posibles soluciones para el caso de que la profecía de Keynes cobrara definitivamente vida. Algunos pueden ver aquí el triunfo de quienes han predicado los males del trabajo y han alentado a su definitiva y total abolición. Pero si los robots terminan por eliminar la necesidad de trabajo humano en grandes masas de población ello llevaría consigo un nuevo «darwinismo» que nos obligaría, esta vez, a atender a las necesidades de subsistencia para ese creciente y progresivo volumen de población que se verá excluida de los mucho más selectivos mercados de trabajo. Por ello, es necesario afrontar algunos desafíos, entre ellos, uno de los más importantes es el de pensar en cuáles deben ser las políticas públicas más adecuadas para que este mayor bienestar llegue a todas las personas y evite una mayor desigualdad. El reto es gobernar la transformación tecnológica y digital, con niveles reducidos de desigualdad y de tasa de desempleo.

Martin Ford, uno de los teóricos más influyentes en la literatura sobre robótica de los últimos años se plantea en su obra, «*El auge de los robots*» (35), un nuevo paradigma económico para esta nueva era. En él sitúa la necesidad de costear una renta básica que evitara las posibles desigualdades sociales de la nueva sociedad que está naciendo. El establecimiento de una renta básica, «subsidio universal» o incluso «ingreso de ciudadanía», supondría garantizar a todas las personas, de forma automática e incondicionada, un ingreso periódico de subsistencia (36).

---

(34) Las ideas siguientes proceden de M. Sachon, *Impresión 3D: La digitalización de la fabricación*, Revista de Antiguos Alumnos del IESE, 2016, n.º 141, pp. 26-29.

(35) M. Ford, *El auge de los robots*, Barcelona, Paidos, 2016, pp. 252-253.

(36) La literatura sobre esta materia es muy amplia y pueden encontrarse en internet reflexiones de gran interés. Magnífico ejemplo es el trabajo de J. Gimeno Ullastes, *Aproximación a una Renta Básica Sostenible* [en http://www5.uva.es/jec14/comunica/A_EByRB/A_EByRB_9.pdf]. Las bases para tener una conciencia precisa de esta cuestión pueden hallarse en el libro

Las justificaciones que se han buscado a la necesidad de implantar este tipo de ingresos básicos se sitúan en la obligación de toda sociedad de asegurar a todos la satisfacción de las «necesidades esenciales» en nombre de la dignidad y de la condición de ciudadanos de los beneficiarios. Sin embargo, los programas de rentas mínimas han sido duramente criticados, pues se consideran instrumentos que pueden subvencionar la ociosidad. El reciente referéndum planteado en Suiza ha puesto sobre la mesa esta cuestión pero, en una sociedad en las que las máquinas asegurarían elevados índices de productividad, ¿sería eso un problema?

Es posible también imaginar un *«dividendo robot»* (37) que permita retornar a la sociedad al menos una parte de los beneficios financieros que generen a través de fórmulas distintas. El estado de Alaska ofrece una posible solución a través del Alaska Permanent Fund. Una parte de los ingresos del petróleo del Estado se deposita en el fondo y, cada mes de octubre, se reparte un dividendo que se le da a cada residente elegible (38). Esta solución es fruto de la acción humana a través de una decisión democrática. Todo ello pone de manifiesto que cuanto mayor y más complejo resulte el edificio de la civilización en la que habitamos, más necesario será conocer los límites y los fines de nuestras «democracias». En esta línea podrían situarse otras opciones vinculadas al desarrollo de diversos impuestos…

Por otro lado, si, como irónicamente definió el escritor inglés Chesterton, la tecnología es «un conjunto de conocimientos que reduce el número de trabajadores... y de dueños», por qué no pensar en que los seres humanos sean propietarios de robots y éstos trabajen para ellos. La resurrección de esta nueva forma de esclavitud no se separa mucho de la mentalidad de las sociedades griega y romana antigua cuando la vida privilegiada del ciudadano dependía del sudor de aquel puro ganado humano, totalmente desprovisto de derechos civiles y concebido como mera mano de obra («herramientas que hablan», en palabras del erudito romano del siglo I a. C. Varrón), que eran los esclavos (39). No es necesario recordar la enorme riqueza y el impacto económico que tuvo en la economía y, en general, en el desarrollo de nuestra civilización esta terrible forma de explotación. Tampoco debe olvidarse la realidad de una sociedad romana en la que los tiempos de ocio superaban a los tiempos de actividad. El trabajo de los esclavos dejaba a los ciudadanos libres enormes periodos de inactividad.

---

clásico de D. Raventos, El derecho a la existencia, Una propuesta del subsidio universal garantizado, Ariel, 1999.

(37) E. Brynjolfsson, A. Mcafee, *Will Humans Go the Way of Horses?*, *cit.*

(38) Un interesante estudio al respecto puede verse en M. J. Gomez-Millan Herencia, *El ingreso permanente de Alaska como forma de articular la renta básica universal e incondicionada*, RTSS (CEF), 2017, n.º 407, pp. 83-115.

(39) M. Beard, J. Henderson, *El mundo clásico: Una breve introducción*, Madrid, Alianza Editorial, 2016, p. 83.

Todo ello nos puede llevar a la necesidad de una profunda reflexión sobre el valor del ocio en el futuro. Así, se ha propuesto en vez de trabajar más horas con pocos resultados productivos adoptar una semana laboral más corta (implantar medidas como los fines de semana de tres días) y contribuir a salvar nuestro planeta a través de una reducción notable del consumo de energía y nuestro bienestar. Una sociedad que, como se anticipó hace años, parece dirigirse del paro al ocio (40). Un ocio fundado en el trabajo robótico, una entera sociedad del ocio… Algunos pueden ver aquí el triunfo de quienes han predicado los males del trabajo y han alentado a su definitiva y total abolición (41).

En suma, nos enfrentamos a un conjunto de retos y cuestiones de no fácil solución. Pero lo que es evidente es que no podemos apartar la mirada de estos problemas y la sociedad tiene el reto de dar respuestas precisas a estas realidades cada vez más presentes en nuestras vidas.

(40) Tesis anticipada en su día por L. Racionero, *Del paro al ocio*, Barcelona, Anagrama, 1990.

(41) Provocadora pero verdaderamente divertida es la obra de B. Black, *La abolición del trabajo*, Pipas de Calabaza, 2013 que nos actualiza la clásica de P. Lafargue, *El derecho a la pereza*, Madrid, Fundamentos, 1980. Obra que veía, precisamente, en la máquina «la redentora de la humanidad, el Dios que liberará al hombre de las *sordidae artes* y del trabajo asalariado, el Dios que le dará el ocio y la libertad».

CAPÍTULO 30
ECONOMÍA COLABORATIVA

LUIS ANTONIO VELASCO SAN PEDRO
Catedrático de Derecho Mercantil
Universidad de Valladolid

1. INTRODUCCIÓN (1)

El término *economía colaborativa* o *participativa* (*sharing economy*), pese a su imprecisión, se ha acabado imponiendo para designar

(1) El presente capítulo se realiza en el marco del proyecto del Ministerio de Economía y Competitividad, DER2014-58744-R «Competencia y Distribución: nuevos retos en la sociedad globalizada y en contextos de crisis económica». En parte es tributario de aportaciones anteriores del autor, aunque se revisan y matizan algunos planteamientos, particularmente a la luz de la

nuevos modelos de intercambio de bienes o servicios, surgidos en la llamada *sociedad de la información* (2), a partir de plataformas *ad hoc* creadas en Internet. Los sectores más desarrollados hasta el momento son los que tienen que ver con el transporte de personas –*Uber*, *Cabify*, *BlaBlaCar*–, y los del alojamiento temporal o turístico –*Airbnb*, *TripAdvisor Rentals, Hipmunk*–. No obstante, el fenómeno excede de estos ámbitos, y afecta a otros muchos aspectos como los de la financiación colaborativa y el micro mecenazgo (*crowdfunding*) –*Lendix, Verkami*, *Kickstarter*–, la venta de bienes de segunda mano –*eBay, Wallapop, ThrepUP* (especializada en ropa)–, el trabajo temporal –*Hulajob*–, el suministro de comida a domicilio –*Just Eat, UberEATS, Compartoplato*–, la restauración a domicilio –*Just Cook It*–, los bancos de tiempo (intercambio de servicios entre particulares), etc. (3).

No todas estas manifestaciones son *negocios en la red* (en el sentido de *business*), pues también actúan en este ámbito simples particulares que tratan solamente de compartir bienes o servicios entre ellos y/o sin contraprestación a través de Internet (de *consumo colaborativo* se habla en estos casos, aunque como se verá más adelante con cierta impropiedad). Ésta es la cara *amable* de la economía colaborativa que, por presentar una dinámica de cooperación o de compartir con otros, ni suscita críticas ni se censura su existencia (4). No ha ocurrido lo mismo, sin embargo, con las modalidades que suponen contraprestaciones de carácter remuneratorio y, por tanto, auténticos negocios, que además, al entrar en conflicto (en competencia) con modelos más tradicionales o por sus externalidades, han sido en algunos casos –como son los del trasporte y el alojamiento turístico– fuertemente cuestionados.

---

reciente sentencia del Tribunal de Justicia en el caso *Uber*. Concretamente de los trabajos (Velasco San Pedro, L. A.) «El consumo colaborativo en el transporte de personas», en Petit Lavall, M.ª V./Puetz, A. (dirs.): *La eficiencia del transporte como objetivo de actuación de los poderes públicos: liberalización y responsabilidad*, Marcial Pons, Madrid 2015, pp. 193 y ss. (el trabajo fue anticipado en *Diario La Ley*, n.º 8601, Sección Documento on-line, 9 de septiembre de 2015) y «El transporte colaborativo *hic et nunc*», en *Revista de Estudios Europeos*, n.º 70, 2017, pp. 398 y ss.

(2) Sobre los orígenes y los rasgos que caracterizan a la *sociedad de la información*, *vid.* Salvat Martinrey, G./Serrano Martín, V.: *La revolución digital y la sociedad de la información*, Comunicación Social, ediciones y publicaciones, Manganeses de la Lampreana 2011, esp. p. 14, donde señalan cómo este término se generalizó a partir de la publicación en 1981 de la obra del sociólogo japonés Yonei Masuda *The Information Society as Post-Industrial Society*, quien además de vaticinarla la situaba como una sucesora de la *sociedad industrial*.

(3) Tampoco dejan de tener una conexión con el fenómeno las nuevas *criptomonedas*, de las que el *bitcoin* es la más desarrollada, habida cuenta de que también se originan de forma colaborativa en la red [*vid.*, entre otros trabajos recientes, Echebarría Sáez, M.: «Contratos electrónicos autoejecutables (smart contract) y pagos con tecnología blockchain», en *Revista de Estudios Europeos*, n.º 70, 2017, pp. 69 y ss., y Pastor Sempere, C.: «Criptodivisas: ¿una disrupción jurídica en la eurozona?», en *Revista de Estudios Europeos*, n.º 70, 2017, pp. 284 y ss.]. La especificidad de esta materia, sin embargo, ha aconsejado dejarla al margen de este capítulo.

(4) Herrero Suárez, C.: «La economía colaborativa en el sector del alojamiento turístico», en Miranda Serrano, L. M.ª/Pagador López, J.: *Retos y tendencias del Derecho de la contratación mercantil*, Marcial Pons, Madrid 2017, p. 146.

En cualquier caso, desde una óptica jurídica la economía colaborativa carece a la fecha de un régimen general que le sea aplicable por igual a todas sus manifestaciones, en el conjunto del Derecho comparado, y en el español y el europeo, si bien es cierto que, como se verá más adelante, el entramado legal básico existente respecto a la *sociedad de la información*, sí que lo será en ciertos aspectos relacionados con la actividad de los operadores de las plataformas colaborativas (5). Ello supone la existencia de un *vacío legal* (6) que, según los casos y tiempos, ha sido aprovechado por estos operadores –particularmente por los más cuestionados– para expandirse, o por los que se sitúan enfrente de algunas manifestaciones –en relación principalmente con el transporte y los alojamientos turísticos– para tratar de frenar o, al menos, obstaculizar su desarrollo.

En este proceso, que dista de estar cerrado, y en relación con los sectores controvertidos, han intervenido de un lado los propios operadores de las plataformas de intercambio y autoridades favorables a la expansión del fenómeno (en España la CNMC, en Europa la CE y el CESE), y de otro lado competidores que se sienten perjudicados (asociaciones de taxistas y otros transportistas, hoteleros, etc.) y autoridades contrarias o, al menos, reticentes con estas manifestaciones (en España principalmente autoridades locales y autonómicas, aunque también el Ministerio de Fomento). Los conflictos han ido derivando hacia procedimientos judiciales, donde se registran, en el caso específico de España, pronunciamientos favorables y contrarios a algunas manifestaciones en los sectores del transporte y del alojamiento.

En el ámbito europeo hay que destacar la reciente sentencia del Tribunal de Justicia de la UE de 20.12.2017, en el asunto C-434/15 *Uber*, precisamente en respuesta a una cuestión prejudicial planteada por un juez español, y que creo que marca *un antes y un después* en la materia. Esta sentencia, sin pronunciarse en contra o a favor del fenómeno, reconduce a las reglas nacionales del transporte el funcionamiento de ciertas tipologías de plataformas de transporte colaborativo. Esto supone en la práctica la prohibición de modelos de negocio, como era el que sirvió de base al procedimiento –la plataforma *UberPop*–, de transporte metropolitano prestado por particulares en vehículos privados, por ser incompatibles con regulaciones fuertemente restrictivas, como eran en el caso concreto

(5) *Vid.* en el ap. 5.

(6) Sí hay en España una regulación del *crowdfunding* en los artículos 46 y ss. de la Ley 5/2015, de 27 de abril, de fomento de la financiación empresarial. Sobre esta modalidad de economía colaborativa, *vid.* Moreno Serrano, E.: «El *crowdfunding* en el marco de la contratación internacional», en Miranda Serrano, L. M.ª/Pagador López, J.: *Retos y tendencias*... cit., pp. 847 y ss., y Hernández Sainz, E.: «El *crowdfunding* inmobiliario mediante contratos de cuentas en participación: una fórmula de inversión participativa ¿alegal o prohibida?», en *Revista de Estudios Europeos*, n.º 70, 2017, pp. 126 y ss.

las del taxi en España (en la sentencia representadas por el Reglamento metropolitano del taxi en Barcelona). Lo cual abre la puerta a que, al menos esta manifestación de la economía colaborativa, se someta a prohibiciones o restricciones puramente nacionales.

Con todo, los operadores de las plataformas de economía colaborativa más controvertidas han podido hasta la fecha «capear el temporal», mostrando una gran capacidad de adaptación ante los panoramas regulatorios hostiles. Así sucedió en España y otros países, con la referida plataforma *UberPop* creada por *Uber*, que antes de la sentencia del Tribunal de Justicia de la UE ya había sido abandonada por esta empresa a la búsqueda de otros ámbitos regulatorios más confortables, como ha sido en España, el de los *vehículos de alquiler con conductor* (VTC), que actualmente se usa como cobertura legal no solo por *Uber*, sino también por otros operadores como *Cabify* (7). El conflicto, sin embargo, lejos de amainar continúa, y se anuncian en España nuevas regulaciones restrictivas en este último ámbito, y en otros paralelos como los del alojamiento temporal o turístico.

Las anteriores circunstancias delinean un panorama de todavía fuerte incertidumbre jurídica, y con numerosos problemas abiertos, a la espera de que algún día los legisladores (europeo y/o nacional), establezcan un marco claro para estas actividades y, en todo caso, más equilibrado, evitando los actuales sesgos en uno u otro sentido, teniendo en todo caso muy claro que, como también se ha dicho, la economía colaborativa ha llegado para quedarse (8).

A la espera de esos momentos –si es que alguna vez llegan–, en este capítulo nos vamos a referir, en apartados sucesivos, por una parte, a *aspectos generales* de la economía colaborativa, como son su caracterización y la distinción de sus principales modalidades [2]; la valoración de lo que hay de nuevo y de antiguo en el fenómeno [3]; el debate en torno a sus aspectos positivos y negativos [4] y su subsunción en el Derecho de la UE [5]. Por otra parte, se analizarán, con la brevedad que impone una obra de carácter general, las *manifestaciones de la economía colaborativa* más desarrolladas y, en cualquier caso, polémicas, como son, por un lado, el transporte colaborativo [6], y, por otro, el alojamiento temporal o turístico [7].

(7) El Tribunal Supremo, como vaticinaba la doctrina [Doménech Pascual, G.: «La regulación de la economía colaborativa en el sector del taxi y los VTC», en Montero Pascual, J. (dir.): *La regulación de la economía colaborativa. Airbnb, BlaBlaCar y otras plataformas*, Tirant lo Blanc, Valencia 2016, p. 356] ha procedido a reconocer el derecho a obtener licencias VTC de diversos solicitantes, que utilizaron la *ventana de liberalización* del sector desde la reforma de la Ley de Ordenación de los Transportes Terrestres de 2009, y la ulterior anulación de su desarrollo reglamentario, a la reforma reglamentaria restrictiva de 2015, en las dos primeras sentencias de un aluvión de las que se esperan sobre la materia, y que se están usando como cobertura para sus plataformas por *Uber* y *Cabify*. *Vid.* http://www.iustel.com/diario_del_derecho/noticia.asp?ref_iustel=1171278.

(8) Herrero Suárez, C.: *op. cit.*, p. 148.

2. CARACTERIZACIÓN, DISTINCIÓN DE ASPECTOS Y NATURALEZA DE LAS RELACIONES QUE SURGEN DE LA ECONOMÍA COLABORATIVA

Como se acaba de indicar, el término *economía colaborativa* es relativamente impreciso. Tratando de dotarle de una mayor concreción, la reciente comunicación de la CE de 2016 sobre *Una Agenda Europea para la economía colaborativa* (9), la describirá, más que definirá, como *«modelos de negocio en los que se facilitan actividades mediante plataformas colaborativas que crean un mercado abierto para el uso temporal de mercancías o servicios ofrecidos a menudo por particulares»* (10).

Lo decisivo en esta descripción, como se apuntó anteriormente, es la intervención de las *plataformas colaborativas*, ya que sin ellas no puede hablarse de economía colaborativa, en el marco de Internet y con aplicaciones específicas (*apps*) que pueden ser usadas también por *smartphones* y *tablets*, creadas *ad hoc* por prestadores de servicios en la red como son *Uber*, *Airbnb*, etc., que, en principio, hacen de ello un negocio, obteniendo por su intermediación (profesional) rendimientos económicos directos o indirectos (11).

La *actividad de la plataforma* consiste inicialmente en facilitar a través de estas tecnologías, la *puesta en contacto entre oferentes y demandantes* de concretos bienes o servicios y, en su caso, la celebración de los correspondientes contratos. En este punto, debe distinguirse de la *actividad subyacente* constituida por el suministro o el intercambio efectivo de tales bienes o servicios (12), aunque en ciertos casos dicha actividad puede prestarse también por la plataforma (13). Como ya se ha indicado esta actividad puede ser diversa, y consistir en transporte, alojamiento, financiación, intercambio de viviendas o vehículos, etc.

Tanto los oferentes como los demandantes que intervienen en la actividad subyacente, pueden ser los dos *profesionales* (14), por lo que estaríamos hablando de relaciones B2B; serlo solo uno de ellos –el oferente

(9) Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *Una Agenda Europea para la economía colaborativa* {SWD(2016) 184 final}. Bruselas, 2.6.2016, COM(2016) 356 final.

(10) Comunicación, ap. 1, p. 3.

(11) Con todo, aunque no es el supuesto de mayor frecuencia, existen también plataformas creadas por entidades sin ánimo de lucro, como suele ser, p. ej., el caso de los *bancos de tiempo* para intercambio de servicios entre particulares, frecuentemente promovidos en España por administraciones locales.

(12) Esta distinción entre la *actividad de la plataforma*, y la *actividad subyacente*, aparece delimitada con bastante claridad y acierto en el informe del Abogado General en el citado asunto *Uber* (Conclusiones del Abogado General Sr. Maciej Szpunar presentadas el 4.7.2017, asunto C320/16 *Uber France SAS*).

(13) Este es el caso, según parece, de las actuales plataformas de transporte colaborativo a través del automóviles con licencias VTC (*Uber* y *Cabify*).

(14) Desde la óptica del artículo 1 del Código de comercio español se trataría de *empresarios*.

lógicamente–, en cuyo caso se trataría de relaciones B2C; o no serlo, finalmente, ninguno de los dos, tratándose en este supuesto de relaciones C2C, o *entre pares* (P2P), como prefiere decir la citada Comunicación de la CE de 2016 (15). En este último aspecto, se habla también de *consumo colaborativo* como una submodalidad de la economía colaborativa (16), aunque el término *consumo* se utiliza aquí más en sentido económico que jurídico, pues las *relaciones de consumo* consideradas por el llamado *Derecho del consumo*, se caracterizan siempre por la intervención de un profesional frente a un consumidor –en realidad se trata de proteger a los consumidores en sus relaciones con éstos (17)–; esto es, tienen que ser siempre relaciones B2C.

La caracterización de estas relaciones inicialmente resultará de la propia configuración que haga la aplicación. P. ej. en transporte existen aplicaciones dirigidas tanto a profesionales (taxistas, titulares de VTC), como pueden ser en la actualidad en España, *Uber* y *Cabify*; como aplicaciones dirigidas a particulares, como es el caso de *BlaBlaCar*. Pero esta calificación inicial debe ulteriormente depurarse con un análisis sustantivo de la actividad subyacente, para ver si la misma puede o no considerarse una actividad profesional. Es lo que pasaba con *UberPop*, una plataforma inicialmente desarrollada para cualquier tipo de conductor, entre ellos principalmente los particulares, pero que por su configuración, permitía el desarrollo a través de ella de la prestación de servicios que merecen desde un punto de vista sustantivo su consideración como una actividad profesional de transporte público. Lo mismo puede suceder con las plataformas de alojamiento turístico, como *Airbnb*, que *de facto* pueden acabar acogiendo a profesionales del alquiler turístico en forma de personas que adquieren viviendas *ad hoc* y quieren hacer de ello su modo de vida, y no de personas que solo ocasionalmente quieren arrendar su vivienda infrautilizada (18).

---

(15) Ap. 2.1, p. 5.

(16) Véase Dictamen del Comité Económico y Social Europeo (CESE) sobre *Consumo colaborativo o participativo: un modelo de sostenibilidad para el siglo XXI* (Dictamen de Iniciativa), DOUE C 177/1, de 11.6.2014, ap. 3.1, que define a este consumo como *«[l]a manera tradicional de compartir, intercambiar, prestar, alquilar y regalar a través de la tecnología moderna y las comunidades»*.

(17) Este matiz fue ya en su momento destacado por la Sentencia del Tribunal Constitucional 71/1982, de 30.11.1982 sobre el Estatuto del Consumidor del País Vasco, al interpretar el artículo 51 de la Constitución (fundamento de Derecho 11), y se recoge ahora acertadamente en el artículo 2 del Texto refundido de la Ley general para la defensa de los consumidores y usuarios de 30.11.2007 (*«[e]sta norma será de aplicación a las relaciones entre consumidores o usuarios y empresarios»*), superando la falta de técnica que a este respecto acreditaba la anterior Ley general para la defensa de los consumidores y usuarios de 1984.

(18) A ello cabe añadir que las plataformas pensadas para particulares, pueden acabar siendo utilizadas por profesionales del transporte o el alojamiento, como señala Herrero Suárez, C.: *op. cit.*, p. 147.

La distinción señalada, no es una cuestión de mera taxonomía jurídica, sino como se verá más adelante, un aspecto esencial para determinar en el momento presente el régimen jurídico aplicable, en relación con aquellas actividades empresariales que estén reguladas, como han precisado algunas sentencias judiciales en España, y la ya citada del Tribunal de Justicia en el asunto *Uber*, a las que más adelante se hará referencia.

3. LO QUE HAY DE NUEVO Y DE ANTIGUO EN LA ECONOMÍA COLABORATIVA

Pese a su aparente novedad, muchas de las manifestaciones de la actual economía colaborativa *han existido desde antiguo*. Desde compartir vehículo para ir a trabajar o hacer viajes largos (p. ej. el viejo *autostop*), pasando por intercambiar cosas (cromos, sellos, novelas, tebeos…) o servicios (yo te doy unas clases de inglés, y tú me arreglas el jardín, etc.), hasta compartir casas (entre estudiantes o compañeros de trabajo) o alquilar habitaciones en residencias particulares, por periodos largos o por días, o apartamentos turísticos en las épocas en que no iban a ser ocupados por sus propietarios (19). Aunque en alguno de estos supuestos había contraprestaciones –no en todos, ciertamente (20)–, que solían ser una manifestación de lo que, en términos piadosos, podemos llamar *economía informal* (21), la cuestión no llamaba la atención ni a las autoridades públicas, por su escaso impacto (tributario, urbanístico, etc.), ni a los sectores que ofrecían prestaciones análogas de manera profesional (taxistas, hoteleros, etc.), al recoger aquellos una demanda más bien residual.

Lo que hay de nuevo es el inusitado auge que han tenido estas manifestaciones con la llegada de las nuevas tecnologías de la información y la comunicación –Internet, aplicaciones específicas, *tablets*, *smartphones*, etc.– y la aparición de las plataformas especializadas, que han hecho de estas actividades su objeto de negocio. También, sin duda, ha coadyuvado a todo ello la *crisis económica de 2007-2008*, que ha visualizado la necesidad de muchos ciudadanos de contar con nuevos ingresos, y en todos la de reducir costes (22). A este respecto, y en relación con el transporte colaborativo, es patente que permite conseguir nuevos ingresos (sean estos profesionales o simplemente para compartir gastos), y reducir sobrecostes en forma de *precios supracompetitivos*, al estar al margen del

(19) Todavía recuerdo como en otros tiempos cuando arribabas en verano a una ciudad costera por tren o automóvil, solía haber personas que ofrecían a los viajeros alojamiento en casas particulares.

(20) P. ej. no las había ni las hay en el *autostop*, ejemplo paradigmático de transporte colaborativo.

(21) Es decir, *de facto* no sometida a impuestos.

(22) Insistía en este aspecto el ya citado Dictamen del CESE, ap. 4.2.

control administrativo de operadores y de tarifas, característico del transporte tradicional regulado administrativamente, y, por tanto, sometido a mayores presiones competitivas, por la irrupción de nuevos agentes, la libertad de precios y la drástica reducción de las asimetrías de información, entre otros aspectos (23).

Ante este auge, se ha generado la reacción de los sectores tradicionales en competencia, que han visto en estas actividades un contrapeso hasta entonces inexistente, y de las autoridades públicas que ya no pueden seguir ignorando estas manifestaciones, que ya no tienen efectos marginales, ni sobre los impuestos (24), ni sobre otras normas legales (regulatorias, laborales, etc.), incidiendo en todo caso sobre la competencia, que todos los estados quieren defender y, al menos teóricamente, promover (25).

Se trata en todo caso, de un sector en crecimiento exponencial. Como informa la Comunicación de la CE de 2016, en 2015 las plataformas colaborativas generaron unos ingresos brutos de 28.000 millones de euros, doblando en cinco sectores estratégicos las cifras de 2014. Se prevé además un potencial en el futuro para la economía de la UE de entre 160.000 y 572.000 millones de euros (26).

4. EL DEBATE

4.1 **Los bandos del debate y sus argumentos básicos**

El debate sobre la economía colaborativa, centrándonos en dos de los sectores que han generado mayor polémica, como son los del transporte y el alojamiento turístico, tiene dos bandos bien diferenciados de partidarios y detractores, con su respectivo argumentario.

---

(23) Sobre los efectos económicos del transporte colaborativo, véase la acertada síntesis de Doménech Pascual, G.: *op. cit.*, pp. 362 y ss.

En todo caso, los *precios supracompetitivos* como es bien sabido son una (mala) característica de los mercados sin competencia o con competencia restringida, como enseña la *teoría del monopolio*, de la que hay además abundante evidencia empírica. Por todos, *vid.* Posner, R. A.: *Antitrust Law*, 2.ª ed., The University Chicago Press, Chicago-London 2001, pp. 9 y ss.

(24) Una manifestación clara de lo que estoy diciendo, en relación con la incidencia fiscal de estas operaciones, lo tenemos en el sector de las *ventas de objetos de segunda mano*, tradicionalmente al margen del pago de impuestos cuando se realizaban entre particulares, y la llamada de atención del Ministerio de Hacienda, acerca de que estas operaciones realizadas en plataformas de internet como *Wallapop* o *eBay*, deben tributar por el *impuesto de transmisiones patrimoniales* [véase la noticia del Diario *ABC* de 16.11.2017, «Montoro afirma que la compraventa de productos de segunda mano está sujeta al pago de impuestos» (http://www.abc.es/economia/abci-montoro-afirma-compraventa-productos-segunda-mano-esta-sujeta-pago-impuestos-201711161144_noticia.html)].

(25) Un problema importante en la regulación de estos aspectos, lo genera la *captura del regulador* por alguno de los sectores (o lobbies) implicados, que deriva en una normativa protectora de sus intereses que no siempre es conforme al interés general. Una referencia a ello en Doménech Pascual, G.: *op. cit.*, pp. 374 y ss.

(26) Ap. 1, p. 2.

En el *bando favorable* militan, además lógicamente de las empresas que han creado y gestionan las diversas plataformas, también una *mayoría silenciosa* de particulares y operadores, que utilizando sus servicios como usuarios o prestadores, les están permitiendo su creciente implantación y el fuerte contrapeso que están ejerciendo en relación con los sectores tradicionales. En relación con entidades públicas, son también claramente favorables organismos europeos, como el CESE o la CE, a través de sus respectivos dictamen y comunicación de 2014 y 2016 (27), así como en España la CNMC (28), como lo viene demostrando su activismo judicial contra las regulaciones restrictivas que obstaculizan el desarrollo de la economía colaborativa en estos sectores (29).

Los argumentos en favor de la economía colaborativa, en línea con lo que se apuntaba en el apartado anterior, y se puede rastrear en las comunicaciones e informes de las entidades oficiales que la apoyan, se basan fundamentalmente en cuatro razones; a saber: [1.º] introduce *más competencia* en los sectores afectados, con las ventajas que se asocian a la misma; [2.º] promueve el *consumo sostenible* (menos despilfarro) (30); [3.º] supone una *racionalización y maximización* de utilidades, y [4.º] *aprovecha a los sectores menos favorecidos* (nuevas posibilidades de empleo e ingresos, costes más reducidos, etc.).

En el *bando contrario* a la economía colaborativa se encuadran los profesionales de los sectores tradicionales a los que se hace competencia y sus asociaciones gremiales (taxistas, transportistas, hoteleros…). También han hecho oír su voz, en relación específicamente con el alojamiento turístico, particulares (vecinos) y asociaciones y partidos, contrarios a la saturación de ciudades turísticas y a las molestias que originan los turistas, así como al encarecimiento de los alquileres. En el ámbito de las entidades oficiales, en el caso de España, claramente están manteniendo políticas contrarias a la expansión de la economía colaborativa en estos sectores del transporte y el hospedaje, mediante regulaciones restrictivas, el

(27) Citadas respectivamente en las notas 16 y 9.

(28) Trasluce este posición favorable el documento Resultados preliminares E/CNMC/004/15 *Estudio sobre los nuevos modelos de prestación de servicios y la economía colaborativa*, 11.3.2016 (https://docs.google.com/document/d/1n65MjUaTmRLuZCqTllqyWvobVqreR-iAzsz1mhxy2y0/edit).

(29) En materia de transporte destaca la impugnación del desarrollo reglamentario estatal de la normativa sobre VTC, justificada en el *Informe económico sobre las restricciones a la competencia incluidas en el Real Decreto 1057/2015 y en la Orden FOM/2799/2015, en materia de vehículos de alquiler con conductor –UM/085/15 y acumulados.* Sobre alojamiento turístico, p. ej. el recurso contra la normativa de apartamentos de Canarias, justificada en el *Informe económico sobre el Decreto 113/2015, de 22 de mayo, por el que se aprueba el Reglamento de las viviendas vacacionales de la comunidad autónoma de canarias –LA/03/15*, recientemente estimado en parte por la sentencia del Tribunal Superior de Canarias, Sala de lo Contencioso Administrativo, sección 2.ª, de 21.3.2017.

(30) En relación con los vehículos particulares, Doménech Pascual, G.: *op. cit.*, p. 352, señala que se está aprovechando apenas un 1 % de la capacidad productiva del parque de estos vehículos, permaneciendo éstos el 96 % de su vida útil estacionados, y cuando circulan lo hacen con solo el 20 % de sus plazas ocupadas.

Estado (Ministerio de Fomento), las comunidades autónomas y ayuntamientos de grandes municipios.

El argumentario de este sector, no siempre explicitado, aunque con frecuencia las regulaciones restrictivas acometidas hablan por sí solas, bascula en torno a cuatro tipos de razones: [1.º] las plataformas están *infringiendo normas regulatorias* (sobre transporte, actividad hotelera, urbanismo...); [2.º] son fuente de economía sumergida (en materia tributaria, laboral y de seguridad social); [3.º] su actividad competitiva con los sectores tradicionales es desleal [por infracción de normas *ex* artículo 15.2 de la Ley de competencia desleal (LCD)] y [4.º] está produciendo (o puede producir) daños colaterales contrarios al interés general, como el encarecimiento de viviendas para el alojamiento permanente (por la presión al alza de los alquileres turísticos) o molestias medioambientales (incremento de la circulación de vehículos en las ciudades, molestias vecinales en los alojamientos, invasión de espacios urbanos…).

4.2 **Un fenómeno ambivalente**

El anterior debate plantea, sin duda, cuestiones de calado, donde además, como ya señalé en otro momento, caben muchos matices –entre el blanco y el negro de las posturas extremas hay un amplio abanico de grises–. Algunas preguntas, por otro lado, no encuentran una respuesta clara, o al menos a mí así me lo parece.

Comencemos porque no es fácil determinar *cui prodest* en realidad de la economía colaborativa. Por partidarios y detractores se pone el acento en los usuarios, o en los prestadores del servicio (propietarios y/o conductores), incluso en ambos, según se acaba de ver. Pero si nos centramos en los *prestadores del servicio* –propietarios de viviendas y de vehículos, y conductores– las plataformas tienen un aroma similar al del *outsourcing*, lo que a su vez implica una serie de preguntas inquietantes: ¿quién es el que arriesga aquí?, ¿quién es el que invierte?, ¿quién el que responde? No será que al final todos ellos («hoteleros», conductores…) se convertirán en *autónomos*. Y en este caso, ¿qué pasa con los derechos de los trabajadores que tanto ha costado que se reconozcan en la evolución de los modernos estados sociales y democráticos de derecho? (31).

(31) Recientemente se ha confirmado en apelación en el Reino Unido la sentencia estimatoria de la demanda de dos conductores que reclamaban derechos laborales a *Uber*. *Vid.* «Uber ordered to treat its drivers as workers with full rights after losing appeal», en el Diario *The Independent* de 11.11.2017 (https://www.pressreader.com/uk/the-independent/20171111/281616715650756).

Por otro lado, y desde otra perspectiva, ¿no son las plataformas, normalmente empresas extranjeras radicadas en otros países, una *nueva forma de deslocalización* de empresas? En el supuesto de que paguen impuestos por sus actividades y por sus beneficios, ¿dónde se pagan? (32)

Asimismo las actividades consideradas –alojamiento y transporte– tienen asociadas *externalidades*, en forma (acaso) de más tráfico, más ruido, más problemas de convivencia en edificios y barrios. ¿Quién las soporta y quién tendría que compensarlas a los perjudicados?

No es este lugar apropiado para responder a estas preguntas, lo que requeriría sin duda de análisis detallados y rigurosos, pero sí para llamar la atención sobre que el fenómeno de la economía colaborativa es bastante *ambivalente*, por mucho que se empeñen partidarios y detractores en todo lo contrario. Por ello, y pese a la falta de interés en regular en serio el supuesto que ha demostrado la CE en su Comunicación de 2016 (33), necesita de una *regulación apropiada*, que permita conservar las ventajas que sin duda están asociadas a estas fórmulas, pero frenando o limitando sus aspectos más inquietantes, en particular en relación con los aspectos laborales y tributarios, y puesto que estamos en un mercado integrado, mejor que se haga a nivel de toda la UE, que por países o (en el caso de España por nuestro localismo característico) por cada comunidad autónoma o ciudad (34).

---

(32) Como indica el artículo de Jesús Sérvulo González, «Las nuevas plataformas de transporte apenas declaran beneficios en España», publicado en el Diario *El País* de 20.11.2017, en el ejercicio 2016, las principales plataformas de transporte colaborativo en España (*Cabify*, *BlaBlaCar*, *Uber y Amovens*), registraron una facturación conjunta de poco más de 31,7 millones de € en España, con pérdidas o beneficios pírricos (sic), pagando en su conjunto 1,67 millones de € por el impuesto de sociedades (https://elpais.com/economia/2017/11/18/actualidad/1510997965_581238.html).

(33) La introducción de esta Comunicación, ap. 1, pp. 2 y 3, es bastante transparente al indicar lo siguiente:

> «*La presente Comunicación tiene por objeto ayudar a recoger estos beneficios* (de la economía colaborativa) *y abordar las preocupaciones sobre la incertidumbre acerca de los derechos y las obligaciones de las personas que participan en la economía colaborativa. Ofrece orientación jurídica y política a las autoridades públicas, los operadores del mercado y los ciudadanos interesados con vistas a un desarrollo equilibrado y sostenible de la economía colaborativa, tal como se anunció en la estrategia para el mercado único. Estas orientaciones no vinculantes sobre la manera de aplicar la legislación vigente de la UE a la economía colaborativa abarca las cuestiones fundamentales a las que se enfrentan tanto los operadores del mercado como las autoridades públicas. Se entienden sin perjuicio de las iniciativas que pueda adoptar la Comisión en este ámbito en el futuro ni de las prerrogativas del Tribunal de Justicia por lo que respecta a la interpretación de la legislación de la UE.*»

(34) La regulación de los taxis en España está encomendada a ordenanzas locales. La de viviendas de uso turístico a las comunidades autónomas, como se verá más adelante en el ap. 7.

Mantiene también la conveniencia de una regulación a nivel europeo, Rojo Álvarez Manzaneda, R.: «El Derecho Mercantil y el consumo colaborativo», en Miranda Serrano, L. M.ª/Pagador López, J.: *Retos y tendencias*... cit., p. 144.

5. SUBSUNCIÓN DE LA ECONOMÍA COLABORATIVA EN EL DERECHO DE LA UE

Como ya se ha dicho, en la actualidad no existe normativa europea referida a la *economía colaborativa* en su conjunto, ni respecto a sus manifestaciones más características, como son el transporte, el hospedaje o la financiación colaborativa. Tampoco existen previsiones de que este tema se aborde a este nivel a corto o medio plazo, habiéndose limitado la CE a publicar la indicada Comunicación de 2016 (35).

En este contexto, el problema que se plantea es ver si la economía colaborativa puede quedar afectada y en qué medida por otras normativas europeas de carácter más general. Como pone de relieve el asunto *Uber* enjuiciado recientemente por el Tribunal de Justicia en la ya citada sentencia de 20.12.2017, la principal disyuntiva que se plantea es la de ver si las prestaciones ofrecidas por las plataformas merecen ser calificadas de *servicios de la sociedad de la información*, que se beneficiarían del *principio de libre prestación de servicios* establecido por el artículo 4 de la Directiva 2000/31 de comercio electrónico (36), o si están dentro del ámbito de algunos de los servicios exceptuados por la Directiva 2006/123 relativa a los servicios del mercado interior y que, por tanto, de momento siguen sometidos exclusivamente a los Derechos de los EE. MM. (37).

A este respecto, si nos atenemos al artículo 2.2 de esta última Directiva, se descubren exclusiones de su ámbito de aplicación, que podrían afectar *prima facie* a algunas modalidades de economía colaborativa:

> « (…)
> b) los servicios financieros, como los bancarios, de crédito, de seguros y reaseguros, de pensiones de empleo o individuales, de valores, de fondos de inversión, de pagos y asesoría sobre inversión, incluidos los servicios enumerados en el anexo I de la Directiva 2006/48/CE;
> (…)
> d) los servicios en el ámbito del transporte, incluidos los servicios portuarios, que entren dentro del ámbito de aplicación del título V del Tratado;
> (…)
> e) los servicios de las empresas de trabajo temporal;
> (…)»

(35) Previamente se publicó una comunicación específica sobre el *crowdfunding*: Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, *Liberar el potencial de la microfinanciación colectiva en la Unión Europea*, Bruselas, 27.3.2014, COM(2014) 172 final.

(36) Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8.6.2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (*Directiva sobre el comercio electrónico*).

(37) Directiva 2006/123/CE del Parlamento Europeo y del Consejo de 12.12.2006, relativa a los servicios en el mercado interior.

La de la letra b) sería de posible aplicación a la financiación colaborativa; la de la letra d), al transporte colaborativo, y la de la e) a las plataformas de trabajo temporal.

La sentencia del Tribunal de Justicia en el asunto *Uber*, se enfrentó al problema en relación con el *transporte colaborativo*. Acogiendo en términos generales la propuesta del Abogado General (38), aunque con menor riqueza argumentativa, la sentencia distingue entre la labor de intermediación de la plataforma entre pasajero y conductor, y el servicio (subyacente) de transporte. La primera «responde en principio a los criterios para ser calificado como "servicio de la sociedad de la información", en el sentido del artículo 1, punto 2, de la Directiva 98/34, al que se remite el artículo 2, letra a), de la Directiva 2000/312 (sobre comercio electrónico)» (39). El segundo, en cambio, sería «un servicio de transporte urbano no colectivo (que), como un servicio de taxi, debe ser calificado de "servicio en el ámbito del transporte", en el sentido del artículo 2, apartado 2, letra d), de la Directiva 2006/123, a la luz del considerando 21 de ésta» (40).

Llegados a este punto el Tribunal se plantea si la plataforma (*Uber*), limitaba su actuación en el presente caso a la mera intermediación, o si por el contrario, intervenía en el servicio de transporte. A este respecto, llega a la conclusión por diversas circunstancias (imprescindibilidad de la plataforma para que los conductores presten sus servicios, influencia decisiva en las condiciones –precio máximo–, control sobre calidad e idoneidad y comportamiento de los conductores) que efectivamente era así (41). Por esta razón estimará que el servicio de intermediación en realidad formaba parte «integrante de un servicio global cuyo elemento principal es un servicio de transporte y, por lo tanto, que no responde a la calificación de "servicio de la sociedad de la información"… sino a la de "servicio en el ámbito del transporte"» (42), al que no le es aplicable la Directiva de 2000/31 sobre comercio electrónico, ni la Directiva 2006/131 relativa a los servicios del mercado interior (43). En atención a ello, y ante la falta de normativa común en la materia, considera que *«incumbe a los Estados miembros regular la prestación de servicios de intermediación como*

(38) Conclusiones del Abogado General Sr. Maciej Szpunar presentadas el 11.5.2017, asunto C-434/15 *Asociación Profesional Élite Taxi* c. *Uber Systems Spain, S. L.*

Sobre estas conclusiones, *vid.* también Chamorro Domínguez, M.ª C. «Las nuevas modalidades de prestación de servicios de transporte urbano desde la óptica del Derecho de la competencia», en *La Ley mercantil*, n.º 38, 1.6.2017, pp. 7 y s., y Velasco San Pedro, L. A.: «El transporte colaborativo...» cit., pp. 410 y ss.

(39) Ap. 35.

(40) Ap. 36.

(41) Ap. 39.

(42) Ap. 40.

(43) Aps. 42 y ss.

los controvertidos en el litigio general, siempre que se respeten las normas generales del Tratado FUE» (44).

Aunque la respuesta del Tribunal de Justicia formalmente es correcta, se echa de menos que la sentencia no descienda al análisis de las condiciones sumamente restrictivas de la regulación en España (y otros países) del transporte no colectivo metropolitano, y no haga aportación alguna a este respecto. Yendo más lejos, la Comunicación de la CE de 2016, aun admitiendo que las plataformas colaborativas, cuando se impliquen en las actividades subyacentes, pueden estar sometidas a autorizaciones (45), señala que en tal caso «los EE. MM. deben garantizar que las condiciones para obtenerlas sean… claras, proporcionadas y objetivas, y que las autorizaciones se concedan en principio sin límite de tiempo» (46), circunstancias que con toda evidencia no concurrían en la regulación controvertida (Reglamento metropolitano del taxi de Barcelona), que como todas las relacionadas con este sector en España, hacen sencillamente imposible la consecución de cualquier nueva licencia o autorización.

Como fuere, a la vista de esta doctrina resultaría, por tanto, que aquellas plataformas colaborativas que limiten su actuación a la mera intermediación entre oferentes y demandantes de los bienes o servicios, estarían amparadas por la libre prestación de servicios reconocida a los operadores de la sociedad de la información. No obstante, si prestasen o, al menos, intervinieran decisivamente en la actividad subyacente, habría que ver si dicha actividad goza de la libre prestación de servicios reconocida en la Directiva 2006/131 relativa a los servicios del mercado interior, o si, por el contrario, está exceptuada de dicha libertad, quedando su ejercicio sometido a lo que establezcan las normativas internas de los EE. MM., en tanto en cuanto no haya normas comunes en la materia.

Ya hemos visto que algunas de estas excepciones pueden afectan a determinadas modalidades de economía colaborativa; concretamente en

(44) Ap. 47.

(45) La Comunicación se refiere a las condiciones requeridas para ello en el ap. 2.1., p. 4, y son las siguientes:

- *«Precio: ¿fija la plataforma colaborativa el precio final que debe pagar el usuario como beneficiario del servicio subyacente? El hecho de que la plataforma colaborativa solo recomiende un precio o de que el prestador de los servicios subyacentes sea libre de adaptar el precio fijado por una plataforma colaborativa, indica que puede que no se cumpla este criterio.*
- *Otras condiciones contractuales clave: ¿establece la plataforma colaborativa términos y condiciones distintos del precio que determinan la relación contractual entre el prestador de los servicios subyacentes y el usuario (por ejemplo, instrucciones obligatorias sobre la prestación del servicio subyacente, incluida cualquier obligación de prestar el servicio)?*
- *Propiedad de activos clave: ¿posee la plataforma activos clave para prestar el servicio subyacente?»*

(46) Ap. 2.1., p. 5.

materia de financiación, transporte y trabajo temporal. No obstante, en estos casos para llegar a una respuesta definitiva, habría que analizar la implicación de la plataforma en la actividad subyacente.

6. EL TRANSPORTE COLABORATIVO

6.1 **Caracterización y modalidades**

Lo característico del *transporte colaborativo* es la presencia de plataformas especializadas, como las señaladas *Uber*, *BlaBlaCar*, *Cabify*, etc., que ponen en contacto a los usuarios demandantes y a los conductores o propietarios de los vehículos oferentes. La actividad subyacente sería aquí el transporte, en cuanto la finalidad última perseguida por los demandantes sería el traslado de personas y/o cosas de un lugar a otro, aunque desde una perspectiva técnica no siempre quepa hablar de transporte propiamente dicho.

Igual que sucedía con la economía colaborativa en general, el transporte puede realizarse por y para *particulares* –C2C o P2P– que tratan simplemente de optimizar el uso de sus vehículos privados infrautilizados, compartiendo su uso y los gastos que ello genera con otros particulares, que asimismo se benefician de menores costes que en los transportes profesionales. En estos casos, la plataforma colaborativa no realiza la actividad subyacente, limitándose a ser intermediaria.

Pero también la actividad puede desarrollarse por *profesionales*, en nombre propio o con colaboradores, desde vehículos destinados específicamente a ello. Aquí se trataría de un tráfico B2C o B2B, y la plataforma, dependiendo de supuestos, puede ser mera intermediaria o también realizar ella misma la actividad subyacente (47).

Como luego se verá, la diferenciación en estos aspectos del transporte colaborativo es a día de hoy crucial, en la medida en que la ordenación del transporte en casi todos los países –y así sucede en el caso de España– suele diferenciar el transporte profesional o *público*, sometido a un fuerte intervencionismo administrativo (sistema de concesión y/o de autorización o licencias), del trasporte entre particulares o *privado*, al margen de estos controles. Ello explica en gran medida por qué en España, las resoluciones judiciales habidas hasta el momento, han sido contrarias a la admisibilidad de las plataformas del primer tipo de transporte, por incumplimiento de normas regulatorias, y favorables a las del segun-

(47) Las distintas variantes que pueden plantearse permite hablar desde un punto de vista sustantivo, dependiendo de supuestos, de empresarios *ex* artículo 1 del Código de comercio y, dentro de éstos en ciertos casos, de trabajadores autónomos o, incluso de trabajadores autónomos dependientes, a los que se refiere el capítulo III, del título II, de la Ley del Estatuto del Trabajo Autónomo, como de trabajadores ordinarios empleados por la plataforma.

do, al estimar que quedaba fuera de tales normas (48). Es la orientación que asimismo, como se ha adelantado, expresa la sentencia del Tribunal de Justicia de la UE sobre *Uber*.

La ya amplia praxis que existe sobre distintas plataformas de transporte colaborativo o actividades concomitantes, permite introducir otras diferenciaciones distintas a la que se acaba de examinar, y que también van a tener en su caso transcendencia en cuanto la regulación administrativa y el régimen contractual jurídico privados aplicables, toman cuenta de ellas (contrato de transporte, alquiler de vehículos con y sin conductor…).

Por el ámbito de actuación, hay plataformas especializadas en el *transporte urbano o metropolitano*, como *Uber, Cabify, Avancar* o *Drivy*, siendo alternativas al taxi y a los clásicos vehículos de alquiler con conductor (VTC). Otras, en cambio, operan en el *transporte interurbano*, como *BlaBlaCar*, *Amovens* o *Shareling*, siendo alternativas de las líneas regulares de transporte de viajeros.

Por la *presencia o no de conductores, y su carácter*, por un lado, están las plataformas con *conductores profesionales* como *Uber*, *Cabify* o *Ntaxi* (esta última desarrollada por taxistas para facilitar compartir trayectos entre varios clientes), y las plataformas con *conductores no profesionales* (*carpooling* o *ride sharing*) como *BlaBlaCar* o *UberPop* (49). Por otro, las *plataformas sin conductor* (*carsharing*), como *Avancar*, *Drivy* o *Socialcar* (autocaravanas…).

6.2 **Régimen jurídico del transporte colaborativo**

A la vista de la doctrina de la sentencia *Uber*, las plataformas de transporte colaborativo en España, en la medida en que intervengan en la actividad subyacente de transporte, quedarían sometidas a los requisitos y reglas que se establezcan por la legislación interna. Por otro lado, y con independencia de esto, la actividad subyacente de transporte –sea esta prestada por quien sea–, debe asimismo acomodarse a lo dispuesto en la legislación nacional.

Como ya se ha dicho, en la actualidad se carece en España de una regulación legal específicamente referida al transporte colaborativo, si bien es cierto que algunas modificaciones reglamentarias recientes –me refiero a la normativa sobre VTC– se han producido con vistas en él, y no precisamente para favorecerlo, sino más bien para todo lo contrario (50).

---

(48) Véase más adelante en el siguiente apartado.

(49) En relación con esta diferenciación y las notas distintivas entre ambas modalidades, véase con cierto detalle Armengol i Gasull, O./Olmos Castro, N.: «El impacto de la economía colaborativa en el transporte interurbano: un análisis jurídico del ride sharing», en Montero Pascual, J. (dir.): *La regulación…* cit., pp. 327 y ss.

(50) Real Decreto 1057/2015, de 20 de noviembre, *por el que se modifica el Reglamento de la Ley de Ordenación de los Transportes Terrestres, aprobado por Real Decreto 1211/1990, de 28 de septiembre,*

Por lo que respecta a la *actividad subyacente de transporte*, no obstante, le son aplicables las normas regulatorias del transporte de viajeros por carretera, contenidas básicamente en la Ley de ordenación de los transportes terrestres (LOTT) y en su Reglamento (51). A mi juicio, como ya adelanté en un primer trabajo sobre la materia, para su correcto encuadramiento en esta normativa deben distinguirse las distintas tipologías de las plataformas (52).

Dejando al margen los supuestos que implican la mera *cesión del uso de vehículos sin conductor* que, con independencia de su naturaleza jurídica como *comodato* (si fuera gratuita) o *alquiler* (si fuera con contraprestación), estarían fuera de esta regulación por no ser propiamente *transporte* (53); en los demás debe diferenciarse claramente entre los supuestos de transporte a cargo de conductores profesionales o para profesionales, como sería el caso de plataformas como *Uber* y *Cabify*, y transporte con conductores que son particulares, como es el de *BlaBlaCar*.

Esta diferenciación se ve claramente en las resoluciones del Juzgado de lo Mercantil n.º 2 de Madrid (magistrado Sánchez Magro), que se ha tenido que enfrentar a demandas y solicitudes de medidas cautelares sobre ambos modelos de plataformas. Por un lado, el auto de 9.12.2014, concediendo la medida cautelar de suspensión de la actividad de *Uber* –en su modalidad *UberPop* (54)– en toda España, por estimar *prima facie* que habría un incumplimiento de las reglas regulatorias del transporte público (profesional), para el que se exigen autorizaciones o licencias administrativas que faltaban aquí, por lo que constituiría un *acto de*

---

en materia de arrendamiento de vehículos con conductor, para adaptarlo a la Ley 9/2013, de 4 de julio, por la que se modifica la Ley 16/1987, de 30 de julio, de Ordenación de los Transportes Terrestres y la Ley 21/2003, de 7 de julio, de Seguridad Aérea y Orden FOM/2799/2015, de 18 de diciembre, *por la que se modifica la Orden FOM/36/2008, de 9 de enero, por la que se desarrolla la sección segunda del capítulo IV del título V, en materia de arrendamiento de vehículos con conductor, del Reglamento de la Ley de Ordenación de los Transportes Terrestres, aprobado por Real Decreto 1211/1990, de 28 de septiembre*, actualmente impugnados ante los tribunales por la CNMC.

(51) LOTT de 30.7.1987, y Real Decreto 1211/1990, de 28 de septiembre, por el que se aprueba el Reglamento de Ordenación de los Transportes Terrestres, disposiciones reiteradamente modificadas. Cuando se corrigen pruebas de este trabajo modificadas en cuanto a las licencias VTC por el Real Decreto-ley 3/2018, de 20 de abril, con el objetivo de hacer frente a una eventual estimación de los recursos a los que se hizo referencia en la nota anterior.

(52) Velasco San Pedro, L. A., «El consumo colaborativo…» *cit.*, pp. 195 y ss.

(53) El artículo 133.1 de la LOTT señala que *«[l]a actividad de arrendamiento de vehículos sin conductor podrá ser realizada libremente por todas aquellas empresas que cumplan las obligaciones que, por razones de índole fiscal, social y laboral o de seguridad ciudadana o vial, les vengan impuestas por la legislación reguladora de tales materias»*.

(54) Esta plataforma estaba prevista para conductores «particulares», pero que podían dedicarse «profesionalmente» a prestar sus servicios a través de ella. Posteriormente, como ya se ha indicado, *Uber* se ha adaptado a la situación marcada por el auto de suspensión de esta variante, desarrollando en España otra plataforma para VTC.

competencia desleal ex artículo 15.2 de la LCD (55) (56). Por otro, el auto de este mismo juzgado de 26.1.2016, denegando una medida cautelar semejante en relación con la actividad de *BlaBlaCar*, por estimar que estaríamos en presencia de un transporte privado no sometido a este régimen de autorizaciones, y la sentencia de 2.2.2017, desestimando ya definitivamente, por la misma razón, la demanda contra *BlaBlaCar* por competencia desleal (57).

Personalmente considero, a la vista de la actual regulación del transporte en España, que el *planteamiento dual* del Juzgado de lo Mercantil n.º 2 de Madrid, es el correcto en estos momentos. El transporte *prestado profesionalmente* forma parte de los *transporte públicos discrecionales de viajeros* definidos por los artículos 62.1, 63.a) y 64.1 de la LOTT, y es un transporte sometido a autorizaciones o licencias administrativas por parte de las autoridades competentes (estatales, autonómicas o locales), en el marco de lo previsto en el artículo 99 de la LOTT. Una plataforma para este tipo de transporte sin que los conductores o los propietarios de los vehículos tengan autorización o licencia administrativa para ello, no es compatible con la actual regulación. Sin embargo, sí lo sería si se acogiera a alguna de las modalidades previstas para este tipo de transporte, como se ha hecho por parte de la propia *Uber* y *Cabify* que ahora mismo están encauzando su negocio por la vía de las autorizaciones VTC (58).

No ocurre lo mismo, en cambio, con el *transporte prestado por particulares*, que simplemente buscan compartir gastos, y que cabe encuadrar dentro de los *transportes privados particulares* a los que se refiere el artículo 101.1.a) de la LOTT, no sometidos a estas autorizaciones o

---

(55) El auto recurrido por *Uber* fue confirmado por otro de 22.5.2015, que además aclaraba que la suspensión se refería únicamente al servicio *UberPop*. El recurso de apelación interpuesto contra el mismo fue desestimado por sentencia de la Audiencia Provincial de Madrid, sección 28, de 23.1.2017. Por otro lado, como ya se ha indicado, este juzgado presentó una cuestión prejudicial sobre el asunto principal ante el Tribunal de Justicia de la UE mediante auto de 27.5.2015, que está pendiente de resolución, aunque la reciente sentencia de 2017 anticipa su resultado.

Sobre este asunto, entre otros, véase Górriz López, C.: «Uber. Transporte de pasajeros y competencia desleal», en *Revista de Derecho del Transporte*, n.º 16, 2015, pp. 77 y ss., y Chamorro Domínguez, M.ª C.: *op. cit.*, pp. 5 y ss. Sobre asuntos similares en otras jurisdicciones en los que era asimismo parte demandada *Uber*, Górriz López, C.: «Reflexiones sobre Uber a propósito de la decisión de la Court of Appeals for the Seventh Circuit», en *Revista de Derecho del Transporte*, n.º 19, 2017, pp. 232 y ss.

(56) El artículo 15.2 de la LCD señala que *«[t]endrá también la consideración de desleal la simple infracción de normas jurídicas que tengan por objeto la regulación de la actividad concurrencial»*.

(57) Sobre esta sentencia, véase Boboc, S.: «BlaBlaCar: ¿un posible supuesto de competencia desleal? (comentario a la sentencia del Juzgado de lo Mercantil n.º 2 de Madrid, de 2 de febrero de 2017», en *Revista de Derecho del Transporte*, n.º 19, 2017, pp. 232 y ss.

(58) La sentencia del Juzgado de lo Mercantil n.º 12 de Madrid de 13.6.2017 ha absuelto a *Cabify*, que se acoge al sistema de VTC, de la demanda por competencia desleal interpuesta por la Federación Profesional del Taxi de Madrid, por entender que las irregularidades formales en que pudieran incurrir los conductores, derivadas de la (*discutible*, añadimos nosotros) normativa administrativa, no serían imputables a la plataforma, sino en su caso a éstos, no obteniendo además de ello ninguna ventaja económica. Véase Chamorro Domínguez, M.ª C.: *op. cit.*, pp. 11 y s.

licencias como puntualiza el artículo 101.2 de la LOTT. Bien es cierto que para delimitar este transporte y evitar abusos, el referido artículo 101.1.a), habla del transporte del *titular del vehículo y sus allegados*, expresión esta última que permitiría diversas interpretaciones, pero que de acuerdo con la realidad actual del momento –de la que hay que partir para interpretar las normas jurídicas como indica el artículo 3 del Código civil (C. c.)–, habría que extender a los usuarios que voluntariamente forman parte de una red creada por una plataforma, como puede ser la de *BlaBlaCar* (59).

La cuestión, sin embargo, plantea por elevación la necesidad de concretar si en ambos casos o solo en alguno de ellos, las plataformas de transporte colaborativo, están obligadas ellas mismas a someterse a autorizaciones o licencias administrativas.

En el caso de las que actúan en el ámbito del transporte puramente privado (*BlaBlaCar*), parece que su actuación se limita básicamente a la mera intermediación entre particulares oferentes y demandantes de transporte, por lo que estaría amparada por la libertad de prestación de servicios de la sociedad de la información. A mayor abundamiento, la actividad subyacente de transporte que se presta (por terceros particulares) queda al margen, como ya se ha dicho, del intervencionismo administrativo de la LOTT.

Respecto a las que están actuando en el marco de un transporte profesional (*Uber; Cabify*), aunque su implicación en la actividad subyacente parece en principio indudable, no está muy claro el régimen aplicable. La norma de referencia es el artículo 22.2 de la LOTT, pues estamos en el ámbito del *transporte de viajeros*, que señala lo siguiente:

> «Como regla general, los servicios de transporte terrestre de viajeros podrán ser contratados y facturados por todos aquellos que sean titulares de una licencia o autorización de transporte público que habilite para la realización de esta clase de transporte.
> No obstante, la prestación de aquellas modalidades de transporte de viajeros que tengan atribuido el carácter de servicio público de titularidad de la Administración sólo podrá ser contratada en concepto de porteador por el contratista a quien el órgano competente hubiese adjudicado su gestión o, en su caso, por el ente, organismo o entidad que la Administración competente haya creado para la gestión o coordinación de esa clase de servicios.
> La intervención de agencias de viajes y otros intermediarios en la contratación de cualesquiera modalidades de transporte de viajeros se regirá por la legislación específica de turismo. Sin perjuicio de ello, las cooperativas de transportistas y sociedades de comercialización podrán intermediar, en todo

(59) En similar sentido, Armengol i Gasull, O./Olmos Castro, N.: *op. cit.*, pp. 346 y 347.

caso, en la contratación de transportes discrecionales de viajeros que vayan a ser prestados por aquellos de sus socios que sean titulares de autorización de transporte de viajeros.»

¿Cuál es el régimen concreto que hay que aplicar aquí? Inicialmente cabría pensar que podría ser el relativo a las *agencias de viaje* y *otros intermediarios de transporte*, que sería el previsto en la *legislación turística*. El problema es que esta legislación, actualmente de ámbito autonómico, solo contempla la actividad de las agencias de turismo, conceptualmente bastante diferente a la que realizan estas plataformas, y que en todo caso suele estar sometida a licencias y requisitos específicos no pensadas para este caso (60). En esta tesitura, lo más apropiado sería exigir el tipo de autorización o licencia que se exige para el transporte subyacente que es su objeto, vía que además se apunta en el primer ap. del precitado artículo 22.2. Ante la imposibilidad material de obtención de licencias de taxi, limitadas en muchas regulaciones locales a personas naturales y bloqueadas desde hace años (61), la única vía disponible actualmente serían las autorizaciones de VTC, que es además la que en la práctica están siguiendo las plataformas actualmente implantadas en España (62).

Cuestión distinta a las planteadas hasta ahora, es que el modelo de intervención administrativa de este transporte público diste de ser el más correcto, tanto en relación con los taxis, cuya normativa altamente restrictiva encuentra cada vez menos justificaciones, como con la regulación de los VTC, artificialmente endurecida para entorpecer la operativa de las nuevas plataformas.

6.3 **La responsabilidad de las plataformas de transporte colaborativo**

Al margen del régimen de control administrativo que acaba de examinarse, cabe plantearse qué responsabilidad tienen las plataformas frente a los usuarios (63) en relación con la prestación de los servicios de transporte que constituyen la actividad subyacente, tanto en lo relativo a su

(60) Véase p. ej. el artículo 5 del Decreto 25/2001, de 25 de enero, *por el que se aprueba el Reglamento de las Agencias de Viajes, que ejerzan su actividad en la Comunidad de Castilla y León*.

(61) Lo que ha generado un floreciente mercado secundario de licencias, como es bien sabido.

(62) Vía acuerdos con los titulares concretos de las mismas, normalmente otras personas o entidades.

(63) En relación con la protección de los usuarios consumidores en la economía colaborativa, véanse la Comunicación de la CE de 2016, ap. 2.3., pp. 9 y ss. y Muñoz Pérez, A. F.: «Economía colaborativa y consumidores», en Montero Pascual, J. (dir.): *La regulación… cit.*, pp. 195 y ss.

correcta ejecución, como respecto a accidentes de circulación y otras vicisitudes como la pérdida o deterioro de equipajes.

De nuevo, como ya indiqué en otro momento, creo que aquí se impone la diferenciación de supuestos (64). En el caso de *transportes profesionales* y de implicación de la plataforma en la actividad subyacente, la empresa titular de la misma debería responder civilmente frente a los usuarios por estas circunstancias, porque es el criterio que en relación con la *responsabilidad de los intermediarios del transporte de mercancías*, se trasluce de la normativa aplicable –del artículo 22.1 en relación con los artículo 119 y ss. de la LOTT para los *operadores de transporte* (aunque era más claro el anterior art. 120.2 LOTT) y, sobre todo, del actual artículo 6.1 de la Ley de contrato de transporte terrestre para los *porteadores contractuales* (65)–, donde básicamente se los equipara a los *porteadores efectivos*, normativa que cabría aplicar aquí por analogía. A este respecto debe tenerse además en cuenta que no operarían las *exenciones de responsabilidad* (o *puerto seguro*) previstas para los prestadores de servicios de la sociedad de la información, establecidas para el derecho español en los artículos 14 a 17 de la Ley de servicios de la sociedad de la información (LSSI), trasladando los criterios de la Directiva 2000/31 de comercio electrónico, en la medida en que estas actividades no están expresamente previstas en aquella normativa, y no se darían a mayor abundamiento las condiciones de *neutralidad* establecidas en la jurisprudencia del Tribunal de Justicia, a la hora de interpretar el alcance de tales excepciones (66).

Sin embargo, en el caso de los *transportes privados* y al no existir implicación de la plataforma en la actividad subyacente, entiendo que empresa titular de la plataforma sí estaría amparada en dichas exenciones de la LSSI, al encajar su papel intermediario con la función de un *alojador de datos* de particulares que quieren compartir vehículo, que facilita mediante operaciones automáticas y neutrales su selección (67) y puesta en contacto, así como un mecanismo que asegura compartir los gastos (68).

---

(64) Velasco San Pedro, L. A. «El consumo colaborativo...» *cit.*, p. 197.

(65) Sobre esta última norma, *vid.* Emparanza Sobejano, A., en Duque Domínguez, J./Martínez Sanz, F. (dirs.): *Comentarios a la Ley de Transporte Terrestre*, Aranzadi, Cizur Menor 2010, sub artículo 6, pp. 99 y ss.

(66) Sentencias del Tribunal de Justicia de la UE de 23.3.2010, asuntos ac. C-236/2008 a C-238/2008 *Google AdWords*, y 12.7.2011, asunto C-324/09, *L'Oreal vs. eBay*.

(67) En este punto tienen gran importancia los *bancos de reputación* que van generando las plataformas a la vista de los viajes realizados y las valoraciones y comentarios de los participantes en la misma.

(68) En este sentido, debe resaltarse que el artículo 101.1.a) de la LOTT no impide que se compartan gastos en el transporte privado, sino más bien todo lo contrario al permitir expresamente la «*percepción de dietas o gastos de desplazamiento*» por el titular del vehículo.

La CE, por otro lado, parece mantener criterios semejantes cuando en su Comunicación sobre economía colaborativa señala lo siguiente (69):

> «La aplicabilidad de esta exención de responsabilidad dependerá de los elementos de hecho y de derecho relacionados con la actividad realizada por la plataforma colaborativa y dicha exención se aplica cuando las actividades en cuestión se consideran servicios de alojamiento de datos con arreglo a la Directiva sobre el comercio electrónico. Para ello, su realización debe ser meramente técnica, automática y pasiva. La exención de responsabilidad se aplica a condición de que la plataforma colaborativa no desempeñe un papel activo que le permita adquirir conocimiento o control de la información ilícita y en cuanto tenga conocimiento actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible.»

7. ALOJAMIENTO TEMPORAL O TURÍSTICO

Otras de las modalidades de la economía colaborativa, está constituida por las plataformas que ofrecen *alojamiento temporal*, generalmente identificado como *alojamiento turístico*, porque son los turistas los que más habitualmente precisan de alojamientos temporales, pero que no necesariamente tiene que ser demandado por personas que tengan esta condición.

Dentro de este panorama, igual que sucedía con el transporte colaborativo, pueden distinguirse diversas modalidades. La que menos problemas plantea, porque conecta con la idea de cooperación o colaboración propias de los intercambios gratuitos, son las *plataformas de intercambio de casas o pisos –GuesttoGuest*, *Home for Home–*. Siguiendo la doctrina de la sentencia *Uber* habría que distinguir, de nuevo, entre la actividad de intermediación y la actividad subyacente. En estos casos, la plataforma solo realiza una función de intermediación en la red, aunque cobre por ella (70), ya que la actividad subyacente –el intercambio de casas o pisos– la hacen exclusivamente los usuarios, y por lo tanto estaría amparada por el principio de libertad de prestación de servicios para los prestadores de servicios de la sociedad de la información, así como por las exenciones de responsabilidad que recoge la LSSI siguiendo a la Directiva 2000/312 de comercio electrónico. La actividad subyacente merece seguramente desde un punto de vista jurídico la calificación como *contratos de comodato de inmueble*, ya que no se paga emolumento alguno al que cede el uso (*vid.* art. 1741 del C.c.). En nuestro Derecho, este contrato se regula en los artículos 1741 y ss. del C.c., y carece de restricción administrativa alguna.

Mucho más problemáticas son las plataformas que ofrecen *alojamiento temporal*, sea de casas o pisos completos, sea de habitaciones, a cambio

(69) Ap. 2.2, p. 8.

(70) Las plataformas suelen cobrar una cuota de inscripción para anunciar las ofertas de intercambio.

de una remuneración a los que ceden su uso, la más característica de las cuales al día de hoy es *Airbnb*. La actividad de estas plataformas, en principio, también debe considerarse como propia de un operador de la sociedad de la información, ya que su función es esencialmente de intermediación y no se involucran en la realización de la actividad subyacente (71).

La calificación de la actividad subyacente, en cambio, no resulta tan clara. Al percibirse una contraprestación podríamos pensar, por contraste con el comodato, que se trataría de un *arrendamiento*. Sin embargo, debe tenerse en cuenta que el artículo 5, e) de la Ley de arrendamientos urbanos (introducido por la reforma de la Ley 4/2013, de 4.6.2013), señala que queda excluida del ámbito de aplicación de dicha Ley «[l]a cesión temporal de uso de la totalidad de una vivienda amueblada y equipada en condiciones de uso inmediato, comercializada o promocionada en canales de oferta turística y realizada con finalidad lucrativa, cuando esté sometida a un régimen específico, derivado de su normativa sectorial». En este punto son bastantes las comunidades autónomas que, usando sus competencias en materia de turismo, se han apresurado a establecer *normativas sectoriales*, donde se contemplan en ciertos casos algunas exigencias a los que ofrecen las viviendas que asemejan el contrato a las características del *contrato de hospedaje*, regulado sumaria y fragmentariamente en los artículos 1783 y 1784 del C.c., al establecer determinados requisitos dirigidos «teóricamente» a garantizar el confort de los «huéspedes» alojados (medidas de habitaciones y camas, disponibilidad de perchas, toallas, puntos de luz, aire acondicionado, etc.) (72). Con todo, lo más importante es que diversas normativas autonómicas, e incluso locales de grandes municipios, usando en este último caso de facultades en materia de urbanismo, han ido establecido o, en su caso, proyectan establecer, diversas restricciones a estas actividades que obedecen probablemente, más que al deseo de hacer una regulación equilibrada, a un intento de frenar sin más la expansión de esta modalidad de la economía colaborativa, y que, cuando se escriben estas líneas, en parte han sido anuladas por desproporcionadas y arbitrarias por los tribunales de justicia y, en parte, están pendientes de resolución, ante recursos en los que ha mostrado un gran activismo, como ya se señaló, la CNMC (73).

Llegados a este punto el *quid* de la cuestión es determinar si tales restricciones, con independencia de que les afecten a los propietarios de

(71) Comparte este criterio Herrero Suárez, C.: *op. cit.*, p. 151.

(72) *Vid.* una referencia a estas exigencias en Lora-Tamayo, M.: «Economía colaborativa y alojamiento», en Montero Pascual, J. (dir.): *La regulación…* cit., pp. 313 y s.

(73) Contienen referencias de cierto detalle a estas regulaciones y a sentencias que las han declarado en su caso parcialmente nulas, Herrero Suárez, C.: *op. cit.*, p. 153, esp. nota 26, y Benavides Velasco, P.: «La nueva regulación de viviendas con fines turísticos», en Miranda Serrano, L. M.ª/ Pagador López, J.: *Retos y tendencias*... cit., pp. 166 y ss. Sistematiza las principales restricciones de la normativa autonómica, Lora-Tamayo, M.: *op. cit.*, pp. 301 y ss.

las viviendas o habitaciones cedidas, que podrían ser sancionados administrativamente por ello (y de hecho están comenzando a serlo en algunos casos), les afectan también a las plataformas colaborativas, que ya hemos dicho ejercen una función más bien de intermediación, o si por el contrario, igual que sucedía con el transporte, le serían asimismo de aplicación, representando una excepción a la señalada libertad de prestación de servicios.

En mi opinión, si partimos de la doctrina de la sentencia *Uber*, la actividad que realizan las plataformas colaborativas están también aquí indudablemente amparadas por la libertad de prestación de servicios que se recoge en la Directiva 2000/312 de comercio electrónico y, por tanto, en coherencia con ello no se le podría exigir una autorización especial para ejercer esta actividad (74). Respecto a las exenciones de responsabilidad que configura la misma y por su reflejo la LSSI, la misma depende como se dijo en relación con el transporte y en coherencia con la jurisprudencia del Tribunal de Justicia de la UE, de si la actuación de la plataforma en relación con la información que almacena sobre la actividad subyacente de alojamiento, tiene carácter meramente técnico y neutral. No parece ser este el caso, sin embargo, de plataformas como *Airbnb*, que desempeñarían un papel activo que les permite *«adquirir conocimiento o control de la información ilícita»,* por lo que, siguiendo el criterio establecido por la Comunicación de la CE de 2016, debieran responder si, en cuanto tengan conocimiento de dicha información –particularmente de que no se cumple la normativa legal aplicable a los alojamientos turísticos–, no actuasen *«con prontitud para retirar los datos* (de los alojamientos fuera de la normativa) *o hacer que el acceso a ellos sea imposible»* (75).

(74) Diversas normativas autonómicas exigen comunicaciones responsables e inscripción en determinados registros, de la que se debe dar cuenta en la publicidad de la vivienda. *Vid.* Lora-Tamayo, M.: *op. cit.*, p. 301 y ss.

(75) Ap. 2.2, p. 8. Parece compartir este criterio, Herrero Suárez, C.: *op. cit.*, p. 156.

VIII

MERCADO DIGITAL Y COMPETENCIA

CAPÍTULO 31

BIG DATA Y DERECHO DE LA COMPETENCIA (1)

CARMEN HERRERO SUÁREZ
Profesora Titular de Derecho Mercantil
Universidad de Valladolid

«The statement, if you don't like Google, you can remove yourself from their listings and go elsewhere is about as realistic as recommending to an opponent of nuclear power that he just stop using electricity (...)» (*)

(*) DÖPFNER, M.: «An Open Letter to Eric Schmidt: Why We Fear Google?», *Frankfurt Allgemeine*, 17 de abril de 2014.

(1) Este trabajo se enmarca en el Proyecto de Investigación: «Competencia y Distribución: nuevos retos en la sociedad globalizada y en contextos de crisis económica» (DER2014-58774-R), del Ministerio de Economía y Competitividad (2014-2017).

1. LA NUEVA ECONOMÍA DE LOS DATOS

1.1 **Sobre la importancia y valor de los datos: ¿qué ha cambiado?**

La revolución tecnológica digital que se ha venido produciendo en las últimas décadas ha, indudablemente, convulsionado la actividad económica, modelando y redirigiendo la forma de hacer negocios de las empresas. El crecimiento exponencial de la contratación electrónica en el comercio de productos y en la prestación de servicios (transporte, bancario, seguros, etc.); la aparición de las denominadas plataformas de economía colaborativa; la oferta de nuevos servicios empresariales, como buscadores de Internet o comparadores de precios; el surgimiento de redes sociales de muy distinta naturaleza que exploran las nuevas posibilidades relacionales o el, más reciente, *Internet of Things* o Internet de las cosas (2), son sólo algunas de las muchas manifestaciones de la economía digital. Todas estas actividades virtuales comparten una característica fundamental: su capacidad para generar o producir información. Información que puede ser utilizada para obtener un beneficio comercial y cuyo crecimiento paulatino ha dado lugar a la aparición de un nuevo término en el marco de la economía digital: la economía de los datos o, más precisamente, la economía de los grandes datos o, en su manifestación más extendida, del *Big Data*.

En este sentido, en los mercados hemos venido asistiendo en los últimos años a la aparición de un número de empresas con importantes volúmenes de producción basadas en modelos de negocios que implican, precisamente, la recolección y uso comercial de datos o información (generalmente personal). Algunas de ellas cuentan con una cuota muy alta de usuarios en el sector de servicios en el que operan (así, por ejemplo, el buscador Google, o la red social Facebook). El modelo de negocio de estas empresas, es representativo de esta nueva economía de datos y se encuadra dentro de lo que se conoce como mercados de doble o múltiple cara (*two-sided* o *multisided markets)*. Estos mercados se caracterizan por la existencia de una empresa-plataforma que pone en contacto a dos colectivos distintos, vendiendo u ofreciendo dos o más productos o servicios a los dos grupos de consumidores, con demandas relacionadas indirectamente. Una de las características principales de estos mercados es la interdependencia entre ambos lados del mercado, lo que puede llevar a la plataforma a optar por estrategias de fijación de precios que permitan subsidiar el lado del mercado más sensible al precio por parte del lado más

(2) El denominado *Internet of Things* o Internet de las cosas hace referencia a la comunicación digital entre objetos. Supone el diseño de una estructura de red interconectada que permite que distintos dispositivos se comuniquen entre sí con la capacidad para compilar, transmitir y analizar datos (electrodomésticos inteligentes, *smartwatches*, alarmas, cámaras *web* con sensor de movimiento, etc.).

sensible al tamaño del otro lado del mercado. La plataforma, para maximizar beneficios, puede optar así por ofrecer el servicio de forma gratuita para obtener mayores ingresos en la otra parte del mercado en base a la mayor información recopilada como consecuencia de la gratuidad del servicio. En este sentido, por ejemplo, Google ofrece servicios gratuitos –o al menos sin coste monetario– a sus usuarios (buscador de Internet, servicio de traducción, etc.), a cambio de conseguir un gran volumen y variedad de datos por los que pagarán los anunciantes para publicitarse de manera más efectiva y personalizada (3). A esta estrategia basada en el valor económico asociado a los datos (*freemium*) es reconducible igualmente, la política empresarial de Facebook, que oferta gratuitamente el acceso a una red social.

Ahora bien, la economía de los datos no sólo se proyecta en estos sectores: motores de búsqueda, redes sociales o publicidad *online*. La información, el desarrollo de métodos de captación y procesamiento de datos es igualmente relevante en otros ámbitos como el de la energía, telecomunicaciones, seguros, banca o transportes. De hecho, el paulatino desarrollo del *Internet of things*, al que aludimos previamente, determinará que los datos no circunscriban su importancia a los mercados de servicios sino que la extiendan a su vez a los mercados de productos.

Pero, ¿a qué nos referimos con el término *data* o *Big Data*? Antes de entrar a valor las distintas definiciones y características estructurales de estos datos, resulta conveniente, a nuestro juicio, realizar dos precisiones. En primer lugar, entre los distintos tipo de información posible, el debate actual, al menos en lo que se refiere a la protección del consumidor o la competencia frente a utilizaciones de la información por parte de las empresas, se circunscribe a los datos personales, que engloban la información referida a una persona física identificada o identificable (4).

En segundo lugar, y para poder entender este fenómeno y sus implicaciones, es necesario tener en cuenta que no nos encontramos con algo sustancialmente novedoso. La búsqueda de datos por parte de las empresas o los intentos de captación de información de los clientes o consumidores en general, para crear o mejorar productos o servicios o para diseñar publicidad personalizada, siempre han existido (sistemas de cupones,

(3) *Vid.* sobre el funcionamiento de los mercados de doble cara. Fuensanta Alcaraz,: «Mercados de doble cara (I): Características y estrategia», 2017, disponible en http://blognewdeal.com. Se trata ésta de una de las características estructurales de la economía de datos que más implicaciones puede tener para la competencia y que, como tendremos ocasión de examinar, exige un conocimiento sólido de estos mercados por parte de las autoridades de la competencia para valorar el verdadero alcance de las conductas empresariales de prestación de servicios gratuitos en todos los sectores implicados.

(4) *Vid.* Artículo 2 de la Directiva 95/46/EC del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, *relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la libre circulación de estos datos.*

tarjetas de fidelidad, encuestas, etc.) (5). De forma paralela a lo que ha ocurrido en el campo de la economía colaborativa se ha producido una variación en la escala. Lo que ha cambiado, por tanto, ha sido la cantidad de información generada y la posibilidad de extraer valor económico de la misma. ¿Cuáles son los factores que han conducido a esta nueva dimensión? La capacidad actual de captación de una ingente cantidad de información así como de su rápido procesamiento es el resultado de la confluencia de una serie de factores tecnológicos. El primero de ellos es la desmaterialización de la información a través de la digitalización. Como señala la Autoridad Catalana de la Competencia se ha producido un fenómeno de transformación de los bienes físicos (átomos) a la información (*bits*) (6). Estamos viviendo en la era de la «datificación» en la que todos los aspectos o facetas de la vida (profesional, lúdico, etc.) pueden ser convertidas en datos. A la desmaterialización de la información hay que sumar las posibilidades actuales de interacción digital gracias al desarrollo de Internet y a la conectividad continua que resulta del crecimiento de los dispositivos móviles (tabletas, *smartphones*, etc.). La generación y captación de datos es más fácil en la etapa del «Internet relacional» o «Internet 2.0», que posibilita el contacto o comunicación digital, entre sujetos y, cada vez más, entre objetos.

Actualmente, se generan cada día millones y millones de *bytes* de información sobre toda clase de fenómenos y actividades. Esta información puede resultar tanto de transacciones de comercio electrónico, en las que los clientes facilitan voluntariamente sus datos personales, como, por ejemplo, de la posibilidad de seguimiento de su historial de compra. No sólo. Una consulta en un buscador, como Google, es información. Un *tweet* es información. Un «me gusta» en Facebook o Instagram es información. También es información un comentario en una página *web* de reservas hoteleras o la opinión sobre un restaurante. Información que se produce, difunde o almacena a través de medios tan variados como un teléfono móvil, una red social o la memoria de una cámara de seguridad, un pulsómetro, un frigorífico inteligente, etc.

Finalmente, esta generación ingente de información digital se ha visto acompañada del desarrollo de nuevas técnicas que permiten el procesamiento de una creciente cantidad de datos reduciendo los tiempos necesarios para dicha labor (7). Todo ello ha dado lugar a que la información,

(5) La captación, procesamiento y análisis de grandes cantidades de datos tampoco resulta ajena a las Administraciones Públicas. Puyol Montero, J.: *Aproximación jurídica y económica al Big Data*, Tirant lo Blanch, Valencia, 2015, p. 23, recoge como ejemplo de uno de los primeros proyectos de recolección de grandes datos, la elaboración del censo de EE. UU. en 1790.

(6) Autoritat Catalana de la Competència: *La Economía de los Datos. Retos para la competencia*, 2016, p. 6.

(7) *Vid.* Bundeskartellamt/Autorité de la Concurrence: *Competition Law and Data*, 2016, p. 8. Puyol Montero, cit., pp. 22 y ss. Para un desarrollo pormenorizado de algunas de estas técnicas,

ahora los macrodatos, datos masivos o *Big Data*, ocupen un lugar predominante en la actividad económica.

1.2 **Concepto y características del *Big Data***

El uso del término *Big Data* frecuentemente es vago e impreciso, admitiendo distinto alcance en la práctica. No obstante, las distintas definiciones existentes suelen partir de las características estructurales de esta nueva modalidad de información, como son la existencia de un gran volumen de datos y la imposibilidad de analizarlos a fin de extraer valor útil, empleando los métodos tradicionales (8).

Una de las descripciones de las características del *Big Data* más extendida, recogida por la mayoría de autores y organismos administrativos, es la de las cuatro «v». Con arreglo a la misma, se consideran rasgos definitorios de los datos masivos: el volumen, la variedad, la velocidad (de procesamiento) y el valor (9).

El volumen se manifiesta ya en la propia caracterización de los datos como «masivos» o «macrodatos». Significa la acumulación de grandes cantidades de datos y su incremento exponencial, como consecuencia de la ubiquidad de la actividad en red y su capacidad de generar continuamente datos digitales.

La velocidad de generación, acceso, procesamiento y análisis de los datos también se ha incrementado, posibilitándose en algunas aplicaciones que éstas actividades puedan llevarse a cabo a tiempo real (10).

Además, los datos pueden ser muy variados, tanto en lo que se refiere a su tipología, formato o estructuras empleadas para su presentación. La posibilidad de recabar datos de una pluralidad de fuentes va a permitir a las empresas acceder no sólo a información «tradicional» de sus clientes como dirección (física o IP), edad o género, sino a otro tipo de contenidos, como, por ejemplo, hábitos alimenticios, orientaciones ideológicas, historial de adquisiciones, viajes realizados y programados, etc.

La última «v» hace referencia al valor, como característica para definir el *Big Data*, ya que el análisis de los datos y la extracción de información

---

vid. García-Alsina, M.: *Big Data. Gestión y explotación de grandes volúmenes de datos*, UOC, Barcelona, 2017, pp. 93 y ss.

(8) *Vid. ad.ex.*, la definición propuesta por Puyol Montero, cit., p. 10, quien señala que se trata ésta de «una expresión utilizada en tecnología para referirse a la información o grupo de datos que por su elevado volumen, diversidad y complejidad no pueden ser almacenados ni visualizados con herramientas tradicionales».

(9) *Vid.* un desarrollo pormenorizado de estas características en: Stucke, M. E./Grunes, A. P. : *Big Data and Competition Policy*, Oxford University Press, Oxford, 2016, pp. 15 y ss.; Rubinfeld, D. L./Gal, M. S.: «Access Barriers to Big Data», 59, *Arizona Law Review*, 2017, pp. 345 y ss. Otros autores añaden más «v» a la caracterización: verificación, variabilidad, viabilidad y visualización. García-Alsina, cit., pp. 28 y ss.

(10) OCDE: *Big Data: Bringing Competition Policy to the Digital Era*, 2016, pp. 6-7.

crean conocimiento que puede ser utilizado como fuente de innovación, competitividad y productividad. El valor de los datos deriva de la existencia de tecnologías que permitan organizar, almacenar y, fundamentalmente, analizar en profundidad los datos, convirtiéndolos en información inteligente para las empresas y las administraciones públicas (11).

1.3 **Balance de efectos positivos y negativos asociados al *Big Data***

La utilización de las nuevas tecnologías y analíticas de *Big Data* puede ser enormemente ventajosa para las empresas, ayudándolas a mejorar la toma de decisiones y su rendimiento lo que puede traducirse, a su vez, en beneficios para sus clientes, trabajadores y para la economía y sociedad en general (12). Los datos puede ser utilizados así, como un insumo, al igual que el capital o el trabajo, en el desarrollo de la actividad empresarial. Mayoritariamente, el recurso por las empresas a técnicas de análisis de datos masivos tiene como principal objetivo obtener un mejor conocimiento del cliente y realizar previsiones sobre su comportamiento. La identificación de las opiniones, necesidades y valoraciones de sus clientes, posibilita a las empresas la mejora de los productos y servicios existentes, así como la explotación de nuevas oportunidades de negocio. Se facilita así que las compañías evalúen, mediante el análisis de datos, sus productos, obteniendo información muy valiosa que les permite crear nuevos productos o rediseñar los ya existentes. Las empresas pueden prever el desarrollo de las tendencias del mercado y actuar en consecuencia, mejorando la eficiencia del proceso productivo o distributivo.

A su vez, la extracción de conocimiento específico posibilita la segmentación de los clientes y facilita que las empresas puedan orientar sus servicios y satisfacer las necesidades de éstos de forma particularizada, por ejemplo, mediante recomendaciones o campañas publicitarias más personalizadas.

Es más, en los mercados de doble cara, al convertirse las políticas de datos en un activo esencial en el diseño de la estrategia competitiva, la necesidad de acceder continuamente a nuevas informaciones o de incrementar la base de datos existentes, conduce a las empresas a competir,

(11) Stucke/Grunes, *cit.*, p. 22, recalcan la interconexión existente entre el *Big Data* y el *Big Analytics*.

(12) El objeto de este trabajo se circunscribe a la posible afectación al desarrollo competitivo de los mercados como consecuencia de la utilización de políticas de datos por parte de las empresas. No obstante, las nuevas posibilidades de captación y procesamiento de datos pueden ser aprovechadas también por las Administraciones Públicas para la consecución de intereses generales (identificación de hábitos y problemas sociales, gestión de pandemias, entendimiento del cambio climático, mejora de los servicios públicos, etc.). *Vid.*, *in extenso*, Puyol Montero, cit., pp. 81 y ss. García-Alsina, cit., pp. 85 y ss.

mediante la mejora o la oferta a los consumidores de diversos servicios que les permiten acceder a sus datos y que son prestados generalmente, a precio cero o a precios muy reducidos (*Data-driven innovation*) (13).

Ahora bien, la irrupción y consolidación de esta nueva economía de los datos no está exenta de polémica y si bien es cierto que el recurso a técnicas o métodos de *Big Data* puede reportar importantes beneficios a los consumidores y ciudadanos, también se han puesto de manifiesto una serie de riesgos o eventuales efectos negativos asociados a la utilización por las empresas de volúmenes masivos de información. Mayoritariamente, la faceta negativa de los *Big Data* se ha centrado en la posible lesión del derecho a la privacidad de los consumidores o clientes. En la era digital, los individuos dejan traza de todas sus actividades (búsquedas, compras, viajes, lecturas…), generando diariamente grandes cantidades de información que son recopiladas y monetarizadas por las empresas, bien mediante su explotación directa o bien mediante su cesión a terceros. Cada rastro digital puede ser utilizado para recrear la vida cotidiana y los comportamientos, individuales o colectivos. De este modo, cuanto mayor sea el rastro creado, más parcelas de intimidad o espacios de privacidad se pierden (14). Las nuevas tecnologías permiten crear perfiles de consumidores con mayor facilidad y precisión y los consumidores, pueden no ser conscientes de la comercialización de sus informaciones personales –o, al menos, del alcance de ésta– (15).

Pero la cara oscura del *Big Data* no se limita a la lesión de la privacidad. En los últimos años, también el Derecho de defensa de la competencia o Derecho *antitrust* está entrando en el debate sobre sus bondades y peligros. La Comisión europea y las autoridades de competencia de los Estados miembros y de otras jurisdicciones, como la estadounidense, están abandonando la despreocupación que, hasta el momento, había conformado su actitud hacia los riesgos del *Big Data* para el desarrollo del proceso competitivo en los mercados. Resulta así significativo la aparición de documentos en los que se analizan las interrelaciones recientes entre *Big Data* y Derecho de la competencia, unida a la apertura de investigaciones y procedimientos contra empresas de referencia en materia de re-

(13) *Vid.* Sokol, D./Comerford, R.: «Does Antitrust Have a Role to Play in Regulating Big Data?, *Cambridge Handbook of Antitrust, Intellectual Property and High Tech*, Cambridge University Press, 2016, disponible en SSRN: https://ssrn.com/abstract=2723693

(14) En EE. UU. se hizo famoso el caso de la tienda de autoservicio Target, que consiguió predecir el embarazo de una joven a través del análisis de los comportamientos y preferencias de los clientes. *Vid.* la descripción del caso y un análisis de las estrategias de datos utilizadas por la empresa estadounidense, en «How companies learn your secrets», artículo del *New York Times*, de 16 de febrero de 2012

(15) A hacer frente a los riesgos a la posible afectación negativa del derecho a la intimidad y privacidad de los sujetos y al control por parte de los mismos de la información que sobre ellos existe *on line* obedecen las distintas normas en materia de protección de datos y está orientada la labor de organizaciones administrativas específicas, como la Agencia Europea de Protección de Datos.

copilación o acceso a datos *online*, de la que es buena muestra la reciente –y mediática– sanción de la Comisión al gigante Google por abuso de posición dominante (16). Se ha abierto un enconado debate que enfrenta a defensores acérrimos del *Big Data* y su carácter procompetitivo, con otras posiciones más recelosas, que alertan sobre la posibilidad de que la captación y explotación de datos pueda ser utilizada por las empresas como instrumento de creación, consolidación o extensión de posiciones de poder de mercado (17). Debate al que se superpone o se une el de la discusión sobre si el Derecho *antitrust* constituye el instrumento más adecuado para tratar con los riesgos o peligros que pueden derivarse para los consumidores de la difusión de modelos comerciales basados en los datos y si, en caso afirmativo, las técnicas y criterios tradicionales de aplicación del Derecho de la competencia resultan adecuados en estos sectores o, por el contrario, se precisa de la adopción de nuevos criterios.

2. EL FENÓMENO *BIG DATA* DESDE EL DERECHO DE LA COMPETENCIA

2.1 **Cambio de rumbo de las autoridades de competencia**

Desde hace unos pocos años, se viene produciendo un cambio de actitud de las autoridades de competencia en relación con los riesgos de las políticas de *Big Data* para la competencia, detectándose una creciente preocupación por el aumento del grado de concentración en mercados vinculados a los datos y el temor de conductas anticompetitivas de las

(16) Decisión de la Comisión de 27 de junio de 2017, Asunto 39740, *Google Searchs (Shop*ping).

(17) La doctrina, fundamentalmente estadounidense, se ha hecho eco de este debate. *Vid.* entre otros: Stucke/Grunes: *Big Data and Competition Policy*, cit.; *Idem:* «Debunking the Myths Over Big Data and Antitrust», *CPI Antitrust Chronicle*, 2015; *idem:* «Data-opolies», 2017, disponible en ssrn.com/abstract= 2927018; *idem:* «No Mistake About It: The Important Role of Antitrust in the Era of Big Data», *Antitrust Source*, 2015, disponible en https://ssrn.com/abstract=2600051; Balto, D. A./Lane M. C.: «Monpolizing Water in a Tsunami: Finding Sensible Antitrust Rules for Big Data», 2016, disponible en SSRN: https://ssrn.com/abstract=2753249; Sokol, D. D./Comerford, R.: «Does Antitrust Have a Role to Play in Regulating Big Data?, *cit.*; *idem:* «Antitrust and Regulating Big Data», 23, *George Mason Law Review*, 2016, pp. 1129 y ss os cada vez más complejos y antempetencia, cit., pp. Eral Budeskartellamt de Google aludiendo al caracter on beneficios econura.; Lerner, A. V: «The Role of Big Data in Online Platform Competition», 2014, disponible en: https://ssrn.com/abstract=2482780 or http://dx.doi.org/10.2139/ssrn.2482780; Newman, N.: «Antitrust and the Economics of the Control of User Data», *Yale Journal on Regulation*, Vol. 30, No. 3, 2014; Lundqvist, B.: «Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet of Things World», 2016 disponible en: https://ssrn.com/abstract=2891484; Tucker, D. S.; Wellford, H.: « Big Mistakes Regarding Big Data», *Antitrust Source*, 2014, disponible en: https://ssrn.com/abstract=2549044; Manne, G. A./Sperry, B.: «The Law and Economics of Data and Privacy in Antitrust Analysis», 2015, disponible en: https://ssrn.com/abstract=2418779; *idem:* «The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework», *CPI Antitrust Chronicle*, 2015: Woodcock, R: «Big Data, Price Discrimination, and Antitrust», *Hastings Law Journal*, Vol. 68, 2017; Manne, Geoffrey A. and Sperry, Ben, The Problems and Perils of Bootstrapping Privacy and Data into an Antitrust Framework (May 29, 2015). CPI Antitrust Chronicle, May 2015; Colangelo, G/Maggiolino, M.: «Data Protection in Attention Markets: Protecting Privacy Through Competition?», 2017, disponible en https://ssrn.com/abstract=2945085; Bamberger, K. A./Lobel, O.: «Platform Market Power», *Berkeley Technology Law Journal*, Vol. 32, No. 3, 2017.

empresas líderes que controlan cantidades ingentes de informaciones personales. Como señalamos anteriormente, la publicación de diversos documentos (18) en los que se valoran las implicaciones del *Big Data* desde una perspectiva competitiva y una mayor agresividad en la política de aplicación de las normas por parte de las autoridades de la competencia (19) son manifestaciones claras de este nuevo temor y de que, el control de información ha dejado de ser un asunto extraño o irrelevante en el marco del Derecho *antitrust*.

Para poder entender la orientación actual de las autoridades administrativas en relación a los eventuales riesgos que del control de grandes volúmenes de datos pueden derivarse para la competencia, es preciso tener en cuenta que, hasta hace muy poco tiempo, las investigaciones en los mercados digitales de las grandes empresas del sector se habían centrado en las fuentes tradicionales de adquisición de poder de mercado, como el control de infraestructuras o la titularidad de propiedad intelectual o industrial. La posibilidad de que una empresa pudiera adquirir una posición dominante como consecuencia del control de informaciones personales se consideraba poco realista. Esto unido a la existencia de beneficios ciertos para los consumidores asociados a la utilización por parte de las empresas de técnicas de *Big Data*, como servicios «gratis», mejora cualitativa de las plataformas o de los productos o servicios ofertados así como una actividad publicitaria mejor focalizada determinó la escasa relevancia del *Big Data* en el marco del análisis *antitrust* y que los eventuales riesgos o problemas que pudieran derivarse fueran encomendados a otros sectores del ordenamiento jurídico, como la normativa especifica de protección de datos o el Derecho del consumo.

Ahora bien, el surgimiento de gigantes empresariales en la prestación de determinados servicios *online* ha desatado el temor de las autoridades de la competencia de que un incremento en la captación y tratamiento de

(18) *Vid.* Bundeskartellamt/Autorité de la Concurrence: *Competition Law and Data*, *cit.*; Autoritat Catalana de la Competència: *La economía de los datos. Retos para la competencia: cit.*; OCDE: *Big Data: Bringing competition policy to the digital era*, cit.; Agencia Europea de Protección de Datos: *Privacy and competitiveness in the age of big data. The interplay between data protection, competition law and consumer protection in the Digital Economy*, 2014.

(19) Las políticas empresariales de los gigantes del sector están siendo objeto de escrutinio por parte de la Comisión europea y de las autoridades de competencia de los Estados miembros. En este sentido, en el marco europeo se han abierto investigaciones a Facebook tanto en relación a nuevas conductas como a operaciones enjuiciadas favorablemente y que ahora despiertan nuevos recelos, como la concentración entre Facebook y la plataforma WhatsApp. En Diciembre de 2016, la Comisión envió un pliego de cargos a Facebook, alegando que la empresa había proporcionado información engañosa sobre su pretendida política de privacidad durante la investigación realizada en el marco de la concentración con WhatsApp. También en 2016, el *Bundeskartellam*t incoó un procedimiento contra Facebook por posible abuso de su posición de dominio en el mercado de las redes sociales. Todo ello además con el trasfondo de la polémica sanción por parte de la Comisión a Google, acusado de haber abusado de su posición dominante en el mercado de los navegadores por favorecer sus propios servicios de comparadores de precios y de la existencia de otras investigaciones abiertas contra el gigante estadounidense por el uso del sistema operativo Android.

la información pueda conducir a una intensificación del grado de concentración de los mercados y manifestarse en conductas anticompetitivas, lo que ha determinado un replanteamiento de las dos grandes premisas que sustentaban la desatención anterior: que los datos no son una fuente idónea de poder de mercado y erección de barreras de entrada y que la protección de la privacidad es un objetivo extraño al Derecho de la competencia. Aparecen así nuevas preocupaciones, que se van a manifestar en una redefinición en la aplicación de la prohibiciones: nuevas delimitaciones de los mercados relevantes y teorías de los efectos anticompetitivos, así como nuevas posibilidades de lesión o daño de los consumidores.

2.2 ***Big Data* y poder de mercado**

El poder de mercado constituye un elemento vertebral del Derecho de la competencia y de la política de aplicación de sus normas. Todas las prohibiciones de conductas empresariales acaban, en último término, girando en torno al concepto de poder de mercado, entendido, desde una perspectiva jurídica, como la posibilidad de comportamiento independiente o autónomo de las empresas en el mercado (20). El control de las concentraciones entre empresas está orientado, precisamente, a impedir la formación de posiciones de poder, unilaterales o colectivas, en los mercados. La posición de dominio constituye un requisito previo para establecer la existencia de un abuso prohibido por el artículo 102 TFUE (y sus equivalentes nacionales) y la posibilidad de exención de los acuerdos restrictivos del artículo 101 TFUE depende, en gran medida, de que las partes implicadas tengan o no poder de mercado. Por tanto, el poder de mercado y la utilización abusiva del mismo constituyen el corazón del Derecho de la competencia, sin éste, las propias fuerzas libres del mercado, impedirán la causación de daño a los consumidores, beneficiarios últimos de sus normas.

Tradicionalmente, doctrina –económica y jurídica– y autoridades de competencia han contemplado con sumo escepticismo, en el marco de los negocios *online*, la posibilidad de que el mero control de datos, con independencia de su volumen, pudiera ser suficiente para conferir a una empresa poder de mercado y, por tanto, constituir una preocupación desde una perspectiva competitiva.

(20) El concepto de posición de mercado, pese a su importancia no es definido en el Tratado, sino que está labor será asumida por la Comisión y el TJUE en su labor y aplicación de las normas, fundamentalmente, del abuso de posición de dominio. Rechazando definiciones de naturaleza económica (que sí son acogidas en otros sistemas como el estadounidense) que se centran en la capacidad de la empresa dominante para restringir de forma sustancial la producción del mercado, en el maraco europeo se considera como posición de dominio: «una posición de poder económico de la que disfruta una empresa que le permite impedir el mantenimiento de una competencia efectiva en el mercado relevante al posibilitarle en medida apreciable comportamientos independientes respecto a sus competidores y clientes y, en definitiva, de los consumidores» (sentencia del TJUE de 14/2/1978, asunto 27/76 *United Brands)*.

Es cierto que la economía de los datos presenta como una característica singular la presencia habitual de efectos de red (*network effects*) en los mercados implicados, especialmente en el caso de los mercados de doble cara, que significa que el valor de un producto o servicio está en función del número de usuarios que tiene. Así, por ejemplo, cuanto mayor sea el número de usuarios de una plataforma, mayor será su valor para los anunciantes. Los efectos de red suelen traducirse, desde una perspectiva estructural, en la concentración de la actividad en manos de muy pocas empresas (21).

Ahora bien, la existencia de elevadas cuotas de mercado no significa necesariamente la tenencia de poder de mercado. En este sentido, se han apuntado diversas características económicas de los datos que determinan que su acumulación no implica, en si misma, la creación de barreras de entrada y no otorga automáticamente a la empresa titular de los mismos el incentivo o la habilidad de excluir a las empresas competidoras, expandir o consolidar su propia posición de domino o lesionar la competencia de cualquier otro modo (22).

En primer lugar, se suela afirmar que, la mayoría de los mercados digitales –de los que los mercados relacionados con los datos formarían un subtipo o categoría– se caracterizan por la ausencia o la falta de importancia de barreras de entrada. Se trata de mercados muy dinámicos en los que el elemento clave de competencia no es el precio, sino la innovación, lo que facilita que las empresas que irrumpan con productos o servicios novedosos puedan obtener el favor de los consumidores y conseguir rápidamente la información que precisan para mejorar su oferta y desplazar a las empresas incumbentes (23). En apoyo de esta afirmación se suele citar el ejemplo de empresas como Google o Facebook que consiguieron desbancar a operadores muy asentados, como Yahoo o Lycos en el primer caso, y My Space, en el segundo (24). La propia Comisión Europea defendió la facilidad de entrada en los mercados de aplicaciones digitales para los consumidores, en el marco de la concentración entre Facebook y WhatsApp (25).

---

(21) Sobre los distintos efectos de red que pueden estar presentes en los mercados relacionados con los datos, *vid.*, in extenso, Stucke/Grunes: *Big Data and Competition Policy*, cit., pp. 200 y ss.; Autoridad Catalana Competencia: cit., pp. 11 y ss.

(22) *Vid.*, Sokol/Comerford; «Antitrust and Regulating Big Data», *cit.*; Tucker/Wellford: cit.; Balto/Lane:, cit.

(23) El presidente de Google, Eric Schmidt, minimizó cualquier posibilidad de efectos anticompetitivos derivados de la conducta de su empresa aludiendo al carácter abierto de los mercados digitales. «Las barreras de entrada son insignificantes, porque la competencia está a un solo click», «The Tinkerer's Apprentice», disponible en https://www.project-syndicate.org/commentary/google-european-commission-and-disruptive-technological-change-by-eric-schmidt-2015-01.

(24) *Vid.* Tucker/Wellford, cit., p. 7.

(25) Decisión de la Comisión de 3 de octubre de 2014, Asunto M.7217, *Facebook/WhatsApp*, párrafo 132: «*consumer communications apps are a fast– moving sector, where customers' switching costs and barriers to entry/expansion are low. In this market any leading market position even if assisted by network effects is unlikely to be incontestable. The market of*

En cualquier caso, se ha defendido que las propias características económicas de los datos personales: ubicuidad, bajo coste, amplia accesibilidad y obsolescencia, impedirían que una empresa adquiriera poder de mercado mediante su captación y explotación, sin importar la entidad de las cantidades de datos manejadas.

Los datos son ubicuos y su captación fácil y asequible. La información se encuentra en todas partes (*Big Data is everywhere*) (26) y las fuentes de suministros de datos *online* están en continuo crecimiento, que se prevé aún más intenso en un futuro con la consolidación plena de las tecnologías del Internet de las cosas.

Además, a diferencia de otros *inputs*, la utilización de los datos por una empresa no excluye un posible uso de los mismos por parte de terceros. No es posible una apropiación en exclusiva de los datos. La captación de una información determinada por parte de una empresa no impide a otras acceder a ella empleando los mismos medios u otros diversos. Los consumidores pueden compartir sus datos con una pluralidad de empresas. De hecho, la multiconexión o *multihoming*, es decir, la utilización de una pluralidad de proveedores para obtener el mismo servicio, puede ser un importante factor de desestabilización de posiciones de poder de mercado. En último término, además, las empresas pueden adquirir los datos o informaciones que precisan de un tercero, existiendo numerosas empresas en el mercado dedicadas precisamente al almacenamiento, análisis y comercio de información (*Data brokers*).

Los datos se quedan pronto obsoletos y pierden su utilidad rápidamente. La tenencia de largas bases de datos no supone una ventaja significativa a menos que éstas sean continuamente actualizadas y cuidadosamente organizadas.

Finalmente, el valor de las informaciones personales no reside en su cuantía, sino en la habilidad de una empresa para explotarlas, siendo mucho más importantes los algoritmos y tecnologías que se utilicen que los meros datos. La fusión de diferentes fuentes de datos, como resultado de una fusión corporativa o de otro tipo, no supone necesariamente una mejora de la capacidad de las empresas para explotar esos datos.

---

consumer communications apps has a long track record of entry by new players. Also, competing consumer communications apps are able to grow despite network effects, both over time and following disruptions in the market. Such threat from new players constitutes and is likely to keep constituting a significant disciplining factor for the merged entity, regardless of the size of its network».

(26) Precisamente, la ubicuidad de los datos y la posibilidad de acudir a otras fuentes alternativas para su captación constituía la base del razonamiento de la autorización, por parte tanto de la FTC como de la Comisión europea de dos importantes operaciones de concentración en estos sectores: la operación Google/Double Click y la adquisición por parte de Facebook de la plataforma WhatsApp.

En conclusión, el control de datos no puede dar lugar a la erección de barreras de entrada y, por tanto, a la existencia de posiciones de poder de mercado. No son un insumo esencial para competir y, en cualquier caso, existen posibilidades de acceso a los mismos asequibles, ya sea directa o indirectamente mediante su adquisición de terceros.

Estas afirmaciones sobre el funcionamiento de los mercados digitales y de las políticas empresariales de *Big Data*, pese a su indudable atractivo y contundencia no gozan de aceptación universal. Tanto desde la doctrina como desde las autoridades de la competencia, algunas de estas premisas están siendo puestas en tela de juicio, cuestionándose su solidez o, cuanto menos, la categorización con la que se presentan (27). De hecho, las principales críticas se centran en la falta de validez de estas afirmaciones como reglas de carácter general. No todos los mercados de la economía digital son iguales, observándose en algunos una feroz competencia y la sustitución continua entre los operadores económicos, y una mayor estabilidad en otros, con presencia de empresas con elevadas y estables cuotas de mercado. La existencia de competencia en un mercado no excluye la posibilidad de barreras de entrada en otro ni que resultados pasados de irrupción en un mercado impliquen necesariamente que esto vaya a ocurrir en el futuro. Las posturas revisionistas alertan sobre los riesgos de dar las cosas por descontado y señalan la necesidad de examinar caso por caso, teniendo en cuenta que las circunstancias particulares de los distintos mercados difieren y que las barreras de entrada en mercados asociados a los datos no son invariablemente altas ni bajas. Cada industria puede ser diferente.

De este modo, si bien es cierto que la existencia de efectos de red puede ser vista como un elemento desestabilizador de posiciones de poder de mercado previas si nuevos entrantes son capaces de atraer a un número significativo de usuarios mediante el ofrecimiento de productos o servicios innovadores, desplazando así a operadores anteriores, también puede ser un factor conducente a la concentración de los mercados y a la erección de barreras de entradas. De hecho, los mercados de doble cara suelen ser mercados altamente concentrados con características de oligopolio natural y elevados costes de entrada, como consecuencia de la necesidad de desarrollar ambos lados del mercado para poder competir. Estos mercados, además, llevan implícito un riesgo estructural ya que, en ellos se plantea el problema del único ganador (*winner takes it all*) que se suele producir cuando el valor de la red es muy alto, los costes de multiconexión muy elevados y menor la diferenciación de la demanda entre los

(27) Entre la doctrina, *vid.*, especialmente, las posiciones de Stucke/Grunes en sus distintos trabajos (cit.); Mahnke, R. P. : «Big Data as a Barrier to Entry», 2, *CPI Antitrust Chronicle*, 2015, pp. 1 y ss.; Rubinfeld, D. L./Gal, M. S.

usuarios. La actividad se concentra así en un grupo muy reducido de empresas «líderes», dejando al resto en posiciones meramente residuales.

Los efectos de red y la consiguiente exclusión de otros competidores puede verse reforzada, además, en estos mercados, por lo que se conoce como el «*feedback loop*», o «bucle de retroalimentación», de los algoritmos de aprendizaje automático (28). Cuantos más usuarios tenga una plataforma, más datos tiene a su disposición y los algoritmos utilizados para determinar las intenciones y preferencias de sus usuarios arrojarán resultados más precisos: resultados de búsquedas más relevantes, anuncios más focalizados o recomendaciones de productos más pertinentes. Cuánto más exacto y personalizado sea la identificación de clientes, más valor tendrá la plataforma para los anunciantes y más pagarán éstos para alcanzar a sus potenciales compradores.

La pretendida accesibilidad de los datos también ha sido cuestionada. La disponibilidad de fuentes alternativas de datos también variará en función de los mercados. Una situación de *multihoming* o multiconexión perfecta es rara en la práctica debido a la existencia de diversos costes de cambio (aprendizaje, efectos de red, etc.) que dificulten a los consumidores el recurso a varios proveedores en la misma proporción. Algunas estrategias empresariales relacionadas con las políticas de datos sector parecen contradecir el pretendido dinamismo de los mercados digitales y la disponibilidad generalizada y asequible de información: ¿Cómo se compagina la defendida ubicuidad y accesibilidad de los datos con las costosas políticas de prestación de servicios a coste cero por parte de las plataformas para mantener y desarrollar su base de datos? y ¿con las costosísimas operaciones de concentración realizadas por las plataformas de adquisición de empresas explicables sólo por la cartera de datos que éstas pueden aportar?

El acceso a los datos y a la información basada en ellos constituye un activo estratégico y valioso para las empresas. El control de una base de datos significativa y de eficaces tecnologías de análisis de dicha información suponen, sin duda, una ventaja competitiva importante sobre los rivales. Las empresas pueden recurrir así a diversas estrategias para mantener o reforzar esa ventaja y excluir a terceros del acceso a los datos: celebración de acuerdos de exclusiva, operaciones de adquisición de empresas, etc. No cabe descartar *a priori* el éxito de dichas maniobras y la eventual afectación negativa a la estructura y al desarrollo del proceso competitivo en los mercados, es decir, no puede excluirse automáticamente la posibilidad de que esa ventaja se traduzca en la formación o consolidación de una posición de poder de mercado, especialmente cuando la entidad de los datos controlados o el valor de las tecnologías de

(28) *Vid.* Miller, cit., p. 9.

análisis sean clave para competir y no puedan ser replicadas por terceras empresas. El debate existente pone de manifiesto, a nuestro juicio, la dificultad de identificar características universales válidas sobre el funcionamiento de los mercados de datos que puedan ser utilizadas sin consideración del caso especifico en el juicio sobre la anticompetitividad o no de una conducta.

2.3 **Aplicación de las normas *antitrust:* posibles riesgos para la competencia**

2.3.1 La adecuación de los instrumentos tradicionales y la privacidad como interés tutelable por el Derecho de la competencia

Descartada la connatural inocuidad de las políticas empresariales vinculadas al *Big Data* desde la óptica del Derecho de la competencia, se plantea ahora la necesidad de identificar los factores presentes en estos mercados y las conductas de los operadores económicos que pueden despertar problemas competitivos, valorándolos desde las distintas categorías de conductas prohibidas: concentraciones, acuerdos colusorios y abuso de posición dominante.

Ahora bien, antes de proceder al análisis de cada una de estas categorías de manera específica, es conveniente realizar dos consideraciones generales que inciden sobre todas ellas. Estas consideraciones derivan de los rasgos caracterizadores de esta nueva economía de datos, así como de la necesidad de clarificar el papel que compete –si alguno– al Derecho *antitrust* frente a lesiones del derecho a la privacidad de los individuos.

En primer lugar, las especiales características de estos mercados determinan que muchas de las herramientas utilizadas actualmente en el análisis *antitrust,* muy centradas en los precios de los productos o servicios, no resulten adecuadas en algunos de los mercados digitales, señaladamente, en los mercados de múltiples lados, especialmente en los casos en que los productos o servicios son ofrecidos gratuitamente. En este sentido, un paso esencial del análisis *antitrust* es la delimitación de los mercados relevantes, que se realiza tradicionalmente atendiendo a criterios como la sustituibilidad de la demanda o de la oferta, para cuya medición se utiliza el conocido como test del monopolista hipotético o SSNIP test con arreglo al cual se estima que forma parte del mismo mercado el mínimo grupo de productos para los cuales un hipotético monopolista encontraría posible y beneficioso realizar un incremento de precios entre un 5 y un 10% (*small but significant non transitory increase in prices*) (29). El test presupone que el producto o servicio en cuestión es ofrecido a cambio de un precio

(29) Comunicación de la Comisión Europea de 9 de diciembre de 1997, *relativa a la definición del mercado de referencia a efectos de la normativa comunitaria de competencia* (DOCE C372/5).

monetario por lo que no resulta adecuado para identificar un mercado cuando el servicio se ofrece a cambio de «datos» o «información» (30). Se ha propuesto como criterio alternativo al SSNIP test el SSNDQ test, que valoraría las respuestas de los usuarios de un servicio en respuesta a «una pequeña pero significativa y no transitoria disminución de la calidad» (*small but significant non transitory decrease in quality)* (31).

Las autoridades de competencia tradicionalmente se han centrado sólo en uno de los múltiples lados de un mercado, el lado remunerado, para determinar la eventual afectación de la competencia, si bien en los últimos pronunciamientos parece estar abriéndose la posibilidad a valorar la incidencia de las conductas empresariales también en la prestación de servicios gratuitos de la plataforma a sus clientes (32).

Una segunda cuestión, interrelacionada, y que está llamada necesariamente a incidir en el desarrollo de las relaciones entre Derecho de la competencia y *Big Data* es la determinación del papel que a este sector del ordenamiento jurídico compete en la protección de la privacidad de los sujetos. Si bien las referencias a la posible afectación del derecho a la privacidad no son ajenas al análisis *antitrust*, sobre todo en el ámbito del control de concentraciones, las autoridades de competencia tendían a rechazar la adecuación de las normas *antitrust* para resolver posibles lesiones de este derecho, reenviando a otras ramas jurídicas, como el Derecho del consumo y las normas específicas sobre protección de datos (33).

---

(30) De hecho, en Alemania el hecho de que los servicios fueran ofrecidos a coste cero impedía delimitar o afirmar la existencia de un mercado relevante a efectos del análisis *antitrust* y ésta es la solución que se defiende desde algunos sectores de la doctrina estadounidense. *Vid. ad.ex.*, TUCKER/WELLFORD, cit., pp. 6 y ss.

(31) *Vid.* OCDE: *Big Data: Bringing Competition to the Digital Era*, cit., pp. 16 y ss.

(32) En este sentido, en la valoración de la concentración entre Facebook y WhatsApp, el análisis de la eventual anticompetitividad se centró en uno solo de los lados del mercado implicados, el de la publicidad online en las plataformas, es decir, en la relación entre la plataforma y sus clientes anunciantes, pero no entró a valorar el mercado de servicios de red social (plataforma-consumidores). En cambio, en el caso Google, la Comisión ha llevado a cabo una delimitación de mercados mucho más amplia, valorando los efectos de la conducta de la empresa, dominante en el mercado de los navegadores, en el mercado de los comparadores de precios. También en el marco de la operación de concentración entre Microsoft y Linkeldn, se ha prestado especial atención al mercado de servicios de redes sociales. En un sentido similar, el Bundeskartellamt, en su reciente investigación contra Facebook por presunto abuso de posición de dominio ha manifestado su preocupación de que las prácticas de la empresa afecten a la competencia en el mercado de las redes sociales.

(33) *Vid.*, el discurso de la Comisaria de competencia, Margrethe Vestager, de 17 de enero de 2016, «*Competition in a big data world*», disponible en https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/competition-big, en el que se afirma expresamente la inconveniencia de acudir a la política de la competencia para resolver cuestiones de privacidad: «*The real question isn`t whether companies are competing to offer more privacy but for us to have adequate data protection rules in place. I don´t think we need to look to competition enforcement to fix privacy problems…*». Igualmente, la Comisión en el caso Facebook/WhasApp, que planteaba problemas de privacidad de los usuarios de ambas redes, consideró que: «… la Comisión ha analizado la concentración potencial de información sólo en relación con que refuerce la posición de Facebook en el mercado de los anuncios digitales o cualquier subsegmento que del mismo dependa. Cualquier cuestión relacionada con la privacidad derivada del incremento de concentración de datos dentro del control de Facebook como consecuencia de la transacción

Ahora bien, en los dos últimos años, tanto la Comisión como los organismos nacionales de competencia han empezado a considerar la pérdida de control sobre la información personal y la lesión del derecho a la privacidad como un posible daño competitivo. Los documentos publicados por diversas autoridades y los más recientes pronunciamientos de la Comisión, como el citado caso Microsoft/Linkeldn, parecen anunciar así un cambio de orientación en el que las consecuencias en privacidad derivadas de un incremento en la concentración de datos van a ser incluidas en el análisis *antitrust*, buscándose para ello vínculos de fundamentos más o menos sólidos (34). Así, se parte de que el bienestar de los usuarios no depende sólo del precio que monetariamente abonan por el servicio sino también de la calidad del mismo y de la variedad de la oferta a su disposición. Entre las variables cualitativas de la competencia se encuentra la privacidad de sus datos. Un incremento en la colección de datos privados podría ser analizado bien como un incremento de precios (*data is the new currency in the Internet*) o como una degradación de la calidad de los servicios provistos.

También sobre la base de la afectación a la competencia, doctrina y autoridades proponen una serie de remedios orientados a solucionar o mitigar los problemas que para la privacidad pueden derivarse de la acumulación de datos en una –o en unas pocas-, empresas-. Las propuestas incluyen medidas como la creación de estándares globales de privacidad, el reconocimiento del derecho a la portabilidad de los datos, la obligación de garantizar el acceso a datos, etc. (35). Soluciones regulatorias, a nuestro juicio, de difícil anclaje en el Derecho *antitrust*, tanto por lo que se refiere a sus objetivos como a su aplicación y que resultarían más adecuadas en el marco normativo especifico de la protección de datos.

2.3.2 Prácticas colusorias

Aunque el debate sobre los posibles riesgos para la competencia de las políticas de *Big Data* se ha planteado mayoritariamente desde la perspectiva de la posible adquisición de poder de mercado como consecuencia del control de información y, por tanto, en relación a la operatividad de las normas sobre control de concentraciones y sobre abuso de posición dominante, no cabe descartar la posibilidad de comportamientos coordinados en mercados relacionados con datos y por tanto, la aplicabilidad de las prohibición de acuerdos restrictivos de la competencia o prácticas colusorias.

---

no cae dentro del ámbito de las normas de competencia europeas sino dentro del ámbito de la protección de datos a nivel europeo» (párrafo 164).

(34) De hecho, el presunto abuso por el que el Bundeskartellamt abrió la investigación contra Facebook consistía en la vulneración por parte de esta compañía de la normativa sobre protección de datos.

(35) *Vid.* Autoritat Catalana de la Competencia: *La economía de los datos. Retos para la competencia,* cit., pp. 24 y ss.

La disponibilidad creciente de información digital sobre precios y otras características de los productos en Internet, y la posibilidad de que esta información sea adquirida y procesada en tiempo real refuerzan extraordinariamente el grado de transparencia de los mercados digitales. La transparencia en el mercado puede tener efectos ambiguos. Por un lado, los consumidores están más y mejor informados sobre precios, calidad y condiciones de compra. No obstante, por otro, la transparencia de precios puede limitar la competencia, propiciando la colusión entre competidores, al facilitar la detección de desviaciones del posible acuerdo (explícito o tácito) (36). Este riesgo se puede ver acrecentado en los mercados digitales, dada la existencia de sistemas dinámicos de fijación de precios que se actualizan continuamente. Los denominados *pricing bots*, algoritmos de fijación de precios, pueden evaluar y ajustar los precios en segundos, teniendo en cuenta una innumerable variedad de factores, como los precios de la competencia. Esto les da la capacidad de responder al momento a posibles descuentos de los rivales, eliminando el incentivo de los competidores de bajar los precios (37). El recurso a algoritmos para controlar las políticas de precios de terceros también podría ser utilizado por los fabricantes para sostener políticas de fijación de precios de reventa, al permitirles detectar rápidamente los eventuales descuentos realizados por los distribuidores por debajo del precio mínimo fijado.

Por último, un peligro nuevo que se vincula a las políticas de datos, es que el recurso a estrategias de seguimiento del líder con el uso de algoritmos automáticos de cálculo de precios, podría dar lugar al surgimiento de conductas de colusión sin que exista un acuerdo de coordinación previo (38). Hipotéticamente podría plantearse una situación en la que algoritmos independientes, cada uno de ellos utilizado por empresas competidoras, decidieran de manera autónoma, que la mejor manera de maximizar el beneficio de sus respectivas empresas es la coordinación en el precio. En este escenario, por el momento más propio de la ciencia ficción, la

(36) El éxito y sostenibilidad de una actuación coordinada entre empresas competidoras requiere de la concurrencia de diversas condiciones. En primer lugar, todo acuerdo o cooperación entraña una dificultad inicial que es la determinación de sus términos y alcance. Superada esta primera barrera, es preciso arbitrar mecanismos eficaces y creíbles de detección y castigo de posibles infractores. La detección de conductas de desvío requiere un elevado grado de transparencia de los mercados. *Vid. in extenso*, Herrero Suárez, C.: «El problema del oligopolio en el Derecho de la competencia comunitario», *Actas de Derecho Industrial*, tomo XXIII, 2002.

(37) Esta preocupación se encuentra expresamente contemplada en los distintos informes de las autoridades de competencia (cit.). *Vid.* un desarrollo del problema de coordinación de conductas en mercados relacionados con los datos en Ezrachi, A./Stucke, M. E.: *Virtual Competition. The Promise and Perils of the Algorithm-Driven Economy*, Harvard University Press, Masssachusetts, 2016, pp. 35 y ss.

(38) *Vid.* el artículo «Price-bots can collude against consumers», publicado en *The Economist*, el 6 de mayo de 2017.

colusión no resultaría del entendimiento humano sino de uno –o varios– programas de *software* (39).

¿Qué puede hacerse desde el Derecho de la competencia para hacer frente al incremento del riesgo de coordinación como consecuencia del uso de estas técnicas matemáticas? El problema que plantean estos casos es la dificultad de persecución de estas conductas. En primer lugar, la transparencia en los mercados, con carácter general, es muy beneficiosa para los consumidores si éstos pueden acceder a la misma información que las empresas. En segundo lugar, el recurso a sistemas automáticos de fijación de precios está ampliamente extendido en el ámbito digital y su utilización no puede sin más, ser causa de sospecha o recelo por parte de las autoridades de la competencia. Como tercer y, en nuestra opinión, punto más importante, es preciso recordar que el artículo 101 TFUE, resulta de aplicación únicamente en los casos en que exista, al menos, un concierto o entendimiento entre las empresas. Así, en principio, este artículo alcanzaría sólo a los supuestos de coordinación de conductas en el mercado que tienen su causa o base en un acuerdo, pero no se extendería a los casos en que esa coordinación o paralelismo, por ejemplo, en materia de precios, es fruto meramente de las propias circunstancias estructurales del mercado, obedece únicamente a la actuación unilateral y racional, si bien interdependiente, de las empresas.

En los supuestos en los que sí exista acuerdo, el recurso a los algoritmos como instrumento para favorecer la ejecución del mismo podría caracterizarse como una práctica facilitadora (*facilitating practices*), entendida como aquella conducta que ayuda a las empresas a coordinar precios o a la realización de cualquier otra conducta anticompetitiva (40). El algoritmo, al ayudar a detectar posibles desvíos del esquema cooperativo, cumpliría una función similar a las cláusulas de alineación o a las conductas de intercambio de información

En cualquier caso y pese a las dificultades de actuación que necesariamente las autoridades de competencia van a tener que afrontar en estos escenarios, la Comisión ya ha avanzado que el hecho de que la fija-

(39) *Vid.* Vernager, discurso de 17 de enero de 2016, «Algorithms and competition», disponible en https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/bundeskartellamt-18th-conference-competition-berlin-16-march-2017.

(40) Bajo este término se engloban todas aquellas prácticas empresariales que pueden ayudar a aliviar los riesgos y dificultades propios de toda coordinación anticompetitiva, disminuyendo la incertidumbre y reduciendo los incentivos para desviarse del esquema cooperativo. Mediante estas conductas, los miembros del oligopolio tratan de cambiar intencionadamente la naturaleza del mercado para posibilitar la adopción en el mismo de comportamientos paralelos, sin tener que recurrir a un acuerdo expreso. El principal riesgo de estas prácticas es, por tanto, su tendencia anticompetitiva en atención a las particulares circunstancias o caracteres de un mercado, más que una anticompetitividad sustancial a las mismas. *Vid.* Herrero Suárez, *cit.*, pp. y ss.; Yao/De Santi: «Game Theory and the Legal Analysis of Tacit Collusion», 38, *Ant. Bull*, 1993, p. 120.

ción de precios resulte de un sistema automático, no impide alcanzar a las empresas que los utilizan y ha recalcado la conveniencia de que las empresas tengan presente las normas *antitrust* en la programación y uso de sus algoritmos de fijación de precios (*antitrust compliance by design*).

2.3.3 Control de las concentraciones entre empresas

Hasta el momento, el único sector en el que realmente se han planteado en la práctica problemas de competencia y *Big Data*, ha sido el de las operaciones de concentración entre empresas. La Comisión y las autoridades de competencia de los Estados miembros y de otras jurisdicciones han tenido que examinar las implicaciones competitivas de operaciones de crecimiento externo de empresas representativas de esta nueva economía de datos (41). Así, entre las operaciones más significativas, a nivel europeo, al menos por la entidad de las empresas implicadas, cabe destacar las concentraciones, *Google/DoubleClick* (42), *Facebook/WhatsApp* (43) y, más recientemente, *Microsoft/Linkedln* (44).

La aplicación de la política en materia de concentraciones a las empresas de la economía de datos plantea una serie de dificultades en la práctica, tanto por lo que respecta a la propia posibilidad de activar el mecanismo de control como a la categorización de la operación y a su evaluación desde una perspectiva sustantiva.

Así, en primer lugar, en los mercados digitales, son frecuentes las concentraciones por las que una gran empresa asentada en el mercado adquiere una empresa recién llegada o *start up*, que ofrece un producto o servicio novedoso, pagándose por ella un precio muy superior al que podría deducirse de su volumen de ingresos. Se trata de operaciones en las que el valor real de la empresa adquirida reside en el carácter innovador de los productos o servicios ofrecidos, la información o datos que controle así como su presencia en el mercado en términos de número de usuarios de sus servicios. El problema que se plantea en estos casos es que los umbrales actuales de notificación –que activan el procedimiento de control– están estructurados en función del volumen de negocios de las empresas participes en la operación (45), por lo que estas operaciones podrían quedar fuera de los mismos, sin que pudiera entrarse a valorar su

(41) *Vid.* un análisis detallado de distintas operaciones de concentración realizadas en mercados digitales relacionados con los datos, tanto en el marco europeo como estadounidense, en Stucke/Grunes: *Big Data and Competition Policy,* cit., pp. 69 y ss.

(42) Decisión de la Comisión de 11 de marzo de 2008, Asunto M.4731, *Google/DoubleClick*.

(43) Decisión de la Comisión de 3 de octubre de 2010, Asunto M.7217, *Facebook/WhatsApp*.

(44) Decisión de la Comisión de 6 de diciembre de 2016, Asunto M. 8124, *Microsoft/Linkedln*.

(45) *Vid.* artículo 1 del Reglamento (CE) n° 139/2004 del Consejo, de 20 de enero de 2004, *sobre* el *control* de las *concentraciones* entre empresas.

eventual incidencia competitiva. En algunos casos, los umbrales centrados exclusivamente en el volumen de negocios, pueden excluir adquisiciones con un impacto importante para el desarrollo futuro de la competencia en los mercados, en las que una empresa relevante, motivada por las perspectivas de obtener acceso a una variedad de fuentes de datos adicionales, compre un pequeño participante que considere con potencial para generar nuevos datos o con acceso a datos valiosos (46). Se ha planteado como solución a este problema la introducción de un umbral complementario, basado no en el volumen de negocios, sino en el valor de la transacción; respuesta adoptada en Alemania recientemente y que constituye el objeto de una consulta pública lanzada por la Comisión en octubre de 2016 (47).

Otro escollo que plantean las concentraciones–vinculada a la dificultad comentada previamente de delimitar mercados relevantes en este sector– es su categorización como horizontales, verticales o conglomerales y la consiguiente aplicación de los correspondientes criterios sustantivos de valoración. En muchos mercados digitales, una fusión entre una empresa establecida y un recién llegado innovador tiene un impacto insignificante en la estructura del mercado existente debido a las bajas cuotas de éste o incluso a la ausencia de superposición horizontal. Sin embargo, en los mercados relacionados con los datos, una fusión de este tipo podría dar como resultado un aumento del grado de concentración de los datos si la nueva empresa tiene acceso a una base de datos significativa (obtenida, por ejemplo, en otro mercado). Tradicionalmente, las autoridades de competencia han desdeñado los eventuales riesgos que pudieran derivarse de la concentración de datos, sobre la base del análisis clásico de la anticompetitividad de las concentraciones centrado en el efecto presumible de la operación en los niveles de precios o producción en los mercados relevantes. En principio, la posibilidad de que la eventual ventaja en datos que pudiera obtener la nueva entidad se tradujera en la formación o consolidación de una posición de poder económico, estaría en función de dos circunstancias: la escasez de los datos (o dificultad de su irreplicabilidad) y el grado en que la escala o alcance de los datos afectan al resultado competitivo de los mercados. No sólo no se han valorados esas circunstancias en los casos examinados, sino que la actitud de la Comisión en las operaciones señaladas ha sido receptiva a las alegaciones de eficiencias y ventajas económicas a la captación de datos.

(46) Finalidades económicas de esta naturaleza, explican operaciones de concentración como la realizada entre Facebook y WhatsApp (*cit.*), Google y DoubleClick (*cit.*) o Google y Waze, una plataforma mediante la que los usuarios podían identificar distintos aspectos del tráfico a tiempo real, lo que resultaba de enorme utilidad en relación al servicio de mapas ofertado por Google.

(47) *Vid.* http://ec.europa.eu/competition/consultations/2016_merger_control/index_en.html

Ahora bien, como señalamos anteriormente, en las operaciones más recientes relacionadas con mercados de doble cara, se desprende un enfoque más amplio, que no ciñe el examen del potencial anticompetitivo de la concentración únicamente a los efectos en los precios de uno de los mercados, sino que, parece ampliar su espectro, identificando más mercados relevantes e introduciendo otras consideraciones en el análisis como los efectos de la misma en la privacidad de los consumidores (48).

2.3.4 Abuso de posición dominante

La aplicación de las prohibiciones de abuso de posición dominante a conductas vinculadas a políticas de *Big Data* ha planteado también una serie de interrogantes –la mayoría, por el momento, en un plano puramente teórico–. Partiendo de la cuestión ya apuntada de si puede considerarse que el control de una base de datos significativa es susceptible de conferir una posición de dominio en los mercados a la identificación de conductas o actividades relacionadas con la explotación de los datos que puedan considerarse abusivas.

En principio, ni la acumulación de datos ni la capitalización de las economías de escala pueden considerarse en si mismas anticompetitivas. No obstante, las autoridades de competencia no descartan la posibilidad de la explotación de los datos como medio para crear o mantener poder de mercado mediante conductas orientadas a limitar el acceso a terceros de esos datos (49). En este sentido, se han dibujado distintos escenarios de conductas excluyentes relacionadas con el control de datos: celebración de contratos de exclusiva con proveedores de datos; conductas de *tying o bundling*; negativa a suministrar datos o, con un cariz más explotativo, la utilización de los datos como instrumento de discriminación de precios (50).

3. UN INCIERTO CAMINO POR RECORRER

El desarrollo de la economía de los datos, el surgimiento continuo y progresivo de operadores económicos que hacen de la captación y tratamiento de la información su modelo de negocio, exige determinar el papel que al Derecho de la competencia compete desempeñar en cuanto sector

(48) *Supra.*

(49) *Vid.* OCDE: *Big Data: Bringing Competition Policy to the Digital Era*, cit. pp. 20 y ss.; Bundeskartellant/Autorité de la Concurrence: *Competition Law and Data*, cit., pp. 17 y ss.; Autoritat Catalana de la Competencia: *La Economía de los Datos. Retos para la competencia*, cit., pp. 19 y ss.

(50) Al recopilar datos sobre sus clientes, una empresa recibe mejor información sobre sus hábitos de compra y se encuentra en una mejor posición para evaluar su disposición a pagar por un determinado bien o servicio. Siempre que tenga poder de mercado, la empresa podría usar esa información para establecer precios diferentes para los diferentes grupos de consumidores que ha identificado gracias a la información recopilada.

del ordenamiento jurídico encargado de la ordenación de los mercados y garante del adecuado desarrollo del proceso competitivo en los mismos.

La economía del *Big Data* plantea cuestiones novedosas y complejas desde una perspectiva *antitrust*. Las especiales características de la información como producto o como insumo y la existencia de mercados complejos con interrelaciones entre distintos grupos de clientes dificulta la aplicación de los instrumentos tradicionales de análisis. Las autoridades de competencia tienen por delante un escenario de adaptación al rápido cambio de los mercados *online* y se enfrentarán al análisis de casos cada vez más complejos y a la difícil tarea de asentar un camino de actuación claro para todos los operadores involucrados. El posible impacto negativo de las políticas empresariales de *Big Data* no resulta de manera evidente. De hecho, hasta el momento los riesgos identificados son más teóricos o especulativos que reales y la inclusión de consideraciones de privacidad como un parámetro a valorar en la determinación de la incidencia competitiva de una conducta debe ser ponderada con mucha cautela para no introducir distorsiones en el análisis *antitrust* que alteren su coherencia y provoquen situaciones de inseguridad jurídica.

CAPÍTULO 32

FINTECH & INSURTECH: SUPERVISIÓN EN LA ERA DEL *BLOCKCHAIN*

María Gracia Rubio de Casas
RdC Abogados

1. ¿DE QUÉ HABLAMOS CUANDO DECIMOS *FINTECH* E *INSURTECH?*

Llamamos *fintech* al conjunto de innovaciones tecnológicas cuya combinación están produciendo una modificación profunda del sector financiero, entendido como aquella industria que sirve las necesidades de financiación, por una parte, y de inversión del ahorro, por otra: banca, servicios financieros y seguros.

Estas innovaciones tecnológicas comprenden (por citar las que hoy hemos identificado, que podrían, mañana, no ser todas) el *big data,* la inteligencia artificial, la computación en la nube, la criptografía, la extensión del alcance de Internet o la tecnología de registros compartidos *(distributed ledgers technology),* de la que la tecnología de cadena de bloques *(blockchain)* es una aplicación (1). Combinadas, estas innovaciones tecnológicas están dando lugar a una explosión de nuevas aplicaciones que abarcan todo un arco, desde los servicios de pagos hasta el asesoramiento o la gestión de carteras automatizados, el *social trading,* la financiación a las PYMES o la operativa sobre divisas; estas tecnologías también se refuerzan recíprocamente, en el fenómeno conocido como «espiral de la innovación».

El *insurtech* sería una categoría, dentro del *fintech:* la aplicación de las innovaciones tecnológicas a la originación, distribución y administración de productos de seguros: por ejemplo, la utilización por parte de los asegurados de prendas o artefactos, como relojes, que monitorizan continuadamente sus datos de salud (los llamados *wearables)* puede mejorar la precisión con la que la compañía aseguradora calibra el riesgo de una póliza; o la utilización combinada por parte de la compañía de seguros de herramientas de *big data* e inteligencia artificial puede permitirle ofrecer la contratación de pólizas de seguro de forma automatizada, desde un teléfono inteligente *(Smartphone)*. En adelante nos referiremos a ambos, de forma genérica, como *fintech*.

Esta modificación tiene todas las características de lo que se ha llamado «modificación sísmica», por oposición a la modificación por incrementos. Así lo ha expresado José Manuel González-Páramo, Consejero Ejecutivo del BBVA *«… the presence of this radical disruptive force, the digital revolution, has changed everything»* (2). Una modificación por

(1) Natarajan, Harish; Krause, Solvej Karla; Gradstein, Helen Luskin. *Distributed Ledger Technology (DLT) and blockchain (English)*. FinTech note; no. 1. Washington, D. C., World Bank Group 2017. Accesible en: http://documents.worldbank.org/curated/en/177911513714062215/Distributed-Ledger-Technology-DLT-and-blockchain

(2) González Páramo, José Manuel, «Financial innovation in the digital age: challenges for regulation and supervision», *Revista de Estabilidad Financiera*, Banco de España, n.º 32, 05/2017. Accesible en:

https://www.bde.es/f/webbde/GAP/Secciones/Publicaciones/InformesBoletinesRevistas/RevistaEstabilidadFinanciera/17/MAYO%202017/REF_Mayo2017.pdf

incrementos es la de la página web de una pasarela de pagos que permite añadirle nuevas funcionalidades y mejorar la experiencia del usuario; una modificación sísmica es la que crea, y satisface, una necesidad que el consumidor no sabía que tenía: hasta hace tan pocos años que muchos de nosotros aún lo recordamos, no sabíamos la falta que nos hacían los teléfonos inteligentes sin los que ahora no podríamos vivir; o, en el ámbito financiero, el cajero automático (3). En términos más formales, la innovación sísmica se ha definido como aquella en que (4):

(i) consiste en una innovación, o un conjunto de innovaciones estrechamente ligadas entre sí, que se está aplicando por primera vez, o de una forma inesperada, a un nivel tal –en términos de volumen, de alcance o de magnitud– que desborda toda la experiencia anterior, de forma que el regulador carece de un precedente comparable que pueda extrapolar para entender esta innovación;

(ii) el ritmo de aplicación o de adopción de la innovación es tan rápido que no permite al regulador allegar datos actualizados suficientes para determinar cómo reaccionar y

(iii) esa innovación tiene el potencial de alterar de forma significativa el ámbito sobre el que la regulación opera.

En fin, cualquier reflexión sobre las implicaciones del *fintech* tiene que pasar por una constatación anodina de puro evidente: ni la industria financiera, ni la tecnología, reconocen la existencia de fronteras, y todos los acercamientos que se han hecho al *fintech* pasan, necesariamente, por la necesidad de una aproximación global.

En la fecha en que esto se escribe, el ejemplo más claro sea quizás la reacción mixta de perplejidad y atención que han suscitado, en los reguladores globales, la emisión de activos representados en forma criptográfica, los llamados criptoactivos, que pueden o no presentarse como monedas –criptomonedas o *criptocurrencies*– o como unidades que dan a su dueño acceso a determinados derechos (los llamados *tokens),* emitidos mediante oferta pública (los llamados *initial coin offering (ICO)* (5). La conclusión del Comunicado del G20 tras su última reunión los días 19-20 de marzo de 2018 es que no es posible más que una posición coordinada para la supervisión de este fenómeno: «Reconocemos que las innovacio-

(3) Shepherd-Barron, James: *Meet the true star of financial innovation – the humble ATM* https://www.ft.com/content/052f9310-5738-11e7-80b6-9bfa4c1f83d2.

(4) Ford, Christie: *Innovation, regulation and justice*, Cambridge University Press, 2017, pp. 167.

(5) Zetsche, Dirk; Buckley, Ross P.; Arner, Douglas A.; Föhr, Linus «The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators (February 15, 2018). University of Luxembourg Law Working Paper No. 11/2017; UNSW Law Research Paper No. 83; University of Hong Kong Faculty of Law Research Paper N.º 2017/035; European Banking Institute Working Paper Series 18/2018. Disponible en SSRN: https://ssrn.com/abstract=3072298 or http://dx.doi.org/10.2139/ssrn.3072298.

nes tecnológicas, incluyendo aquellas subyacentes a los criptoactivos, tienen el potencial de mejorar la eficiencia y hacer más inclusivo el sistema financiero y a la economía en su conjunto. Los cripto-activos, sin embargo, plantean cuestiones relacionadas con la protección de los consumidores e inversores, la integridad de los mercados, la evasión impositiva, el lavado de dinero, y el financiamiento al terrorismo. Los cripto-activos carecen de los principales atributos que tienen las monedas soberanas. En algún momento pueden tener implicancias para la estabilidad financiera. Nos comprometemos a implementar los estándares del GAFI en materia de criptoactivos, esperamos la revisión de estos estándares por parte del GAFI, y reclamamos su implementación global. Pedimos a los organismos que establecen estándares internacionales que continúen el monitoreo de los cripto-activos y sus riesgos, de acuerdo a sus mandatos, y evalúen las acciones multilaterales necesarias» (6).

2. EUROPA FRENTE AL *FINTECH:* EL PLAN DE ACCIÓN DE LA COMISIÓN EUROPEA EN MATERIA DE TECNOLOGÍA FINANCIERA

El día 8 de marzo pasado, la Comisión Europea presentó su *Plan de Acción en materia de tecnología financiera* (7) *(Plan de Acción,* en lo sucesivo) que incluye 19 medidas dirigidas a facilitar el crecimiento de modelos de negocio innovadores, apoyar la adopción de nuevas tecnologías, y aumentar la ciberseguridad y la integridad del sistema financiero. Por ahora, la medida más tangible de las propuestas por la Comisión es un proyecto de Regulación europea de las plataformas de financiación participativa *(crowdfunding),* que acaba de iniciar su tortuoso procedimiento de discusión.

El Plan de Acción sitúa al *fintech* («tecnofinanzas», en la traducción castellana del Plan) «a caballo entre los servicios financieros y el mercado único digital», y establece el objetivo de que «… los marcos reglamentario y de supervisión de Europa [permitan] a las empresas que operan en el mercado único de la UE sacar partido a la innovación financiera y ofrecer a sus clientes los productos más apropiados y accesibles» y a la vez «garantizar un alto nivel de protección para los consumidores e inversores y garantizar la resiliencia y la integridad del sistema financiero». La Comisión, ha aprobado este Plan de Acción después de un procedimiento de consulta pública, en el que han intervenido una multitud de actores, privados y pú-

(6) https://back-g20.argentina.gob.ar/sites/default/files/media/comunicado_espanol_vf.pdf

(7) Comisión Europea, *Comunicación de la Comisión al Parlamento europeo, al Consejo, al Banco Central europeo, al Comité Económico y Social europeo y al Comité europeo de las regiones: Plan de acción en materia de tecnología financiera: por un sector financiero europeo más competitivo e innovador*. Bruselas 08/03/2018 COM (2018) 109 final.

blicos, iniciado con un documento de Consulta (8) en el que establecía como principios rectores de la regulación y la supervisión los siguientes:

— la neutralidad tecnológica, para asegurar que una misma actividad queda sujeta a una misma regulación, con independencia del modo en que el Servicio se preste, para fomentar la innovación y preservar la igualdad en el campo de juego;

— la proporcionalidad, para tener en cuenta el modelo de negocio, su tamaño y su importancia sistémica, así como la complejidad y la actividad transfronteriza de las entidades reguladas;

— la necesidad de promover la integridad de Mercado, puesto que la aplicación de tecnologías en la prestación de servicios financieros debería promover una mayor transparencia del mercado, beneficiando a los consumidores y empresas, sin crear riesgos injustificados (por ejemplo, de abuso de mercado, malas praxis de venta, riegos de ciberseguridad o riesgo sistémico).

En el Plan de Acción, la Comisión concluye que «… actualmente, existen pocos argumentos en favor de una actuación o reforma amplia de tipo legislativo o normativo a nivel de la UE». Pero sí plantea modificaciones en el marco de la supervisión.

2.1 **El cambio propuesto en el modelo de supervisión: el supervisor como «facilitador de innovación»**

A los efectos de este trabajo, lo que resulta más interesante del Plan de Acción, por lo novedoso del modelo propuesto, es la propuesta de la Comisión de que las distintas autoridades nacionales de supervisión consideren la posible implantación de «facilitadores de innovación» *(Fintech facilitators),* por cuanto esta aproximación a la supervisión parece replantear algunos de los principios sobre los que la supervisión se ha venido articulando. La función de estos facilitadores sería doble: una primera función consistiría en ofrecer orientación general a las empresas, durante su proceso de obtención de una autorización administrativa que les permita prestar servicios en todo el mercado interior (9). Los negocios de

(8) European Commission, Directorate General Financial Stability, Financial Services and Capital Markets Union «Consultation Document: Fintech: A More Competitive and Innovative European Financial Sector», 23 de marzo de 2017, accesible en https://ec.europa.eu/info/sites/info/files/2017-fintech-consultation-document_en_0.pdf

(9) Toda la regulación financiera sectorial establece la regla de que, una vez que una entidad ha sido autorizada por su autoridad nacional competente, esta autorización válida para toda la Unión Europea y permitirá a una empresa de servicios de inversión prestar los servicios o realizar las actividades para las que haya sido autorizada en toda la Unión Europea, ya sea al amparo del derecho de establecimiento, inclusive de una sucursal, o de la libre prestación de servicios: es el llamado «pasaporte europeo». Artículo 6 Directiva 2014/65/UE, del Parlamento Europeo y del Consejo, de 15 de mayo de 2014 (para empresas de servicios de inversión); artículo 33 Directiva 2013/36/UE, del

nueva creación y aquellos que emplean tecnologías o modelos innovadores que se apartan de las prácticas estándar para las que la regulación fue concebida tendrán una acogida difícil en el procedimiento de autorización ordinario: pensemos, por ejemplo, en el caso de una empresa de servicios de inversión que presta servicios de gestión automatizada de carteras, de un agregador de información sobre cuentas bancarias que quiere además ofrecer el servicio de asesoramiento financiero, o de una PYME que quiere financiar su actividad mediante una oferta pública de venta de *tokens*, En ninguno de estos casos, existe norma que prohíba llevar a cabo la actividad propuesta. Pero tampoco existe una norma que regule con precisión los requisitos que debe cumplir quién pretenda llevarla a cabo. Si la opción de política legislativa es favorecer la innovación, como pretende la Comisión Europea, será indispensable que quienes pretenden llevar a cabo esos servicios innovadores puedan recibir, del supervisor-facilitador, orientación continuada.

La segunda función de los facilitadores sería permitir a los supervisores entender mejor las últimas tecnologías y conocer a quienes operan en esa industria. Uno de los reproches habituales a los supervisores financieros es que corren el riesgo de ser *capturados* por las entidades supervisadas (10): permitir a los supervisores desarrollar relaciones continuadas con los disruptores que proponen fórmulas innovadoras puede ser una forma eficaz de evitar o paliar los efectos de esa aludida captura.

La Comisión Europea señala que acogería favorablemente la continuación de los estudios que han llevado ya a cabo las Autoridades Supervisoras Europeas (Agencia Bancaria Europea-*EBA* (11), Autoridad Europea de Valores Mobiliarios -*ESMA* (12) y Autoridad Europea de Supervisión de las Pensiones y Seguros de Jubilación -*EIOPA* (13)) sobre facilitadores de innovación, para determinar cuáles son las mejores prácticas a escala

---

Parlamento Europeo y del Consejo, de 26 de junio de 2013 (para entidades de crédito); artículo 15 Directiva 2009/138/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (para empresas de seguro).

(10) Poulain, Mathilde «Regulatory Capture in Financial Supervision», en Ed. Raphaël Douady, Clément Goulet, Pierre-Charles Pradier, *Financial Regulation in the EU: From Resilience to Growth*, Springer 2017.

(11) Establecida por el Reglamento (UE) n.º 1093/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010. La función principal de la EBA está definida como «… *contribute to the creation of the European Single Rulebook in banking whose objective is to provide a single set of harmonised prudential rules for financial institutions throughout the EU. The Authority also plays an important role in promoting convergence of supervisory practices and is mandated to assess risks and vulnerabilities in the EU banking sector*». http://www.eba.europa.eu/about-us

(12) Establecida por el Reglamento (UE) No 1095/2010 del Parlamento Europeo y del Consejo, de 24 de noviembre de 2010. La función principal de la ESMA está definida como *«… contribute to safeguarding the stability of the European Union's financial system by enhancing the protection of investors and promoting stable and orderly financial markets»*. https://www.esma.europa.eu/about-esma/who-we-are

(13) Establecida por el Reglamento (UE) n.º1094/2010 del Parlamento Europeo y del Consejo de 24 de noviembre de 2010. La responsabilidad fundamental de EIOPA se define como *«… to support the stability of the financial system, transparency of markets and financial products as*

de la UE y fijar principios y criterios comunes para los polos de innovación y los entornos de prueba normativos... «otras medidas de seguimiento podrían incluir la creación de polos de innovación en todos los Estados miembros y la coordinación de sus actividades. Esto podría llevar a que se considerase la posibilidad de un marco de experimentación de la UE para adoptar nuevas tecnologías y adaptarse a ellas». En el Anexo al Plan de Acción (14), la Comisión fija esta meta para el primer trimestre de 2019.

2.2 **Modelos de «facilitador de innovación»: el *«polo de innovación financiera» (innovation hub) y el «entorno de prueba normativo» (sandbox)***

De las tres autoridades de supervisión financiera, la que más ha adelante ha ido en la publicación de su análisis y valoración de los distintos modelos de facilitadores de innovación ha sido la Agencia Bancaria Europea. En su Documento de Trabajo sobre su aproximación a las tecnofinanzas, base de la Consulta que sobre esta cuestión lanzó en 2017 (15), definía al polo de innovación financiera como «… un régimen institucional por el que entidades reguladas y no reguladas [es decir, empresas todavía no autorizadas a prestar el servicio financiero en cuestión] mantienen un diálogo con las autoridades competentes para discutir cuestiones relacionadas con las tecnofinanzas (compartir información, intercambiar opiniones, etc.) e intentar que se aclaren cuestiones como la compatibilidad de sus modelos de negocio con el marco normativo o los requisitos normativos o de concesión de licencias (esto es, orientación individual a las empresas sobre la interpretación de las normas vigentes)» y al entorno de pruebas normativo como «… un espacio en el que experimentar con soluciones tecnofinancieras innovadoras, con el apoyo de una autoridad de supervisión, durante un periodo de tiempo limitado, permitiéndoles validar y probar su modelo de negocio en un entorno seguro».

---

well as the protection of policyholders, pension scheme members and beneficiaries». https://eiopa.europa.eu/about-eiopa/missions-and-tasks

(14) La Comisión invita a las autoridades competentes a nivel de los Estados miembros y de la UE a adoptar iniciativas para facilitar la innovación sobre la base de estas mejores prácticas, e invita a la AES a facilitar la cooperación en materia de supervisión, incluyendo la coordinación y la difusión de información relativa a tecnologías innovadoras, la creación y administración de polos de innovación y entornos de pruebas normativos y la coherencia en las prácticas de supervisión. T1 2019 La Comisión presentará, basándose en el trabajo de las AES, un informe sobre mejores prácticas para entornos de prueba normativos.

http://eur-lex.europa.eu/resource.html?uri=cellar:6793c578-22e6-11e8-ac73-01aa75ed71a1.0019.02/DOC_2&format=PDF

(15) *EBA, Discussion Paper on the EBA's approach to financial technology (FinTech)*, 4 de agosto de 2017

https://www.eba.europa.eu/documents/10180/1919160/EBA+Discussion+Paper+on+Fintech+%28EBA-DP-2017-02%29.pdf/7a1b9cda-10ad-4315-91ce-d798230ebd84

2.2.1 La posición de la EBA

La EBA ha hecho público recientemente su Plan de trabajo *(Roadmap)* sobre Fintech para el 2018/2019 (16), y ha establecido, entre sus prioridades, la de «supervisar el perímetro regulatorio, lo que requerirá evaluar las aproximaciones actuales a la autorización de entidades para las entidades FinTech, analizar los entornos de pruebas y polos de innovación financiera, con el propósito de desarrollar un conjunto de mejores prácticas para fomentar la consistencia y facilitar la coordinación entre supervisores» (17). Ha anunciado igualmente la creación de un *FinTech Innovation Hub,* un lugar de encuentro entre autoridades nacionales de supervisión, incumbentes y nuevos entrantes en la industria financiera u otras firmas *FinTech,* proveedores de tecnología y otras partes relevantes.

De su análisis preliminar, la EBA concluye que los entornos de prueba varían significativamente entre Estados Miembros, por ejemplo, en cuanto a quienes pueden participar en ellos (sólo las entidades ya autorizadas o los nuevos entrantes), el ámbito de los servicios financieros que pueden prestarse (sólo servicios de pago o cualquier otra actividad de las reservadas a las entidades de crédito), las obligaciones regulatorias exigibles o los criterios de salida de este entorno. Se propone por tanto, como parte de su Plan de trabajo, continuar con su análisis para definir las características comunes de estos entornos y las mejores prácticas de entre las llevadas a cabo por los distintos Estados miembros, y para asegurar su compatibilidad con el derecho comunitario. Este análisis abarcará distintos aspectos (18) y concluiría con una Opinión de la EBA, una propuesta, o en su caso, unas Directrices *(Guidelines)* para promover las mejores prácti-

(16) *The EBA's Fintech Roadmap conclusions from the Consultation on the EBA's approach to financial technology (fintech)*, 15 de marzo de 2018.

https://www.eba.europa.eu/documents/10180/1919160/EBA+FinTech+Roadmap.pdf

(17) «… the EBA explains the approach it will take in relation to the policy areas identified in the FinTech Discussion Paper and sets out the following priorities for 2018/2019: … monitoring the regulatory perimeter, including assessing current authorisation and licencing approaches to FinTech firms, analysing regulatory sandboxes and innovation hubs with a view to developing a set of best practices to enhance consistency and facilitate supervisory coordination.

(18) Punto 66 del Plan de Trabajo: «*This work will … extend to an assessment of:*

a. operational aspects of sandboxes (e.g. objectives, scope, entry and exit conditions, regulatory requirements, typical duration of operation and cooperation arrangements among authorities involved in the supervision of firms participating in the sandbox);

b. the use of discretions by Member States and competent authorities in developing and operating sandboxes, including the extent to which use is made of discretions already embedded in EU law;

c. the number and types of firms participating in sandboxes, including the types of financial services provided and financial innovations applied;

d. any legal constraints to establishing sandboxes;

e. any opportunities and risks arising from sandboxes».

cas y mejorar la consistencia supervisora en el manejo de estos entornos de prueba por parte de los distintos supervisores nacionales (19).

2.2.2 La posición de la ESMA

ESMA, por su parte, ha mantenido una posición más bien guardada. En su respuesta (20) a la Consulta de la Comisión Europea sobre *fintech,* antes citada, ESMA manifestó su reticencia a tratar de modo distinto a las *start-ups* de *fintech* por el solo hecho de que sean start-ups y necesiten de mayor flexibilidad para desarrollarse, considerando por el contrario, que el eje de la regulación y supervisión debería ser la actividad que estas entidades llevan a cabo y no la forma de la entidad (personalmente, me llama la atención que ESMA no parezca prestar relevancia alguna a la preponderancia del uso de la tecnología para la prestación del servicio); sí está dispuesta a admitir, sin embargo, que estas start-ups puedan necesitar de mayor acompañamiento del supervisor en la maraña normativa *(«… more advice or help from supervisors to navigate the applicable legal framework»)* para concluir que *«… innovation hubs or other dedicated structures recently created in some national competent authorities and that are aimed at guiding and advising Fintech start-ups are interesting and should be encouraged»*.

Esta cautela se refleja también en un discurso pronunciado recientemente por el Presidente de ESMA, Steven Maijoor, desde su mismo título *(«A Measured Approach to Fintech»)* (21) y cuya conclusión parece ser, en lo que respecta a la transformación de la supervisión, que deben adoptarse las medidas necesarias para asegurar que la UE es el un buen lugar para que las entidades en la avanzada tecnológica pueden innovar y desarrollar sus negocios –cumpliendo con todos las exigencias regulatorias, y que para asegurar la uniformidad de los criterios utilizados por las distintas autoridades nacionales, ESMA recabará información de éstas y establecerá los mecanismos para compartirla, de modo que cada autori-

(19) Es interesante dejar aquí constancia de la distinta aproximación seguida por el Comité de Basilea de Supervisión Bancaria. En su documento de febrero de 2018, *«Sound Practices: Implications of fintech developments for banks and bank supervisors»*, concluye que los *innovation hubs* y *sandboxes* están definidos a la medida del supervisor que los implanta y deberían por tanto evaluarse con cautela, y que es aún demasiado pronto para extraer conclusiones sobre su utilidad, beneficios y riesgos. Accesible en https://www.bis.org/bcbs/publ/d431.pdf

(20) «ESMA response to the Commission Consultation Paper on Fintech: A more competitive and innovative financial sector», 7 de junio 2017, accesible en https://www.esma.europa.eu/sites/default/files/library/esma50-158-457_response_to_the_ec_consultation_on_fintech.pdf

(21) Steven Maijoor, «*Keynote Address: A Measured Approach to Fintech*». Afore Consulting's Second Annual FinTech and Digital Innovation Conference: Regulation at the European Level and Beyond – Stanhope Hotel Brussels, 27 de febrero de 2018. Accesible en https://www.esma.europa.eu/sites/default/files/library/esma71-319-70_second_annual_fintech_and_digital_innovation_conference_-_stanhope_hotel_brussels.pdf

dad pueda establecer el *technological innovation hub* que mejor satisface sus necesidades.

2.2.3 La posición de EIOPA

En su respuesta (22) a la Consulta de la Comisión Europea sobre ***fintech***, antes citada, EIOPA (23) informa de haber comenzado un ejercicio para allegar información sobre las iniciativas innovadoras adoptadas por otras autoridades de supervisión, para fomentar la innovación financiera en sus respectivas jurisdicciones. Los objetivos de este ejercicio serían determinar cuáles son las mejores prácticas, y evitar una competencia desordenada entre supervisores.

Posteriormente (24), EIOPA ha anunciado la creación de un Grupo de trabajo, con el mandato de liderar el trabajo de EIOPA sobre las cuestiones surgidas del *insurtech*. Parte del trabajo de este Grupo se centrará en la continuación del ejercicio de obtención de información descrito más arriba, considerando en particular cómo están aplicando otras autoridades de supervisión el principio de proporcionalidad en el ámbito de la innovación financiera (por ejemplo, las start-ups de InsurTech que ofrecen seguros de particulares a otros particulares *(peer-to peer insurers).* El objetivo sería determinar las prácticas de supervisión más eficaces y efectivas e identificar las posibles barreras regulatorias a la innovación financiera.

3. EE UU FRENTE AL *FINTECH:* LA POLÍTICA DE INNOVACIÓN DEL *CONSUMER FINANCIAL PROTECTION BUREAU* Y EL *WHITE PAPER* DEL *OFFICE OF THE COMPTROLLER OF THE CURRENCY*

En febrero de 2016, el Consumer Financial Protection Bureau (el ***«CFPB»***) (25) publicó su política para «reducir la incertidumbre regulatoria para productos innovadores que prometen beneficios significativos a los consumidores» (la «**Política de Innovación**») (26).

(22) EIOPA «Response to the Commission's public consultation on FinTech: A more competitive and innovative European Financial Sector», 16 de junio de 2017, accesible en https://eiopa.europa.eu/Publications/Letters/EIOPA%20response%20to%20EC%20FinTech%20consultation%20.pdf

(23) EIOPA suscita también una cuestión que por su interés no me resisto a mencionar: la necesidad de dirimir cómo se asignan las responsabilidades cuando interviene la tecnología, como parte de la protección de la integridad del mercado (citando el ejemplo de la conducción automatizada).

(24) EIOPA, Insurtech Task Force, Mandate, 29 de septiembre de 2017. Accesible en https://eiopa.europa.eu/Publications/Administrative/InsuTech%20Task%20Force%20Mandate%20-%20BoS.pdf

(25) El Consumer Financial Protection Bureau es la agencia responsable de la protección de los consumidores financieros.

(26) Consumer Financial Protection Bureau, *«Policy to Reduce Potential Regulatory Uncertainty for Innovative Products that Promise Significant Consumer Benefits»*, 2 de febrero de 2016, accesible en https://files.consumerfinance.gov/f/201602_cfpb_no-action-letter-policy.pdf

Esta Política de Innovación se enmarca dentro de la iniciativa llamada *Project Catalyst,* cuyo propósito es fomentar la innovación favorable para los consumidores dentro del Mercado de productos y servicios financieros (27). El propósito de esta Política es facilitar el cumplimiento normativa en aquellos casos en los que un producto o servicio podría representar una ventaja importante para los consumidores, pero existe incertidumbre acerca de los términos de su inserción en el marco normativo existente.

Para lograr este propósito, el CFPB ha establecido un procedimiento para permitir a los innovadores solicitar una *No-Action Letter* (28) respecto del producto o servicio que están desarrollando. En opinion del CFPB, este mecanismo ofrece una doble ventaja: por una parte, permite a los innovadores obtener un marco seguro de actuación; y por otra parte, desincentiva el ofrecimiento indiscriminado de productos o servicios financieros tecnológicamente innovadores, sin consultar previamente al supervisor, con la alegación de la incertidumbre regulatoria. El CFPB anticipaba que solo excepcionalmente concedería *No-Action Letters,* puesto que habrían de cumplirse al menos dos requisitos: (i) que la concesión de la No-Action Letter fuera necesaria para reducir una incertidumbre regulatoria significativa, y (ii) que la *No-Action Letter* representara la mejor forma de enfrentarse a esa incertidumbre regulatoria significativa, en vez de utilizar otros medios, como una modificación normativa o la publicación de un criterio interpretativo de alcance general. Hasta la fecha, el CFPB sólo ha emitido una *No-Action Letter* (29).

Casi simultáneamente, la *Office of the Comptroller of the Currency (la «**OCC**»*), el supervisor del Sistema bancario federal norteamericano, publicó un documento de consulta (el «***White Paper***») (30) describiendo su aproximación a la innovación responsable en el sector bancario. En él, la OCC explicaba que el fomento de la «innovación responsable» forma parte de su misión, y proponía conceder una licencia bancaria especial, la llamada *fintech charter,* a aquellos prestadores de servicios bancarios que acreditasen «*… the use of new or improved financial products,*

(27) https://www.consumerfinance.gov/about-us/project-catalyst/

(28) Una No-Action Letter es una declaración vinculante de los servicios de la CFPB, en la que, tras describir la solicitud presentada, analizar el supuesto de hecho acerca del que se consulta y el derecho que le sería applicable, los servicios concluyen con una manifestación de que no recomendarían al Consejo del CFPB emprender actuaciones contra el solicitante, por los hechos a los que la consulta se refiere.

(29) El CFPB ha emitido esta No-Action Letter para Upstart Network, Inc., una plataforma de crédito californiana, que valora las solicitudes de crédito de los consumidores atendiendo a los criterios tradicionalmente utilizados (morosidad) pero también criterios innovadores, tales como el nivel educativo o la vida laboral. Accesible en https://www.consumerfinance.gov/about-us/newsroom/cfpb-announces-first-no-action-letter-upstart-network/

(30) Office of the Comptroller of the Currency, «Exploring Special Purpose National Bank Charters for Fintech Companies», 31 de marzo de 2016. Accesible en https://www.occ.treas.gov/topics/responsible-innovation/comments/special-purpose-national-bank-charters-for-fintech.pdf

services, and processes to meet the evolving needs of consumers, businesses, and communities in a manner that is consistent with sound risk management and is aligned with the bank's overall business strategy.» Para valorar si éste era el caso, la OCC proponía utilizar ocho principios: (i) apoyar la innovación responsable, considerando si la regulación existente es suficiente y buscando simplificar y acelerar el procedimiento ordinario para la concesión de autorizaciones, creando una oficina central de innovación en la que los innovadores pudieran presentar sus ideas antes de solicitar una autorización; (ii) fomentar una cultura interna receptiva a la innovación, mejorando la formación de sus equipos donde fuera necesario; (iii) explotar la experiencia y conocimientos de sus servicios, designando líderes expertos que pudieran dirigir y apoyar a los equipos; alentar la innovación responsable que favorezca la inclusión financiera, publicando sus criterios acerca de las condiciones que deberían reunir los productos y servicios dirigidos a la población de rentas más bajas; fomentar la seguridad de la operativa con una mejor gestión de los riesgos, en particular el ciber-riesgo; Alentar a los bancos, de cualquier tamaño, a integrar la innovación responsable en su planificación estratégica; considerando posible colaboraciones con entidades no-bancarias para ofrecer productos o servicios innovadores; promover un diálogo continuado con bancos, innovadores y otras partes interesadas, acogiendo, por ejemplo «ferias del innovador» a las que concurrieran bancos, entidades no bancarias y los equipos de la OCC, para tratar de las exigencias regulatorias y las expectativas del supervisor financiero; y en fin, colaborar con otros reguladores, para asegurar que las entidades supervisadas reciben mensajes coherentes.

Por ahora, la OCC no ha concedido ninguna licencia a entidades *fintech,* porque tanto la *Conference of State Bank Supervisors* como el *Department of Financial Services* de Nueva York interpusieron acciones contra el propósito anunciado por la OCC de conceder esas *fintech charters,* por invadir las competencias de los Estados y la OCC suspendió el pronunciamiento anunciado (31).

4. ¿CÓMO SUPERVISAR AL *FINTECH* EN LA ERA DEL BITCOIN?

Tras la crisis financiera de 2008, como es sabido, se produjo una masiva oleada regulatoria con el propósito de intentar evitar una segunda cri-

(31) La sentencia del District Court Southern District of New York del 12 de diciembre de 2017 rechazó, por prematura, la demanda del *Department of Financial Services* de Nueva York, puesto que la OCC se había limitado a anunciar su intención de conceder las *fintech charters* pero no había concedida aún ninguna.

Accesible en https://www.bloomberglaw.com/public/desktop/document/Vullo_v_Office_of_the_Comptroller_of_the_Currency_et_al_Docket_No/4?1513110990

sis. Desafortunadamente, este tsunami normativo puede ser incapaz de establecer un modelo de supervisión adecuada para el *fintech,* porque está predicado para un modelo de industria financiera modificado, de modo sísmico, por la tecnología. La tecnología lo ha alterado todo y podría estar alterando incluso lo que consideramos dinero.

El desajuste entre la normativa existente y la realidad ***fintech*** se funda en tres razones (32). La primera es que la normativa dictada para prevenir el riesgo sistémico parte de la idea de que éste está ligado sólo a las entidades demasiado grandes como para que puedan fracasar, el famoso «*too big to fail*». La segunda es que los supervisores no disponen de herramientas adecuadas no ya sólo para supervisar, sino incluso para entender la forma en que las entidades *fintech* prestan sus servicios o incluso la naturaleza de éstos. La tercera es que el temor al riesgo reputacional, que sí puede actuar como una herramienta indirecta de supervisión para las entidades ya establecidas, no lo es para las entidades ***fintech***.

Para abordar el riesgo sistémico en un mercado, se suele atender a cuatro factores: (i) hasta qué punto cada uno de los operadores del Mercado es vulnerable a shocks rápidos y adversos (ii) la existencia de circuitos por los que un shock podría extenderse de un operador a otro (iii) el nivel de asimetría informativa en el mercado y (iv) el tamaño del mercado en su conjunto.

Una regulación de prevención del riesgo sistémico centrada en las entidades *too big to fail* no considera la vulnerabilidad individual de las entidades *fintech* frente un shock: estas entidades son característicamente de reducido tamaño, con los recursos estrictamente indispensables para el desarrollo de su actividad, sin diversificación apenas de sus fuentes de ingresos y esto las hace fácilmente vulnerables frente a cambios adversos. En segundo lugar, hay un riesgo común a todas ellas, el ciber riesgo; si las herramientas tecnológicas que muchas de ellas comparten tienen fallos, podrían verse todas afectadas. Se ha mencionado también el riesgo de la automatización de los procesos de decisiones, por ejemplo en la negociación algorítmica o la de gestión de carteras, que puede provocar ventas masivas simultáneas de ciertos activos que provocan una espiral de pérdidas que desencadena más ventas. En tercer lugar, existe un nivel significativo de asimetría informativa respecto de las entidades ***fintech***, principalmente porque no están sujetas a obligaciones de publicación o registro de información. En cuarto lugar, la industria es ahora pequeña, pero parece evidente que seguirá creciendo (33).

---

(32) Magnuson, William J., Regulating Fintech (August 26, 2017). Vanderbilt Law Review, Forthcoming; Texas A&M University School of Law Legal Studies Research Paper No. 17-55. Accesible en SSRN: https://ssrn.com/abstract=3027525

(33) González Páramo, José Manuel, «*… over the past few years we have seen an increase in the number of new players coming from the digital world, the «fintechs». Their objective is*

Tampoco disponen ahora mismo los supervisores de herramientas para comprender y evaluar la actividad de las ***fintech***, en primer lugar por su naturaleza descentralizada, lo que es particularmente cierto en los casos en los que la entidad actúa como un nodo entre particulares: en estos casos, la única fuente cierta de información es este nodo. Una segunda dificultad para recabar información radica en que la entidad *fintech* no necesariamente está establecida en la jurisdicción en la que opera, algo especialmente posible en la era de Internet. A este respecto, es interesante la aproximación seguida por el legislador italiano, que trasponiendo a derecho nacional la Quinta Directiva en materia de Prevención del Blanqueo de Dinero y la financiación del terrorismo, antes de su aprobación definitiva por el Parlamento Europeo (34), ha considerado sujetas a la ley italiana a todas las plataformas que permiten a los residentes italianos almacenar o negociar bitcoins, cualquiera que sea su lugar de establecimiento (35). Pero considerando el número de operadores que pueden intervenir en el mercado, y lo proteico de su actividad, se puede hacer muy difícil para los supervisores llevar a cabo un seguimiento.

Por último, tampoco pueden confiar los supervisores en que el temor al riesgo reputacional tenga un efecto disuasorio de las malas conductas: el temor reputacional opera mejor cuando los operadores están bien identificados y tienen un cierto tamaño, las normas están claras y los operadores pretenden permanecer en el mercado durante un período de tiempo largo.

¿De qué herramientas puede pues valerse el supervisor?

Distintos autores invocan las ventajas del *sandbox* o entorno de pruebas como fórmula que podría permitir limitar los riegos arriba descritos y ofrecer al supervisor una herramienta de aprendizaje útil (36).

---

to concentrate on specific segments of the value chain […] unbundling or disaggregating the services previously originated and sold by the banking sector. These companies start without the burden of having to maintain a physical distribution network, the rigidities of corporate culture, the upkeep of obsolescent technological systems or tough banking regulations. Also, the sector will have to compete not only with providers emerging in the financial sector, but also with those arriving from other areas, in particular, the major digital companies, Google, Apple, Facebook and Amazon… Thus, the real question is not whether banking will change radically, which it undoubtedly will, but rather whether banks will still play a significant role in the new financial ecosystem».

(34) http://www.europarl.europa.eu/legislative-train/theme-area-of-justice-and-fundamental-rights/file-revision-of-the-anti-money-laundering-directive-(aml)

(35) Decreto Legislativo 25 maggio 2017, n. 90, http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2017-06-19&atto.codiceRedazionale=17G00104&elenco30giorni=false

(36) González Páramo, José Manuel *«… The creation of supervised and safe pre-market testing environments, the socalled regulatory sandboxes, emerges as an option that fosters innovation while preserving systemic stability».* Magnuson, William J. *«… regulators should create incentives for fintech firms to provide information about their business and voluntarily seek guidance on the applicability of current regulations. One way to do this would be to create a kind of «regulatory sandbox,» an approach adopted by the United Kingdom. The UK's Financial Conduct Authority has created a regulatory project that allows fintech startups to launch new financial products*

En segundo lugar, y puesto que existen ya barreras de entrada significativas a la prestación de servicios en la industria financiera, podría colocarse el énfasis de la supervisión en el suministro de información por parte de las *fintech* al supervisor. Y aquí es donde la misma tecnología que hace tan compleja la supervisión podría simplificarla: ¿por qué no pensar en un modelo de *«suptech»?* La supervisión está basada sobre la idea de que la entidad produce información y la remite al supervisor, eso sí, por medios telemáticos. La producción de la información es costosa para las entidades, sobre todo teniendo en cuenta, como se ha dicho, que son de reducida tamaño y apuran sus recursos y a sus equipos al máximo. Y por otra parte, son notorios los límites que la información producida por las propias entidades ofrece, como medida de protección de los consumidores. ¿Qué impediría al supervisor acceder por sí a la información (más allá del temor a incurrir en riesgos de responsabilidad si fallase en la apreciación de la importancia de un dato, o su omisión), directamente?

En tercer lugar, la supervisión podría tratar de prevenir o paliar el contagio entre entidades, estableciendo, por una parte, medidas ex ante para prevenir las correlaciones adversas (por ejemplo obligando a los gestores automatizados a incluir en sus algoritmos «interruptores» que evitasen ventas masivas automáticas en caso de situación adversa de mercado, o, en el caso de las ICO, obligando a los emisores a asegurar la solidez de los mecanismos de llevanza de registro) y medidas *ex post* para reducir el impacto sobre el mercado de la incapacidad de una entidad para hacer frente a sus compromisos; en este sentido, y aunque la inexistencia de mecanismos públicos de rescate tiene probablemente por sí sola un efecto salutífero, parece de especial interés la obligación de las entidades, como condición de su autorización, de establecer mecanismos de continuidad (37).

En cuarto lugar, podría considerarse la adopción de códigos de buena conducta, redactados por la propia industria y cuyo cumplimiento fuera supervisado por ésta, como ocurre ya con la industria farmacéutica (38).

---

on an accelerated basis and with minimal regulatory barriers.218 The advantages of such an approach are clear, as it promotes greater transparency in the industry while simultaneously encouraging innovation».

(37) Artículo 55.i) de la ley 5/2015, de 27 de abril.

(38) https://www.codigofarmaindustria.org/servlet/sarfi/codigo/codigo.html

CAPÍTULO 33

LA CONTRATACIÓN PÚBLICA DE SERVICIOS DIGITALES

Luis S. Moll Fernández-Fígares
Letrado de la Comunidad de Madrid (Exc.)
Director de los Servicios Jurídicos de la Agencia para la Administración Digital de la Comunidad de Madrid
Doctor en Derecho

Luis Gamo Sanz
Jefe del Área de Coordinación Jurídica de la Agencia para la Administración Digital de la Comunidad de Madrid
Abogado

INTRODUCCIÓN

No tenemos por objetivo, en las páginas que siguen, realizar una explicación de los principios y procedimientos de la contratación pública o tratar la contratación electrónica, ni siquiera con la excusa de la reciente Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

Tampoco hemos de centrarnos en hacer acopio de las herramientas informáticas de que se proveen nuestras Administraciones Públicas para llevar a cabo el efectivo cumplimiento de sus funciones o, en muchos casos sencillamente, para cumplir la Ley (1). Esto parece más propio de un planteamiento técnico que jurídico. Por lo mismo la exposición debe realizarse en palabras necesariamente sencillas y simplificadoras, renunciando a la precisión y terminología técnica.

Trataremos de poner encima de la mesa algunas circunstancias y vicisitudes por las que pasa la contratación pública de las tecnologías de la información y la comunicación, a la vista de las disposiciones normativas y las necesidades de la gestión pública. Sirva al menos para reunir situaciones y problemas, como objeto de reflexión.

1. EL PRINCIPIO DE NEUTRALIDAD TECNOLÓGICA

La neutralidad tecnológica (2) consiste, muy sencillamente, en afirmar que la tecnología adquirida o desarrollada por las Administraciones Públicas, no puede ser discriminatoria, afectar a la independencia de una sociedad abierta, a su soberanía, a la libre competencia, disminuir derechos o influir negativamente en la libertad. Asimismo, debe garantizar que el Estado no incurra en situaciones de «cautividad», respecto de empresas privadas.

En nuestro ordenamiento Jurídico el principio de neutralidad tecnológica está legalmente reconocido en un amplio número de normas (3)

(1) Sabido es por todos que una de las novedades sobre las que más se ha llamado la atención, a raíz de la aprobación de las leyes 39 y 40/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de Régimen Jurídico del Sector Público, es la profundización en lo que se ha denominado «administración electrónica», siguiendo la estela de la derogada Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

(2) Véase sobre el tema la resolución de la Comisión del Mercado de las telecomunicaciones de 29 de abril de 2013 o la STS de 18 de noviembre de 2009 (recurso contencioso administrativo núm. 54/2006).

(3) Y se concibe como principio que debe inspirar la actividad normativa. *Vid. Verbi gratia:* Resolución de 15 de marzo de 2017, aprobada por la Comisión Mixta para las Relaciones con el Tribunal de Cuentas, en relación con el Informe de fiscalización de la contratación celebrada durante los ejercicios 2006 a 2009 por la Gerencia de Informática de la Seguridad Social. Publicada en el

pero, en el tema que nos ocupa, debemos hacer referencia a la citada Ley 9/2017 (4). Señala el artículo 126 (apartados 1 y 6), que: «1. Las prescripciones técnicas a que se refieren los artículos 123 y 124, proporcionarán a los empresarios acceso en condiciones de igualdad al procedimiento de contratación y no tendrán por efecto la creación de obstáculos injustificados a la apertura de la contratación pública a la competencia. (…) 6. Salvo que lo justifique el objeto del contrato, las prescripciones técnicas no harán referencia a una fabricación o una procedencia determinada, o a un procedimiento concreto que caracterice a los productos o servicios ofrecidos por un empresario determinado, o a marcas, patentes o tipos, o a un origen o a una producción determinados, con la finalidad de favorecer o descartar ciertas empresas o ciertos productos. Tal referencia se autorizará, con carácter excepcional, en el caso en que no sea posible hacer una descripción lo bastante precisa e inteligible del objeto del contrato en aplicación del apartado 5, en cuyo caso irá acompañada de la mención «o equivalente». Este principio debe conectarse, por supuesto, con el resto de los que inspiran la contratación pública, señalados en el artículo 1 de la LCSP.

Por lo demás, sobre el principio de neutralidad tecnológica, el Tribunal Administrativo Central de Recursos Contractuales, en su Resolución 682/2016 ha tenido ocasión de pronunciarse, señalando que: «El principio de neutralidad tecnológica se concibe como un principio que debe inspirar la actividad reguladora y que supone que la regulación tecnológica debe prestar atención a los efectos de las acciones y no a las acciones y a los medios por ellos mismos. Así concebido, y como se señala en la tan mencionada resolución de la Comisión del Mercado de las telecomunicaciones de 29 de abril de 2013 «Su objetivo consiste en evitar que, a través de la imposición de una determinada tecnología, se pueda influir en las condiciones de libre competencia en que debe desarrollarse el sector de las comunicaciones electrónicas. La aplicación concreta de este principio en el marco de la contratación administrativa se traduce en que los pliegos de cláusulas administrativas aseguren a los operadores económicos el libre acceso a la prestación del servicio, de tal modo que la Administración, al elaborar los mismos, debe evitar imponer con-

«BOE» de 4 de mayo de 2017, en la que se insta al gobierno a desarrollar un marco legal para evitar la denominada cautividad tecnológica en los contratos del sector público.

(4) Que, por otra parte, incorpora a nuestro ordenamiento jurídico la previsiones contenidas en la cuarta generación de directivas en materia de contratación pública *[Directiva 2014/23, del parlamento Europeo y del Consejo, de 26 de febrero, relativa a la adjudicación de contratos de concesión (en adelante Directiva 2014/23/UE), la Directiva 2014/24/UE, del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública (en adelante Directiva 2014/24/UE], y la 2014/25/UE del Parlamento europeo y del Consejo, de 26 de febrero de 2014, relativa a la contratación por entidades que operan en los sectores del agua, la energía, los transportes y los servicios postales (en adelante Directiva 2014/25/UE).*

diciones restrictivas, como puede ser el uso de determinadas tecnologías, que dificulten al libre acceso e imposibiliten la efectividad del principio mencionado. La normativa postula, de este modo, la conveniencia de ofrecer a los operadores, prestadores de servicios, adjudicatarios en concursos públicos, etc., la posibilidad de ofrecer los servicios a través de las tecnologías o infraestructuras que consideren más convenientes, sin limitaciones en la introducción y desarrollo de una tecnología concreta (…) En definitiva, puede de nuevo concluirse que el principio de neutralidad tecnológica es parte esencial del ordenamiento regulador del sector de las comunicaciones electrónicas, sin perjuicio de que las Administraciones públicas en el marco de su actuación puedan en caso de que esté justificado de manera 22/24 objetiva hacer uso de la necesaria flexibilidad que reconoce la normativa sectorial a la hora de aplicar el citado principio.»

Sentado lo anterior, debe notarse que la realidad, es que las AAPP, en algunos ámbitos del sector, se encuentran, en mayor o menor medida, en un estado de cautividad y, en ocasiones, ante situaciones de monopolio *de facto* frente tecnologías propietarias. Veamos.

Por su singular relevancia podemos tomar, a modo de ejemplo, el caso de uno de los grandes, *Microsoft Corporation,* partiendo de los datos extraídos de la Secretaría Estado de Administraciones Públicas, concretamente contenidos en los informes Reina (5).

Fijémonos, en el 2005, el 92 % del parque de ordenadores personales instalados, en ese año, correspondió al entorno Windows, con un 59 % perteneciente a *Windows XP,* un 29 % a *Windows 2000* y un 4 % a *Windows NT*. Posteriormente, el Informe Reina del año 2007 revela que las tecnologías distintas de Microsoft bajaban, así los equipos *Linux* bajan al 16 %, mientras que Unix alcanza una cuota inferior al 6 %.

Pues bien, a continuación, *Microsoft* emprendió una de sus mayores operaciones comerciales: el lanzamiento de un nuevo sistema operativo bajo la denominación de *Vista*, al tiempo que anunciaba el abandono de otros sistemas operativos que había estado comercializando hasta entonces.

Para las Administraciones Públicas, consumidoras masivas de esa tecnología, se planteó un problema de obsolescencia sobrevenida: ¿El nuevo sistema operativo *Vista* ofertado por Microsoft suponía la obligación, para la Administración Pública de renovar su parque informático con esta tecnología? ¿Debía migrar la Administración, masivamente, a la nueva tecnología que le ofrecía *Microsoft?*

(5) Elaborados desde 1988, con una periodicidad anual, presentan un análisis cuantitativo del sector de Tecnologías de la Información y las Comunicaciones en la Administración del Estado, recogiendo los agregados económicos e indicadores más significativos del mismo, junto con las características más representativas del parque de recursos informáticos y efectuando, al mismo tiempo, un contraste con los relativos a otros sectores públicos y privados.

En fin, tras la evolución del sistema operativo, el último informe Reina, señala que el 87 % de los ordenadores personales instalados en 2016 tenían *Windows*, repartidos entre *Windows 7* y *Windows 10*.

Esta situación y otras de cautividad tecnológica han sido criticadas por la doctrina (6).

¿Cómo se ha llegado a este cuasi monopolio? ¿Cómo debe afrontar la Administración la adquisición masiva de productos tecnológicos, sin frustrar el principios básicos reconocidos en el ordenamiento, como el de concurrencia y, al mismo tiempo, garantizar «… la conexión con el objetivo de estabilidad presupuestaria y control del gasto, y el principio de integridad, una eficiente utilización de los fondos destinados a la realización de obras, la adquisición de bienes y la contratación de servicios» que describe el artículo 1 de la LCSP?

¿Están las Administraciones en situación de homologar productos comerciales tecnológicos sin frustrar el Derecho de la Competencia? Teniendo en cuenta la configuración territorial y competencial de nuestro Estado, ¿Cómo debe afrontarse el principio de interoperabilidad, enten-

(6) Señala Acero Martín: «Es evidente, que si usamos un programa que solamente es válido para determinada plataforma tecnológica X (Windows, Linux, FreeBSD, Solaris, etc.) y en él basamos un elevado porcentaje de nuestro modelo de negocio, o de nuestra gestión. Dicha elección nos impedirá, o como poco, nos dificultará, por problemas técnicos, o incluso, por consideraciones económicas muy propias de economías de escala (frecuentes en las Administraciones), cambiar a otra plataforma, o adoptar una determinada mejora tecnológica con la necesaria y obligatoria libertad y neutralidad tecnológica que contempla la Ley. Lo mismo ocurre, si elegimos un hardware que solamente dispone de controladores para una determinada plataforma tecnológica. Por ejemplo, si dicho hardware solamente funciona con el sistema operativo X. Si queremos cambiar al sistema operativo Y en algún momento, tendremos serios problemas y en el peor de los casos, incluso nos podría implicar la necesidad de adquirir nuevo hardware compatible con la plataforma tecnológica. En fin hemos de tener en cuenta, que no siempre lograremos esa obligatoria libertad de elegir. El simple hecho de que se finalice el soporte de una aplicación, se produzca un diseño fallido de una plataforma tecnológica, una mala aceptación del mercado, o la simple quiebra económica de una determinada empresa, puede llevarnos a una situación complicada, en la que el «legacy» sea un problema casi irresoluble». El autor propone posibles soluciones: «Ya hemos visto que para garantizar las libertades de los ciudadanos es necesario usar estándares abiertos y de forma complementaria, aquellos que son de uso generalizado por los ciudadanos, con eso nos basta, pero que para lograr aplicar el principio de Neutralidad Tecnológica puertas adentro y a lo largo del tiempo, necesitamos algo más, quizás, mucho más. Mi propuesta sería añadir en el Esquema Nacional de Interoperabilidad (ENI) las directrices necesarias para minimizar el impacto del «legacy» y entre ellas, se podrían considerar las siguientes: a) Usar estándares abiertos en todas las aplicaciones de la Administración y de forma complementaria estándares de uso generalizado con los ciudadanos, sola y exclusivamente para relacionarse con los ciudadanos. b) Asegurarse de que el hardware que se adquiere pueda funcionar con varias plataformas tecnológicas o sistemas operativos. c) Asegurarse de que las aplicaciones de la Administración puedan funcionar en varias plataformas distintas. d) Asegurarse de que las herramientas de desarrollo utilizadas para la creación de aplicaciones, disponen de versiones para varias plataformas y que puedan generar código para dichas plataformas. e) Aplicar con exquisito cuidado los principios de eficacia y eficiencia a la hora de elegir las tecnologías, así como la normativa de contratación pública, garantizando tal como obliga la Ley, la pluralidad tecnológica y la libre competencia en un libre mercado. f) Asegurarse en la medida de las posibilidades, que un determinado bien o servicio se puede obtener de empresas distintas y con distintas plataformas, fomentando desde la Administración tecnologías, servicios y empresas, que lo hagan posible en un mercado de libre competencia». Acero Martín, F., «El principio de neutralidad tecnológica de la Ley 11/2007, un problema de legacy». http://fernando-acero.livejournal.com/54049.html.

diendo éste, como la capacidad que tiene un producto o un sistema, cuyas interfaces son totalmente conocidas, para funcionar con otros productos o sistemas existentes o futuros y eso sin restricción de acceso o de implementación.? ¿Y a nivel europeo?

2. LAS SITUACIONES DE EXCLUSIVIDAD

A continuación, debemos hacer una reflexión sobre el uso excesivo, por parte de las Administraciones Públicas, del procedimiento negociado por exclusividad regulado, hoy día, en apartado a) segundo del artículo 168 de la LCSP.

El recurso a este procedimiento, basándose en la existencia de un proveedor único o en situaciones de entregas complementarias de otras contrataciones anteriores, pone de manifiesto la existencia de ciertas relaciones de dependencia y cautividad generadas por la celebración, con carácter previo, de determinados contratos.

Así, una decisión inicial, sobre la adquisición de una determinada aplicación informática o de un determinado equipo, puede dar inicio a una situación de auténtica dependencia tecnológica respecto de un determinado proveedor, que condiciona, absolutamente, contrataciones futuras, para ampliaciones o actualizaciones del suministro inicial, o su mantenimiento, normalmente con crecientes importes y durante períodos de tiempo que exceden, con mucho, el plazo máximo de tres años previsto, en la normativa contractual, para las contrataciones complementarias. Todo ello sin que la importancia global y futura del proyecto hubiese sido advertida, con la publicidad y concurrencia correspondientes a los procedimientos abiertos, en la primera de las contrataciones efectuadas.

Debe recordarse que constituye una regla esencial del Derecho comunitario europeo, y también del Derecho interno español, por trasposición de aquel, que la aplicación del procedimiento negociado, sin publicación de un anuncio de licitación, supone una excepción a los principios generales de transparencia, publicidad, libre concurrencia y no discriminación e igualdad de trato, entre los posibles licitadores.

Por ello, su interpretación debe ser restrictiva, y su ámbito de aplicación no puede extenderse sino a los casos estrictamente comprendidos en las normas por las que se regulan (7).

(7) Señala el Considerando 50 de la Directiva 2014/24/EU del Parlamento Europeo y del Consejo, sobre contratación administrativa: «En razón de sus efectos perjudiciales sobre la competencia, los procedimientos negociados sin publicación previa de un anuncio de licitación deben utilizarse únicamente en circunstancias muy excepcionales».

Apuntemos además, respecto de esta situación, un caso *sui géneris* pero que ocurre en la práctica, y es que las situaciones de exclusividad, en ocasiones, se generan de hecho.

Imaginemos: la Administración adquiere un determinado *software* que necesita un soporte o mantenimiento. Ese mantenimiento o soporte únicamente lo puede prestar, por razones de exclusividad técnica, una empresa que, a su vez, lo cede, en exclusiva, a otra, que es quien tiene contratada la Administración, a través del procedimiento mencionado. A continuación, la empresa fabricante y dueña de la licencia descontinúa su actividad por disolución de la empresa, extinguiéndose la exclusividad cedida para el mantenimiento de su herramienta tecnológica, a la otra compañía. Ahora bien, la Administración, que es propietaria de la licencia, opta por continuar con ella, ya sea porque le satisface, por motivos económicos o de oportunidad, pero necesita contratar el mantenimiento. La empresa que lo prestaba, continúa en condiciones de seguir prestándole el servicio de mantenimiento, al menos por un tiempo, dados los conocimientos técnicos que posee, y que sólo ella posee, pues ha sido la única cesionaria de dicho mantenimiento, en exclusiva, antes de la extinción de la empresa fabricante.

Observamos que se crea, aquí, una suerte de exclusividad *de facto* (no jurídica pues esta empresa mantenedora ya no tiene vínculos jurídicos de exclusividad con la fabricante, que se ha extinguido), que tiene como alternativa volver a realizar una inversión, que puede ser importante, para adquirir una nueva herramienta en el mercado y su mantenimiento correspondiente.

El hecho se puede ver agravado pues, es probable que la empresa fabricante, en nuestro ejemplo, no avise, incluso porque no lo sospeche, que se va a producir su extinción, lo que puede dejar al ente público sin capacidad de reacción a la hora de plantearse una nueva solución y tramitar un nuevo procedimiento de licitación, a veces, para prestar servicios que son de singular interés público.

Visto lo anterior ¿Cómo deben abordar las Administraciones Públicas, estas complejas situaciones?

La respuesta no es fácil. No existe una única solución para cada una de las innumerables situaciones que deben afrontar las Administraciones, en la adquisición de bienes y servicios en materia de tecnología y de comunicaciones, pero si debe obligarnos a reflexionar sobre cómo, para evitar estas situaciones de «cautividad tecnológica» o, en todo caso, paliarlas en la medida de lo posible, mediante la utilización de mecanismos que potencien la concurrencia y la transparencia de las licitaciones.

Al menos, los contratos iniciales, que condicionan contrataciones posteriores, sin posibilidad de ulterior concurrencia, deben realizarse me-

diante procedimientos abiertos, en los que la Administración determine, claramente, la necesidad a satisfacer y sea luego el mercado, con la máxima publicidad y concurrencia, el que determine la solución tecnológica más adecuada.

3. DIFICULTADES EN EL EJERCICIO DE LAS COMPETENCIAS DE CONTRATACIÓN

3.1 **Conflictos en el ejercicio de competencias**

Esta circunstancia no es exclusiva del sector de las tecnologías, pero si se da, quizá con una cierta intensidad, como consecuencia de que las necesidades electrónicas han ido penetrando en la Administración, de forma planificada pero, también, por la fuerza de los hechos, en los últimos años y cada vez con más rapidez.

Debemos partir de que, con arreglo al artículo 28 de la LCSP: «Necesidad e idoneidad del contrato y eficiencia en la contratación: 1. Las entidades del sector público no podrán celebrar otros contratos que aquellos que sean necesarios para el cumplimiento y realización de sus fines institucionales.(…) 4. Las entidades del sector público programarán la actividad de contratación pública, que desarrollarán en un ejercicio presupuestario o períodos plurianuales y darán a conocer su plan de contratación anticipadamente (…)».

Sentado lo anterior, podemos referirnos a diversas cuestiones.

En primer lugar, en materia de atribución de competencias para contratación de TICs, las decisiones de oportunidad en las distintas Administraciones han sido diferentes. Hay quien ha optado por que cada centro directivo contratara su propia «informática» para atender a sus necesidades, como si ponemos por caso que cada Ministerio, Consejería u organismo licite sus contratos informáticos.

En otras ocasiones se ha optado por centralizar esta actividad, de forma que se crean entidades o se atribuyen competencias a una determinada Dirección General, que contrata las soluciones tecnológicas para toda la administración territorial.

También hay soluciones mixtas, que pasan por que, centralizadamente se contraten servicios informáticos, que pueden calificarse de «transversales» e, individualmente, los propios de una rama de actividad administrativa.

Sea de una forma o de otra se pueden observar, dentro de la distribución de competencias que se realiza en una Administración, competencias concurrentes en la materia. Así, por ejemplo, en la Comunidad de Madrid, la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas regula, en su artículo 10, la Agencia para la Administración Digital de la

Comunidad de Madrid, a la que atribuye, en general, la prestación de los servicios informáticos y de comunicaciones a la Comunidad de Madrid, a través de medios propios o ajenos, señalando, además, que la entidad ejercerá sus funciones, en el ámbito de la Administración General y sus Organismos Autónomos. Por su parte, la Disposición Adicional primera de esta Ley preceptúa que las funciones de la Agencia no se extienden a las competencias sobre los «sistemas de informática médica, gestión sanitaria y a aquellas relativas a las relaciones del sistema sanitario con los ciudadanos, profesionales sanitarios, oficinas de farmacia, sanidad privada y cualesquiera otras personas físicas o jurídicas distintas de la Administración de la Comunidad de Madrid, sus organismos autónomos, entidades de derecho público y demás entes públicos» (8).

A veces, el objeto contractual es difícil de encuadrar en unas u otras competencias específicas. Por poner un ejemplo, en la adquisición de tarjetas de plástico con chip para almacenar información, dependerá de si, se le asocian prestaciones adicionales como funcionalidades o desarrollos vinculados al objeto principal, para determinar si estamos ante un simple suministro de un producto o nos encontramos con producto vinculado con las tecnologías de la información y la comunicación, y entonces estaríamos ante un suministro cualificado de tecnología.

En otras ocasiones, las dificultades se plantean por la imprecisión de la Ley, como cuando se refiere (como hemos visto) a entidades de derecho público «y demás entes públicos» en vez de, si esa es su voluntad, referirse, con precisión, a entes «del sector público», en el entendimiento que, dentro del concepto genérico de «sanidad pública» se incluyen, por ejemplo, fundaciones privadas (y por tanto no entes públicos), eso sí, de capital, patrimonio o aportaciones públicas.

(8) Y en el apartado siguiente de esta misma Disposición Adicional: «5. No obstante lo anterior, la Agencia de Informática y Comunicaciones de la Comunidad de Madrid desarrollará en todo caso sobre el ámbito expuesto en el párrafo anterior las siguientes competencias: a) Las que le corresponden de ordinario para la implementación de los productos y servicios declarados por el órgano competente como de uso uniforme y exclusivo en toda la Comunidad de Madrid, así como las que le corresponda en su ámbito general respecto a las comunicaciones de voz y datos, puestos de trabajo ofimáticos y las acciones de todo tipo necesarias para el funcionamiento ordinario de los mismos. b) Las que le corresponden para la implantación de los sistemas de información y servicios corporativos o institucionales, de aplicación en toda la Comunidad de Madrid. Están comprendidos en esta categoría, en particular, los sistemas de información para las transacciones económico-financieras, para la gestión de personal, para la contratación de bienes y servicios, los sistemas de información georeferenciados, los sitios web y los portales de Internet e Intranet. c) La emisión de informe sobre los contenidos de los pliegos de condiciones y demás documentos de contratación de los del apartado 4 de esta disposición adicional, en aquellos aspectos relacionados con su ámbito de actuación ordinario, la correspondiente coordinación institucional y la compatibilidad informática. d) Informe técnico de evaluación de ofertas y participación en mesas de contratación de las del apartado 4 de esta disposición adicional que tengan relación con su ámbito de actuación ordinario».

3.2 **Novación subjetiva de los contratos**

En este apartado hemos de referir el hecho de que, no obstante el mencionado artículo 28 de la LCSP, durante la ejecución de un contrato público, pueden ocurrir diversas vicisitudes, como la modificación de competencias de entes de la administración institucional o, incluso extinción de estos, consecuencia del poder de autoorganización de las administraciones públicas, o incluso la existencia de competencias concurrentes entre distintos organismos (a la que nos hemos referido en el apartado inmediato anterior) (9), que aparecen redactadas de manera más o menos amplia. Pero es que, además existen, en el marco de la gestión, incluso convenios administrativos (10) que prevén la licitación de contratos por parte de un ente público (que cuenta con el conocimiento o incluso puede acaparar ciertas líneas, propias o ajenas, de financiación) para que luego se ejecuten por otro ente público, con distinta personalidad jurídica, perteneciente a la misma o diferente Administración.

Se plantea, entonces, el problema de que contratos licitados por una determinada entidad puedan pasar a ser ejecutados, en todo o en parte, por una distinta.

Esta situación a veces aparece solucionada en la propia Ley [que prevé, *verbi gracia,* la extinción del organismo determinando a quien corresponderán sus derechos y obligaciones (11)] o en la norma que dispone la modificación de competencias.

---

(9) Se examinaron, *ut supra*, las competencias que, con carácter general, corresponden a La Agencia para la Administración Digital de la Comunidad de Madrid (artículo 10 de la citada Ley de Medidas 7/2005). Esto no obstante, por ejemplo, el artículo 9 del Decreto 244/2015, de 29 de diciembre, del Consejo de Gobierno, por el que se establece la organización, estructura y régimen de funcionamiento de la Agencia de Vivienda Social de la Comunidad de Madrid, señala que corresponden a la Secretaría General de este organismo autónomo «La planificación y desarrollo de la política de la Agencia en materia de organización informática y sistemas de información, sin perjuicio de las competencias de la Agencia de Informática y Comunicaciones de la Comunidad de Madrid». Por su parte, el artículo 12 del Decreto 127/2017, de 24 de octubre, del Consejo de Gobierno, por el que se establece la estructura orgánica de la Consejería de Educación e Investigación, atribuye Dirección General de Infraestructuras y Servicios de esa Consejería: «f) El desarrollo de las inversiones relacionadas con la mejora de las tecnologías de la información y de la comunicación en los centros docentes en lo relativo a equipamiento informático y redes telemáticas, incluyendo los procedimientos administrativos de contratación y trabajos técnicos para su ejecución». Y, en fin, otras entidades y organismos realizan contratación Tic en el ejercicio de competencias que tienen atribuidas de manera más genérica y que, en todo caso, implican las «necesarias» para el cumplimiento de sus fines.

(10) Así, por ejemplo, el convenio interadministrativo de colaboración entre el Estado, (Ministerio de educación, cultura y deporte) *Red.es*, y algunas Comunidades Autónomas para la extensión del acceso a la banda ancha ultrarrápida de los centros docentes españoles en el que se prevé la cesión a las CC.AA. u organismos de estas, de los contratos que *Red.es* firme (después de la licitación correspondiente) con los proveedores de servicios de telecomunicaciones para dotar de conectividad a los centros docentes.

(11) Artículo Único. 2 de la Ley 4/2011, de 28 de julio, de Extinción de MINTRA (Madrid, Infraestructuras del Transporte).

Cuando no es así cabe pensar en la novación subjetiva del contrato público, pero ojo, en la parte de la Administración que lo licita, no en la del contratista, que es el supuesto previsto en la LCSP (12).

No podemos ahondar más sobre el tema que, por lo demás, ha sido estudiado por la doctrina (13) y alguno de nuestros órganos consultivos (14).

4. EMPLEO DE MEDIOS PROPIOS

En ocasiones, la administración territorial crea, dentro de su sector público, un ente al que dota de competencias para la contratación de las Tics de forma diríamos centralizada. Esto, en contra de lo que significa que cada ministerio o consejería, por poner un ejemplo, se provea de la tecnología que precise, puede suponer una cierta economía de escala y una centralización del conocimiento.

Ahora bien, las competencias de estas entidades no se ejercen, frecuentemente, respecto a la totalidad de entes que integran la Administración o el poder público en sentido amplio, sino que tienen un ámbito definido. Pensemos, por ejemplo, en autoridades reguladores u organismos independientes, respecto de los que el ente en cuestión no puede proveer de informática porque no lo prevén su acto de creación o norma que regula sus competencias.

Se ha pretendido solucionar la falta de medios informáticos de estas otras entidades a las que no se extiende el ámbito de actuación de los primeros acudiendo, bien a los convenios administrativos, bien al empleo de la figura a los medios propios o de la encomienda de gestión.

Respecto de estas situaciones baste decir que la prestación de servicios informáticos constituye uno de los contratos administrativos tipificados en la LCSP.

El empleo de convenios choca con la propia definición de convenio administrativo y con la prohibición taxativa de que estos tengan por objeto prestaciones contractuales, como bien claramente se deduce de los artículos 6 de la LCSP y 47 y ss. de la Ley 40/2015. Lo mismo ocurre con el pretendido empleo de la figura de la encomienda regulada en el artículo 11 de la Ley 40/2015 (15).

---

(12) Artículos 214 y ss.

(13) Puede verse el interesante artículo: Villar Ezcurra, J.L: «la verdadera naturaleza jurídica de los contratos del sector público y su alteración arbitraria», en: *Estudios jurídicos*, febrero, 2017. https://www.arinoyvillar.com/.

(14) Informe 3/2014, de 27 de febrero, de la Junta Consultiva de Contratación Administrativa de la Generalitat de Catalunya. Informe 4/1999, de 30 de abril de 1999, de la Junta Consultiva de Contratación Administrativa de las islas Baleares. Informe del Servicio de contratación y suministros de la Diputación Provincial de Valencia de 3 de diciembre de 2015.

(15) *Vid.* Circular 6/2009, de 14 de julio de 2009, de la Abogacía del Estado: «la encomienda de gestión (…), queda circunscrita siendo este su ámbito propio, a aquellas actividades o actuaciones que por su contenido sean ajenas a la legislación de contratación pública y no guarden relación con ella».

Respecto del encargo, no se suelen cumplir los requisitos de realizar la parte esencial de la actividad para el encargante y las demás limitaciones para ser considerado medio propio que regulan los actuales artículos 32 y 33 de la LCSP (16).

5. FRACCIONAMIENTO DE LOS CONTRATOS

Sabido es que el fraccionamiento de los contratos, con la finalidad de excluir las normas de publicidad, está claramente proscrito en el derecho comunitario y en la normativa interna (17).

Su relación con la contratación de soluciones informáticas pasa por lo siguiente. En ocasiones la Administración adquiere, a través de un contrato menor, una determinada herramienta informática, de la que tiene una necesidad muy limitada. Pensemos en un sistema de gestión que usen determinados empleados públicos. A medida que se amplía la plantilla (nuevas plazas por concurso u oposición...), se realizan nuevas adquisiciones de licencias por contratos menores [que con la legislación anterior, y para aquellos entes que disponían de instrucciones de contratación, a veces no eran tan «menores» (18)] con fundamento en una nueva necesidad, y no en la intención de eludir la publicidad.

Este supuesto, que en muchas ocasiones se debe a falta de previsión por la administración, podría hoy quizás solucionarse a través de acuerdos marco o usando sistemas dinámicos de adquisición (19).

En otros casos el fraccionamiento se produce como consecuencia de la existencia de pretendidas situaciones de hecho de exclusividad, que se originan por la compra inicial de licencias informáticas, sobre las que se construye y desarrolla un sistema de información, con una considerable inversión económica y en recursos humanos. Pues bien, si se hace necesario extender la solución a otras áreas, se requiere de más y más licencias que, entonces, se van adquiriendo «a trozos», frente a la alternativa de desechar el sistema, lo que supondría la consiguiente pérdida de la inversión con infracción, incluso, de los principios de eficiencia y estabilidad presupuestarias. A las situaciones de pretendida exclusividad nos hemos referido *ut supra*.

6. INDETERMINACIÓN DEL OBJETO

Otro de los puntos a incidir, en el tema de las contrataciones TIC, es el de la necesidad de definir claramente y de forma completa el objeto del contrato. En ocasiones nos encontramos ante proyectos en los que

(16) *Vid.* Moll Fernández-Fígares, L.S., *Los encargos a medios propios en la Legislación actual*, Ed. Reus, 2017.
(17) 99 de la LCSP.
(18) Artículo 191.b del antiguo TRLCSP.
(19) 219 y ss. y 223 y ss. de la LCSP.

convergen varias circunstancias, como son la especial complejidad técnica o la dificultad determinar, con precisión las posibles vicisitudes de la prestación del servicio que, a veces empujan a los gestores a diseñar un contrato, más o menos abierto, en el que lo que tratan de asegurarse, son medios personales y materiales durante un determinado periodo de tiempo, con unos fines, si quizá, más definidos, pero en el que el proceso y actuaciones concretas para alcanzarlos adolecen de concreción.

A nadie se le escapa la dificultad que plantea esta situación en la que, sin que necesariamente se trate de perjudicar la concurrencia, se impide a los licitadores calcular las posibles ofertas a realizar, más allá de la puesta a disposición de herramientas y personas, durante un tiempo.

Algunas de estas dificultades han de solucionarse necesariamente, ahora, mediante el diálogo competitivo (20).

7. PROBLEMAS DE LA CONTRATACIÓN TIC RELACIONADOS CON EL DERECHO LABORAL

Como venimos señalando, en la adquisición de bienes y servicios TICs y debido, en ocasiones, a la complejidad de los procesos a desarrollar y su evolución, se diseñan contratos más o menos abiertos para asegurar, principalmente, medios personales y materiales, durante un determinado periodo de tiempo con unos fines, pero en el que las actuaciones concretas para alcanzarlos no están suficientemente especificadas.

Estos contratos se definen de forma genérica, en función de distintos materias, como pueden ser la seguridad, la atención de soporte, las comunicaciones, la gestión de aplicaciones, etc., sin que haya en general, *a priori*, una determinación concreta de proyectos definidos por objetivos. Adicionalmente, el precio del contrato se establece mediante el sistema de tarifa/hora, en función de las categorías profesionales de los trabajadores que prestan los servicios y luego, la ejecución de estos contratos y el pago del precio no se vincula a la correcta ejecución y entrega de proyectos bien determinados previstos en los pliegos, sino, en función de las horas efectivamente trabajadas.

Para colmo de males, se prevén, en los pliegos, para el ente público contratante, facultades de dirección y organización del trabajo. Trabajo que puede, incluso, desarrollarse en los locales de aquel que licitó, lo que puede dar lugar a supuestos de cesión ilegal de trabajadores, situación prevista en el artículo 43.2 del Estatuto de los Trabajadores y, aún más,

(20) 172 y ss. de la LCSP.

vulnerar las normas reguladoras de la función pública, evidenciando una clara falta de medios personales en la Administración de que se trate (21).

8. SERVICIOS PRESTADOS EN LA NUBE

8.1 ***Software as a service***

El *software* es un producto que se puede distribuir de varias maneras. De forma clásica, se realiza mediante una instalación directa en los equipos del cliente. Ahora bien, actualmente, las compañías suelen ofrecer el *Software as a service* en la nube donde, el soporte lógico y los datos que se manejan, se alojan en servidores del fabricante o distribuidor, a los que se accede vía Internet. La proveedora TIC se ocupa del servicio de mantenimiento, de la operación diaria y del soporte.

Este modelo también puede suponer, en ocasiones, una desventaja para la Administración, desde el punto de vista de la continuidad de los servicios. Veamos.

Si la Administración adquiere una licencia de *software*, esto es, en sentido clásico, ésta pasa a ser de su propiedad. Cierto que necesitará, quizás, mantenimiento y soporte. Sin embargo esas licencias continuarán funcionando con el tiempo, a pesar de que puedan surgir nuevas versiones o modificaciones de las mismas.

Cuando este *software* o cualquier servicio se aloja en la nube, por un lado la Administración tiene que pasar por las versiones que vaya produciendo la empresa licenciataria, por otra, a la expiración del plazo del contrato, se le retirará el acceso a la herramienta instantáneamente, de manera que, si la Administración si no planifica debidamente, se quedará sin capacidad de reacción.

En adición, imaginemos que la empresa proveedora quebrara. También lo haría el servicio, sin que en ningún caso pudiese accederse al denominado *código fuente,* que permite realizar las actividades necesarias para procurar el cambio de solución y que, cuando se sigue el sistema clásico, es objeto de depósito notarial a través del denominado contrato de *scrow*.

8.2 **Servicios en la nube y protección de datos**

Destaquemos, a continuación el supuesto de servicios informáticos prestados en la nube, a través de servidores o centros de tratamiento situados en el extranjero y su relación con la protección de datos.

(21) *Vid*., a título de ejemplo, la mencionada Resolución de 15 de marzo de 2017, aprobada por la Comisión Mixta para las Relaciones con el Tribunal de Cuentas, en relación con el Informe de fiscalización de la contratación celebrada durante los ejercicios 2006 a 2009 por la Gerencia de Informática de la Seguridad Social, «BOE» de 4 de mayo de 2017.

Pensemos en un contrato cuyo objeto consiste en tratar imágenes o audio, de manera que puedan introducirse herramientas buscadoras que permitan acceder a momentos concretos de grabaciones (pongamos, por ejemplo, de vistas judiciales).

El que servicio se presta en la nube de forma que los datos que contengan tales grabaciones van a ser tratados en un país extranjero, no necesariamente de la Unión europea. Nos encontramos ante un caso de transferencia internacional de datos.

Dichas transferencias (sin perjuicio de otras limitaciones derivadas de la aplicación de nuestra propia LOPJ y leyes procesales, en nuestro ejemplo) pueden ser contrarias a lo dispuesto en los artículos 33 y 34 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y en el Título VI del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre [actualmente debe tenerse en cuenta el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, totalmente aplicable a partir de mayo de 2018]. En todo caso plantean un interesantísimo y difícil problema, sobre el que se hace necesaria una profunda reflexión, por parte de nuestros legisladores.

Veremos que no es este el único caso en que las posibilidades de contratación de tecnología chocan con los derechos en materia de protección de datos.

9. MODIFICACIONES IMPREVISTAS

Citaremos tan sólo el caso de las modificaciones imprevistas. En ocasiones, los pliegos técnicos, en la materia que nos ocupa, incluso, las ofertas de los operadores económicos que participan en los procedimientos de licitación, son muy complejos, y no es infrecuente que no se incluya algún *item*, que luego resulta necesario para la ejecución del contrato, pero que tiene un coste ínfimo.

Al no estar previsto, frente a la alternativa que obligaría a modificar el pliego si se dieran los requisitos para ello, previstos en la Ley, y a seguir todo un procedimiento, en la realidad se dan casos en que, por lo despreciable del valor, estos problemas se solucionan en una liquidación final del contrato (artículo 210.4 de la LCSP).

10. LA INNOVACIÓN TECNOLÓGICA: DOMINIOS EN INTERNET. LAS ADMINISTRACIONES PÚBLICAS COMO OPERADORES DE REGISTRO DE DOMINIOS

Sin lugar a dudas, las Administraciones Públicas, trabajan permanente en la mejora de su productividad y en el uso racional de los recursos. El uso intensivo de la tecnología, y en concreto el uso de Internet, se convierte en una herramienta fundamental para conseguir estos objetivos.

Dentro del abanico de las TICs al alcance de las AAPP (22) ocupa un lugar destacado, por su proyección internacional y tremenda potencialidad, la posibilidad de constituirse, estas, en autoridad de registro de dominios de internet de primer nivel lo que exige, a su vez, la contratación con la *Internet Corporation for Assigned Names and Numbers (ICANN)*.

ICANN es la entidad que gobierna los dominios de Internet en el mundo. Esta organización es responsable de asignar espacio de direcciones numéricas de protocolo de Internet (IP), identificadores de protocolo y de las funciones de gestión del sistema de nombres de dominio de primer nivel genéricos (gTLD) y de códigos de países (ccTLD), como de la administración del sistema de servidores raíz. Así mismo, se encarga de supervisar la distribución de los identificadores técnicos únicos que se usan en las operaciones de Internet, y delegar los nombres de dominios de primer nivel.

En ella participan Gobiernos, organizaciones internacionales en sentido clásico, empresas y personas físicas en distintos roles. El representante español en su «Comité Asesor Gubernamental», es el Subdirector General de Fomento de la Sociedad de la Información y la Agenda Digital del Ministerio de Energía, Turismo y Agenda Digital.

No hay lugar aquí para explicar el origen y funcionamiento de esta entidad que surgió vinculada al gobierno de los Estados Unidos (23).

Baste señalar que, con independencia de los dominios territoriales, como el *.es* (España) o *.fr* (Francia) (24), que tienen una explicación di-

(22) Se configura como un elemento privilegiado para posibilitar el acceso de los ciudadanos, a los Servicios públicos a través de internet, dentro del contexto iniciado por la, ya derogada, Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y, ahora, las Leyes 39 y 40/2015. Por otra parte, el nombre de dominio es la puerta de entrada a la denominada «sociedad de la información», expresión empleada por la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos del comercio electrónico en el mercado interior y utilizada por la legislación española en su Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico. Los nombres de dominio son, también, un instrumento fundamental para el desarrollo del comercio en el entorno electrónico.

(23) Las referencias, tanto en la red, como tradicionales son muy numerosas. En todo, entre nosotros, véase: Barrio Andrés, M.: *Fundamentos del derecho de internet*. Ed. Centro de estudios constitucionales, Madrid, 2017 y Lastiri Santiago, M.: *La comercialización del nombre de dominio*. Marcial Pons, 2014.

(24) Los dominios territoriales corresponden a cada país, que designa sus gestores, públicos o privados y establece las reglas para conceder dominios, de segundo nivel, de acuerdo

ferente (25), como consecuencia de la decisión de *ICANN* liberalizar, en un momento dado, los dominios genéricos, pudieron presentarse, en momentos temporales determinados, candidaturas, públicas y privadas, para optar a constituirse en operador de registro.

En España, contamos con diversos ejemplos como el *.seat,* el *.mango,* etc. Los entes públicos intervienen de forma, más o menos directa (muchas veces simplemente mediante participación del ente público televisivo, autonómico, etc.), a través de fundaciones, que gestionan estos nombres, como en los supuestos de *.cat, .barcelona17* o *.eus18,* o asociaciones, como .gal.

En otras ocasiones ha sido la propia Administración territorial la que ha ganado su candidatura, como la Comunidad de Madrid, a través de *.madrid.*

En fin, el negocio jurídico a realizar con ICANN a que hacemos referencia, es un contrato (26) denominado «de delegación», en virtud del cual ICANN designa al Operador de registro como operador de registro del TLD, con el fin de delegar el dominio de nivel superior, de manera que el Operador de registro estará autorizado a prestar los Servicios de registro (27) descritos en las cláusulas y la entrada en la zona raíz.

El contrato, obviamente derivado del sistema jurídico anglosajón incluye multitud de cláusulas, algunas técnicas: «Interoperabilidad, Publicación de información de la zona raíz», Algunas más propias del sector: «Nombres reservados, obligación de contar con registradores acreditados», algunas más generales: «custodia de datos del registro; cláusulas de protección y cesión de datos (28), cláusulas penales, limitaciones de res-

---

con las prescripciones de ICANN. En España, la gestión del.*es* corresponde a la Entidad Pública Empresarial *Red.es*.

(25) «.es» se creó en abril de 1.988 – así lo indica el informe http://www.iana.org/reports/2005/es-report-05aug2005.pdf - ver «Factual and Procedural Background, realizado con motivo de la redelegación del «.es en la base de datos de IANA (Internet Assigned Numbers Authority, que es la predecesora en muchas de las funciones que hoy realiza ICANN) en 2004, cuando el dominio.es dejó de figurar como gestionado por RedIRIS, y pasó a figurar como registro Red.es, que legalmente ya tenía esa competencia desde 2.000. *Vid.* Sanz, M.A. (entonces coordinador del Área de Red de RedIRIS), http://www.rediris.es/rediris/boletin/28/enfoque1.html.

(26) No encontramos un fácil encaje en los negocios excluidos de la sección segunda del capítulo primero del Título preliminar de la Ley con lo que necesariamente debe estudiarse la calificación como un contrato privado al amparo del artículo 26 de la LCSP.

(27) En esencia, el servicio último se presta a través de dos negocios jurídicos: uno entre la autoridad de registro delegada de ICANN con las empresas del sector, que se denominan registradores; y otro entre estos y los destinatarios finales. Este esquema plantea multitud de retos desde el punto de vista jurídico; como que naturaleza jurídica tienen estos negocios en el caso de que la autoridad de registro sea una Administración pública, que naturaleza tienen los actos realizados por esta para dar el servicios, cual debe ser la vía para impugnar estos actos o que sistemas alternativos de resolución de conflictos pueden establecerse para solventar disputas entre registradores y destinatarios entre sí o con otros destinatarios finales, así como entre la autoridad de registro y las empresas del sector.

(28) Debe llamarse la atención sobre las consecuencias que este tipo de contratos pueden tener en relación con el problema de la transferencia internacional de datos. *Vid.* Artículos 33 y 34 de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD) y en el Título VI del Reglamento de desarrollo de la Ley Orgánica de Protección de Datos de Carácter Personal, aprobado por el Real Decreto 1720/2007, de 21 de diciembre. En relación con EE.UU., *vid.*

ponsabilidad, confidencialidad…», también de solución de conflictos, como la mediación y arbitraje (29). Ciertas de estas obligaciones podrían, incluso, discutirse desde el punto de vista del derecho continental: *«El Operador de registro cumplirá y aplicará todas las Políticas de consenso y Políticas temporales que se encuentran en* http://www.icann.org/general/consensus-policies.htm*. Lo anterior resulta de aplicación tanto en la Fecha de vigencia como para el futuro si las mismas se amplían o adaptan de acuerdo con los Estatutos de ICANN (…) En caso de la que la Junta directiva de ICANN resuelva que conviene modificar […] este acuerdo…»* (30)

El Precio de los Servicios de registro, por último, plantea una problemática especial, en el supuesto de que el delegado y autorizado para operar sea una Administración Pública. Cuando quien actúe como autoridad de registro sea una empresa particular, e incluso una fundación privada de capital público podrá cobrarse un precio privado. Cuando la autoridad de dominio es una administración territorial, en España se ha evolucionado desde el cobro de una tasa a un precio público (31).

La Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016. *Vid.* 44 y ss. del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. El Reglamento europeo de Protección de Datos entró en vigor el 25 de mayo de 2016 y será de obligatorio cumplimiento el 25 de mayo de 2018.

(29) Medios de solución de conflictos que, en el ámbito de las Administraciones territoriales exigen previa autorización de los gobiernos o consejos de gobierno. *Vid.*, *Verbi gratia*, artículo 7.3 de la Ley 47/2003, de 26 de noviembre, General Presupuestaria, artículo 31 de la Ley 33/2003, de 3 de noviembre, del Patrimonio de las Administraciones Públicas artículo 10.3 de la Ley 3/2001, de 21 de junio, de Patrimonio de la Comunidad de Madrid.

(30) Recuérdese, sin más, el artículo 1.256 o el 1.115 de nuestro código civil.

(31) E, incluso, podría discutirse si un precio privado. *Vid.* Moll Fernández-Fígares, L.S. «El precio de los nombres de dominio en internet». *Revista jurídica de la Comunidad de Madrid.* 09/05/2018. http://www.madrid.org/revistajuridica/index.php/articulos-doctrinales. Del mismo autor: «El precio de los nombres de dominio». *III Congreso del Consejo Superior de Letrados y Abogados de Comunidades Autónomas. Derecho y nuevas tecnologías.* 21 de septiembre de 2017, Campus Madrid-Princesa, Universidad Nebrija. https://youtu.be/GE52SxrrnZ8.

IX

CREATIVIDAD, ACCESO A LA CULTURA Y DEPORTE EN UN MUNDO DIGITAL

CAPÍTULO 34
LA PROPIEDAD INTELECTUAL EN EL MUNDO DIGITAL

JUAN A. CUERVA DE CAÑAS
Abogado, Clifford Chance. Profesor-colaborador
Universitat Oberta de Catalunya

1. INTRODUCCIÓN

Si algo nos demuestra la práctica a aquellos que hemos mantenido un contacto cercano con la Propiedad Intelectual a lo largo de los años es que el derecho de autor es especialmente permeable al cambio tecnológico. El tocadiscos, la radio, el casete, la doble pletina, el video, el CD, el DVD, los discos duros, los teléfonos móviles y un largo etcétera han hecho necesario que la legislación de Propiedad Intelectual tuviera que ir adecuándose a golpe de tecnología –y no siempre a la velocidad deseada– a la nueva realidad de los tiempos. Puestos en perspectiva, de todos esos cambios tecnológicos, el que mayores incertidumbres jurídicas ha generado es, sin

duda, internet y la explotación digital de las obras y contenidos. Y ello es así por la propia idiosincrasia de la red. Es inherente al funcionamiento de internet la realización masiva de actos de reproducción [art. 18 de la Ley de Propiedad Intelectual (1)] y comunicación pública (art. 20 de la Ley de Propiedad Intelectual) a través de los cuales los datos viajan de un punto a otro y los contenidos son puestos a disposición del público con un solo *click*. Precisamente la creciente importancia del derecho de comunicación al público (en la modalidad de puesta a disposición) en el entorno digital ha provocado que el Tribunal de Justicia de la Unión Europea («TJUE») haya centrado gran parte de sus pronunciamientos sobre Propiedad Intelectual en delimitar los contornos de este derecho. Pero, más allá de la necesidad delimitar los derechos de explotación en el ámbito digital, la dinámica de funcionamiento de la red ha tenido una incidencia efectiva no sólo en el contenido de las cesiones de derechos de Propiedad Intelectual sobre obras y prestaciones protegidas sino que ha generado, de forma paralela, una cultura propia de la red donde la creación es concebida, en muchas ocasiones, como un proceso colaborativo entre usuarios donde se acepta, como «regla de juego», que la obra debe circular gratuitamente y expuesta a una permanente transformación/actualización. Junto a los interrogantes diarios que plantea internet, la irrupción de nuevas formas de tecnología, como la impresión 3D y la inteligencia artificial, permite vislumbrar que la Propiedad Intelectual inexorablemente deberá afrontar en los próximos años importantes retos.

2. TRÁNSITO DE LA AUTORÍA TRADICIONAL A NUEVAS FÓRMULAS DE CREACIÓN COLABORATIVAS. TRANSMISIÓN DE DERECHOS DE PROPIEDAD INTELECTUAL PARA LA EXPLOTACIÓN *ON-LINE* DE OBRAS Y PRESTACIONES

Todavía es habitual, cuando se habla de Propiedad Intelectual, evocar la romántica escena del pintor refugiado en una buhardilla plasmando sobre un lienzo las vistas de la urbe parisina. Y es que, desde antiguo, la obra ha sido el resultado del proceso creativo individual de un autor que la divulgaba, en la inmensa mayoría de las ocasiones, bajo su nombre o, en otras, bajo pseudónimo (2). En ambos casos, el autor voluntariamente opta por compartir con el público la autoría de su obra informando a la sociedad de la identidad del «padre» de la creación. Tal es la importancia que adquiere el derecho moral de paternidad en el ámbito de la Propie-

(1) Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia (BOE número 97, de 22 de abril de 1996).

(2) Es cierto que los autores de algunas obras son anónimos, pero el porcentaje es tan bajo que resulta anecdótico.

dad Intelectual que el artículo 6 bis del Convenio de Berna para la Protección de las Obras Literarias y Artísticas sólo se refiere a este derecho moral y al de integridad.

Frente a las formas individuales de creación, la legislación de Propiedad Intelectual también prevé fórmulas colaborativas entre distintos autores. Es el caso de las obras en colaboración (art. 6 de la Ley de Propiedad Intelectual) y de las obras colectivas (art. 7 de la Ley de Propiedad Intelectual) (3). En el primer caso, todos los autores pueden exigir el reconocimiento de su autoría (derecho de paternidad) sobre la obra. En el segundo, los distintos autores que contribuyen a la obra creada por la iniciativa y bajo la coordinación de la persona que la edita y divulga bajo su nombre ostentan un derecho de paternidad exclusivamente sobre su aportación y no sobre el conjunto de la obra. Por ello, no tienen derecho a que su nombre aparezca mencionado de forma destacada en la portada, sino sólo donde se mencione, en su caso, su colaboración (4). Lo relevante, a los efectos que ahora nos ocupan, es que tanto en el caso de obras de creación individual, como en el caso de obras fruto de la reunión de distintos autores, en el marco tradicional de creación todos los autores estaban perfectamente identificados.

Sin embargo, el desarrollo de internet ha traído de la mano nuevas fórmulas de producir, crear y compartir información y conocimiento. La propia dinámica e interactividad en la red ha dado lugar a nuevas formas de creación colaborativa en las que, en contraste con los esquemas clásicos de creación, en ocasiones unos creadores desconocen la identidad de los otros y en las que se articula un determinado régimen de licencias que posibilita la transformación permanente de las obras. En este sentido, el régimen de licencias conforma la explotación *on-line* de obras y prestaciones protegidas por derechos de Propiedad Intelectual que son las que nutren a internet de contenidos.

2.1 ***Software* colaborativo y *software* libre**

Quizá la manifestación más representativa de *software* colaborativo sea el proyecto que lidera la Wikimedia Foundation, Inc. y cuyo máximo exponente es Wikipedia (5). A través del *software* conocido como *wiki*, gran cantidad de sujetos pueden crear contenidos y editar un mismo documento de forma global y sucesiva en el tiempo. Lógicamente, en este entorno, el

(3) Asimismo, sería el caso de las obras derivadas, también llamadas compuestas (arts. 9 y 11 de la Ley de Propiedad Intelectual).

(4) *Vid.* Sentencia de la Audiencia Provincial de Madrid, de 12 de septiembre de 2000 (JUR 2001, 16594).

(5) Además de Wikipedia, otros proyectos en marcha bajo los auspicios de Wikimedia Foundation, Inc. son Wiktionary, Wikibooks, Wikiquotes y un largo etcétera. *Vid.* www.wikimedia.org.

concepto de «originalidad» como criterio legal para atribuir protección al resultado creativo sigue siendo, por así exigirlo el artículo 10 de la Ley de Propiedad Intelectual, de plena aplicación, si bien, como ha apuntado la profesora Navas Navarro, en los contextos de creación colaborativa, los contribuidores «no crean de la nada, antes bien, combinan y recombinan materiales ya existentes» (6), abriendo la puerta así a que la obra derivada (arts. 9 y 11 de la Ley de Propiedad Intelectual) adquiera importancia.

Wiki es una tecnología sencilla que permite a sus usuarios la generación y edición a través de HTML de páginas web cuyos contenidos están conectados a través de enlaces o *links*. En estos entornos, el usuario *wiki* ha desplazado al editor en las que fueran sus funciones tradicionales y lo ha reconvertido en una suerte de supervisor de contenidos. Es decir, el editor ya no edita propiamente, sino que ofrece a sus usuarios el *software* colaborativo y el soporte necesarios para que sean ellos los que puedan (auto)editar los contenidos siguiendo una dinámica que retroalimenta al entorno *wiki* en cuestión. Lo que sí que conserva el administrador *wiki*, como el editor, es una función de filtrado y control de los contenidos que son incorporados al entorno *wiki*.

Desde el prisma de la Propiedad Intelectual, la cuestión que se ha planteado respecto de los entornos *wiki* es la categorización de las obras creadas en los mismos en uno de los regímenes de pluriautoría que prevé la Ley de Propiedad Intelectual. La respuesta a esta cuestión no tiene, en mi opinión, una respuesta unívoca y general, sino que dependerá de cada caso concreto. En el supuesto, por ejemplo, de Wikipedia (o cualquiera de los otros proyectos gestionados por Wikimedia Foundation, Inc.) no es descabellado pensar que el administrador del entorno *wiki* no se limita a ser un mero proveedor de herramientas técnicas. El hecho de ostentar funciones de control y dirección de una obra preconcebida lo aproximaría al rol de coordinación de la «persona natural o jurídica que la edita y divulga bajo su nombre y está constituida por la reunión de aportaciones de diferentes autores cuya contribución personal se funde en una creación única y autónoma, para la cual haya sido concebida […]» (art. 8 de la Ley de Propiedad Intelectual) (7). En contraste con estos casos que podrían encuadrarse en la categoría de obra colectiva, podrán identificarse otros supuestos en los que el entorno *wiki* no responde a una estructura jerar-

(6) Navas Navarro, S., «Dominio público, diseminación *on-line* de las obras del ingenio y cesiones «creative commons» (Necesidad de un nuevo modelo de propiedad intelectual)» en *Actas de Derecho Industrial*, número 32 (2011-2012), pp. 239-262.

(7) Aunque Wikipedia permite la participación colectiva a los usuarios, todo ello no ha surgido de forma espontánea, sino que responde a los objetivos de Wikimedia Foundation, Inc., que controla y supervisa los contenidos. Asimismo, los recursos humanos y económicos para financiar el proyecto también proceden de la referida fundación. Sobre la financiación de Wikipedia, puede verse el trabajo de Sánchez Roger, M., «Crowdfunding y la economía de Internet», en *Análisis Financiero*, 2015, número 127, p. 9.

quizada o piramidal y en los que los usuarios hacen sus aportaciones de forma libre e improvisada, sin obedecer a un plan de ruta preconcebido. En estos casos donde el *software wiki* simplemente opera como una herramienta colaborativa, sin que exista una persona que supervise y controle los contenidos, cabrá plantearse si nos encontramos ante una obra en colaboración «resultado unitario de la colaboración de varios autores», correspondiendo los «derechos de propiedad intelectual […] a todos los autores en la proporción que ellos determinen» (art. 7 de la Ley de Propiedad Intelectual). En esos supuestos, pues, donde la creación colaborativa no responde a una estructura jerárquica, las aportaciones de cada usuario, si son originales, constituirán una modificación (transformación) de una aportación (obra) previa, lo que planteará la necesidad de contar con la autorización de su autor conforme a lógica propia de la obra compuesta o derivada (arts. 9 y 11 de la Ley de Propiedad Intelectual). Esta circunstancia que podría suponer un obstáculo jurídico a la constante actualización de contenidos ha sido resuelta en los entornos *wiki* recurriendo a la aplicación de licencias *Creative Commons* que permiten la transformación de la obra preexistente siempre y cuando el nuevo contenido generado se someta a idénticas condiciones que la obra originaria (8). De este modo, se asegura la retroalimentación permanente de contenidos por un cauce jurídicamente viable.

Al hilo de lo anterior, las nuevas formas colaborativas de creación que han emergido en el entorno *on-line* ha propiciado, como decimos, la aparición de nuevos modelos de licencias para facilitar un uso colectivo de las obras. Es en este contexto en el que deben enmarcarse las referidas licencias *Creative Commons* y, más en particular, la licencia CC BY-NC-SA (*Attribution-NonCommercial-ShareAlike*) que permite, reconociendo la autoría de la obra, su explotación no comercial y su transformación y, por ende, la creación de obras derivadas por otros usuarios, siempre y cuando tampoco se haga un uso no comercial de dichas obras derivadas.

Este movimiento a favor de contribuir al uso colectivo y libre de obras se ha extendido también al campo del *software* donde, desde los años ochenta, han surgido diversas iniciativas. Nos referimos al *software* no propietario que, como categoría, comprende tanto el *software* libre (*free software*), como el *software* de código abierto (*open source software*) (9).

---

(8) Es el caso de la licencia BY-SA (*attribution + sharealike*) que permite la transformación de la obra primera, la generación de una nueva versión y el sometimiento de esta última a las mismas condiciones de la primera. Sobre las distintas licencias *Creative Commons vid.*: https://creativecommons.org/share-your-work/ [fecha última consulta: 10 de marzo de 2018], así como el trabajo de Xalabarder Plantada, R., «Les llicències Creative Commons: una alternativa al copyright?» en *Revista sobre la Societat del Coneixement*, número 2, 2006 (UOC) disponible on-line: http://www.uoc.edu/uocpapers/dt/cat/xalabarder.html [fecha última consulta: 12 de marzo de 2018].

(9) Sobre este tipo de software puede verse el trabajo del profesor De Miguel Asensio, P., «Derechos de Propiedad Intelectual» en *Derecho Privado de Internet. Estudios y Comentarios*

El *software* libre tiene su origen primero en la *Free Software Foundation* que, con Richard M. Stallman al frente, puso en marcha el proyecto GNU con el propósito de desarrollar un sistema operativo libre que funcionase como una alternativa a los productos Microsoft®. Linux fue el primer sistema operativo distribuido como *software* libre bajo una licencia GNU *General Public License* (GPL). Otros ejemplos posteriores son Apache u Mozilla Firefox. El *open source software*, a grandes rasgos, permite el uso libre y facilita al usuario el código fuente, de forma que éste puede revisarlo y modificarlo. Ciertamente, en la medida en que permiten acceder al código fuente, las licencias de este tipo de *software* autorizan a llevar a cabo cualquiera de las actividades no comprendidas dentro de los límites de los derechos de explotación del artículo 100 de la Ley de Propiedad Intelectual, por lo que este tipo de licencias están orientadas claramente a facilitar la transformación del programa de ordenador por cualquier usuario.

Aunque la licencia de referencia sea la GNU GPL, existe una amplia tipología de licencias de *software* no propietario que prevén unas condiciones de uso del programa de ordenador muy diversas (10). No obstante es posible identificar un núcleo básico de cláusulas comunes a todas ellas, como es el caso del reconocimiento de los autores del programa de ordenador y la prohibición de alterar la mención a los mismos (derecho de paternidad), la atribución de derechos no exclusivos de uso y reproducción del programa de ordenador, la posibilidad de acceso y transformación del código fuente, la posibilidad de transformación del programa y la difusión de nuevas versiones, etc. (11). En lo relativo a la difusión de nuevas versiones del programa de ordenador, el régimen que prevé cada tipología de licencia varía de forma considerable. Sin embargo, es habitual prohibir al usuario la utilización del código fuente para desarrollar programas de ordenador derivados cuyos derechos de propiedad intelectual queden reservados al autor (*software* propietario), imponiéndose la obli-

---

Legislativos. Aranzadi, 2015. Disponible *on-line* en Aranzadi: BIB 2015\13 [fecha última consulta: 10 de marzo de 2018].

(10) Kennedy, M. D., «A Primer on OpenSource Licensing Legal Issues: Copyright, Copyleft and Copyfuture», *St. Louis U. Pub. L. Rev.*, vol. 20, 2001, pp. 345-377. Disponible *on-line*: http://www.cs.miami.edu/home/burt/learning/Csc322.052/docs/opensourcedmk.pdf [fecha última consulta: 12 de marzo de 2018].

(11) La eficacia de este tipo de licencias ha sido admitida por los Tribunales norteamericanos en el asunto *Jacobsen v. Katzer* (535 F.3d 1373, 1378-79; Fed. Cir. 2008). En Francia, la *Cour d'Appel* de Paris consideró eficaz la licencia GNU GPL (CA Paris, 16 Sept. 2009, Pôle 5 ch. 10, n.° 04/24298; disponible *on-line* en: http://fsffrance.org/news/arret-ca-paris-16.09.2009.pdf [fecha última consulta: 12 de marzo de 2018]). En el caso de España, la Sentencia de la Audiencia Provincial de León (Sección 1.ª) número 405/2009, de 22 de julio de 2009 (JUR 2009\361980) que, como tantas otras, admite la eficacia de las licencias *Creative Commons*, hace mención de la licencia GPL en los siguientes términos: «Fuera de *Creative Commons* pueden existir –y existen– modelos de dominio público y licencias generales públicas *(GPL: General Public License),* pero es preciso que la parte que ha obtenido la obra a partir de ellas identifique la obra y su autor y –por supuesto– que demuestre que esa concreta obra se consiguió a partir de esa licencia general pública.»

gación de difundir el programa de ordenador derivado con el código abierto (sistema de licencias *copyleft*). Esta última cuestión hace que, en la práctica, este tipo de licencias no esté exento de problemas para aquellos desarrolladores que, debido al contenido relativo complejo de dichas licencias, desconozcan que terceros pueden obtener ingresos considerables a partir de su trabajo e, incluso, en función de la licencia de que se trate, puedan transformar el código fuente para desarrollar *software* propietario. De ahí que resulte aconsejable, con carácter previo a crear un nuevo programa de ordenador, conocer el concreto alcance de la licencia de *software* no propietario en cuestión.

2.2 **Transmisión de derechos de propiedad intelectual para la explotación *on-line* de obras y prestaciones**

Siendo internet una red descentralizada que permite a sus usuarios acceder a multitud de contenidos, muchos de ellos originales, todas las obras y prestaciones *on-line* teóricamente deberían encontrarse a disposición del público por así haberlo autorizado sus autores o titulares de derechos de Propiedad Intelectual. Dicha autorización presupone, pues, la existencia de una licencia o cesión de derechos que legitima el uso *on-line* de la obra o prestación so pena, en caso contrario, de existir una infracción de los derechos de Propiedad Intelectual (12). De esta forma, el régimen de licencias determina y delimita el modo y el alcance de la explotación *on-line* de obras y prestaciones protegidas por derechos de Propiedad Intelectual.

A este respecto, debemos recordar que el artículo 17 de la Ley de Propiedad Intelectual dispone que «[c]orresponde al autor el ejercicio exclusivo de los derechos de explotación de su obra en cualquier forma y, en especial, los derechos de reproducción, distribución, comunicación pública y transformación, que no podrán ser realizadas sin su autorización, salvo en los casos previstos en la presente Ley». Así, pues, la Ley de Propiedad Intelectual atribuye al autor un monopolio respecto de la explotación de su obra «en cualquier forma», donde debe considerarse compren-

(12) Un caso habitual es, por ejemplo, el de las redes de intercambio p2p o *peer-to-peer*. Al respecto, pueden verse los trabajos de Bercovitz Rodríguez-Cano, R. y Marín López, J. J., «Dictamen sobre el límite de copia privada y las redes de intercambio «peer to peer»» en *Revista jurídica de deporte y entretenimiento*, número 20, 2007 [disponible *on-line* en Aranzadi: BIB 2007/931], González de Alaiza y Cardona, J. J., «La sentencia de la Corte Suprema estadounidense en el caso *Grokster*: la matizada condena de los operadores P2P» en *Pe.i.: Revista de Propiedad Intelectual*, número 20, 2005, pp. 137-148, Carbajo Cascón, F., «El pulso en torno a la copia privada» en *Pe.i.: Revista de Propiedad Intelectual*, número 16, 2004, pp. 9-54, Garrote Fernández Díez, I., «Acciones civiles contra los prestadores de servicios de intermediación en relación con la actividad de las plataformas P2P: *Su regulación en la Ley 34/2002 y en la Ley de Propiedad Intelectual*» en *Pe.i.: Revista de Propiedad Intelectual*, número 16, 2004, pp. 55-104 y Casas Vallés, R., «La lucha por el derecho en las redes peer-to-peer: el caso Grokster ante el Tribunal Supremo de los EE. UU.» en *Revista jurídica de deporte y entretenimiento*, número 15, 2005, pp. 527-544.

dida también la explotación *on-line*. Dichos derechos de explotación –*«en especial, los derechos de reproducción, distribución, comunicación pública y transformación»*– se caracterizan por ser transmisibles *inter vivos* y *mortis causa* (arts. 42 y 43 de la Ley de Propiedad Intelectual) y la cesión podrá serlo con carácter exclusivo o no exclusivo (arts. 48 y 50 de la Ley de Propiedad Intelectual), de todos o de sólo algunos de los derechos de explotación pues, como ha destacado Plaza Penadés, estos derechos «son independientes entre sí» (art. 23 de la Ley de Propiedad Intelectual), «en el sentido de que son disponibles para el autor y transmisibles o disponibles por separado» (13). Luego, es posible que la cesión de unos y otros derechos de explotación a un mismo individuo pueda estar sujeta a un ámbito objetivo, territorial y temporal distinto. Es importante destacar, asimismo, que, a pesar de que en algún momento se quiso sostener por parte de los movimientos que defienden la circulación libre y gratuita de obras y prestaciones que las licencias *Creative Commons* quedarían al margen del régimen legal de los artículos 42 y siguientes de la Ley de Propiedad Intelectual, actualmente es cuestión pacífica que el hecho de que tales licencias permitan un uso en dichas condiciones no justifica su exclusión del marco normativo de la Ley de Propiedad Intelectual en tanto que, a través de las licencias *Creative Commons*, se autoriza la explotación patrimonial de obras y prestaciones (art. 17 de la Ley de Propiedad Intelectual). Es decir, las licencias *Creative Commons*, aunque no exista remuneración, constituyen una autorización a explotar patrimonialmente una obra o prestación en las condiciones acordadas y a las mismas les resulta de aplicación el régimen de transmisión de derechos de la Ley de Propiedad Intelectual (14).

Como decimos, salvo en aquellos supuestos en los que sea el propio autor (o titular de derechos) el que ponga su obra a disposición del público en la red, en el resto de casos, para poder explotar *on-line* una obra o prestación, será necesario contar con la autorización del autor. Dicha autorización deberá materializarse en un negocio jurídico *inter vivos* (art. 43.1 de la Ley de Propiedad Intelectual) que deberá delimitar oportunamente el alcance material de la cesión (derechos de explo-

(13) *Vid.* Plaza Penadés, J., *Propiedad Intelectual y Sociedad de la Información (Tratados OMPI, Directiva 2001/29/CE y Responsabilidad Civil en la Red)*, Aranzadi, Cizur Menor, 2002, pp. 97 y siguientes.

(14) Aunque los Tribunales españoles no se han pronunciado expresamente sobre este aspecto, no cuestionan la validez y eficacia de este tipo de licencias. *Vid.* las Sentencias de la Audiencia Provincial de Madrid (Sección 28.ª), número 150/2007, de 5 de julio de 2007 (AC\2007\1768), número 9/2011, de 21 de enero de 2011 (AC\2011\368), número 234/2014, de 12 de septiembre de 2014 (AC\2014\2036) y número 130/2011, de 15 de abril de 2011 (JUR\2011\226742), la Sentencia de la Audiencia Provincial de Tarragona (Sección 1.ª), número 390/2009, de 19 de noviembre de 2009 (JUR\2010\44100), la Sentencia de la Audiencia Provincial de Badajoz (Sección 2.ª), número 245/2010, de 3 de septiembre de 2010 (AC\2010\1362) y la Sentencia de la Audiencia Provincial de Burgos (Sección 3.ª), número 393/2017, de 28 de julio de 2017 (AC\2017\1217).

tación cedidos, modalidades de explotación, ámbito territorial y temporal) (15). En defecto de alguna de estas condiciones, guiadas siempre por los principios de interpretación restrictiva de los términos de la cesión (16) e independencia de derechos consagrado en el artículo 23 de la Ley de Propiedad Intelectual, resultarán de aplicación las previsiones supletorias previstas en el artículo 43.2 de la Ley de Propiedad Intelectual: «La falta de mención del tiempo limita la transmisión a cinco años y la del ámbito territorial al país en el que se realice la cesión. Si no se expresan específicamente y de modo concreto las modalidades de explotación de la obra, la cesión quedará limitada a aquella que se deduzca necesariamente del propio contrato y sea indispensable para cumplir la finalidad del mismo».

Cuando la cesión de los derechos de explotación sea exclusiva (art. 48 de la Ley de Propiedad Intelectual), el cesionario gozará del monopolio de explotación respecto de los derechos cedidos y en la modalidad en que han sido cedidos, excluyendo incluso al autor en la explotación de la obra respecto de los derechos y modalidades cedidas. Claro está, ese monopolio quedará limitado a los confines propios de la licencia. De modo que, por ejemplo, el licenciatario exclusivo al que se ha autorizado a explotar una obra o prestación *on-line* deberá tolerar la explotación de esa misma obra o prestación por terceros –incluso con carácter exclusivo– a través de cualquier otra modalidad y/o respecto de otros derechos, como sería el derecho de distribución a través de ejemplares físicos (17). En relación con la explotación *on-line* debe traerse a colación el artículo 43.5 de la Ley de Propiedad Intelectual según el cual, «[l]a transmisión de los derechos de explotación no alcanza a las modalidades de utilización o medios de difusión inexistentes o desconocidos al tiempo de la cesión», de forma que deberá entenderse que los términos de la cesión previstos en negocios jurídicos perfeccionados antes de que la explotación *on-line* fuese una realidad excluyen la explotación digital en la red (18).

En contraste con el cesionario en exclusiva, el licenciatario no exclusivo no ostenta la titularidad de los derechos económicos en todo su al-

(15) *Vid.* Gete Alonso y Calera, M. C., «Comentario al artículo 43» en Bercovitz Rodríguez-Cano, R. (Coordinador), *Comentarios a la Ley de Propiedad Intelectual*, Tecnos, Madrid, 2007, pp. 757-785. Lógicamente, la cesión tendrá por objeto exclusivamente derechos económicos o de explotación, habida cuenta que los derechos morales son «irrenunciables e inalienables» (art. 14 de la Ley de Propiedad Intelectual).

(16) Rodríguez Tapia, J. M., «Comentario al artículo 43» en Rodríguez Tapia, J. M. (Director), *Comentarios a la Ley de Propiedad Intelectual*, Civitas (Aranzadi), Cizur Menor, 2007, p. 359.

(17) Rodríguez Tapia, J. M., «Comentario al artículo 49» en Rodríguez Tapia, J. M. (Director), *op. cit.*, p. 374, considera que «de identificar modalidades, tiempo y espacio de la exclusiva, se desprende la posibilidad de que puedan coexistir de forma simultánea muchos cesionarios en exclusiva de una misma obra: basta que tengan derechos, espacios o tiempos distintos para no ser incompatibles».

(18) *Vid.* Sentencia de la Audiencia Provincial de Barcelona (Sección 15.ª) número 110/2006, de 10 de marzo de 2006 (JUR\2008\63662).

cance o respecto a modalidades de explotación concretas, sino que simplemente queda «facultado para utilizar la obra de acuerdo con los términos de la cesión y en concurrencia tanto con otros cesionarios como con el propio cedente», siendo su derecho, además, intransmisible, salvo en los supuestos previstos en el artículo 49, último párrafo, de la Ley de Propiedad Intelectual. Tradicionalmente, en lo que a la explotación de obras y prestaciones se refiere, era habitual el otorgamiento de una cesión exclusiva al intermediario que, a cambio de un precio, se aseguraba la eliminación de la competencia. Con las nuevas modalidades de explotación *on-line*, sin embargo, el papel del intermediario (editor, productor, etc.) ha ido menguando progresivamente a favor de la figura del autor, que opta por licenciar directamente su obra en la red. Este tipo de autorizaciones, ya sean gratuitas o sujetas a remuneración, no comportan la cesión de la titularidad de los derechos de propiedad intelectual. De modo que el autor, podrá continuar cediéndolos sin exclusividad mediante el negocio jurídico correspondiente.

Dentro de esta nueva dinámica del entorno *on-line*, donde es el autor el que decide directamente autorizar el uso de su obra en la red sin necesidad de contar con la intervención de un intermediario, han surgido nuevas formas de licenciamiento tendentes a poner una obra o prestación en circulación y favorecer su utilización libre y colectiva. Así, *Creative Commons* ofrece varios modelos de licencia lo más amplios posibles, cuyos términos están predeterminados y no admiten negociación (el único margen del que dispone el autor es optar por uno u otro modelo de licencia). Ello ha llevado a Navas Navarro a considerar este tipo de licencias una suerte de «contrato de adhesión redactado en clave de condiciones generales y que se celebra en serie o en masa» (19). Estas licencias que, como ya hemos adelantado, quedan igualmente sujetas al régimen de transmisión de derechos de la Ley de Propiedad Intelectual, tienen en común que imponen el reconocimiento de la autoría (*attribution*). A partir de ahí, los seis modelos de licencia *Creative Commons* disponibles oscilan entre la amplia licencia CC BY, que permite a su beneficiario reproducir, distribuir, comunicar públicamente y transformar la obra, siempre y cuando se respete el derecho de paternidad del autor o licenciante, hasta la mucho más restrictiva licencia CC BY-NC-ND que permite la reproducción, distribución y comunicación de la obra, pero no así su transformación, ni tampoco el uso de la misma para fines comerciales. Situadas entre estos dos extremos encontramos las otras cuatro

(19) Navas Navarro, S., «Dominio público, diseminación on-line de las obras del ingenio y cesiones «creative commons» (Necesidad de un nuevo modelo de propiedad intelectual)», *op. cit.*, p. 247.

licencias *Creative Commons* (20): CC BY-SA, CC BY-ND, CC BY-NC y CC BY-NC-SA (21). Un aspecto de las licencias *Creative Commons* que ha suscitado cierta controversia es el hecho de que las mismas parecen tener vocación de permanencia o, en otras palabras, supuestamente autorizan un uso de la obra o prestación a perpetuidad. El hecho de que este tipo de licencias no contengan una delimitación del ámbito temporal de las mismas ha llevado a considerar que, a falta de mención del plazo de duración, por aplicación del artículo 43.2 de la Ley de Propiedad Intelectual, las mismas tendrían una duración de 5 años (22). Solución que comparto plenamente.

En conclusión, el alcance de las facultades de los usuarios respecto de los contenidos disponibles en la red, así como el monopolio que el autor conserve sobre los mismos queda delimitado por dos elementos. Uno de naturaleza técnica, que serán las medidas tecnológicas de protección y control de acceso que existan sobre las obras y prestaciones y un segundo elemento de naturaleza jurídica, como lo es, el contenido y alcance de las licencias sobre contenidos *on-line* a las que nos acabamos de referir.

3. DELIMITACIÓN DEL DERECHO DE COMUNICACIÓN AL PÚBLICO EN EL ENTORNO *ON-LINE*

Partiendo de la premisa de que la mayoría de contenidos disponibles en internet están protegidos por derechos de Propiedad Intelectual, resultará fundamental, como hemos visto, haber obtenido la correspondiente autorización del titular de tales derechos para subir un determinado contenido (*uploading* o descarga ascendente) a una página web en línea (tanto internet como una intranet) y para descargarlo (*downloading* o descarga descendente). A este respeto, debemos recordar que el proceso de transmisión de contenidos *on-line* entraña la realización de sucesivos actos de reproducción (art. 18 de la Ley de Propiedad Intelectual) y de comunicación al público en la modalidad de puesta a disposición [art. 20.2 i) de la

(20) Junto a estas seis licencias, *Creative Commons* ofrecía otras que, por motivos diversos, ha retirado. Las concretas licencias y las razones de su retirada se explican en: https://creativecommons.org/retiredlicenses [fecha de última consulta: 12 de marzo de 2018].

(21) Una explicación del contenido de dichas licencias la facilita la propia *Creative Commons* en el siguiente enlace: https://creativecommons.org/licenses/?lang=es_ES [fecha de última consulta: 12 de marzo de 2018].

(22) Es la opinión de Navas Navarro, S., «Dominio público, diseminación on-line de las obras del ingenio y cesiones «creative commons» (Necesidad de un nuevo modelo de propiedad intelectual)», *op. cit.*, p. 248, quien también considera que tales licencias chocan con el artículo 1.583 del Código Civil que prohíbe la vinculación contractual indefinida en el tiempo. Otro argumento adicional que se ha invocado para negar el carácter eterno de este tipo de licencias es que se vaciaría de contenido el derecho moral de retirada de la obra (art. 14.6 de la Ley de Propiedad Intelectual). Sobre este último punto, *vid.* Vicent López, C., *Internet y Derechos de Autor: Nuevos Modelos de Explotación Online* (monografía asociada a la Revista Aranzadi de Derecho Patrimonial), número 39, Cizur Menor, 2017, p. 133.

Ley de Propiedad Intelectual]. El titular de una página web que quiera difundir *on-line* un determinado contenido ajeno protegido por derechos de Propiedad Intelectual tendrá que obtener la correspondiente autorización para la reproducción o carga –*upload*– en el correspondiente servidor, así como del derecho de comunicación al público para el posterior acto de puesta a disposición a través del cual el contenido en cuestión se hará accesible al público en el sitio web. Al otro lado de la pantalla, el usuario que accede a los contenidos *on-line* (i) estará efectuando, al navegar por las distintas páginas web, reproducciones provisionales en la memoria RAM de su ordenador; y (ii) en el caso de descargarse un determinado contenido (*downloading*) de forma permanente en cualquier dispositivo de almacenamiento –disco duro interno o externo, dispositivo USB, tarjeta de memoria, etc.– estará realizando un nuevo acto de reproducción que, para ser lícito, requerirá, asimismo, la autorización del titular de los derechos de Propiedad Intelectual. La ausencia de esa autorización se traducirá en la comisión de un acto de infracción. Ahora bien, que el contenido de una página web sea accesible de forma libre (sin necesidad de registrarse) y gratuita, como tantas veces sucede, no significa que el usuario tenga carta blanca para disponer libremente y de forma absoluta de los contenidos del sitio web. En estos casos, debe entenderse que existe una autorización siquiera tácita del titular de los derechos de Propiedad Intelectual para que el usuario pueda reproducir los contenidos accesibles *on-line* de forma temporal (*streaming*) o de forma permanente (impresión o descarga) pero exclusivamente para su uso privado y personal (23). El usuario, por tanto, no podrá, por ejemplo, distribuir fuera de la red cualesquiera soportes que reproduzcan el contenido de la página web ni podrá tampoco reproducir el contenido de la página web y ponerlo a disposición del público en otro sitio web distinto. Pero ¿puede el usuario enlazar, mediante un hipervínculo (*link*), el contenido de un sitio web con el de otro sitio web sin la autorización del titular de los derechos de Propiedad Intelectual del contenido enlazado o, por el contrario, la actividad de enlazar el contenido de una página web con otra mediante el uso de hipervínculos (*linking*) (24) debe ser autorizado por el titular de los derechos de Propiedad Intelectual? En definitiva, lo que plantea esta cuestión es si la provisión de enlaces (*linking*) debe ser considerado un nuevo acto de comunicación al público de una obra que ya ha sido puesta a disposición del público *on-line* y que,

(23) Esta autorización también puede ser expresa informando previamente al usuario de las condiciones de acceso y uso de los contenidos de la web y solicitando su aceptación. En el resto de casos, cuando no se solicita tal consentimiento con carácter previo, deberán respetarse las condiciones de uso de la web (*terms & conditions*) que normalmente incluirán una licencia de usuario (*end user license*).

(24) Los hipervínculos o *links* pueden ser de distinto tipo. Normalmente se distingue entre *surface links* (enlaces de superficie), *deep links* (enlaces profundos), *embedded links* (enlaces ensamblados) y *frames* (marcos).

por tanto, requiere de autorización del titular de derechos de propiedad intelectual, o si, por el contrario, no es más que una actividad que permite referenciar un contenido, es decir, remitir a los usuarios de la red al sitio *on-line* donde se encuentra la información, sin que tal actuación requiera de autorización alguna.

Las dudas que esta cuestión ha generado entre los Tribunales de los Estados miembro a raíz de la interpretación del artículo 3 de la Directiva 2001/29/CE (25) han dado lugar a que el TJUE haya tenido oportunidad de delimitar, mediante sus pronunciamientos en los casos Svensson (26), GS Media (27) y Bestwater (28), el derecho de comunicación al público en el entorno *on-line* y, más en particular, con relación a la actividad de establecer enlaces (*links*) a contenidos protegidos por derechos de Propiedad Intelectual. Sobre esta cuestión el TJUE ha resuelto que:

a) Para apreciar su infracción, el derecho de comunicación al público requiere la existencia de dos elementos acumulativos: (a) un «acto de comunicación» de la obra o prestación no autorizado por el titular de derechos de Propiedad Intelectual; y (b) la comunicación de ésta a un «público».

b) Para que exista un «acto de comunicación» no es necesario que haya un acceso efectivo a las obras (o prestaciones), sino que «basta con que la obra se ponga a disposición de un público de tal forma que quienes lo compongan puedan acceder a ella, sin que sea decisivo que dichas personas utilicen o no esa posibilidad».

c) El concepto de comunicación al público debe ser apreciado de forma individualizada, debiendo tomarse en consideración «varios criterios complementarios, de naturaleza no autónoma y dependientes unos de otros», que, «en las diferentes situaciones concretas, pueden darse con intensidad muy variable» y que «procede aplicarlos tanto individualmente como en sus interacciones reciprocas». Entre esos criterios se encuentra el papel que juega el usuario y el carácter deliberado de su intervención. De tal modo, debe entenderse que existe un acto de comunicación al público cuando el usuario «interviene, con pleno conocimiento de las consecuencias de su comportamiento, para dar a sus clientes acceso a una obra protegida, especialmente cuando, si no tuviera lugar tal intervención, los clientes no podrían, en principio, disfrutar de la obra difundida».

---

(25) Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, *relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información*; Diario Oficial número L 167, de 22 de junio de 2001, pp. 10-19 («Directiva 2007/29/CE»).

(26) Sentencia del TJUE de 13 de febrero de 2014 (C-466/12; Svensson).

(27) Sentencia del TJUE de 8 de septiembre de 2016 (C-160/15; GS Media).

(28) Auto del TJUE de 21 de octubre de 2014 (C-348/13; Bestwater).

d) El hecho de facilitar una página web enlaces sobre los que se puede pulsar y que conducen a obras (o prestaciones) publicadas sin ninguna restricción de acceso en otro sitio web ofrece a los usuarios de la primera página web un acceso directo a dichas obras (o prestaciones), de tal forma que éstos pueden acceder a ellas desde el lugar y en el momento que elijan. En tales circunstancias, pues, el hecho de facilitar en un sitio web enlaces para redireccionar al usuario a obras (o prestaciones) protegidas por derechos de propiedad intelectual, según el TJUE, «debe calificarse de «puesta a disposición» y, en consecuencia, de «acto de comunicación» en el sentido de la referida disposición [art. 3 de la Directiva 2001/29/CE]».

e) Con relación al segundo elemento del derecho de comunicación al público, es decir, que la obra (o prestación) debe ser comunicada a un «público», el TJUE, atendiendo a sus propios precedentes, ha considerado que el «público» está integrado por un número indeterminado y considerable de destinatarios potenciales. Por tanto, con la provisión de un hipervínculo el contenido al que se redirecciona resulta accesible por un «público» y, por ende, existe un acto de comunicación pública. Ahora bien, para determinar la legalidad de la provisión de un enlace a la misma obra (o prestación) que ya había sido previamente puesta a disposición del público con la misma técnica (internet), el TJUE considera que lo determinante es si el enla*ce (*link) hace la obra accesible a un «público nuevo» o no. Sólo cuando el público pueda ser considerado un «público nuevo», existirá infracción del derecho de comunicación al público. No siendo ese público un «público nuevo» porque el «público destinatario de la comunicación inicial era el conjunto de los usuarios potenciales de la página en la que se realizó, porque, sabiendo que el acceso a las obras en esa página no estaba sujeta a ninguna medida restrictiva, todos los internautas podían consultarla libremente», no es «necesario que los titulares de derechos de autor autoricen una comunicación al público».

f) El carácter lucrativo del acto de comunicación al público es otro factor a ponderar, hasta el punto de que en el caso GS Media el TJUE lo ha utilizado como criterio dirimente para determinar si existe un acto de comunicación al público que requiere o no de autorización del titular de derechos de Propiedad Intelectual. Así, el TJUE ha concluido que:

1) Si el enlace que remite a una obra o prestación protegida libremente accesible en internet lo realiza una persona sin ánimo de lucro, debe tenerse en cuenta la circunstancia de que esa persona no sepa, y no pueda saber razonablemente, que dicha obra o prestación ha sido difundida en la *red* sin consentimiento del titular de los derechos de propiedad intelectual. En estos casos (usuario que enlaza sin ánimo de lucro) no

existirá, pues, un acto de comunicación al público que requiera de autorización del titular de derechos, salvo que:

i. Se acredite que esa persona sabía o debía saber, por ejemplo, por haber sido advertida de ello por el titular de los derechos de propiedad intelectual, que su enlace redirige a contenidos puestos a disposici*ón on-line* ilícitamente.

ii. El usuario haya colocado un enlace que permite a los usuarios del sitio web en el que se halla dicho enlace eludir las medidas tecnológicas de restricción adoptadas por el sitio enlazado (donde se encuentran las obras o prestaciones protegidas) para limitar el acceso al mismo por parte del público. En este escenario, a pesar de la ausencia de ánimo de lucro, el TJUE estima que existe una intervención deliberada del usuario sin la que el resto de usuarios que se benefician del enlace (público nuevo) no podrían acceder a las obras difundidas.

2) Por el contrario, cuando el enlace que remite a una obra o prestación protegida accesible libremente en internet sin el consentimiento del titular de los derechos de propiedad intelectual lo realiza una persona con ánimo de lucro, el TJUE considera que «cabe esperar del que efectúa la colocación que realice las comprobaciones necesarias para asegurarse de que la obra de que se trate no se publica ilegalmente en el sitio al que lleven dichos hipervínculos, de modo que se ha de presumir que la colocación ha tenido lugar con pleno conocimiento de la naturaleza protegida de dicha obra y de la eventual falta de autorización de publicación en Internet por el titular de los derechos de autor. En tales circunstancias, y siempre que esta presunción *iuris tantum* no sea enervada, el acto consistente en colocar un hipervínculo que remita a una obra publicada ilegalmente en Internet constituye una «comunicación al público» en el sentido del artículo 3, apartado 1, de la Directiva 2001/29» que requerirá el consentimiento del titular de derechos de Propiedad Intelectual.

En conclusión, según la interpretación del TJUE, el *linking*, como regla general, es una actividad libre, que no requiere autorización del titular de derechos de Propiedad Intelectual cuando los enlaces remiten a obras y prestaciones protegidas disponibles en un sitio web de libre acceso *con* el consentimiento del titular de los derechos de Propiedad Intelectual. En cambio, sí debe considerarse incluido dentro del ámbito del derecho de comunicación al público (en la modalidad de puesta a disposición) el *linking* a obras y prestaciones protegidas difundidas en la red *sin* la autorización del titular de derechos que se realiza (i) *con* ánimo de lucro, ya sea directo o indirecto (presunción *iuris tantum* que admite prueba en contrario); o bien (i) *sin* ánimo de lucro, cuando el usuario que enlaza conoce

que los contenidos enlazados están disponibles en internet *sin* consentimiento del titular de derechos de Propiedad Intelectual (29).

4. IMPRESIÓN 3D

No hay duda de que en el entorno *on-line*, donde los contenidos son puestos a disposición del público para que éste acceda a los mismos desde el lugar y momento que elija, el derecho de comunicación al público en la modalidad de puesta a disposición es el derecho de Propiedad Intelectual estrella que le ha ido arrebatando protagonismo al derecho de reproducción (30). En el entorno *off-line*, en cambio, el derecho de reproducción sigue conservando su tradicional relevancia. No en vano, en el actual sistema económico donde se ha impuesto el sistema de producción en cadena o en serie, cualquier producto adquirido es una reproducción o copia realizada a partir de una matriz (ejemplar primero). Por tanto, en el plano material, el binomio reproducción-distribución continúa manteniendo toda su vigencia. Se hacen copias (reproducciones) en soportes tangibles y esas copias son distribuidas entre el público, que las adquiere.

Siguiendo en el contexto de la realidad material, como tantas otras veces sucede en el ámbito de la Propiedad Intelectual, la aparición de una nueva tecnología, como lo es la tecnología de impresión 3D, tiene implicaciones en el plano jurídico. Hasta ahora, la legislación de Propiedad Intelectual, en lo que respecta al derecho de reproducción en el ámbito privado (particulares personas físicas), había centrado su atención, básicamente, en las reproducciones 2D (fotocopias y copias de materiales impresos) y en la reproducción de archivos sonoros (obras y prestaciones musicales) y contenidos visuales y/o audiovisuales, siendo marginales las reproducciones de objetos físicos en tres dimensiones (por ejemplo, réplicas de piezas de joyería originales). Sin embargo, es previsible que esta realidad cambie en los próximos años con la irrupción de la tecnología de impresión 3D.

(29) En su posterior Sentencia de 14 de junio de 2017 (C-610/15; The Pirate Bay), el TJUE ha tenido ocasión de aplicar la doctrina de los casos Svensson, GS Media y Bestwater a los sitios web de indexación de metadatos de archivos que son intercambiados por los usuarios mediante el protocolo BitTorrent. En particular, en dicha sentencia de 14 de junio de 2017, el TJUE tuvo que resolver si la actividad desarrollada por *The Pirate Bay*, consistente en poner a disposición y gestionar en internet una plataforma que indexa metadatos relativos a archivos que contienen obras y prestaciones protegidas y ofrece un motor de búsqueda que permite a sus usuarios localizar dichas obras y prestaciones para intercambiarlas a través de un red *peer-to-peer*, como lo es BitTorrent, constituye un acto de comunicación al público. El TJUE concluyó que existía infracción del derecho de comunicación al público. Sobre este asunto puede verse, Cuerva de Cañas, J. A., «Sentencia del Tribunal de Justicia de la Unión Europea de 14 de junio de 2017 (C-610/15): *The Pirate Bay* es en realidad el arrecife en el que ha escollado el barco pirata», *Comunicaciones en Propiedad Industrial y Derecho de la Competencia*, CEFI. Instituto de Derecho y Ética Industrial (IDEI), número 81, mayo-agosto 2017, pp. 107-128.

(30) Sin perjuicio, lógicamente, de que el derecho de reproducción continúe jugando un papel fundamental en la subida (*upload*) de contenidos.

Como es sabido, la tecnología de impresión 3D permite, a través de equipos específicos y mediante la superposición de capas sucesivas de material, la reproducción de objetos en tres dimensiones. Actualmente, existe un gran número de tecnologías disponibles para la impresión 3D, diferenciándose unas de otras en la forma en la que las diferentes capas son usadas para crear piezas. Algunos métodos usan fundido de material para producir las capas, que sería el caso, por ejemplo, del láser selectivo (SLS) o del modelado por deposición fundida (FDM), mientras que otras depositan materiales líquidos que son solidificados con diferentes tecnologías. En el caso de la manufactura de objetos laminados, se cortan capas delgadas para ser moldeadas y unidas juntas. Todas estas tecnologías tienen en común que el resultado final es la impresión (reproducción) 3D de un objeto físico.

Pues bien, desde el prisma de la Propiedad Intelectual, en el proceso hasta alcanzar el resultado de la impresión 3D pueden distinguirse distintos actos de explotación del derecho de reproducción en el caso de que el objeto que sea, valga la redundancia, objeto de la impresión 3D sea un creación original y, por ende, obra en el sentido del artículo 10 de la Ley de Propiedad Intelectual. En este sentido, la protección a través de la Propiedad Intelectual de un objeto ante la impresión tridimensional no plantea ninguna peculiaridad específica. El derecho de autor protege la obra original impresa tridimensionalmente, así como el derecho de su creador a reproducirla (art. 1 de la Ley de Propiedad Intelectual y arts. 20 y 33 de la Constitución Española).

En el caso de que la obra original a imprimir en 3D sea creada desde cero, a través de un programa informático, como puede serlo AutoCAD, el acto de impresión del objeto 3D constituirá, conforme al artículo 18 de la Ley de Propiedad Intelectual, un acto de reproducción. Existirá también un acto de reproducción previo en aquellos casos en los que, siendo el objeto a imprimir tridimensionalmente preexistente, el proceso de impresión 3D comporte la utilización de un escáner 3D. En estos casos, el escaneado 3D del objeto en cuestión también constituirá un acto de reproducción. Por tanto, el proceso de impresión 3D comportará cuando menos un acto de reproducción y, si existe intervención de un escáner 3D, hasta dos actos de reproducción (sin perjuicio de que el almacenamiento del archivo informático que contiene la imagen del objeto escaneado también constituya un tercer acto de reproducción). Todo ello comporta, desde el punto de vista práctico, que la reproducción 3D exige necesariamente disponer de los derechos de Propiedad Intelectual necesarios para poder llevar a cabo lícitamente los referidos actos de reproducción. En caso contrario, la realización de cualquiera de estos actos de reproducción sin consentimiento del titular de los dere-

chos de Propiedad Intelectual constituirá una infracción que permitirá al autor (y/o al titular de derechos) el ejercicio de acciones frente al infractor de conformidad con los artículos 138 y siguientes de la Ley de Propiedad Intelectual. Dicha infracción se haría extensiva, asimismo, a los actos de distribución entre el público de los objeto ilícitamente impresos tridimensionalmente.

A mayor abundamiento, no siendo dudoso que el objeto original impreso tridimensionalmente estaría protegido por el derecho de autor, también cabría considerar que el archivo digital en 3D que contiene la información para la impresión tridimensional se beneficiaría de dicha protección. De hecho, ello sería perfectamente coherente con la lógica que inspira el artículo 10 de la Ley de Propiedad Intelectual en el que no sólo tienen cabida las obras ya terminadas, sino también los materiales preparatorios. En este sentido el referido precepto de la Ley de Propiedad Intelectual protege, como obra, los «proyectos, planos, maquetas y diseños de obras arquitectónicas y de ingeniería». De este modo, lo que el plano es a la obra arquitectónica, el archivo digital 3D lo sería respecto del objeto original impreso tridimensionalmente.

Aunque en la actualidad pueda considerarse muy minoritario el grupo de personas físicas que disponen, a título particular y no como parte de un proceso productivo empresarial o de investigación, de una impresora 3D, la proliferación de la tecnología de impresión 3D desde sus orígenes y el abaratamiento de este tipo de impresoras hace necesario que debamos plantearnos la posible realización en un futuro no muy lejano de copias privadas de objetos impresos tridimensionalmente. Como ya hemos mencionado, la impresión 3D comporta necesariamente la realización de actos de reproducción que exigen el consentimiento del titular de los derechos de Propiedad Intelectual. Ahora bien, en aquellos sistemas legales, como el español, donde se prevé un límite de copia privada (limitación) al derecho de reproducción, es posible que las copias realizadas por personas físicas a través de tecnologías de impresión tridimensional pudieran tener cabida en el ámbito de dicha limitación si cumplieran los requisitos legalmente previstos en el artículo 31.2 de la Ley de Propiedad Intelectual. La reproducción tridimensional de un objeto protegido por derechos de autor que reúna cumulativamente los requisitos impuestos por el citado artículo 31.2, en tanto que «copia privada», no precisará autorización del titular de derechos, «sin perjuicio de la compensación equitativa prevista en el artículo 25». Esto es, como ya sucediera en su momento con los cassettes, videos, CDs, DVDs, etc., ante la imposibilidad de controlar las copias que hagan personas físicas en sus domicilios, sería razonable que los aparatos y equipos de impresión 3D pudieran quedar sujetos al pago de una compensación equitativa, pasando a formar parte del elenco de equi-

pos y soportes que generan dicha obligación de pago a los titulares de derechos de Propiedad Intelectual.

5. INTELIGENCIA ARTIFICIAL Y ROBOTS

Cuando se utilizan los términos «Inteligencia Artificial» que acuñara John McCarthy en 1956, nos referimos a la inteligencia computacional exhibida por máquinas. Máquinas dotadas de «inteligencia» que son capaces de percibir su entorno y/o circunstancias concretas y adaptar su respuesta a las mismas para alcanzar un determinado objetivo o completar una tarea. En pocas palabras, se trata de máquinas que son capaces de aprender y de resolver problemas sin necesidad de la intervención del ser humano. Actualmente, existen ejemplos de inteligencia artificial aplicada a las áreas de control de sistemas, de la planificación automática, del reconocimiento de escritura, reconocimiento del habla, reconocimiento de patrones, diagnósticos médicos, respuesta a consultas de consumidores, videojuegos, usos militares y de defensa y un largo etcétera. Para aquellos que sean aficionados al ajedrez, todavía perdurará en el recuerdo las partidas jugadas entre 1996 y 1997 por G. Kasparov y las computadoras de IBM Deep Blue I y II (31). Actualmente, a partir de la obra de Rusell y Norvig (32), se viene aceptando la distinción entre cuatro tipos distintos de inteligencia artificial:

1) Sistemas que piensan como humanos y emulan el pensamiento del ser humano como, por ejemplo, las redes neuronales artificiales. Dicha inteligencia artificial deviene de aplicación en actividades como la toma de decisiones, la resolución de problemas y el aprendizaje.
2) Sistemas que actúan como seres humanos, es decir, imitan el comportamiento humano, que sería el caso de la robótica.
3) Sistemas que piensan racionalmente y tratan de imitar o emular el pensamiento lógico racional del ser humano.
4) Sistemas que actúan racionalmente y tratan de emular de forma racional el comportamiento humano.

Por su parte, un robot, de acuerdo con la definición proporcionada por la Real Academia Española, es una «máquina o ingenio electrónico programable, capaz de manipular objetos y realizar operaciones antes reservadas solo a las personas». García-Prieto Cuesta clasifica a los robots, en función de su inteligencia, en cuatro grupos (tipo A-D), distinguiendo,

(31) Mientras que Deep Blue I fue batido en 1996 por el maestro ajedrecista, en 1997 Deep Blue II salió victorioso en su enfrentamiento contra el célebre campeón de ajedrez. Un año después, la máquina inteligente se imponía al hombre.
(32) Russell, S. y Norvig, P., *Artificial intelligence: A Modern Approach*. Disponible on-line: http://aima.cs.berkeley.edu/contents.htm [última consulta 12 de marzo de 2018].

asimismo, tres generaciones de robots. Los robots de tercera generación, tipo D («capaz de adquirir datos de su entorno, readaptando su tarea en función de estos»), serían una concreta manifestación de la inteligencia artificial (33).

Un robot o máquina inteligente podría, pues, potencialmente concebir y crear obras originales en el sentido del artículo 10 de la Ley de Propiedad Intelectual, como una pintura, una obra literaria, una composición musical, una escultura o, incluso, un programa de ordenador. En definitiva, la inteligencia artificial, entendida como máquinas autónomas con capacidad de razonamiento y decisión, lleva a cuestionarse si una máquina de este tipo podría ser considerada «autor» de una creación original objeto de Propiedad Intelectual (34). Debemos recordar ahora que, salvando las diferencias, un debate similar ya se planteó en los años noventa con ocasión de las obras realizadas por ordenador. Lo que discutió en aquel entonces era si un programa de ordenador podía ser considerado autor de la obra creada a través del mismo (35). Un sector de la doctrina consideró que el debate en cuestión debía ser abordado no como un problema de autoría (quién es el autor), sino como un problema de originalidad (existencia o no de obra): cuando la intervención del programa de ordenador tiene una relevancia tal que priva de originalidad al proceso de creación del usuario del programa de ordenador no puede existir obra. Sería el caso de los programas de ordenador que sirven como meras herramientas mecánicas, los que asisten al autor en el proceso de creación o, incluso, aquellos cuyo resultado o actividad es previsible en atención a la información recopilada por el programa de ordenador. Pero también el de la inteligencia artificial, donde el autor (persona física) no realiza ninguna aportación original a la creación, que es fruto directo de la actividad de la máquina inteligente.

En cualquier caso, tanto si se considera un problema de originalidad, como si se considera un problema de autoría, con la actual redacción de la Ley de Propiedad Intelectual, la respuesta al interrogante de si una máquina inteligente (inteligencia artificial) puede ser considerada «autor» de una creación original (obra) es clara: no. Y ello por cuanto el vigente artículo 1 de la Ley de Propiedad Intelectual dispone que «[l]a propiedad intelectual de una obra literaria, artística o científica corresponde al autor por el solo hecho de su creación» y, conforme al artículo 5 del mismo tex-

(33) *Vid.* García-Prieto Cuesta, J., «¿Qué es un robot?» en Barrio Andrés, M. (Director), *Derecho de los robots*, Wolters Kluwer, Madrid, 2018, pp. 39 a 45.

(34) Lógicamente, el software que, en su caso, incorpore la máquina inteligente podrá estar protegido de forma autónoma como programa de ordenador si es original *ex* artículo 96.2 de la Ley de Propiedad Intelectual.

(35) *Vid.* al respecto Carrasco Perera, Á., «Comentario al artículo 5 de la Ley de Propiedad Intelectual» en Bercovitz Rodríguez-Cano, R. (Coordinador), *Comentarios a la Ley de Propiedad Intelectual*, Tecnos, Madrid, 2007, pp. 102 a 105.

to legal, «[s]e considera autor a la persona natural que crea alguna obra literaria, artística o científica». Luego, la propiedad intelectual corresponde al autor «persona natural», que es aquella cuya personalidad civil, según los artículos 29 y 32 del Código Civil, se adquiere y se extingue, respectivamente, con el nacimiento y la muerte. En suma, no siendo «persona natural», ninguna forma de inteligencia artificial ni ningún robot podría ser considerado «autor» a los efectos de la vigente Ley de Propiedad Intelectual. Consecuencia directa de lo anterior es que, no existiendo «obra» en un sentido jurídico, el común de la sociedad podrá beneficiarse y disfrutar de forma gratuita y sin limitación (tampoco existirían derechos morales) de las creaciones originales resultado de la actividad de máquinas y/o robots inteligentes.

CAPÍTULO 35

IMPRESIÓN 3D

MIGUEL RECIO GAYO
Abogado

1. INTRODUCCIÓN

La tecnología de impresión tridimensional o impresión 3D (*3D printing*) es, junto con otras como los robots, la inteligencia artificial o la Internet de las cosas, una de las que están transformando y revolucionando

«nuestra manera de producir, trabajar, desplazarnos y consumir», tal como ha señalado la Comisión Europea (1).

Esta tecnología, de origen estadounidense, se ha desarrollado durante varias décadas, desde que en 1984 Charles W. Hull patentara su *stereolitography* (2), y, en particular en el ámbito europeo, ha sido objeto de atención por las instituciones europeas dadas sus implicaciones jurídicas y éticas entre otras.

En concreto, a modo de reflexión, a continuación se plantea la necesidad de prestar atención a las implicaciones jurídicas de la impresión 3D, ya que puede plantear retos, en el sentido de la necesidad de revisar si las leyes vigentes en diferentes áreas del Derecho suponen un límite inadecuado a las posibilidades de la innovación tecnológica, o, lo que es lo mismo, la necesidad de contar con un marco jurídico alineado con la innovación tecnológica que permita dar una respuesta concreta a las múltiples interrogantes a las que podría dar lugar aquélla.

Al mismo tiempo, la impresión 3D, como muestra específica de la innovación tecnológica, tiene implicaciones éticas, especialmente cuando es utilizada para fabricar determinados objetos, como podría ser un arma, o la generación de órganos humanos o células, lo que plantea, entre otras, la cuestión del acceso por los pacientes.

Los beneficios sociales a los que puede dar lugar la impresión 3D, además de otros de carácter económico, son, en definitiva, los que requieren de acciones y medidas adecuadas por los diferentes sujetos que tienen responsabilidades en la materia, tales como legisladores, autoridades reguladoras y otros actores jurídicos. Y cualquier acción o medida relacionada con la impresión 3D va a requerir una aproximación integral, ya que de no ser así se correría un elevado riesgo de perder oportunidades e incluso de limitar indebidamente derechos.

Por último, se incluyen las correspondientes conclusiones a las que da lugar la exposición de las diversas y diferentes implicaciones, con especial referencia a las jurídicas, que tiene la impresión 3D.

2. CONCEPTO Y EVOLUCIÓN DE LA IMPRESIÓN 3D

La impresión 3D, como indica el Parlamento Europeo, es «un término genérico que abarca diversos tipos de tecnologías que permiten, a partir

(1) Comisión Europea: *Documento de reflexión sobre el encauzamiento de la globalización*, *COM(2017) 240 final*, Bruselas, 2017, p. 12.

(2) Fontrodona Francolí, J. y Blanco Díaz, R.: «Estado actual y perspectivas de la impresión 3D», *Artículos de economía industrial*, *Generalitat de Catalunya*, Barcelona, 2014. [Consultado en: http://empresa.gencat.cat/web/.content/19_-_industria/documents/economia_industrial/impressio3d_es.pdf].

de un archivo digital y mediante el uso de una impresora 3D, fabricar objetos físicos» (3).

Desde el punto de vista de la impresión 3D aplicada a las tecnologías de producción y a la cadena de suministro, se trata de un concepto que se incluye en el término más amplio de fabricación aditiva (*additive manufacturing*, AM). Como proceso, Fontrodona Francolí y Blanco Díaz (4), explican que «es el proceso de unir materiales para hacer objetos a partir de un modelo digital, normalmente poniendo una capa encima de otra, por contraposición a las metodologías de fabricación sustractivas, tales como el mecanizado tradicional».

Esto supone que la impresión 3D sirva para fabricar objetos, que pueden personalizarse, e incluso otros, tales como órganos humanos o células.

Desde 1984, cuando Charles W. Hull obtuvo la patente para su *stereolitography apparatus* (5) como un sistema para la generación de objetos tridimensionales, se ha producido una importante evolución de la impresión 3D que ha estado marcada, en el ámbito europeo, por una mayor atención, especialmente desde que en 2014 se produjera la expiración de una de las patentes clave (6), lo que en la práctica supuso una caída relevante del precio que permitiría un mayor acceso tanto por *startups* como por particulares.

Conforme a las cifras que maneja la Comisión Europea (7), y que se basan en estudios y proyecciones de algunas consultoras y empresas de investigación sobre tecnología, se estima que en 2021 la impresión 3D supondrá un mercado que alcanzará los 9,64 billones de euros.

Esto supondrá superar la fase actual que, como subraya el Parlamento Europeo, está marcada porque es todavía «marginal y es probable que lo siga siendo, a medio plazo, dadas las limitaciones de los materiales accesibles a los consumidores» (8). Y ello a pesar de que el acceso a la impresión 3D se ha extendido entre los consumidores durante los últimos años por los motivos indicados y por otros, tales como el aumento de sus aplicaciones que trasciende claramente al de generación de prototipos en sus orígenes, alcanzando tanto a multitud de sectores como a usos, incluso en por lo que se refiere a la impresión de células, proteínas y órganos humanos.

---

(3) Comisión de Asuntos Jurídicos: *Documento de trabajo sobre la impresión 3D, un reto en los ámbitos de la propiedad intelectual y la responsabilidad civil*, Parlamento Europeo, 2017, p. 2.

(4) *Op. cit.*, véase p. 3.

(5) Al respecto, puede verse más información sobre esta patente en https://patents.google.com/patent/US4575330A/en

(6) Comisión Europea: *The disruptive nature of 3D printing*, Digital Transformation Monitor, Bruselas, 2017, p. 4.

(7) *Op. cit.*, véase p. 3.

(8) *Op. cit.*, véase p. 2.

Ahora bien, como cualquier otra tecnología, la impresión 3D plantea cuestiones que requieren de atención por todos los actores involucrados y que nos llevan a afrontar, una vez más, la cuestión sobre la innovación tecnológica y los derechos y libertades de las personas físicas, sin que ello deba suponer, necesariamente, que todo tiene que ser legislado.

3. IMPLICACIONES DE LA IMPRESIÓN 3D

Con carácter general, la impresión 3D presenta implicaciones éticas y jurídicas relevantes que tendrán un importante impacto en el desarrollo de esta tecnología durante las próximas décadas. Y dichas implicaciones alcanzan también a cualquier actor que intervenga en la cadena de producción, ya que la impresión 3D representa una oportunidad para fabricantes y para los consumidores o usuarios.

Por lo que se refiere a las implicaciones jurídicas de la impresión 3D, es necesario tener en consideración que son o pueden ser múltiples, ya que se plantean o pueden plantearse, entre otras, cuestiones en materia de propiedad intelectual, protección de los consumidores, responsabilidad civil, protección de datos personales o seguridad medioambiental.

Al mismo tiempo, la impresión 3D, como innovación tecnológica, se desarrolla en el marco del correspondiente ordenamiento jurídico que sea aplicable, ya sea el estadounidense, el europeo u otro, lo que implica que deba atenderse a la existencia de lagunas, normas inadecuadas para abordar la evolución tecnológica o a la necesidad de analizar qué medidas deberían adoptarse, en su caso.

Más allá de las implicaciones jurídicas, la impresión 3D, como una tecnología disruptiva, plantea retos para modelos de negocio actuales e incluso para cualquier tipo de control gubernamental, así como retos sociales, económicos y éticos.

Es decir, la impresión 3D tiene implicaciones relevantes que deben analizarse desde diferentes perspectivas, que pueden ser jurídica, social, ética, económica, etc. Al mismo tiempo, debe considerarse el impacto que tendrá en la evolución y uso de la impresión 3D el marco jurídico, económico y social correspondiente. La impresión 3D, como innovación tecnológica, plantea cuestiones que hacen que el Derecho avance, ya sea a través de cambios legislativos, regulatorios o a través del impulso de instrumentos de autorregulación.

Por lo tanto, la impresión 3D está sujeta a un notable escrutinio jurídico y social que requiere prestar atención a que la innovación tecnológica respete los derechos y libertades fundamentales de las personas físicas. La innovación tecnológica, como la impresión 3D, requiere desarrollarse en un marco flexible, en el sentido de adaptable, que considere las normas éticas, sociales y jurídicas para, de esta manera, suponer un avance en

beneficio de la sociedad, al mismo tiempo que se hace desde una perspectiva que trasciende las fronteras nacionales.

4. IMPLICACIONES JURÍDICAS DE Y SOBRE LA IMPRESIÓN 3D

Las implicaciones jurídicas de la impresión 3D plantean, por una parte, la necesidad de atender a las cuestiones que se suscitan en virtud de diversas materias del ordenamiento jurídico, tales como la propiedad intelectual, la privacidad o el derecho de los consumidores, y, por otra parte, a la necesidad de que las normas existentes faciliten el desarrollo tecnológico, al mismo tiempo que se analice si dichas normas son las adecuadas o qué medidas, en su caso, serían oportunas.

Una innovación tecnológica que no cumpla con requisitos jurídicos no es aceptable, puesto que iría en última instancia contra la sociedad misma. E igualmente, es necesario que los diferentes operadores jurídicos involucrados, ya sean jueces, legisladores, actores gubernamentales u otros, tengan que considerar la adecuación del ordenamiento jurídico para facilitar e impulsar la innovación tecnológica.

Es así que, a continuación, se presentan tanto algunas de las implicaciones jurídicas, en particular por lo que se refiere a propiedad intelectual, propia imagen, protección de datos personales y responsabilidad civil de la impresión 3D, como la cuestión relativa a la necesidad de que el marco jurídico esté alineado con la innovación tecnológica.

4.1 **Las implicaciones de la impresión 3D para el Derecho**

La impresión 3D tiene implicaciones, entre otras áreas, en materia de propiedad intelectual, protección de datos personales o responsabilidad civil. Estas implicaciones jurídicas, que pueden haber sido analizadas ya en otros lugares, especialmente en Estados Unidos donde surge esta tecnología, requieren y van a requerir de análisis en el caso de la Unión Europea y de otras jurisdicciones alrededor del mundo donde se haga uso de esta.

4.1.1 Propiedad intelectual e industrial

Por propiedad intelectual, como explica el Parlamento Europeo, puede entenderse el «conjunto de derechos exclusivos sobre las creaciones intelectuales. Se divide en dos ramas: la propiedad industrial, que incluye los inventos (patentes), las marcas, los dibujos y modelos industriales y las indicaciones geográficas; y los derechos de autor, que abarcan las obras literarias y artísticas» (9).

(9) Parlamento Europeo: *La propiedad intelectual, industrial y comercial*, Fichas técnicas sobre la Unión Europea, 2018. [Consultado en: http://www.europarl.europa.eu/RegData/etudes/fiches_techniques/2017/N54576/04A_FT(2017)N54576_ES.pdf].

En esta materia, el Consejo Superior de la Propiedad Literaria y Artística Francés (Conseil supérieur de la propriété littéraire et artistique français) concluye en un informe que, si bien en este momento una actuación legislativa sería prematura, es necesario observar los nuevos desarrollos tecnológicos o modelos innovadores asequibles ya que en los próximos años será posible que los profesionales y los particulares puedan hacer copias 3D de buena calidad de obras protegidas a un precio razonable (10). Es decir, según el citado Consejo y como pone de manifiesto la Comisión de Asuntos Jurídicos del Parlamento Europeo en su documento de trabajo sobre la impresión 3D, «no parece, hasta la fecha, provocar problemas graves de violación de los derechos de autor» (11).

No obstante, esta posición no es única, siendo posible encontrar argumentos en sentido contrario que alertan sobre la posible infracción de derechos de propiedad intelectual por el uso de la impresión 3D. Al respecto, según un estudio de la Oficina de Propiedad Intelectual Británica (Intellectual Property Office), la posibilidad de reproducir exactamente un objeto físico plantea interesantes cuestiones sobre una infracción potencial en la materia (12).

En materia de propiedad intelectual, como expone el Parlamento Europeo, a través del documento de trabajo de su Comisión de Asuntos Jurídicos, hay que distinguir entre el uso privado y el uso comercial de la impresión 3D ya que uno y otro cuentan con una diferente aproximación y reglas en la normativa sobre propiedad intelectual e industrial.

En cualquier caso, como señala la propia Oficina de Propiedad Intelectual Británica, todavía nos encontramos ante un número limitado de estudios sobre las implicaciones jurídicas y prácticas de la impresión 3D que, en particular, requiere de atención en nuestro país, incluso trascendiendo a la cuestión de si esta tecnología emergente tendrá un impacto, y cómo será este, en la normativa sobre propiedad intelectual.

Cabría, por tanto, considerar acciones, siguiendo el ejemplo de otros Estados miembros en la Unión Europea (13), tales como analizar las implicaciones de la impresión 3D para nuestra legislación en materia de pro-

(10) Conseil Supérieur de la Propriété Littéraire et Artistique Français: *Commission du CSPLA sur l´impression 3D*, Francia, 2017. [Consultado en: http://www.culture.gouv.fr/content/download/151134/1609938/version/2/file/3D%20printing%20and%20copyright%20-%20summary.pdf].

(11) *Op. cit.*, véase p. 4.

(12) Intellectual Property Office: *A Legal and Empirical Study of 3D Printing Online Platforms and an Analysis of User Behaviour*, New Port., Reino Unido, 2015. Pág. 14. [Consultado en https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/549045/Study-I.pdf].

(13) Además del ya citado informe del Conseil Supérieur de la Propriété Littéraire et Artistique Français, cabría considerar ejemplos como los del Reino Unido donde la cuestión ha sido analizada desde un punto de vista de cuestiones de política pública. Sissons, A. y Spencer, T.: *Three Dimensional Policy: Why Britain needs a policy framework for 3D* Printing', Big Innovation Centre, 2012. [Consultado en http://www.nibec.ulster.ac.uk/uploads/documents/3d_printing_paper_final_15_oct.pdf].

piedad intelectual y viceversa. Debería ser un análisis tanto de implicaciones jurídicas, en sentido amplio, como de cuestiones de política pública a las que se deba atender en relación con la impresión 3D.

4.1.2 Propia imagen

En nuestro ordenamiento jurídico la imagen de la persona física está protegida específicamente en virtud de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, que desarrolla el derecho fundamental consagrado en el apartado 1 del artículo 18 de la Constitución Española.

La impresión 3D podría tener implicaciones también para este derecho fundamental, especialmente por lo que se refiere a la propia imagen, ya que el escaneo tridimensional podría producirse sin el consentimiento necesario de la persona cuya imagen es escaneada.

Este escaneo tridimensional de la imagen de la persona, que puede ser lícito cuando se cumplan los requisitos necesarios ya sea sobre la base del consentimiento o con fines exclusivamente privados en el ámbito personal o doméstico, puede implicar también que el tratamiento de la imagen suponga un tratamiento de datos personales conforme a la normativa aplicable en la materia (14).

4.1.3 Protección de datos personales

La posibilidad de que las impresoras 3D puedan ser utilizadas para fabricar objetos, en particular como puede ocurrir en el caso del uso con fines sanitarios cuando se generan prótesis personalizadas, implica que puedan tratarse datos personales, en cuyo caso será necesario aplicar medidas para cumplir con la normativa sobre protección de datos personales.

Este uso específico implicaría un tratamiento de datos personales relativos a la salud, entendidos estos, tal como los define el Reglamento General de Protección de Datos en su artículo 4.15), como «datos personales relativos a la salud física o mental de una persona física, incluida la

(14) La imagen de la persona será considerada dato personal cuando identifique o permita identificar a la persona a la que se refiere. Por datos personales se entiende «toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona», según el artículo 4.1) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) [DO L 119, de 4 de mayo de 2016].

prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud».

Por tanto, si el uso de una impresora 3D implica el tratamiento de datos personales, será necesario también cumplir con la normativa aplicable para garantizar el derecho fundamental a la protección de datos personales, protegiendo así los derechos digitales de las personas físicas cuyos datos personales son objeto de tratamiento.

4.1.4 Responsabilidad civil

El hecho de que la impresión 3D se base en el uso de archivos y permita imprimir objetos da lugar a que, como expone la Comisión de Asuntos Jurídicos del Parlamento Europeo (15), deba considerarse la responsabilidad civil derivada, por una parte, por los daños provocados por un archivo defectuoso y, por otra parte, en el caso de los daños que pueda ocasionar un objeto que ha sido impreso utilizando dicha tecnología.

Como implicación jurídica que es objeto de la normativa nacional, la relativa a la responsabilidad civil requerirá, en su caso, de armonización tanto a nivel europeo como internacional.

La responsabilidad civil que, en su caso, pudiera derivarse requiere atender a los diferentes sujetos que pueden intervenir en la cadena, ya que pueden incluir al fabricante de la impresora 3D, a quien proporciona el programa informático para hacer funcionar a la impresora 3D, a quien proporciona los archivos digitales para imprimir un objeto y al propio usuario de la impresora 3D. Es decir, puede tratarse de un amplio grupo de personas cuya responsabilidad, en su caso, tendrá que ser determinada conforme a lo previsto en el ordenamiento jurídico aplicable.

Unido a lo anterior, específicamente por lo que se refiere a la responsabilidad derivada de los objetos que puedan ser fabricados mediante el uso de una impresora 3D, debe considerarse tanto el derecho de protección de los consumidores como los seguros. En relación con esta última cuestión, la Comisión de Asuntos Jurídicos del Parlamento Europeo subraya, en particular, que «si la responsabilidad en un ámbito no es clara, el seguro tiende a ser costoso o a no estar disponible, lo que repercute en la disponibilidad de capital riesgo» (16).

Finalmente, como plantea la Comisión de Asuntos Jurídicos del Parlamento Europeo, todavía está abierta la cuestión sobre si los fabricantes de impresoras 3D tienen una mayor responsabilidad o una responsabilidad

(15) *Op. cit.*, véase p. 5.
(16) *Op. cit.*, véase p. 5.

distinta a la de otros fabricantes de dispositivos que permiten fabricar objetos (17).

4.1.5 Otras áreas del Derecho

Sin perjuicio de las ya expuestas, la impresión 3D puede tener también implicaciones para otras áreas del Derecho, tales como en materia de contratos, ya sea conforme al Derecho civil o mercantil; la confidencialidad o el secreto de la información, como los diagramas o esquemas para la impresión, parámetros de configuración, los registros (logs) de impresión, etc.; cuestiones medioambientales derivadas tanto de los materiales utilizados para imprimir como de las propias impresoras 3D; otras como la seguridad pública y la seguridad nacional (18); la responsabilidad de los prestadores de servicios de la sociedad de la información, cuando se proporcionan archivos en línea u otros servicios relacionados con la impresión 3D, o incluso al derecho laboral por lo que se refiere a la seguridad de los trabajadores en el uso de estas impresoras.

Esto permite poner de manifiesto que la impresión 3D plantea, siendo también una oportunidad, la necesidad de considerar si el marco jurídico actual, ya sean leyes, regulaciones u otros instrumentos, es el adecuado para la innovación tecnológica de la que aquella es un ejemplo concreto.

Es así que, si bien algunas áreas del Derecho, tales como la propiedad intelectual, pueden ser las que más atención tengan en primera instancia por su impacto, la impresión 3D requiere considerar la innovación tecnológica de manera integral, atendiendo a todas las posibles implicaciones que puede tener para el ordenamiento jurídico, ya que se trata de asegurar que se protegen de manera adecuada los derechos digitales y cualesquiera derechos de las personas físicas en el mundo físico.

4.2 **Un marco jurídico alineado con la innovación tecnológica**

La impresión 3D es uno de los ejemplos específicos de por qué es necesario que la innovación tecnológica pueda desarrollarse sobre la base de un marco jurídico que sea adecuado o flexible, en los términos ya explicados, para adaptarse a la misma, sin necesidad de que todo sea objeto de regulación, ya que ello conlleva un coste importante que hay que considerar.

No se trata de que el marco jurídico tenga que ir por delante, ya que ello incluso podría dar lugar a limitar la innovación, sino de que prevea de

(17) *Op. cit.*, véase p. 5.

(18) En el caso de las implicaciones jurídicas que puede tener la impresión 3D en los Estados Unidos, puede verse el análisis de Reed Smith: *3D Printing: The Next Disruptive Technology to Test Existing Law*, LexisNexis, Estados Unidos, 2016.

antemano las cuestiones que se plantean para, en su caso, dar una respuesta adecuada y a tiempo.

Buena muestra de lo anterior es el hecho de que la impresión 3D haya dado lugar a cuestiones tales como la igualdad de acceso, que transcienden lo jurídico al ser también cuestiones éticas, en el caso de la posibilidad de imprimir órganos humanos.

La impresión 3D es parte de la economía y sociedad digitales, lo que significa que la misma tenga que respetar los derechos y libertades fundamentales, que se encuentran consagrados tanto en los Tratados y en el Derecho de la Unión Europea como en nuestro ordenamiento jurídico, que en buena medida trae causa de aquél. Desde la Carta de los Derechos Fundamentales de la Unión Europea (19) hasta cualquier medida, legislativa o de otra naturaleza, que pudiera adoptarse a nivel nacional constituyen el marco en el que se desarrollará la impresión 3D.

Ahora bien, la innovación tecnológica es una cuestión que tiene implicaciones globales, de manera que cualquier medida jurídica debe tener en consideración el alcance y las repercusiones que podría tener en términos de globalización, competencia económica e impacto en la sociedad. Y como parte de las implicaciones deben considerarse todas. Es decir, la innovación 3D puede plantear retos, pero también trae importantes beneficios.

El punto de partida en relación con la innovación tecnológica y la necesidad de un marco jurídico adecuado está claro. Como ha indicado Rodotà, actualmente «vivimos ya en una *law-saturated society*, una sociedad repleta de derecho, de reglas jurídicas de las más variadas procedencias, dictadas por poderes públicos o privados, con una intensidad que evoca no tanto una necesidad como una imparable deriva. La conciencia social no acaba de estar a la altura de la complejidad de un fenómeno como éste, que produce asimetrías y desequilibrios enormes, espacios llenos y vacíos, con un derecho demasiado presente en algunos ámbitos y, a la vez, ausente en lugares en que sería más necesario» (20).

4.3 **Los diferentes sujetos relacionados con la impresión 3D**

Cualquier acción o aproximación a la impresión 3D requerirá considerar que en el proceso de fabricación de objetos u otros productos puede involucrar a un amplio rango de sujetos para los que cualquier legislación, regulación o medida autorregulatoria tendrá implicaciones.

---

(19) Carta de los Derechos Fundamentales de la Unión Europea, *DO* C 202, de 7 de junio de 2016.

(20) Rodotà, S.: *La vida y las reglas. Entre el derecho y el no derecho*, traducción de Andrea Greppi, Trotta, Madrid, España, 2010, pp. 25 y 26.

La impresión 3D implica que deba prestarse atención, entre otros, al fabricante de impresoras 3D; a quien facilita, en cada caso, los materiales necesarios para poder imprimir; en su caso, a quien diseña y/o proporciona los archivos para llevar a cabo la impresión y otros sujetos que podrían intervenir en la cadena relacionada con aquélla.

Cada uno de estos sujetos, incluyendo al usuario, tienen derechos y obligaciones que deben determinarse claramente para evitar dudas o situaciones de ineficiencia, en términos económicos, jurídicos u otros.

Lo anterior determina que sea necesario también prever el impacto de la impresión 3D para las cadenas de suministro actuales, la logística y el comercio, ya que podría tener un impacto significativo o relevante en costes, medioambiente y otros aspectos relacionados con el comercio y la fabricación de productos. Es decir, una aproximación integral a la impresión 3D requiere considerar también las oportunidades que puede ofrecer, en términos de nuevas oportunidades para la economía digital.

5. IMPLICACIONES ÉTICAS

Piñar Mañas afirma que «hemos pasado de una época de *valores generalmente compartidos* a una situación de *politeísmo de valores*» (21), lo que, como sugiere el autor, lo que conduce a que «además del derecho y la técnica ha de darse voz a la ética» (22).

En particular, que se puedan imprimir órganos y células abre también un debate ético al que debe atenderse, por una parte, por lo que se refiere a la propia impresión 3D y, por otra parte, a los beneficios que podría suponer para la salud.

La ética en la innovación tecnológica, incluida la impresión 3D, es una cuestión que adquiere cada vez mayor relevancia, tal como pone de manifiesto a nivel europeo el programa de investigación e innovación europeo Horizon 2020 (23), siendo ya una cuestión prioritaria cuando los proyectos de investigación europeos reciben financiación pública en el marco del citado programa (24). Además, en el ámbito de la Unión Europea, es consustancial al cumplimiento normativo y regulatorio, tanto de la ya citada Carta de Derechos Fundamentales de la Unión Europea como la legislación nacional, europea (25) e internacional.

---

(21) Piñar Mañas, J. L.: *Derecho e innovación tecnológica. Retos de presente y futuro*, Facultad de Derecho, Universidad CEU San Pablo, CEU Ediciones, Madrid, 2018, p. 15.

(22) *Op. cit.*, p. 16.

(23) Comisión Europea: *Work Programme 2018-2020, Science with and for Society*. [Consultado en http://ec.europa.eu/research/participants/data/ref/h2020/wp/2018-2020/main/h2020-wp1820-swfs_en.pdf].

(24) Al respecto, puede verse más información en https://ec.europa.eu/programmes/horizon2020/en/h2020-section/ethics

(25) Un claro ejemplo del impulso por las autoridades competentes, como cuestión prioritaria, se da en el caso de la protección de datos personales, debiendo destacar la inclusión de

Considerando también el fenómeno de la globalización, la ética alcanza a la competencia, como pone de manifiesto que se aplique ya el concepto *ethics dumping* en aquellos casos en los que la investigación o la innovación se llevan a cabo sin cumplir con los estándares éticos y normativos o regulatorios requeridos.

La aplicación o uso de la impresión 3D en la salud es ya una realidad y seguirá avanzando en los próximos años. Actualmente la impresión 3D se utiliza con diversos fines, tales como la fabricación de audífonos o prótesis y también órganos humanos y células, siendo estas últimas cuestiones objeto específico de investigación a nivel global (26).

Los usos de la impresión 3D en el ámbito de la salud suscitan relevantes cuestiones éticas que, en unos casos, ya se habían planteado, por ejemplo, en relación con los trasplantes de órganos humanos, pero que dan lugar a nuevas cuestiones tales como si el paciente tendría que consentir que se le trasplante un órgano generado a través de la impresión 3D, y, en otros casos, podría dar lugar a cuestionar si las posibilidades que ofrece la impresión 3D para generar dispositivos como los audífonos deben utilizarse para facilitar el acceso a los mismos a un precio muy inferior al de otros que se encuentran en el mercado. En relación con esto último, de nuevo vuelven a producirse interrelaciones con otras cuestiones, tales como la propiedad industrial, ya que el titular de un diseño industrial está protegido por la normativa en la materia a nivel nacional (27), europeo e internacional.

En definitiva, el uso de la impresión 3D y su evolución, actual y futura, plantean importantes cuestiones éticas que deben considerarse tanto desde un punto de vista de otras que ya se hubieran planteado, por ejemplo, en relación con los trasplantes de órganos humanos, como interrelacionadas con el marco jurídico aplicable en su caso y el papel que desempeñe o pudiera desempeñar también la autorregulación. Estamos, por tanto, ante una oportunidad de que la impresión 3D pueda ser ejemplo de cómo la innovación tecnológica es responsable, especialmente en una era de rápido cambio tecnológico y globalización.

---

la ética en la Estrategia 2015-2019 del Supervisor Europeo de Protección de Datos y la creación de un Grupo Asesor de Ética (Ethics Advisory Group). Este Grupo Asesor de Ética fue creado en virtud de la European Data Protection Supervisor Decision of 3 December 2015 establishing an external advisory group on the ethical dimensions of data protection («The Ethics Advisory Group»), y su principal objetivo es analizar la relación entre los derechos humanos, la tecnología, los mercados y los modelos de negocio.

(26) IDEA Consult, AIT, VTT, CECIMO: *Identifying current and future application areas, existing industrial value chains and missing competences in the EU, in the area of additive manufacturing (3D-printing)*, *Final Report*, Comisión Europea, Executive Agency for Small and Medium-Sized Enterprises, Bruselas, 2016, p. 102. [Consultado en http://ec.europa.eu/DocsRoom/documents/18741/attachments/1/translations/en/renditions/native].

(27) Ley 20/2003, de 7 de julio, de Protección Jurídica del Diseño Industrial publicada en el *BOE* núm. 162, de 8 de julio de 2003.

6. OTRAS IMPLICACIONES DE LA IMPRESIÓN 3D

Las implicaciones jurídicas y éticas no son las únicas que plantea la impresión 3D. Una aproximación integral a la impresión 3D requiere atender también a cuestiones de política pública en relación con la innovación tecnológica que van desde los actores que pueden intervenir en la misma hasta los beneficios mismos que podría aportar a la sociedad.

Como cuestiones de política pública, el impacto de la impresión 3D para el modelo de negocio, lo que incluye la cadena de producción, y la competencia entre países o regiones a nivel internacional, requieren también una atención específica. En este sentido, las barreras a las que pueda hacer frente la impresión 3D (28) son las mismas que en otros ámbitos de la innovación tecnológica, tales como la falta de habilidades (*skills*), formación y conocimiento relacionado con los materiales y procesos relacionados con aquélla. Se plantean, por tanto, diversas cuestiones que afectan al desarrollo de la impresión 3D que requieren de una aproximación integral y no segmentada o parcial.

Esto da lugar a la impresión 3D ponga de manifiesto también la necesidad de cooperación entre las autoridades competentes, ya que una aproximación parcial solo respondería a cuestiones específicas o limitadas, sin atender al impacto real que puede tener para la sociedad.

El desarrollo de la impresión 3D, los usos y beneficios sociales a los que pueda dar lugar la misma, determinan la necesidad de desarrollar programas de políticas públicas que, si bien puedan generarse a nivel nacional, consideren las implicaciones de la investigación y la innovación tecnológica en el ámbito internacional y global.

Lo anterior explica por qué la Unión Europea impulsa de manera decidida una aproximación común entre los diferentes Estados miembros que permita superar iniciativas nacionales que dan lugar a aproximaciones fragmentadas que debilitarían las capacidades y posibilidades, comerciales o no, de la impresión 3D.

Es decir, la impresión 3D, como uno de los ejemplos concretos de la innovación tecnológica, requiere considerar tanto los actores como los factores que inciden en la cadena de valor, ya sea en el ámbito de la salud, la fabricación de partes o componentes utilizados con diferentes fines, objetos decorativos, textiles o, incluso, construcciones o alojamiento económicos.

Entre estos factores hay que atender tanto a la disponibilidad y acceso a materiales que puedan utilizarse para la impresión 3D, que pueden ser el acrilonitrilo butadieno estireno, que es un termoplástico, el ácido polilático o el tereftalato de polietileno, pero también otros en casos concretos como la salud.

(28) Al respecto, véase https://ec.europa.eu/growth/content/report-3d-printing-current-and-future-application-areas-existing-industrial-value-chains-0_en

7. CONCLUSIONES

Las implicaciones jurídicas, éticas y otras, tales como en materia de políticas públicas en relación con su impacto económico y social, a las que da lugar y que se plantean en relación con la impresión 3D requieren que se lleve a cabo una aproximación que considere todos los aspectos, ya que de lo contrario se podrían limitar indebidamente los derechos digitales de los usuarios en el caso de que estos sean personas físicas.

Por lo que se refiere a las implicaciones jurídicas, la impresión 3D plantea todavía numerosas interrogantes en varias áreas del Derecho que requieren de análisis para, en última instancia, conseguir que el marco jurídico esté alineado con la innovación tecnológica, de manera que ello facilite alcanzar los beneficios que aquélla ofrece.

En estrecha relación con lo anterior, las implicaciones éticas, en particular, de la impresión 3D y, en general, de la innovación tecnológica, especialmente cuando esta se aplica en ámbito como el relativo a la salud requieren de atención específica.

Por último, la impresión 3D tiene otras implicaciones, en términos de políticas públicas, que habrá que considerar tanto a nivel nacional como internacional, dado que actualmente nos encontramos ante rápidos cambios tecnológicos en un escenario claramente marcado por la globalización.

CAPÍTULO 36

LA PROPIEDAD INDUSTRIAL EN EL ECOSISTEMA DIGITAL

ANTONIO CASTÁN PÉREZ-GÓMEZ
Socio Elzaburu, S. L. P.
Profesor Universidad Pontificia Comillas

1. PREMISAS GENERALES PARA MEDIR EL IMPACTO DE LO DIGITAL SOBRE LOS DERECHOS DE PROPIEDAD INDUSTRIAL.
2. MANIFESTACIONES DE LA INCIDENCIA DE LO DIGITAL EN LOS DERECHOS DE PROPIEDAD INDUSTRIAL.
   - 2.1 El crecimiento de las invenciones en el campo de las tecnologías 4IR y el cambio de jugadores en la partida por la innovación.
   - 2.2 El cambio de modelo de negocio.
   - 2.3 El riesgo de las patentes frente al propio desarrollo digital.
   - 2.4 Las nuevas formas de defraudación.
   - 2.5 La tramitación de expedientes y la toma de decisiones por las autoridades administrativas.
3. LAS POSIBLES LÍNEAS DE ACTUACIÓN EN ARAS A ASEGURAR UN IMPACTO POSITIVO DE LO DIGITAL SOBRE LOS DERECHOS DE PROPIEDAD INDUSTRIAL.
   - 3.1 La falta de un marco normativo y la voluntad explicitada por la Unión Europea de tomar la iniciativa.
   - 3.2 La necesidad de apoyar la innovación dirigida a la industria digital.
   - 3.3 La necesidad de revisar el régimen sustantivo asociado a las invenciones propias de la tecnología digital.
   - 3.4 La necesidad de reforzar los instrumentos procesales frente a las nuevas formas de defraudación y de soslayar al mismo tiempo el uso inadecuado de los derechos de propiedad industrial frente al desarrollo digital.

1. PREMISAS GENERALES PARA MEDIR EL IMPACTO DE LO DIGITAL SOBRE LOS DERECHOS DE PROPIEDAD INDUSTRIAL

De un tiempo a esta parte parece que toda disciplina jurídica esta llamada a enfrentarse a los retos que conlleva ese *tsunami* tecnológico, social, económico y cultural que ha venido en denominarse la C*uarta Revolución Industrial (4IR).* La *transformación digital* es una fenómeno rico en conceptos, técnicas y expresiones (*Inteligencia Artificial, Internet de las Cosas, Big Data, Blockchain, Robótica*) cuyo alcance último se nos escapa pero cuyos efectos se dejarán sentir en todas *las costas y orillas* (1).

El panorama, en realidad, no es nuevo para la propiedad industrial. Desde la consagración internacional de los derechos de patentes, marcas y diseños en la segunda mitad del siglo XIX con la aprobación del Convenio de la Unión de París de 20 de marzo de 1883 la propiedad industrial se ha visto sometida a un proceso de evolución permanente ante la necesidad de adaptarse a los cambios que el progreso tecnológico lleva consigo. Pero tal vez ahora la situación se revela un poco distinta.

Las sucesivas reformas de los textos legales no han dejado de ser como la cadena que se pone al neumático de un vehículo para poder subir la cuesta de un puerto cubierto por la nieve. Pero la cuestión ahora es si en adelante no habrá que pergeñar una rueda a prueba de incidencias climatológicas o pensar en otro tipo de vehículo impermeable a cualquier factor externo. Y es que la *revolución digital* está socavando buena parte de los principios sobre los que se asientan los derechos de propiedad industrial, está alterando las reglas del juego y está propiciando un relevo en los jugadores. Para muestra valga no uno sino dos *botones*:

— La propiedad industrial parte de un principio de territorialidad (el derecho se vincula a la concesión del título por un organismo nacional cuya decisión enmarca geográficamente el alcance del derecho) que contrasta vivamente con la *globalización* inherente al universo digital, ajeno a fronteras y demarcaciones espaciales; y

(1) *Vid.* Barrio Andrés, M.: *Derecho de los robots*, Wolters Kluwer 2018; Barrio Andrés, M.: *Internet de las cosas*, Reus 2018; de la Torre, I. y Torralba, L.: «La disolución tecnológica ya está aquí», en *Arcano* octubre 2017; Sánchez del Campo Redonet, A.: *Reflexiones de un replicante legal. Los retos jurídicos de la robótica y las tecnologías disruptivas*, Thomson Reuters Aranzadi 2016; Varios Autores: «Desafío a lo humano. La robótica y el transhumanismo, más allá de los límites», en *Revista Claves de razón práctica*, número 257, 2018.

— El derecho se configura como un *ius excludendi alios* que dota a su titular de un monopolio de exclusiva para explotar la invención en solitario, cuando las tecnologías digitales imponen nuevas formas colaborativas de creación y explotación donde las patentes tienden a ser consideradas antes como activos para el comercio que como instrumentos monopolísticos.

Por eso desde que la Unión Europea apostó en el año 2015 por la consecución de un Mercado Único Digital la propiedad industrial ha estado en el *punto de mira*. Si bien es cierto que el régimen de los derechos exclusivos se percibe como una barrera que puede de algún modo frenar las expectativas de la sociedad digital, no lo es menos que nadie discute que la propiedad industrial es el motor mismo que sostiene el impulso por el I+D en cualquier sociedad, en la medida en que garantiza el retorno a la inversión. Por lo demás, el impacto de las industrias asociadas a la propiedad industrial sobre la generación de empleo, el crecimiento económico y las balanzas de pagos es tan alto que ningún *profeta* del *paraíso digital* puede ignorarlo.

Parece inevitable que la pugna legítima e imprescindible por el advenimiento del Mercado Único Digital camine de la mano de la propiedad industrial, buscando sus propias sinergias y rehuyendo inútiles confrontaciones. Así parece haberlo entendido el Gobierno español al adscribir, mediante Real Decreto 903/2017, de 13 de octubre, la Oficina Española de Patentes y Marcas, órgano del que depende la concesión registral de marcas, signos y patentes, bajo la órbita del Ministerio de Energía, Turismo y Agenda digital.

Este artículo sólo pretende ofrecer una radiografía *de urgencia* sobre algunos de las interrogantes que saldrán tarde o temprano a colación a medida que los enigmas de la revolución digital se vayan aclarando y sea necesario tomar *las riendas* de la normativización.

2. MANIFESTACIONES DE LA INCIDENCIA DE LO DIGITAL EN LOS DERECHOS DE PROPIEDAD INDUSTRIAL

2.1 **El crecimiento de las invenciones en el campo de las tecnologías 4IR y el cambio de jugadores en la partida por la innovación**

El impacto de lo digital se manifiesta en primer término en un crecimiento exponencial de las invenciones relativas a las tecnologías que lideran la 4IR. Se ha dicho que a lo largo del último decenio se han triplicado las solicitudes anuales de patentes en el sector de la tecnología robótica(en especial los componentes de automoción y la industria electrónica y eléctrica) y que en los últimos tres años han aumentado hasta en un 54% las

patentes en los tres sectores relevantes: las tecnologías básicas (el software y hardware que permite la transformación de un objeto en digital y la conectividad), las tecnologías intermedias y las tecnologías que se refieren a su proyección industrial en los sectores más diversos (vehículos, hogar, cuidado personal, infraestructura).

El perfil de los solicitantes de patentes ha cambiado sustancialmente también. Sorprende advertir, por ejemplo, que empresas financieras han irrumpido con fuerza en la presentación de solicitudes de patentes en tecnología *blockchain* y que compañías transversales del mundo de las telecomunicaciones, las redes sociales o el comercio electrónico, tales como Google, Amazon, Facebook, Microsoft o Apple, acaparan no ya las patentes propias de la operatividad en la red, sino también aquellas que se refieren a la Inteligencia Artificial, la ciberseguridad, la automoción o el cuidado de la salud. El escenario puede ser desconcertante: la fabricación de vehículos puede depender no de una empresa de este sector sino de un gigante de la venta on-line de cualquier clase de productos. ¡Y un Banco puede ser titular de patentes de invención!

Desde un punto de vista *geopolítico*, también el panorama está cambiando. Los avances en la tecnología digital se concentran en un número reducido de países (Corea, Estados Unidos, China o Japón) y son estos lo que encabezan las listas de países con mayor número de solicitudes de patentes. Esta es precisamente la razón de que las autoridades europeas vean la necesidad de reformular las exigencias relativas a la inscripción como patentes de esta clase de invenciones, así como a su régimen regulatorio y de acceso de los bienes al mercado: si no se dan facilidades, la industria europea *perderá la carrera* y quedará expuesta a la dependencia tecnológica de otras grandes potencias.

Pero resulta además que el proceso mismo de *investigación y desarrollo* ha experimentado su propia transformación. La tecnología digital se lleva frecuentemente a cabo en *clusters* universitarios donde confluyen la inversión pública y la privada. El dinamismo del medio es tan intenso y complejo y la información tan exorbitada que pocas empresas pueden afrontar la investigación en solitario y los proyectos colaborativos, *joint venutres* y alianzas entre empresas radicadas muchas veces en diversos países se multiplican. Esta internacionalización de los equipos de investigadores provoca no pocas dudas sobre la titularidad de la invención y pone en jaque la territorialidad inherente a las concesiones registrales de corte *nacional*.

2.2 **El cambio de modelo de negocio**

Tradicionalmente las patentes se conciben como un activo que las empresas utilizan para preservar una situación de exclusiva que entraña una

ventaja competitiva en el mercado. La explotación comercial del objeto de la invención en condiciones monopolísticas es una idea esencial al derecho de patentes. En la tecnología digital esa idea se ha diluido en no poca medida.

Para empezar en el universo digital la noción de *mercado* se antoja demasiado pequeña. En la economía de la 4IR se prefiere aludir a «*ecosistema»:* un espacio virtual sin fronteras donde convergen plataformas globales que integran un conjunto ingente de productos, servicios y tecnologías interconectadas.

La propia Comisión ha reconocido que el uso de las patentes, en este *ecosistema digital*, ha devenido una compleja herramienta estratégica para las empresas, que trasciende con creces de su originaria *raison d'etre*, a saber, bloquear la competencia asegurándose la fabricación y venta de productos en un terreno acotado y deslindado. Sin embargo en las tecnologías digitales es cada vez más frecuente que las empresas investiguen y patenten desarrollos no con el propósito de amparar sus propuestas comerciales en el lanzamiento de nuevos productos, sino con el objetivo de licenciar directamente la tecnología sin necesidad de estar presente en el sector de la fabricación. El ejemplo pionero de Qualcom, en el sector de la telefonía móvil, ha sido imitado por no pocos agentes. Los liderazgos empresariales se basan ahora exclusivamente sobre un *portfolio* ingente de patentes, pertenecientes a una o varias empresas (los *pools* de patentes) que son explotadas por otros comercialmente a través del régimen de licencias.

Pero es que además está el hecho de que la tecnología digital exige *interoperatividad* e *interconexidad* entre los cientos de miles de patentes que pueden llegar a recaer sobre los componentes diversos de un mismo producto, de manera que las licencias *cruzadas* entre empresas son inevitables si se quiere evitar una escalada imparable de la litigiosidad y una proliferación de *guerras procesales* que se suceden de país en país.

Si el mercado ya no es *mercado* sino *ecosistema* y el beneficio no reside en fabricar productos en un territorio *sin competencia* sino en licenciar patentes para que *todos* puedan explotarlas por un precio, la tipología de contratación prevista en las leyes ya no se sostiene y las patentes como objeto de propiedad pueden llegar a configurarse bajo perspectivas muy distintas a las actuales.

2.3 **El riesgo de las patentes frente al propio desarrollo digital**

Los nuevos modelos de negocio descritos en el punto anterior no siempre presentan un *rostro amable* ni resultan beneficiosos para el sistema en su conjunto. La economía digital se puede ver obstaculizada en su desarrollo por la aparición de ciertas anomalías o disfunciones en esa

actividad comercial. La terminología varía, aunque los efectos son los mismos.

Desde hace tiempo se habla de *patent thickets*, una densa red de solapamiento de miles de derechos de propiedad industrial, patentes en su mayoría, que deben ser analizados para determinar si un nuevo producto o tecnología se encuentra a salvo de infracciones y puede ser lanzado al mercado sin riesgos; se denuncia la actuación de las *Non-Practising Entities (NPE)*, empresas que ni inventan ni explotan patentes sino que compran carteras de patentes para amedrentar a otras empresas con el ejercicio de acciones judiciales, con medidas cautelares de por medio, forzando la suscripción de contratos de licencia bajo condiciones no negociables; y se señala con el dedo o se bautiza a alguno de estos personajes con el nombre de cierta molesta criatura mitológica noruega, los *patent trolls*, para enfatizar los efectos perniciosos que comportan sus prácticas comerciales.

Esta multiplicación de patentes en manos de empresas para las que el título registral constituye no más que un instrumento *recaudatorio,* un pretexto para el lucro, puede llegar a colapsar el desarrollo tecnológico y la emprendiduría. Sólo las empresas más fuertes, poseedoras normalmente de sus propias carteras de patentes, pueden hacer frente a este fenómeno. Pero una pequeña y mediana empresa ¿cómo podría afrontar el análisis del millar largo de patentes que recaen sobre un simple teléfono móvil para saber si puede lanzar un desarrollo tecnológico sin temor a ser demandada?

2.4 **Las nuevas formas de defraudación**

Para el derecho de marcas la revolución digital, al margen de algún que otro socavamiento (anecdótico o no) de la tipología de signos distintivos (las marcas holográficas, por poner un ejemplo) sólo ha traído consigo hasta el momento un aumento exponencial, cuantitativo y cualitativo, de las formas de defraudación. No es una crítica a Internet (que es un vehículo positivo en todo caso para la expansión comercial de cualquier empresa) sino una reflexión sobre el incremento de los riesgos que las marcas deben afrontar en el nuevo escenario.

No es solamente el tráfico de mercancía falsificada a través de la red *(la piratería on line)* cuyo medio hace estéril los instrumentos habituales de defensa mediante las medidas en frontera o la acción policial. Es también la apropiación de marcas a través de nombres de dominio (*cibersquatting*); la clonización íntegra de la página web de una marca para desviar órdenes o dañar su prestigio; los supuestos de *hasking* y *phisihing* o la utilización de las redes sociales para cometer actos de engaño o denigratorios frente a una marca.

El entorno digital ha llevado a las Agencias de *publicidad* a llamarse *empresas de comunicación*, porque los anuncios de una marca y la compra de productos parten de la interactuación, consciente o no, del Internauta a través de un teléfono móvil. Si un usuario se interesa por un determinado modelo de automóvil a través de la red, puede recibir en el acto una propuesta comercial de un modelo de la competencia con mejores prestaciones y un precio más bajo. El uso de algoritmos y la propia ingenuidad del usuario han podido propiciar estas nuevas formas de publicidad que enfrentan a las marcas a situaciones que antes no vivían.

No se puede medir por el mismo rasero, huelga decirlo, unos comportamientos y otros. Pero lo importante es que la actividad de las marcas y los diseños se desenvuelve ahora en un entorno cambiante donde los derechos son puestos a prueba en un contexto para el que el régimen tutelar no estaba preparado.

2.5 **La tramitación de expedientes y la toma de decisiones por las autoridades administrativas**

El universo digital hace tiempo que ha alcanzado a la actuación de la Administración en la tramitación de los expedientes registrales de concesión de marcas, patentes o diseños. La comunicación en línea del interesado con las oficinas de depósito en todas las fases del procedimiento es una realidad en instituciones *europeas* (La *European Union Intellectual Property Office EUIPO* o la *European Patent Office EPO*) y un objetivo declarado y en vías de cumplimiento en lo que respecta a la Administración española (la Oficina Española de Patentes y Marcas). Pero esto son minucias al lado de que lo que está por venir.

La utilización de máquinas inteligentes con capacidad para aprender (*deep-learning)* que tienen la habilidad para procesar millones de datos y analizarlos mediante criterios estadísticos, gracias al uso de algoritmos, puede muy bien en propiedad industrial llegar a desembocar en la toma de decisiones automáticas sin intervención humana. Pensemos, sin ir más lejos, en el requisito de la novedad en materia de patentes. La novedad implica que el objeto reivindicado en una patente no había sido descrito ni divulgado en el estado de la técnica anterior a su fecha de prioridad.

Para determinar si una invención es nueva es necesario confrontar su objeto con los documentos (anticipaciones) que integran ese estado de la técnica anterior. A estos efectos es preciso desmenuzar las reivindicaciones en los elementos que las integran (preámbulo y parte caracterizante) para cotejarlos uno a uno con los documentos de la literatura patente y no patente que por su cercanía pueden privarles de novedad. En algunos campos de la técnica este ejercicio implica la necesidad de procesar e identificar miles de patentes en todos los idiomas. Sin ánimo de dar por

sentada la respuesta, ni mucho menos, pero ¿no podrá ser más fiable, rigurosa y objetiva la decisión que pudiera adoptar una máquina en esta tesitura?

Este ejemplo es, desde luego, extrapolable al campo de los signos distintivos, donde la semejanza entre marcas a efectos de confundibilidad suele tomar en cuenta criterios y precedentes registrales y jurisprudenciales que procesados adecuadamente pueden llevar asimismo, no hay motivo para la alarma, a decisiones sin la intervención de los examinadores.

Es más que probable que el desarrollo de toma de decisiones automatizadas y basadas en algoritmos incida de forma creciente en la actuación de las Administraciones y es seguro que esta tendencia suscitará interrogantes nada despreciables. El principal tiene que ver con las garantías procesales exigibles para impugnar la decisión administrativa. Una resolución concediendo o denegando el registro de una patente, marca o diseño sólo puede ser impugnada si el proceso decisorio aparece reflejado con transparencia e inteligibilidad. La *ratio decidendi* tiene que venir expresada de forma tal que el interesado pueda cuestionar el enjuiciamiento llevado a cabo.

3. LAS POSIBLES LÍNEAS DE ACTUACIÓN EN ARAS A ASEGURAR UN IMPACTO POSITIVO DE LO DIGITAL SOBRE LOS DERECHOS DE PROPIEDAD INDUSTRIAL

3.1 **La falta de un marco normativo y la voluntad explicitada por la Unión Europea de tomar la iniciativa**

El desafío digital resulta todavía más excitante o inquietante, según el talante de cada cual, cuando se repara en que carece de todo marco normativo de referencia. El propio Parlamento Europeo ha constatado que no existe disposición jurídica alguna que pueda servir de guía en la actualidad. La expansión tecnológica digital, con efectos económicos y sociales devastadores, no dispone de cortapisas normativos que puedan encauzar ni limitar sus enfoques ni sus aspiraciones. Por estimulante que pueda parecer a priori un universo digital regido por sus propias inercias y ayuno de toda juridicidad, es claro que los riesgos para la sociedad son demasiado altos. En lo que atañe a los derechos de propiedad industrial, un desfase entre la ley y la realidad digital solo puede llevar a un debilitamiento del derecho y, por ende, al menoscabo del tejido empresarial e industrial que constituye uno de los pilares de la sociedad de consumo occidental.

En esta *carrera* por la normativización del universo digital es claro también que la Unión Europea se propone no quedar rezagada. El Parla-

mento Europeo ha expresado sin tapujos la voluntad de que Unión y sus Estados miembros conserven el control sobre la iniciativa legislativa y no queden a remolque de terceros países que se encuentran a la vanguardia de la robótica y la inteligencia artificial, por ejemplo.

Las pautas generales para un nuevo sistema legal ya han sido esbozadas, pero no sin un hálito de ingenua inconcreción y de buena voluntad. Se dice que el legislador debe ponderar las consecuencias jurídicas y éticas de la inteligencia artificial, pero debe apostar por una concepción flexible del derecho para no obstaculizar ni lastrar con ello la innovación. Se añade que las normas no deben afectar al proceso de investigación y desarrollo en el ámbito de la robótica. Y se repite hasta la saciedad que hay que evitar s*egmentaciones*, *bloqueos geográficos* y *restricciones territoriales*, ¿Cómo casan esos parámetros con una disciplina, como la propiedad industrial, que se asienta precisamente sobre exclusivas territoriales?

Para un Estado miembro de la Unión Europea la pregunta ahora es triple: si debe aguardar pacientemente a que los engranajes legislativos comunitarios *muevan ficha*, si debe participar activamente en impulsar las reformas a través de las instituciones comunes o si puede tomar la delantera aventurándose con cambios legislativos nacionales que podrían quedar más tarde en entredicho. Pero más allá de la respuesta que se pueda dar a estas preguntas, es claro que hay muchas cuestiones sobre las que se puede y debe suscitar una reflexión y otras que admiten una actuación individual.

3.2 **La necesidad de apoyar la innovación dirigida a la industria digital**

Un campo donde los Estados miembros no dependen inexorablemente de la iniciativa legislativa comunitaria es el apoyo a la industria que empuña la tecnología digital como estandarte. Este apoyo, cualquiera que sea la forma que revista (subvención, incentivos fiscales, facilitación de las estructuras jurídicas) se desdobla a mi modo de ver en tres planos:

— De un lado es necesario reconocer el esfuerzo, *acompañando* en la inversión, a aquellas pequeñas y medianas empresas que enfocan su espíritu innovador hacia las tecnologías propias de la revolución digital, en especial las llamadas *startups.* Las empresas emergentes deben encontrar en los poderes públicos un respaldo sin paliativos. No se trata de sustentar fiscalmente la investigación *en abstracto,* sino de premiar aquellas innovaciones que merecen su protección como patente y que presentan una proyección comercial. Solo los inventos que implican un bienestar social por-

que se traducen en propuestas reales de las que el ciudadano se beneficia, deberían ser objeto de apoyo.

— De otro lado es imprescindible también promover el uso de la tecnología digital entre las empresas, impulsando la *reconversión digital* de cuantos sectores puedan verse afectados. La adaptación al nuevo medio exigirá de la industria inversiones sustanciales y serán necesarias estímulos fiscales que contribuyan a vencer las naturales resistencias ante los cambios tecnológicos;

— Por último, habida cuenta la dificultad de la investigación digital en entornos aislados, será también imprescindible ofrecer un marco regulatorio flexible y estimulantes para iniciativas que promuevan la colaboración entre investigadores, empresas e instituciones públicas y privadas, la creación de *joint-ventures*, las fusiones y alianzas entre empresas, la suscripción de licencias cruzadas, las nuevas prácticas de colaboración en la investigación digital o la transferencia de tecnología.

Una política proactiva de los poderes públicos hacia el desarrollo de la tecnología digital y de los derechos de propiedad industrial que le son inherentes no consiste sólo en la *subvención* o en el *inventivo fiscal*. Hay que pensar en las estructuras jurídicas que en los distintos ámbitos (societario, universitario, empresa pública) hacen posible compartir esfuerzos y capitales en aras a un proyecto común.

3.3 **La necesidad de revisar el régimen sustantivo asociado a las invenciones propias de la tecnología digital**

El régimen positivo de las patentes de invención es difícil que pueda sustraerse a una revisión de buena parte de sus postulados a la luz de los impulsos de la transformación digital. Sin ánimo alguno de exhaustividad, cuando menos se puede hacer referencia a varios aspectos.

a) El crecimiento de la tecnología asociada a la 4IR afecta ante todo al régimen de *invenciones patentables*. Tradicionalmente el derecho de patente ha excluido del ámbito de las invenciones patentables algunas que se encuentran en el eje mismo de la revolución digital. Me refiero a temas tales como las ideas, los métodos matemáticos, los planes de negocio o los programas de ordenador. En el entorno digital las invenciones ejecutadas a través de un software o los algoritmos son el caballo de batalla de no pocos desarrollos tecnológicos y su encaje bajo los encorsetados lindes del derecho de patentes actual no es en absoluto pacífico.

El problema, si es que debemos conceptuarlo como tal, es que ante la falta de una cobertura suficiente bajo el paraguas del derecho de paten-

tes, la tecnología digital deberá buscar amparo en otros regímenes tutelares como podría ser el *secreto industrial*. Y en estos otros terrenos la posibilidad de una intervención *oficial* que supervise la *bondad* del derecho es más dudosa. Pero hay algo más: sólo el derecho de patentes garantiza el progreso tecnológico, en la medida en que hace posible la divulgación del objeto patentado. ¿Qué pasaría si los avances en la tecnología digital quedasen amparados por una disciplina que hace del *secreto* su razón de ser?

Sólo una revisión del capítulo de las invenciones patentables bajo el prisma de la apertura de miras puede evitar una migración de la tecnología digital hacia esos otros ordenamientos.

b) La revolución digital afecta también, qué duda cabe, al ámbito de las *excepciones a la patentabilidad*. En el Derecho de patentes no podrán ser objeto de patentes las invenciones cuya explotación comercial sea contraria al orden público o a las buenas costumbres. Aunque el orden público y las buenas costumbres constituyen un *cajón de sastre* donde caben las hipótesis más diversas, con algunas de las manifestaciones de la tecnología digital podía no ser suficiente.

Lo cierto es que cada vez son más las voces que se alzan para llamar la atención sobre los riesgos que la robótica conlleva sobre la seguridad y la salud humana, así como sobre sus consecuencias sociales y medioambientales. Se dice, textualmente, que hay factores susceptibles de poner en peligro a la población; se aboga por el establecimientos de Códigos de Conducta en torno a un *principio de beneficencia* directamente inspirado por las célebres *leyes de Asimov* (los robots deben actuar en beneficio del hombre y no dañar nunca a alas personas); y se propone incluso la constitución de Comités de Ética de la Investigación que sean quienes controlen y supervisen la investigación tecnológica para salvaguardar estos principios.

Lógicamente estas prevenciones ante los derroteros, o mejor dicho, las desviaciones, que puede tomar la investigación en la 4IR, deberán tener reflejo explícito o implícito en el procedimiento de registro de las patentes. En buena lógica aquellas patentes que pueden poner en riesgo a la población, por una transgresión de las leyes de la robótica y los Códigos de conducta, deberán tal vez incorporarse al catálogo de excepciones a la patentabilidad.

c) En el escenario colaborativo actual de los procesos de investigación en tecnología digital, donde los equipos de una o varias empresas se multiplican y las investigaciones se desarrollan en paralelo en países diversos, la noción legal de «*inventor*» y las normas que regulan la *titularidad sobre la patente* deberán ser objeto también de revisión. La posibilidad de que la investigación se lleve a cabo simultáneamente por inves-

tigadores en el marco de una relación laboral, por personal investigador de Universidades públicas y/o por miembros de Entes Públicos de Investigación, pondrá aún más a prueba la idoneidad de las normas existentes para solventar cualquier situación.

Puede darse el caso, sin recurrir en exceso a la fantasía, que la invención sea fruto directo de la utilización de máquinas con inteligencia artificial diseñadas específicamente para encontrar soluciones técnicas a partir de análisis estadísticos de los problemas técnicos existentes, de los métodos conocidos hasta la fecha y de las propiedades que presentan los materiales o ingredientes que la naturaleza pone a nuestro alcance. La configuración *subjetiva* del derecho tampoco permanecerá invariable.

d) La defensa de una concepción elástica de las invenciones patentables para acoger a las nuevas tipologías que afloran en el universo digital no es incompatible con la necesidad de postular una interpretación restrictiva de los *requisitos de validez* de las patentes. Se ha dicho, no sin razón, que el Mercado Único Digital necesita de patentes *de calidad* y que son rechazables aquellas patentes que resultan *insuficientes, triviales y poco desarrolladas*. Las exigencias de novedad, de actividad inventiva y de suficiencia en la descripción deben ser juzgadas con toda severidad si no queremos que el derecho de patentes, como antes se apuntaba, devenga una bola de nieve que conforme avanza se va haciendo cada vez más grande, arrastrando todo a su paso y haciendo imposible cualquier medición, hasta provoca el colapso mismo del sistema.

e) Por último, la *interoperabilidad* y *conectividad* de las invenciones en buena parte de las tecnologías del universo digital obliga a pensar, en lo que se refiere a los *efectos del derecho*, en cómo habrá de configurarse el régimen de la patentes dependientes (aquellas que no pueden ejecutarse sin la ejecución misma de otra patente anterior) y en una potenciación de los sistemas de *normalización* y *estandarización* tecnológica (*Standard Essential Patents*) que garanticen una aplicación equitativa del régimen de licencias FRAND (*Fair Reasonable and Non-Discriminatory*). Estos regímenes de estandarización, donde la exclusiva se transforma en un sistema de licencia *legal* sujeto a condiciones contractuales equitativas, *violenta* en cierta medida el fundamento mismo del derecho de patentes, pero resulta inevitable si se quiere asegurar la consecución del Mercado Único Digital y el propio progreso tecnológico. Hasta qué punto la experiencia, no exenta de dificultades, del ETSI (European Telecommunication Standard Institute) es extrapolable a otros campos afines, es algo que podría dar que hablar en el futuro.

3.4 **La necesidad de reforzar los instrumentos procesales frente a las nuevas formas de defraudación y de soslayar al mismo tiempo el uso inadecuado de los derechos de propiedad industrial frente al desarrollo digital**

En la defensa judicial de los derechos de propiedad industrial en la era digital convergen al mismo tiempo dos tendencias contrapuestas. De una lado es necesario reforzar los instrumentos de defensa frente a las infracciones en la red, pero de otro no es menos necesario impedir el uso abusivo de los derechos cuando estos pueden llegar a frenar el desarrollo mismo del Mercado Único Digital.

No es poco el camino que se ha recorrido hasta ahora en cuanto al desarrollo de instrumentos sustantivos y procesales que facilitan la defensa del derecho frente a las infracciones *en la red*, pero es curioso que muchos de estos avances se circunscriben a los derechos de propiedad *intelectual* y pasan por alto la relación de *hermandad* que estos derechos presentan con respecto a la propiedad *industrial*. La actuación de los *intermediarios* en la Sociedad de la Información, la responsabilidad como infractores *indirectos* de quienes inducen, cooperan o se benefician de la infracción, o la creación de un procedimiento de salvaguarda de carácter administrativo-cautelar frente a las infracciones en la red, son remedios concebidos *esencialmente* para los derechos de autor y que sólo encuentran vagas analogías en alguna que otra norma del derecho de patentes.

Pero al mismo tiempo ningún ordenamiento puede tolerar la concentración abusiva de un número ingente de patentes en manos de empresas que sólo pretenden ejercer acciones judiciales para obtener un beneficio económico. En los casos de *patent trolls* cabe preguntarse si el privilegio que supone la concesión de un monopolio se justifica o no en razón de la recompensa que merecen (o no) este tipo de entidades por su aportación (o falta de ella) al progreso de la técnica.

Da la impresión que el recurso al Derecho de la Competencia como única cortapisa frente a un ejercicio abusivo del derecho de patentes puede ser insuficiente. Tal vez una limitación en el uso de ciertos instrumentos procesales, como las medidas cautelares *inaudita altera parte*, podría ser deseable.

Por lo demás, en esta tesitura de acciones judiciales en materia de patentes sobre tecnología digital, donde la complejidad técnica puede alcanzar niveles estratosféricos, tampoco sería descabellado pensar en la necesidad de promover centros públicos de investigación que puedan desempeñar un papel *pericial* al servicio de los interesados o de los órganos jurisdiccionales. Este tipo de entidades puede servir a un tiempo para reforzar el ejercicio de la acción judicial y para salir al paso de un ejercicio abusivo del derecho.

3.5 **La reorientación de las profesiones liberales asociadas a la propiedad industrial**

Son muchos los indicios que invitan a pensar que algunas de las profesiones que giran en torno a la propiedad industrial deberán *reinventarse* para poder sobrevivir en el entorno digital cuando este alcance sus últimos desarrollos.

Una primera idea es que aquellos servicios que radican en la mera búsqueda de antecedentes y procesamiento de datos, particularmente en el contexto del *prior art* de las patentes de invención, están llamados a desaparecer *en la forma en que se conocen actualmente* La mejor *excelencia profesional* no podrá superar la capacidad de máquinas inteligentes para identificar, clasificar y gestionar en un espacio de tiempo insignificante y entre cientos de miles de documentos aquellos que señalan el estado de la técnica más próximo a la invención cuya validez debe ser enjuiciada.

Una segunda idea es que aquellos servicios que se dirigen a la realización de tareas de escaso valor añadido, como las traducciones en el trance de validación de las patentes europeas o las simples presentaciones de solicitudes, por más que la intervención del profesional *dignifique* jurídicamente el proceso, difícilmente podrán competir con el perfeccionamiento paulatino de los instrumentos alternativos que las propias administraciones promueven mediante conexiones *on-line* gratuitas.

Una tercera idea es que la globalización digital arrastra consigo, nos guste o no, una acentuación de la internacionalización de la propiedad industrial que cristaliza en propuestas como la del *Sistema de la patente europea con efectos unitarios*. No es sólo que los títulos registrales tenderán a sobrepasar las fronteras mediante oficinas de depósito transnacionales, algo que es una realidad en materia de marcas desde hace ya tiempo; es que también ejercerán funciones transfronterizas los *tribunales* que deberán enjuiciar las acciones basadas en tales títulos o encaminadas a su anulación. Es claro que los tribunales deberán mirar sin prejuicios el sacrosanto principio de la soberanía jurisdiccional y acostumbrarse a convivir, si el proyecto sigue adelante, con *experiencias* tan novedosas como el Tribunal Unificado de Patentes.

Una cuarta idea es que pocos de los servicios profesionales que se dirigen a la gestión y administración por las empresas de sus activos inmateriales (los portafolios de marcas, diseños o patentes) podrán ser prestados sin el uso de plataformas colaborativas e interactivas que permitan la comunicación y el trabajo *en la nube*. Estos servicios, además, tendrán menos protagonismo en comparación con el asesoramiento técnico y estratégico en la investigación y explotación comercial de invenciones en las

nuevas ramas de la Ciencia *digital* o en materia de la adopción y licenciamiento de signos distintivos.

Nada de esto debe ser interpretado en términos negativos, lastimeros ni nostálgicos. Al contrario, la revolución digital es la que acabará por conseguir el definitivo a*ggiornamento* de las profesiones asociadas a la propiedad industrial para corroborar, antes que diluir, el fundamento mismo en que descansan. Y es que la orientación estratégica, la interpretación de las normas y de la jurisprudencia, la negociación en operaciones contractuales complejas, el asesoramiento prudencial tendente a minimizar los conflictos o la defensa judicial del derecho son desempeños donde seguirá pesando la intervención de profesionales especializados.

No hay que olvidar, en fin, que la propiedad industrial es un semillero de conceptos jurídicos indeterminados («usuario informado», «público relevante», «experto en la materia», «riesgo de confusión», «notoriedad», «actividad inventiva») donde difícilmente el criterio de un profesional (de un ser humano, se entiende) podrá ser sustituido por la aplicación de procesos automatizados propios de la Inteligencia Artificial.

4. CONCLUSIÓN

Es evidente que el universo digital invita a un *viaje*, uno más, en esa expedición interminable en la que se encuentran inmersos los derechos de propiedad industrial e intelectual desde su origen, obligados a buscar nueva rutas ante el agotamiento de los *recursos naturales* que rodean sus perímetros. Pero como en todo viaje es imprescindible contar con un *puerto de amarre*, una suerte de *Itaca* a la que poder asirse para no perder el rumbo, un timón que permita sortear las tempestades con la esperanza de alcanzar de nuevo *tierra firme*. Y aunque el símil suene rancio porque el universo digital apela a la *nube* como horizonte, tampoco es mala cosa aferrarse a ciertos principios.

Tengo para mi que en lo que respecta a la propiedad industrial tal vez ese *puerto* no sea otro que la necesidad de recompensar a quien *innova* esto es, a quien desde la técnica, el diseño o el signo mercantil invierte en transformar la realidad conocida para mejorar la vida de la comunidad. El privilegio que supone la exclusiva siempre ha sido fruto de la necesidad de premiar la creatividad, la singularidad, la originalidad, el esfuerzo empresarial. Y no hay razón para que el derecho, en estas circunstancias, sufra una merma en su contenido y alcance por el hecho de pasar de la tecnología analógica a la digital.

Al comienzo de este artículo recordaba el nacimiento de la propiedad industrial al hilo de la revolución industrial, con la suscripción de un Convenio Internacional que ha sobrevivido más de un siglo. Quizás ahora con la irrupción de esta Cuarta Revolución Industrial, tan disruptiva con res-

pecto a las anteriores, sea tiempo de pensar en abrir la espita hacia un nuevo instrumento internacional que siente las bases y las reglas del juego en el escenario digital.

En esa tesitura cabe concluir que los derechos de propiedad industrial deben estar en la *cresta de la ola*, y no tomando el sol en la playa, cuando el *tsunami digital* toque tierra. Y es dudoso que un país aislado –o un conjunto de ellos– pueda afrontar todos estos retos sin severo riesgo de equivocarse.

CAPÍTULO 37
LOS *E-SPORTS*

ALBERTO PALOMAR OLMEDA
Profesor Titular (Acred.) de Derecho Administrativo. Magistrado
RAMÓN TEROL GÓMEZ
Profesor Titular de Derecho Administrativo
Universidad de Alicante

1. EL FENÓMENO DE LAS COMPETICIONES DE VIDEOJUEGOS: UNA ACTIVIDAD EN CLARA EXPANSIÓN

Es un hecho que el crecimiento del sector de los videojuegos desde que en 1980 la empresa Atari organizara una competición entre los usuarios del popular videojuego *Space Invaders,* hasta el día de hoy, puede calificarse de espectacular. No sólo por la implantación cada vez más generalizada de internet que permite la participación en línea de multitud de jugadores, sino también por el grado de desarrollo y atractivo de los videojuegos mismos.

Con esos ingredientes, ya en 1997 se creó en Estados Unidos la primera empresa que explota competiciones en videojuegos con el nombre de

Cyberathlete Professional League (CPL), surgiendo a partir de ahí eventos y torneos que cada vez concitan mayor interés. No ya por el número de participantes, sino incluso por el de espectadores que siguen estas competiciones. Incluso en la popular plataforma *Youtube* hay multitud de canales dedicados en exclusiva a comentar y seguir tales eventos, destacando muy especialmente la plataforma *Twitch*, consagrada a este sector y con un éxito ciertamente considerable (1).

La proliferación de organizaciones que explotan este sector es otro hecho, y son muchos los países que cuentan con equipos, pero Estados Unidos y Corea son los que suben a más jugadores a los podios. Todo, a una velocidad de vértigo, creándose la *World eSports Association* (WESA) en mayo de 2016 (2). Previamente, y con estructura organizativa de Federación internacional está la *International eSports Federation* (IeSF), con sede en Seúl, que comenzó a funcionar en 2008, siendo ya muchas las entidades que organizan ligas tanto regionales como nacionales.

Competiciones estas que abarrotan estadios y baten records de audiencia en las distintas plataformas audiovisuales en que retransmiten los encuentros, lo que atrae a patrocinadores e inversores y lleva a que haya jugadores de videojuegos profesionales, que han convertido esa actividad en un modo de vida en algunos casos muy lucrativo, pudiendo alcanzar ganancias de hasta 2.796.311,37 euros en el juego *Dota 2*, o 877.455,15 en el *League of Legends*, donde destacan los jugadores coreanos (3).

A nivel mundial se estima, tal y como indica la consultora NEWZOO, que los ingresos globales que generarán los *e-sports* llegarán a los 906 millones de dólares en 2018, lo que supone un crecimiento interanual del 38.2%, generándose en Estados Unidos 345 millones, y en China 164 de ese total. Estima asimismo que marcas y patrocinadores invertirán 694 millones en la industria de los *e-sports*, que crecerá a 1.400 millones de dólares para 2021 (4). Más optimista es otra consultora especializada, SUPERDATA, que prevé un crecimiento del 26% para 2020, alcanzando unos ingresos globales de 2.300 millones en ese año (5).

---

(1) Fundada en 2011, es la principal red social de aficionados y jugadores de videojuegos, con casi diez millones de usuarios activos al día en la plataforma. Aquí se emiten vídeos de las partidas de videojuegos que comparten y comentan los propios usuarios con otros. Las cifras que se manejan son ciertamente elocuentes, con más de dos millones de emisiones individuales al mes. Su dirección electrónica es: https://www.twitch.tv/.

(2) Sobre ello, Rosell Llorens, M., «Los eSports: una nueva realidad deportiva», *Revista Aranzadi de Derecho de Deporte y Entretenimiento*, n.º 52, 2016, pp. 220-224.

(3) *La Vanguardia*, 9 de septiembre de 2017, p. 29.

(4) Puede consultarse su informe *2018 Global Esports Market Report*, cuyo resumen ejecutivo está disponible en: https://newzoo.com/insights/trend-reports/global-esports-market-report-2018-light/ (26.3.2018).

(5) Superdata, *Esports Courtside: Playmakers of 2017*, december 2017, disponible en: https://superdata-research.myshopify.com/products/esports-courtside-playmakers-of-2017-esports-market-brief (27.3.2018).

También, específicamente en lo que se refiere a los eventos en directo de competiciones de videojuegos, DELOITTE avanza en un reciente y de mayor alcance estudio que se va a pasar de generar 325 millones de dólares en 2015 a 1.000 en 2018 (6).

La proyección de este sector en España es evidente y no resulta controvertida pues, de acuerdo con lo que indica el despacho ONTIER (7), contamos con la mayor competición exclusivamente nacional de Europa como es la Liga de Videojuegos Profesional (LVP), siendo además el único país de Europa en el que las tres principales operadoras de telecomunicaciones han entrado en el sector. De hecho, la plataforma Movistar+ ha incluido entre sus canales uno de competiciones de videojuegos, con lo que estamos hablando de una industria en plena expansión, sin duda, en lo que a nuestro país se refiere.

Asimismo, se considera que la facturación del sector en España va en nítida progresión, estimándose que se pasará de los 795 millones de euros en 2017 a 1.141 en 2019, pues España fue en 2016 el octavo mercado mundial de videojuegos. Un mercado mundial que mide ya su facturación en miles de millones de dólares, y en el que España tiene un nítido espacio para mejorar (8).

Evidenciadas las dimensiones del sector, el análisis que sigue se centra, esencialmente, en la concepción organizativa y de segundo nivel de la actividad en que las competiciones de videojuegos consiste, es decir, la que conecta con la prestación de servicios –organización de una actividad– que tiene una doble dinámica según se refiera a la participación de agentes en la actividad que se oferta o que se trate de la explotación comercial y *ad extra* de la actividad misma (9). A ello nos referimos seguidamente.

2. APROXIMACIÓN GENERAL A LA CUESTIÓN DESDE UNA PERSPECTIVA JURÍDICA

En un hecho que en la sociedad actual se plantean cada día actividades nuevas a las que la regulación jurídica llega, en muchos casos, a posteriori en razón a la propia evolución de la actividad que haya de ser obje-

(6) Deloitte, *Technology, Media and Telecommunications Predictions 2018*, p. 35, disponible en: https://www2.deloitte.com/cn/en/pages/technology-media-and-telecommunications/articles/tmt-predictions-2018.html (26.3.2018).

(7) Ontier, *Guía Legal sobre E-Sports. Presente y futuro de la regulación de los esports en España*, edición 2018, p. 12, disponible en: https://es.ontier.net/publicaciones/186/es/ (27.3.2018).

(8) *El País Negocios*, 4 junio 2017, pp. 2-5.

(9) Con mayor amplitud nos referimos a la problemática indicada en Palomar Olmeda, A. y Terol Gómez, R., *Régimen jurídico de las competiciones de videojuegos. La necesidad de un marco jurídico para los videojuegos en España*, Unidad Editorial, Madrid, 2017, y «Sobre la necesidad de un marco jurídico en España para las competiciones de videojuegos», *Revista Aranzadi de Derecho de Deporte y Entretenimiento*, n.º 57, 2017, pp. 199-251.

to de regulación y –desde luego– a la complejidad jurídica que acaba presentando la ordenación de la misma.

Por decirlo en términos sencillos, hay actividades que pasan del uso y el ejercicio individual a ser una práctica colectiva, con la presencia de actores muy diversos, en la que pueden aparecer elementos o valores que justifiquen el interés público en su regulación o, por el contrario, ubicarse en el marco general de las actividades económicas o asociativas en el que se desarrolla la actividad común de esta índole.

En este terreno se puede situar, en la actualidad, la problemática ordenación jurídica de las actividades relacionadas con los videojuegos cuando trascienden de una actividad diferente al uso individual (10).

Más en concreto, la práctica de competir con otros que juegan al mismo videojuego y su generalización, ya que puede hacerse esto tanto *on line* como presencialmente, ha traído incluso una nueva terminología que incluye conceptos como el de *gaming*, como referencia genérica a la actividad de competir jugando los videojuegos, y el de *gamer* para identificar al jugador, que puede ser incluso profesional. Práctica esta que como veremos se identifica también con el término ya universalizado de eSports (*electronic sports*), literalmente «deportes electrónicos» o competiciones de videojuegos, con las implicaciones que referiremos.

Las pautas de la transformación operada por la actividad son, relativamente, sencillas de entender y van desde la concepción inicial en la que el videojuego es, en realidad, una actividad personal, ligada a la compra de los derechos de una licencia o del uso de la misma, a una actividad que –sin perder el elemento central de la utilización de una licencia– se constituye en el soporte de otra más organizada en la que, primero, se produce una actividad competitiva que, ciertamente, no es sino la puesta en común de las habilidades en el ejercicio de lo que es el objeto de la licencia –el videojuego– y, posteriormente, se produce una organización de la competición que, simultáneamente, introduce otros elementos adicionales que superan el concepto de utilización individual de la licencia y que permiten la explotación y comercialización de la propia actividad tanto desde una perspectiva de los medios audiovisuales –clásicos y modernos– como de industrias ajenas que pueden considerar su actividad como elemento de soporte, como por ejemplo sucede con el juego y las apuestas,

(10) Téngase en cuenta que 155 millones de estadounidenses juegan regularmente videojuegos; que hay un porcentaje promedio de dos jugadores por casa; que el 51 por ciento de los hogares poseen una consola dedicada exclusivamente para jugar videojuegos; que el 42 por ciento de los estadounidenses juegan durante al menos tres horas a la semana, y que cuatro de cada cinco hogares estadounidenses contienen un dispositivo usado para jugar a los videojuegos. Datos extraídos del diario *La Nación* de 15 de abril de 2015. Disponible en http://www.nacion.com/blogs/jugador_1/Datos_y_estadistica_esenciales-videojuegos-2015_10_1481751811.html (21.3.2018).

que pueden tener por objeto los resultados y avatares de la propia competición de videojuegos (11).

Realmente se trata de entender que esa «organización» de la competición introduce diversos elementos adicionales de análisis y de conformación jurídica que transforman la concepción inicial de lo que viene a ser única y exclusivamente disfrutar o «jugar» al videojuego.

La organización de la actividad, en términos competitivos o de cualquier otra índole, introduce nuevos problemas o inseguridades en la propia sociedad que los utiliza, lo que vuelve de inmediato la vista a la Administración y a la necesidad de solucionarlos bien con una regulación pública si consideramos que finalmente el elemento central es el económico, o bien con la identificación de los problemas a los efectos de una solución de corte asociativa si, por el contrario, consideramos que el conjunto del entramado organizativo gira sobre la referencia de un vínculo no profesional para la realización de un actividad u objetivo común.

El primero de los nuevos problemas que se plantean es el relativo a la propia organización de los eventos competitivos. Se trata, claro está, de una actividad de servicios –la organización de la competición misma– ofertada por una entidad que tiene la condición de empresa desde una perspectiva puramente económica o comercial ya que su actividad opera en un mercado, presta servicios a terceros y, eventualmente, comercializa su propia actividad en mercados adicionales como pueden ser los del audiovisual y los de juego o apuestas.

Esa actividad empresarial se presta a priori en régimen de competencia, y se presenta ante la sociedad como una actividad sujeta a diversas legislaciones en función de las condiciones de participación, de la actividad que se ofrece y de la forma de establecer relaciones jurídicas frente al exterior. Es claro, por tanto, que queda sometida a las reglas que rigen las actividades económicas, desde una perspectiva, y a las reglas que protegen a los consumidores y usuarios desde la perspectiva de los que acceden a la práctica de la actividad misma.

El segundo bloque de problemas –en términos puramente enunciativos y secuenciales– es la articulación de la participación y los mecanismos jurídicos para llevar a cabo la misma por parte de los usuarios finales. De esta forma podemos anticipar que no puede considerarse igual una actividad en la que los participantes asumen una relación directa con el organizador de aquellos otros en los que la participación o incorporación a la

(11) La realización de apuestas sobre competiciones de videojuegos es ya toda una realidad. A la problemática que se plantea en Estados Unidos se refieren, por todos, los trabajos de Dobill, M., «Leveling (up) the Playing Field: A Policy-Based Case for Legalizing and Regulating Esports Gambling», *Loyola of Los Angeles Entertainment Law Review*, vol. 37, Issue 2, 2017, pp. 139-174, y Hardenstein, T. S., «Skins in the Game: Counter-Strike, Esports, and the Shady World of Online Gambling», *UNLV Gaming Law Journal*, vol. 7, Issue 2, 2017, pp. 117-138.

actividad se produce con la intermediación de una estructura jurídica diferenciada que asume, a su vez, la articulación, la ordenación y la presentación de los usuarios individuales.

Esta segunda posibilidad incorpora, a su vez, problemáticas difusas como la relativa a la relación del participante con la estructura asociativa que le integra en la «macro-organización» que ofrece el servicio competicional, entendiendo como decimos de ese modo la competición, en cuanto servicio que se presta.

Estos aspectos puramente introductorios tienen como único objetivo poner de relieve que la relación jurídica en cuestión va complicándose desde la concepción inicial muy centrada en el usuario individual que mantiene una relación con el fabricante o el proveedor del elemento central con el que se realiza la actividad, que es el videojuego. Es cierto, sin embargo, y no cabe negarlo, que esa concepción se sitúa en un segundo nivel de complejidad y que puede seguir conviviendo naturalmente con el primer nivel en el que se sitúa la persona que adquiere una licencia de videojuegos y los utiliza para su consumo y su entretenimiento personal sin otro esquema de relación ni de comercio.

De hecho, la complejidad se ha ido traduciendo, realmente, en la propia existencia y proyección de los editores –los creadores– de los videojuegos que no se limitan únicamente a la elaboración de un producto que se comercializa libremente, sino que pueden llegar a acuerdos para la comercialización con los promotores –de las competiciones–, y, en general la utilización no individual de los videojuegos que diseñan y licencian para su uso.

Esta concepción está muy cercana a la provisión de un servicio al mercado, a la delimitación de sus características y a la información sobre el mismo y, por tanto, a las condiciones de uso y de garantía que debe tener un producto de estas características. Se trata, en términos de ordenamiento jurídico, de un sometimiento, de una parte, a la legislación mercantil en lo que se refiere al contrato de compraventa para la adquisición del videojuego y a la legislación de consumo en lo que se refiere a la utilización, garantías, y derechos post venta, entre otros aspectos, del videojuego. A partir de aquí, las condiciones de utilización no individual se desplazan al ámbito contractual.

Cuando se supera esta concepción celular o básica y aparece una empresa que asume la concertación de usuarios individuales –presentados de la misma forma o incluidos en organizaciones asociativas o empresariales– y la realización de una actividad competitiva en cualquiera de sus formas, el proceso se complica y realmente aparece un servicio frente a terceros.

Es cierto que la definición de esta propia relación jurídica no es sencilla y entran elementos diversos en su configuración según que la oferta sea lucrativa, abierta, exclusiva, o mero divertimento, entre otros aspectos.

Este servicio –actividad económica– se plantea en el marco de un mercado diferente al primigenio del uso individual en el que lo que predomina es la organización y presentación pública de la actividad que convoca usuarios, patrocinadores, espectadores o televidentes. Se trata de una oferta de servicios consistente en la organización, resultados, realización y comercialización, que se ubica, de nuevo, a caballo entre la normativa mercantil propia –prestación del servicio– y la garantía del mismo frente a los que contratan-participan en la actividad, en las condiciones de participación, etcétera.

Es cierto, sin embargo, que esta prestación de servicios debe, adicionalmente, cumplir con las reglas de organización y de presencia en los mercados competitivos de forma que ha de respetar las reglas que aseguran la libre competencia y previenen la competencia desleal.

Esta actividad de servicios es o puede ser, ciertamente compleja ya que admite la prestación de servicios como elemento central pero la explotación del servicio admite, a su vez, formas adicionales como la venta de la imagen del evento, su comercialización en medios audiovisuales o, incluso, su vinculación a actividades económicas que toman los hechos ajenos como elemento central de su actividad, lo que es el caso del juego o la apuesta.

Estas formas de explotación se someten, igualmente, a las reglas mercantiles y de participación en los mercados y pueden estar vinculadas o independizadas de la relación entre el organizador y los agentes que participan en la actividad matriz.

Finalmente, si la actividad que se ofrece a terceros no permite la participación individual, sino que la participación debe realizarse mediante estructuras societarias o asociativas –agentes de participación al margen de su verdadera configuración jurídica– se plantean nuevas consideraciones y nuevos problemas que se desplazan, a su vez, a la propia organización y funcionamiento de los agentes de participación. Se trata, claro está, de una cuestión que habrá de resolverse en función de dos parámetros: la naturaleza jurídica del agente y la relación que se establezca entre éste y el usuario individual. Claramente, esta situación va a implicar la aplicación de nuevos parámetros jurídicos entre los que afloran la regulación laboral o de servicios mercantiles.

Los apartados que siguen tienen por objeto analizar los aspectos puntuales que se han mencionado en este apartado, como iremos viendo.

Es cierto que esta evolución no es únicamente jurídica y de estructura sino, sobre todo, de negocio y de caracterización de la actividad.

3. LA EXPRESIÓN *E-SPORT* Y LA PRETENDIDA NATURALEZA DEPORTIVA DE LAS COMPETICIONES DE VIDEOJUEGOS

En el contexto al que brevemente nos acabamos de referir surge la cuestión de la naturaleza jurídica o el encuadramiento de las competiciones de videojuegos en un sector del ordenamiento. Y lo cierto es que, de alguna forma, se han vuelto los ojos de forma inmediata a la regulación del deporte.

Esta referencia se debe a diversos factores. De un lado, la inexistencia de una regulación general de los videojuegos y la sensación contraria de que es una actividad que precisa de dicha regulación y, de otro, la existencia de un ámbito del entretenimiento con una enorme hiperregulación como consecuencia de una estructura consagrada tanto en el ámbito nacional como en el internacional que afecta o consagra dicha regulación y que determina los derechos y los deberes de quienes practican deporte.

La conjunción de estos factores unida, probablemente, a la propia concepción que, en el plano de los valores, tiene el deporte, llevaron a que una parte de la sociedad volviera los ojos al mundo del deporte como la panacea regulatoria, como el modelo regulado y ya asentado en el que habrían de encajar con naturalidad las competiciones de videojuegos.

Tal asimilación ha pesado incluso en la propia denominación de las competiciones de videojuegos como *e-sports*, lo que como ya vimos remite a «deportes electrónicos».

En este sentido y con carácter previo podemos indicar que la aproximación digital al mundo del deporte no supone más allá del 5% de la actividad, esto es, que de todos los videojuegos que se comercializan en el mercado, sólo ese porcentaje de videojuegos simulan competiciones deportivas en las modalidades deportivas clásicas. El resto de la actividad es una actividad de entrenamiento en el que se consiguen objetivos que propone el propio juego pero que no tienen que ver con la actividad deportiva.

Esta circunstancia es ciertamente relevante, pero nos enfrenta con un problema conceptual previo consiste en indicar si, desde la perspectiva de la actividad física que se realiza, estamos realmente ante un «deporte» electrónico.

Nos situamos aquí en un problema central: ¿pueden o deben conseguir los *e-sports* el reconocimiento del ámbito deportivo?. Más en concreto, podemos preguntarnos si realmente tienen o no la condición de actividad deportiva que, en nuestro ámbito, está constreñida a pasar por la condición de modalidad o especialidad deportiva, lo que requiere el reconocimiento expreso de la Administración como requisito previo a la constitución de la correspondiente Federación deportiva; reconocimiento que compete al Consejo Superior de Deportes (CSD) a nivel estatal y, en su caso, al órgano competente de la correspondiente Comunidad Autónoma.

Con carácter previo a pronunciarnos sobre el encaje en los indicados conceptos de modalidad o especialidad deportiva –lo que adelantémoslo es ciertamente complejo–, lo cierto es que el indicado reconocimiento no se ha producido aún en nuestro país.

La única regulación que hasta ahora se ha llevado en Europa al plano normativo ha tenido lugar en Francia, y la misma se ha articulado absolutamente al margen de la relativa al deporte.

Asimismo, sin perjuicio de anuncios puntuales de iniciativas de alguna Comunidad Autónoma de abordar algún tímido intento de regulación, como fue el caso del Gobierno de Canarias en las primeras versiones de un proyecto de ley del deporte (12), lo cierto es que la consideración de deporte de los *e-sports* plantea dificultades en nuestro país.

Al respecto, el Consejo General de Colegios Profesionales de la Educación Física y el Deporte emitió el 31 de octubre de 2017 un comunicado en el que señala que «... Es un hecho que los *e-sports* no han sido reconocidos como deporte o como modalidad deportiva por ninguno de los organismos competentes para tal fin en España y, en consecuencia, consideramos que no es congruente su inclusión en la legislación deportiva estatal o autonómica...», añadiendo que «... Si bien la práctica moderada de los *e-sports* puede conllevar un ejercicio mental que favorezca el desarrollo de determinadas capacidades como la concentración, la rapidez mental y/o la orientación espacio-temporal; estos juegos también suelen caracterizarse por una actividad física reducida (limitada a movimientos distales repetitivos con participación de pequeños grupos musculares) y el mantenimiento de posturas corporales (poco ergonómicas y ocasionalmente forzadas) durante períodos prolongados. En consecuencia, demandamos la necesaria participación de nuestros profesionales colegiados (garantía de máxima cualificación en entrenamiento y supervisión de ejercicio físico saludable) en la preparación multidisciplinar de los jugadores de *e-sports*, con el fin de que alcancen un nivel de acondicionamiento físico especíco que les permita minimizar posibles perjuicios y/o lesiones derivadas de este tipo de prácticas a nivel osteo-articular, circulatorio, muscular o nervioso» (13).

Sin perjuicio de ello, y en lo que a la organización deportiva internacional se refiere, no puede dejar de tenerse en cuenta el anuncio del Comité Olímpico Internacional de incluir competiciones de *e-sport* en el programa de los Juegos Olímpicos de París 2024, aunque no se han concretado

(12) En el momento de escribir estas líneas está en plena tramitación en Canarias un proyecto de ley del deporte que carece de referencias a esta cuestión, publicado en el *Boletín Oficial del Parlamento de Canarias*, IX Legislatura, n.º 32, 29 enero 2018, pp. 1-32.

(13) Publicado en *Revista Española de Educación Física y Deportes*, n.º 419, 4.º Trimestre 2017, pp. 89-90, a donde pertenecen los entrecomillados del texto.

aspectos como qué concretos videojuegos se van a jugar o qué organización o federación, de entre las existentes, se ocupará de las indicadas competiciones.

Otro punto de encuentro está en la prevención del dopaje en este ámbito, de lo que en el plano internacional se han ocupado organizadores de competiciones de videojuegos como la *Electronic Sports League* (ESL) o la *Esports Integrity Coalition* (ESIC), que fundada en 2015 por empresas del sector se ocupa de prevenir los problemas de integridad que puedan plantearse en las competiciones, incluido el dopaje.

Antes de entrar en el complejo encaje de los *e-sports* en la ordenación que para el deporte se ha establecido en nuestro país, vamos a detenernos en dos elementos esenciales del fenómeno deportivo que son la concepción de la propia modalidad deportiva y su estructura territorial, lo que en el caso de los *e-sports* es ciertamente peculiar.

4. EL COMPLEJO ENCAJE DEL FENÓMENO EN LA REGULACIÓN DEL DEPORTE EN ESPAÑA

Como se ha indicado, existen dos grandes nudos en la consideración de los *e-sports* como una actividad deportiva (14). Eso, y que además hay una particularidad adicional que se da en este ámbito y, en ningún caso, en el deporte tradicional: que sobre el objeto de la actividad –el videojuego– existen derechos de propiedad intelectual.

El primero de los señalado nudos está en el concepto de modalidad deportiva, pues de acuerdo con la Ley 10/1990, de 15 de octubre, del deporte, su reconocimiento por la Comisión Directiva del CSD y la consiguiente constitución de una Federación deportiva con la inscripción en el Registro de Asociaciones Deportivas del CSD, implica reconocer a sólo una Federación la exclusividad sobre la indicada modalidad deportiva (15). Modelo de reconocimiento que, en el plano autonómico, se reproduce en las correspondientes leyes ordenadoras del deporte de ese ámbito.

Tal reconocimiento de la modalidad deportiva es un acto administrativo anterior y previo al reconocimiento de la estructura asociativa llamada a gestionarla, lo que en el ámbito de los *e-sports* es, sin duda, uno de los problemas esenciales porque, muy a menudo, el concepto de modalidad está asociado a reglas comunes de práctica y a una práctica también uni-

(14) Un completo tratamiento de la cuestión está en la monografía de Rodríguez Ten, J., *Los e-sports como ¿deporte? Análisis jurídico y técnico-deportivo de su naturaleza y los requisitos legales exigidos*, Reus, Madrid, 2018.

(15) Establece al respecto el artículo 34.1 de la Ley 10/1990 que «Sólo podrá existir una Federación Española por cada modalidad deportiva, salvo las polideportivas para personas con minusvalía a que se refiere el artículo 40 de la presente Ley».

forme porque de hecho cuando se rompe el principio de uniformidad aparecen conceptos como las pruebas deportivas o las especialidades deportivas que muestran ya la existencia de especialidades. Es claro que los deportes, en el ámbito del deporte organizado o federativo, tienen una cierta tradición y responden a unas reglas más o menos uniformes que identifican un planteamiento común en la forma de practicar el mismo y de las habilidades y adiestramientos que deben cumplirse. A partir de ahí se escinden en modalidades deportivas y, posteriormente, en pruebas que articulan la forma concreta en la que se quiere realizar la actividad o competición deportiva en cuestión.

Desde luego, las competiciones de videojuegos no responden a ningún modelo tradicional, y hay que reconocer las dificultades que pueden existir y plantearse desde la Administración para identificar a partir de tal realidad una modalidad deportiva y sus distintas especialidades. Qué es la modalidad deportiva y qué la especialidad no es una cuestión baladí. Téngase en cuenta que, atendiendo a las *IeSF Competition Regulations* de septiembre de 2016, los títulos oficiales son, para videojuegos de equipo *League of Legends* (Riot Games) y *Counter Strike: Global Offensive* (Valve Corporation), y para videojuegos individuales *Hearthstone* (Blizzard Entertainment). Acomodar tal realidad a las categorías deportivas hay que reconocer que es ciertamente dificultoso, ya que cada juego puede tener unas características muy singulares (multijugador, equipos de más o menos jugadores, videojuegos de estrategia, de puntería…) resultando complejo encajarlos a todos en un mismo molde conceptual.

Piénsese en las clásicas modalidades de clasificación por edades y territorios que existen en el deporte convencional, y en su pésimo encaje cuando de *e-sports* hablamos.

El segundo nudo está en la necesidad de la implementación de la actividad sobre una estructura territorial. No se puede perder de vista que, asentándose la regulación del fenómeno deportivo en nuestro país sobre la organización federada, esta es piramidal. La organización deportiva oficial o federada es claro que está organizada, para cada modalidad deportiva de arriba abajo, piramidalmente, llegando del nivel mundial al nacional, pasando por el continental, a través de una muy consolidada estructura organizativa que abarca todos y cada uno de los rincones del planeta donde se practique el deporte en cuestión, de modo que el deportista, mediante la licencia federativa, se integra en la Federación territorial o autonómica radicada donde reside, esta a su vez se integra en la nacional o española, la cual lo está en una de carácter continental y ésta, a su vez, en la internacional correspondiente.

Es claro que los *e-sports*, en el sentido indicado, no tienen territorio, o este no es el elemento determinante de la actividad que desarrollan.

Siendo esto así la pregunta evidente es ¿qué aporta la estructura deportiva y por qué se han vuelto a la misma los ojos de los organizadores de la actividad de videojuegos ligados al deporte?.

Entendemos que, realmente, el problema es que la incipiente organización de los *e-sports* hace que ya se planteen problemas que, en cierta medida, son muy próximos a los que ha superado la actividad deportiva.

En este sentido, y sin ningún ánimo de exhaustividad podemos identificar, al menos, los siguientes:

a) La laboralidad de los trabajadores-jugadores profesionales de *e-sports* o *gamers* y, específicamente, el derecho de retención o de compensación que se plasma para los deportistas profesionales en el RD 1006/1985, de 26 de junio, por el que se regula la relación laboral especial de los deportistas profesionales.

b) La necesaria adopción de medidas adicionales para la protección de los jugadores cuando estos son menores de edad.

c) El tratamiento de los deportistas en forma diferente en el ámbito de las autorizaciones de permiso de trabajo y residencia, dada la internacionalización del fenómeno.

d) La organización de una liga como estructura que, además de resultar idónea para organizar una competición dilatada en el tiempo, reúne lícitamente los derechos sin afectar al derecho de la competencia.

e) La estructuración de los derechos de imagen y retransmisión deportiva sobre la base de la competición deportiva, como resulta clásico en el deporte convencional.

Esto nos permite indicar que el efecto óptico de que los importante es la actividad deportiva y sus reglas de funcionamiento no es en realidad tal de forma exclusiva, sino la necesidad de una regulación satisfactoria que responda a las necesidades de la actividad que se pretenda regular y, desde luego, dé solución satisfactoria a los problemas que puedan plantearse.

Vamos a referirnos, seguidamente, a la regulación del fenómeno que se ha llevado a cabo en Francia, siendo el primer país que se ha ocupado de ello y que, como adelantamos, lo ha hecho al margen de la ordenación del deporte.

5. REFERENCIA A LA REGULACIÓN DEL FENÓMENO EN FRANCIA.

La regulación la afrontó Francia con su Ley n.º 2016-1321, de 7 de octubre, por una República Digital (16), norma esta ciertamente compleja y de mayor alcance que lo referido a la actividad de competiciones de video-

(16) *Loi n.º 2016-1321 du 7 octubre 2016 pour une Republique numérique.*

juegos, que se ocupa –a lo largo de sus 113 artículos– de ordenar la utilización de las nuevas tecnologías de la información y las comunicaciones tanto en el ámbito de las Administraciones públicas como en las relaciones de estas con los ciudadanos y el acceso de estos a la información, entre otras muchas y variadas cuestiones (17).

De entre ellas los artículos 101 y 102 de la Ley se ocupan, respectivamente, tanto de las competiciones de videojuegos como de los jugadores, teniendo en cuenta que estos pueden ser profesionales. Así, y en primer término, el artículo 101 introduce en el Título II del Libro III del Código de la Seguridad Interior, un nuevo Capítulo rubricado «Competitions de jeux vidéo», donde se definen las competiciones de videojuegos indicando que «… enfrenta, a partir de un juego de vídeo, al menos dos jugadores o equipos de jugadores para puntuar u obtener una victoria. La organización de la competición de videojuego en el sentido del presente Capítulo no incluye la organización de una toma de apuestas» (art. L. 321-8), resultando precisa una autorización administrativa.

Dejando fuera los aspectos relativos al juego y las apuestas, la Ley remite al desarrollo reglamentario cuestiones como las condiciones en que puede autorizarse la celebración de competiciones de videojuegos con la presencia física de los participantes cuando se cobre a estos derechos de inscripción o se establezcan premios, más allá de las cantidades que se fijen por Decreto. Asimismo, se regularán por Decreto las condiciones en que se permitirá a los menores de edad participar en las indicadas competiciones.

El señalado desarrollo reglamentario está en el Decreto n.º 2017-871, de 9 de mayo de 2017, relativo a la organización de las competiciones de videojuegos (18), y que centra la atención en los organizadores de las indicadas competiciones. Establece la necesidad de obtener autorización del Ministerio del Interior para organizar competiciones de videojuegos, para lo que el organizador habrá de presentar la correspondiente solicitud como regla general con un año de antelación a la organización de la competición de videojuegos, salvo razones de urgencia, y en todo caso al menos antes de treinta días de antelación a la fecha de inicio de la competición.

A fin de asegurar la solvencia de la competición, de lo que da idea la documentación que se exige para autorizarla, se regulan los premios o cantidades que hay que abonar a los vencedores, el coste o gastos de la organización o los derechos de inscripción. Y en esta línea, se establece que deben

(17) Entre nosotros, una descripción del contenido de la Ley nos la ofrece Boto Álvarez, A., «Transformaciones estructurales en la Administración francesa: cuestiones éticas y tecnológicas», *Revista General de Derecho Administrativo*, n.º 44, 2017.

(18) *Décret n.º 2017-871 du 9 mai 2017 relatif à l´organisation des compétitions de jeux vidéo.*

garantizarse los premios a los participantes que superen los 10.000 euros, permitiéndose la suscripción de seguros para garantizarlos.

Otro aspecto en el que incide la norma es la protección de los menores, prohibiendo directamente que los que tengan menos de doce años de edad participen en competiciones de videojuegos que otorguen premios de naturaleza monetaria. Y para la participación del resto de menores, es imprescindible el consentimiento paterno expreso y por escrito. Permitir la participación de menores de edad en contravención de tales determinaciones, así como organizar competiciones de videojuegos sin haber aportado la documentación prevista en el artículo R.321-41 antes referido, está sujeto a sanciones.

En segundo término, el artículo 102 de la Ley n.º 2016-1321, tal y como hemos indicado, se refiere a los jugadores de videojuegos profesionales, y en su desarrollo se ha aprobado el Decreto n.º 2017-872, de 9 de mayo de 2017, relativo al estatuto de los jugadores profesionales asalariados de videojuegos competitivos (19), cuya entrada en vigor tuvo lugar el 1 de julio de 2017.

El artículo 102 de la Ley n.º 2016-1321 define al jugador profesional de videojuegos como aquella persona que recibe una remuneración por participar en tales competiciones teniendo un vínculo con una sociedad o asociación autorizada por el Ministerio competente *(ministre charge de numérique)* a tal fin.

Se establece además que la duración del contrato no puede ser inferior a doce meses, que es lo que se considera que dura una temporada en las competiciones de videojuegos, permitiéndose que pueda durar menos en determinadas circunstancias, como puede suceder si hay que sustituir a un jugador.

El contrato de trabajo que aquí se regula se declara de duración limitada, pues como máximo no puede exceder de cinco años, aunque puede renovarse o firmarse otro contrato con el mismo empleador, sin que resulte admisible la rescisión unilateral del contrato por parte del empresario. Se prevé que el contrato se tornará en indefinido si se vulneran las disposiciones establecidas en este artículo 102, que además prevé multas de entre 3.750 € y, en caso de reincidencia 7.500 € y seis meses de prisión.

El Decreto n.º 2017-872, en desarrollo del precepto indicado, se centra principalmente en los requisitos para autorizar o acreditar a las entidades o empresas para que puedan contratar a los jugadores de videojuegos, que deberán solicitarlo en incluir en la correspondiente solicitud, y que variarán según se trate de una asociación o de una entidad mercantil. En

(19) *Décret n.º 2017-872 du 9 mai 2017 relatif au statut des joueurs professionnels salariés de jeux vidéo compétitifs.*

este último caso, debe aportar la información que establece el artículo 4 del Decreto, centrada principalmente en las cuentas y estados financieros de la entidad en cuestión.

Presentada la solicitud de autorización, el ministro competente la otorgará si se cumple con las siguientes condiciones, que se establecen en el artículo 5 del Decreto: a) El objeto de la asociación o sociedad incluye la participación en competiciones de videojuegos; b) La asociación o empresa es capaz de proporcionar los recursos humanos y materiales para cumplir con el objeto para el que se solicita la autorización; c) La asociación o empresa ha ejecutado o planificado para sus jugadores profesionales entrenamiento y supervisión psicológica, física y profesional adaptado a su actividad, y d) Que los dirigentes de la asociación o sociedad no han sido objeto de una condena penal, ni de una sanción civil, comercial o administrativa de naturaleza prohibitiva para gestionar, administrar o dirigir una persona jurídica o ejercer una actividad comercial.

La autorización se otorga por un período de tres años renovables, pudiendo retirarse en caso de incumplimiento de los requisitos exigidos y, en particular, por no cumplir con las obligaciones legales en materia de salud y seguridad en el trabajo, realizar otras actividades o no respetar las restricciones al trabajo infantil que establece el artículo 101 de la Ley 2016-1321, ya señaladas.

6. ALGUNOS ELEMENTOS CLAVES EN LA JUSTIFICACIÓN DE LA NECESIDAD DE LA REGULACIÓN

Apuntadas las dificultades que plantea el modelo deportivo en nuestro país, y a la vista de la experiencia regulatoria en Francia, resulta claro que la verdadera naturaleza de las competiciones de videojuegos es la de una actividad de recreación y de ocio hecha en unas ocasiones desde un modelo o una estructura económica y, otras, desde una consideración meramente asociativa o voluntaria.

Esta opción conceptual nos lleva antes de cualquier otra consideración a la determinación de cuál sería la Administración de referencia que debería asumir la regulación fuera del ámbito deportivo y para ello es preciso analizar el régimen de distribución de competencias en el eventual establecimiento de una regulación sobre la materia. Situados en este plano cabe indicar que el artículo 148.1 CE establece que las Comunidades Autónomas puede asumir competencias exclusivas en «19.ª Promoción del deporte y de la adecuada utilización del ocio».

Esto nos lleva a indicar que la recreación y el ocio son, en principio, competencia de las Comunidades Autónomas. De hecho, los distintos Estatutos de Autonomía de las Comunidades Autónomas han ido asumiendo dicha competencia sin mayores dificultades.

Es cierto, sin embargo, que lo que resulta más confuso es la propia configuración del concepto de ocio o de recreación y la determinación de si la competencia de las Comunidades Autónomas precisa o incluye el conjunto de relaciones jurídicas y el régimen jurídico de los agentes que participan en los mismos. Este tema fue planteado en la STC 80/2012, de 18 de abril, señalando que «… En conclusión, el ejercicio de las competencias asumidas como exclusivas por las Comunidades Autónomas en sus respectivos Estatutos de Autonomía, tiene como límite el ejercicio de las competencias propias del Estado, bien como consecuencia de la concurrencia de otros títulos competenciales –como ocurre, por ejemplo, cuando la competencia del Estado en comercio exterior (149.1.10 CE) o sobre la planificación general de la economía (149.1.13 CE) se superpone a la competencia autonómica de turismo (STC 13/1988, de 4 de febrero, FF. 1, 2, 3 y 9, en materia de «ferias internacionales»)–; bien como consecuencia de la afectación de un interés nacional o –como señalamos en la STC 133/1990, de 19 de julio, (en relación con la materia «protección civil»)– de «la necesidad de prever la coordinación de Administraciones diversas, bien por el alcance del evento (afectando a varias Comunidades Autónomas) o bien por sus dimensiones, que pueden requerir una dirección nacional de todas las Administraciones públicas afectadas, y una aportación de recursos de nivel suprautonómico» (F. 6). Límites o condicionamientos que no excluyen *per se* la proyección extraterritorial o internacional de las competencias autonómicas cuando ello sea posible…».

El problema que plantea la regulación a la que nos referimos no es otro que la identificación del sector de actividad en el marco de la recreación y del ocio y, como consecuencia de ello, la posibilidad de que las diferentes Comunidades Autónomas puedan promulgar leyes en función de sus propios intereses que produzcan lo que, probablemente, es un efecto no querido como es la fragmentación de la regulación.

Tal fragmentación del respectivo mercado es, sin duda, un problema más agudo cuando la actividad no tiene un componente presencial esencial porque entonces se produce una ruptura entre la percepción que deriva de la territorialidad y la sensación de que la actividad global no debería quedar sometida a normas territoriales dispersas.

En este terreno se plantean dos elementos que han sido considerados en ocasiones como determinantes de la presencia regulatoria estatal, y que son: el factor de actividad supraautonómica, y la existencia de títulos de carácter estatal inequívocamente mezclados con los puramente territoriales.

En una materia con trascendencia económica y social la posibilidad de que el título de recreación o de ocio pueda ser ejecutado desde una perspectiva y una posición única es, ciertamente, dudoso. En la utiliza-

ción de los videojuegos a los que nos venimos refiriendo hay un componente de Derecho mercantil muy amplio, de Derecho de la competencia, de Derecho de los consumidores y usuarios, de Derecho procesal, de Derecho del trabajo. Todos estos títulos y algún otro que se pueden indicar presentan como característica que se trata de títulos competenciales esencialmente estatales.

De esta forma podemos indicar que, cuando existe una actividad económica que debe ser desarrollada en un mercado general lo razonable es pensar que la delimitación de los aspectos sustantivos de la regulación tiene también un alcance general que se incardina en los títulos competenciales del Estado y que, por tanto, le corresponden a éste su ejercicio.

Esta posibilidad que se ha dado en muchas ocasiones exige proyectar la relación matriz sobre la que corresponde a los agentes, a las obligaciones y, en general, al conjunto de los actos que se realicen. Y en esta línea, hay que destacar un ejemplo que guarda una importante semejanza al esquema que se acaba de plantear y que podemos encontrarlo en la normativa relativa al juego (20). De hecho, se trata de una normativa, esencialmente, autonómica asumida por el conjunto de las Comunidades Autónomas como normativa que les correspondía dictar en el ámbito de sus respectivos territorios y al haber asumido en sus Estatutos esta competencia como propia en defecto de una determinación explícita de la Constitución en la atribución de la competencia a alguna de las Administraciones autonómicas. Y conforme a este esquema se fueron desarrollando un conjunto muy amplio de normativas autonómicas que se centraron, esencialmente, en el denominado juego presencial, esto es el juego que tenía un importante componente territorial en tanto en cuanto su esencia y su referencia era, fundamentalmente, territorial y ligada a un ámbito de actuación del mismo límite.

En un momento determinado se plantea la posibilidad de introducir en el mercado el denominado «juego on line» que tiene diferentes características, siendo una de ellas, precisamente, la pérdida de referencia territorial y la posibilidad de proyectar la actuación sobre el conjunto del territorio.

Los operadores, de un lado, y, posteriormente, las propias Comunidades Autónomas llegan a la conclusión de que la gestión de un negocio global desde una concepción fraccionada y territorial plantea, sin lugar a dudas, muchos problemas y comienzan a abogar por la existencia de una norma estatal que supere el fraccionamiento de los mercados. Como señala el Preámbulo de la Ley 13/2011, de 27 de mayo, de regulación del juego (LRJ)

(20) A esta cuestión nos hemos referido en Palomar Olmeda, A., «La regulación del mercado del juego en España: justificación, modelo previsto y perspectivas de futuro», *En torno al Juego de Azar. Actividad, Regulación y Actores* (Palomar, A., Dir.), Aranzadi, Navarra, 2013, pp. 31-122, y en la obra colectiva *Memento Experto Deporte y Juego* (Palomar Olmeda, A. y Fuertes López, J., Coords.), Ediciones Francis Lefebvre, Madrid, 2015, pp. 251-518.

«…Las aludidas finalidades, así como la necesidad de dotar al sector del juego de una regulación adecuada, ha tenido su reflejo en distintas iniciativas parlamentarias y en mandatos al Gobierno como el establecido, en el ámbito nacional, en la Disposición adicional vigésima de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información y, en el ámbito comunitario, en la Resolución del Parlamento Europeo de 10 de marzo de 2009 sobre la integridad de los juegos de azar en línea…».

Este impulso, cuya justificación en términos competenciales es más que dudoso, se convierte, sin embargo, en la palanca en la que apoyar sólidamente una regulación estatal más demandada por el sector que derivada de un marco competencial relativamente claro.

Sea como fuere se produce la publicación de la LRJ que, en su Disposición Final primera determina que «Esta Ley se dicta en el ejercicio de las competencias exclusivas del Estado previstas en las reglas 6.ª, 11.ª, 13.ª, 14.ª y 21.ª del apartado 1, del artículo 149 de la Constitución Española…».

Esto nos lleva a indicar que, pese a que la competencia había sido asumida como propia por las Comunidades Autónomas, la Ley estatal se funda en títulos abstractos como la legislación civil y mercantil (6.ª Legislación mercantil, penal y penitenciaria; legislación procesal, sin perjuicio de las necesarias especialidades que en este orden se deriven de las particularidades del derecho sustantivo de las Comunidades Autónomas), en el sistema monetario (11.ª Sistema monetario: divisas, cambio y convertibilidad; bases de la ordenación de crédito, banca y seguros.); en la planificación económica general (13.ª Sistema monetario: divisas, cambio y convertibilidad; bases de la ordenación de crédito, banca y seguros.), la hacienda general y deuda del Estado (14.ª), o, las comunicaciones (21.ª Ferrocarriles y transportes terrestres que transcurran por el territorio de más de una Comunidad Autónoma; régimen general de comunicaciones; tráfico y circulación de vehículos a motor; correos y telecomunicaciones; cables aéreos, submarinos y radiocomunicación).

La lectura de los títulos competenciales señalados nos permite afirmar que, a priori, no existe un inconveniente teórico importante para que, en el ámbito de la utilización de videojuegos con carácter organizado y competitivo pudieran aplicarse los mismos títulos competenciales a los que nos acabamos de referir y que se sitúan en la periferia de la actividad pero que, realmente, inciden en el negocio en cuestión al regular el estatus de los que pueden participar en el mismo, el tipo y alcance de las obligaciones que pueden establecerse y las obligaciones o condiciones de la actividad en función de los intereses que se establecen.

A partir de esas determinaciones, la construcción del régimen jurídico que ordene las competiciones de videojuegos habrá de tener en cuenta los principios que establece la Ley 20/2013, de 9 de diciembre, de ga-

rantía de la unidad de mercado. Y desde luego, el marco que proporciona la Ley 15/2007, de 3 de julio, de defensa de la competencia.

Todo un reto afrontar la regulación, aunque no ha de perderse de vista que se trata en España de un sector en plena expansión, en crecimiento. Como indica la Asociación Española de Videojuegos (AEVI), este «... Es un sector en crecimiento, pero todavía inmaduro. La agencia Play The Game cifró los ingresos en España en 4,5 millones de euros en 2016. Según la consultora Newzoo, el número de entusiastas de los *e-sports* en España es de 4 millones. Asimismo, un estudio interno de AEVI cifra en 300 el número de personas que trabajan en el sector, incluidos 100 videojugadores profesionales. AEVI prevé un incremento hasta los 1.000 empleados en 2020» (21).

(21) Así lo indica AEVI al referirse a los *e-sports* en su página web oficial. Puede consultarse en http://www.aevi.org.es/e-sports/ (27.3.2018).

X

JUSTICIA Y TUTELA DE LOS DERECHOS EN UN MUNDO DIGITAL: EL PAPEL DE LA TECNOLOGÍA EN LA REGULACIÓN, LA SUPERVISIÓN Y LA RESOLUCIÓN DE CONFLICTOS

CAPÍTULO 38

CIBERJUSTICIA, MÉTODOS ALTERNATIVOS DE RESOLUCIÓN DE CONTROVERSIAS Y TECNOLOGÍA

KARIM BENYEKHLEF (1) Y ROSARIO DUASO CALÉS (2)

1. INTRODUCCIÓN

Asistimos desde hace ya algunos años a la irrupción de las tecnologías de la información y de la comunicación en el ámbito de la justicia, pudiendo ya emplear el término de ciberjusticia, como resultante de la modernización de los sistemas judiciales y de los medios alternativos de resolución de controversias por la llamada revolución numérica. Expertos en la materia no dudan en afirmar que el sistema judicial puede verse transformado gracias a la innovación y que la llegada de lo digital al campo del dere-

(1) Catedrático y miembro del *Public Law Research Centre* en la Facultad de derecho de la Universidad de Montreal. Director del *Cyberjustice Laboratory* y titular de la *LexUM Chair on Legal Information* de la Universidad de Montreal.

(2) Profesora y coordinadora académica del Máster sobre Protección de Datos, Transparencia y Acceso a la Información y coordinadora académica de la Cátedra *Google* sobre Privacidad, Sociedad e Innovación de la Universidad CEU San Pablo de Madrid. Investigadora asociada del *Cyberjustice Laboratory* y de la *LexUM Chair on Legal Information* de la Universidad de Montreal.

cho y de la justicia no es una moda pasajera, sino más bien un movimiento profundo e instalado ya desde hace tiempo (3).

El acceso generalizado a Internet y el desarrollo de un gran número de actividades en línea trae consigo la necesaria transformación de la justicia con el objetivo de adaptarse a este nuevo contexto. Así, algunos autores no dudan en afirmar que la justicia puede ser presentada como ejemplo de que «lo digital ha pasado silenciosamente de ser un facilitador para la administración a un potente reorganizador de las relaciones entre el Estado y los ciudadanos» (4).

Toma cada vez más peso la idea de que la irrupción de lo digital en el ámbito de la justicia tiene un impacto más allá de los medios utilizados y que el uso generalizado de la tecnología ha dado lugar a una reestructuración de los intercambios e interacciones que la administración de justicia tiene con los ciudadanos en la actualidad. Resulta por lo tanto interesante analizar cuál es la incidencia que puede tener la renovación de la justicia en algunos de los derechos de los ciudadanos y en particular, en el derecho de acceso a la justicia, que sin duda puede verse reforzado por la imparable evolución tecnológica en este contexto.

Este escenario puede sin duda ayudar a acercar la justicia al conjunto de la ciudadanía, pudiendo ya identificar cómo ciertas innovaciones como las que tienen su origen en elementos de inteligencia artificial, si se aplican de forma correcta al ámbito judicial pueden ser «facilitadoras» para el ciudadano y para los profesionales del derecho en un futuro no muy lejano. Más allá de estas consideraciones, en un escenario en el que una controversia haya estado originada en línea, cabe imaginar fácilmente que la solución a la misma puede encontrarse igualmente gracias a Internet. Si los medios tradicionales de resolución de controversias adquieren una importancia creciente ofreciendo a las partes soluciones satisfactorias, cuando estos medios se digitalizan y se ofrecen en línea, pueden responder a una necesidad creciente que encuentra su mejor ejemplo en el campo del comercio electrónico.

Las cuestiones relativas al papel que el humano y la máquina pueden y deben jugar en el ámbito de la justicia han sido objeto de estudio desde hace un tiempo, pues la introducción de las tecnologías en el ámbito de la justicia ha sido constante e imparable. Algunos juristas en los años noventa ya supieron identificar esta problemática, afirmando que «el ordenador, la máquina, no debe juzgar, sino que únicamente del principio al final de los procedimientos judiciales, puede liberar al juez de muchas tareas per-

(3) Institut Montaigne, Rapport *Justice: faites entrer le numérique*, Paris, noviembre 2017, p. 65.

(4) *Ibid.*, p. 81. Traducción libre del francés.

mitiéndole así consagrarse más y mejor a la única misión que tiene en exclusiva» (5).

La irrupción de Internet, de la inteligencia artificial o del *Big Data*, no hacen más que añadir complejidad a esta reflexión y evidencian la necesidad de interrogarse sobre el impacto que en el ámbito de la ciberjusticia podemos identificar en lo relativo a los derechos digitales de los ciudadanos. En las páginas siguientes analizaremos algunas de las cuestiones que los proyectos de ciberjusticia plantean en la actualidad, examinando igualmente la transformación que ciertas innovaciones tecnológicas pueden traer consigo muy especialmente en el contexto de la resolución de controversias en línea. Podremos igualmente ver cómo la tecnología puede jugar un papel central en la voluntad de orientar muchas de estas aplicaciones de ciberjusticia hacia las necesidades del ciudadano como utilizador de las múltiples plataformas a su disposición.

2. HACIA UNA CIBERJUSTICIA POR LA REVOLUCIÓN DIGITAL

Conviene en un primer lugar comenzar por definir el concepto de ciberjusticia como el uso y la integración de las tecnologías de la información y de la comunicación en los procesos de resolución de conflictos de forma judicial o extrajudicial (6).

Atendiendo a este concepto se hace referencia igualmente a la puesta en red de todos los actores de la cadena de información y de decisión en el marco de los procesos judiciales, lo que nos llevaría a hablar de Sistemas Integrados de Información de Justicia o S. I. I. J. (7) Facilitar y garantizar el ejercicio del derecho de acceso a la justicia gracias a la digitalización de los juzgados y tribunales han sido dos de los objetivos primordiales que han guiado la implantación de proyectos de ciberjusticia en los últimos años. El desafío de introducir las tecnologías de la información y de la comunicación en el ámbito de la justicia ha planteado grandes desafíos para todos los actores del mundo de la justicia y para los ciudadanos.

Una de las cuestiones más importantes que ya hemos evocado en las líneas anteriores es el lugar que ha de ocupar lo digital en este ámbito y cual será en el futuro el papel que jugará en la máquina. Ciertos autores afirman a este respecto que las tecnologías no llevan a evacuar al ser hu-

(5) Català Pierre, *Le droit à l'épreuve du numérique, Jus ex Machina*, PUF, Paris, 1998, p. 196. (Traducción libre del francés).

(6) Traducción libre del francés al español de la definición que es utilizada en el marco de los trabajos llevados a cabo por el *Cyberjustice Laboratory*, de la Facultad de derecho de la Universidad de Montreal, Canadá. Esta definición amplia y bastante flexible nos permite poder estudiar el conjunto de los fenómenos que observamos en la actualidad en el contexto del uso de las tecnologías en el ámbito de la justicia.

(7) Esta es igualmente la visión utilizada en los trabajos llevados a cabo por el *Cyberjustice Laboratory* de la Universidad de Montreal, Canadá.

mano del «aparato jurisdiccional» (8) o a «deshumanizar» la justicia, sino que más bien puede contribuir a «rehumanizarla» (9). Esta rehumanización de la justicia vendría de la puesta en funcionamiento adecuada de los recursos digitales, creando nuevos servicios o reorganizando sus procedimientos para satisfacer de manera óptima las necesidades de los ciudadanos en todas las clases de litigios en los que se puedan ser involucrados (10).

Resulta interesante hacer referencia a los trabajos que está realizando la Comisión europea para la eficacia de la justicia del Consejo de Europa (CEPEJ) en materia de ciberjusticia. Dicha Comisión ha publicado en 2016 unas «Líneas directrices para la gestión del cambio hacia la ciberjusticia» (11). Este documento identifica un gran número de elementos clave del éxito de los proyectos de ciberjusticia en el contexto de los sistemas judiciales europeos.

En este documento se afirma que el cambio en materia de ciberjusticia debe estar guiado «judicialmente» y no tecnológicamente, lo que implica una definición de los objetivos de modernización que esté desprovista de toda preocupación ligada a la informática en sí misma (12). Se identifica a esta idea como un requisito indispensable para el éxito de este tipo de proyectos y evitar así que la implementación de los recursos tecnológicos no resulte satisfactoria ni para los litigantes ni para los profesionales de la justicia, corriendo el riesgo de socavar la confianza en el poder judicial. Se aboga por lo tanto por un diálogo entre responsables de la tecnología que deberían entender y conocer el sistema judicial y responsables en el ámbito judicial, para lograr así que la arquitectura de los sistemas responda satisfactoriamente a las necesidades de los tribunales y de los litigantes (13).

Por otra parte, al analizar las razones que en el pasado han podido llevar al fracaso a algunas iniciativas en materia de ciberjusticia, se puede observar que en ocasiones se trató de resolver una situación compleja mediante el uso de una sola solución de *software* y siguiendo un enfoque basado única y exclusivamente en la tecnología (14). En contraposición a este enfoque, se ha privilegiado una estrategia que podemos calificar de

(8) Traducción libre del francés.
(9) Institut Montaigne, *op. cit.*, p. 82.
(10) *Ibid.*
(11) Comisión Europea para la Eficacia de la Justicia del Consejo de Europa (CEPEJ), *Lignes directrices sur la conduite du changement vers la cyberjustice, Bilan des dispositifs déployés et synthèse des bonnes pratiques*, 2016.
(12) *Ibid.*, p. 63.
(13) *Ibid.*, p. 64.
(14) Benyekhlef Karim, Amar Emmanuelle y Callipel Valentin, «ICT-Driven Strategies for Reforming Access to Justice Mechanisms in Developing Countries», (2015) 6 *The World Bank Legal Review*, 325-343. En este artículo se detalla esta estrategia como modelo para implantar con éxito soluciones de ciberjusticia con el objetivo de garantizar el acceso a la justicia.

«modular», en el cual se encuentran soluciones tecnológicas compatibles e interconectadas, con el objetivo de abordar problemáticas precisas e identificadas a través de módulos, en lugar de crear estructuras en red complejas (15).

Por otro lado, de forma paralela a la puesta en red de la justicia, podemos identificar desde hace varios años un movimiento con tendencia a una creciente *desjudicialización* (16), haciendo de los métodos alternativos de resolución de controversias o *Alternative Dispute Resolution* (17) una opción a la que se recurre cada vez más frecuentemente para llegar a encontrar una solución a los conflictos, al margen del sistema judicial. Tanto en el contexto europeo como en el norteamericano, observamos igualmente como las innovaciones tecnológicas son cada vez más numerosas en la carrera por ofrecer la posibilidad de resolver en línea las controversias que puedan surgir en un ámbito digital o no digital, impulsando cada vez más las *Online Dispute Resolution* (18).

La desmaterialización de estos procesos y la incuestionable hegemonía de Internet propician que las ODR se conviertan en herramienta imprescindible en un mundo global, en el que las fronteras físicas se ven cada vez más diluidas y la distancia geográfica entre las partes de un conflicto no puede condicionar la resolución del mismo. Constatamos por lo tanto, que lo digital se está implantando desde hace unos años en el ámbito de lo que se han denominado Sistemas Integrados de Información de Justicia e igualmente en el ámbito de los modos alternativos de resolución de controversias o ADR (19). La irrupción de las innovaciones de carácter tecnológico y de diferentes plataformas en particular, han hecho posible el desarrollo de las ODR.

En el marco de los Sistemas Integrados de Información de Justicia, la tecnología se utiliza con el objetivo de «modelizar» (20) los procedimientos judiciales clásicos y de «poner en línea estos procedimientos y las diferentes etapas administrativas propias del sistema judicial» (21). En el ámbito de los métodos alternativos de resolución de controversias en línea u ODR, «las tecnologías sirven para modelizar y poner en línea los procedimientos de negociación, de mediación, de conciliación, de arbitraje y cualquier otro modo de resolución de controversias» (22). En ambos

(15) *Ibid.*
(16) Chevallier Jacques, *L'État post-moderne*, L. G. D. J., Paris, 2004. El autor hace referencia al término *dé-judiciarisation* para hablar de este fenómeno que es observable desde hace unos años en este ámbito.
(17) ADR.
(18) ODR.
(19) Benyekhlef Karim y Gélinas Fabien, *Le règlement en ligne des conflits, Enjeux de la cyberjustice*, Romillat, Paris 2003, p. 34.
(20) Se puede usar igualmente la expresión de «elaboración de modelos».
(21) *Ibid.* Traducción libre del francés.
(22) *Ibid.* Traducción libre del francés.

casos el objetivo es mejorar la gestión de los conflictos disminuyendo los gastos que éstos generan y los tiempos de espera que todo procedimiento conlleva (23).

D. Reiling identifica tres niveles en los que actúa la tecnología, a través de diferentes herramientas, lo que conlleva una evolución del ámbito judicial hacia un nuevo modelo. Subraya la importancia de una tecnología para lo que esta autora denomina la «trastienda de la oficina», en la que las tecnologías apoyan los procesos relacionados con la administración de casos, la producción de documentos y la gestión de los tribunales. Esta autora identifica en este ámbito herramientas como el procesador de palabras, la base de datos en general (24) y la base de datos de jurisprudencia en particular (25).

Otras innovaciones actúan fundamentalmente en la «sala de audiencias», apoyando todo lo que allí tiene lugar, con tecnologías como cámaras para enfocar pruebas, monitores en el tribunal o amplificadores de sonido (26).

Las tecnologías tienen igualmente por vocación el operar en lo relativo a lo que D. Reiling denomina la «comunicación externa» (27), pudiendo actuar como apoyo para poder comunicar con los interesados y con el público en general fuera de los tribunales. Esta experta lo denomina «Tecnología de la información en redes», incluyendo el correo electrónico, la posibilidad de compartir documentos, aplicaciones colaborativas y de audio, así como las video conferencias (28).

Es en estos tres niveles en los que podríamos por lo tanto identificar cómo y dónde actúa lo digital en el interior de los juzgados y tribunales y por lo tanto en el ámbito judicial. Al referirnos a lo extrajudicial, identificamos, por ejemplo, los procesos de arbitraje o mediación, que, actuando a diferentes niveles, constituyen las ADR en el sentido clásico. El concepto de ciberjusticia al que estamos haciendo referencia en este texto, se extiende igualmente a la implantación de las tecnologías en un contexto en el que a través de Internet se accede a portales o plataformas que ofrecen a través de programas, aplicaciones o *software* herramientas que hacen posible la resolución de controversias en línea u ODR.

---

(23) *Id.* Traducción libre del francés.
(24) Reiling Dory, «E-Justicia: experiencias con las tecnologías de la información en los tribunales de Europa», en *Buenas prácticas para la implementación de soluciones tecnológicas en la administración de la justicia*, J. A. Caballero, C. Gregorio de Gràcia y L. Hammergen (Compil.), IIJusticia, Buenos Aires, 2011, p. 83-119, p. 85.
(25) *Ibid.*, p. 86.
(26) *Ibid.*, p. 88.
(27) *Ibid.*, p. 85.
(28) *Ibid.*, p. 90.

En el ámbito de la UE y desde 2016 se puede acceder a la *Online Dispute Resolution Platform* (29), plataforma multilingüe desarrollada por la Comisión Europea, que ofrece a consumidores y empresas que operan en el ámbito del comercio electrónico, esta herramienta para la resolución de controversias. Dicho recurso ve la luz para dar respuesta al Reglamento sobre resolución de litigios en línea en materia de consumo de 2013, el Reglamento de Ejecución de 2015 (30) y la Directiva sobre Resolución alternativa de litigios para los consumidores de 2013 (31). Esta plataforma reúne los servicios de diferentes organismos de resolución de litigios de los diferentes países de la UE, que han sido objeto de verificación para comprobar que reúnen ciertas normas que la plataforma establece y que están igualmente registrados ante las autoridades nacionales competentes en cada estado miembro.

Podemos igualmente mencionar otras herramientas existentes en otros ámbitos geográficos. En el contexto de la provincia de Quebec, en Canadá, la plataforma PARLe, creada por el *Cyberjustice Laboratory* de la Universidad de Montreal, está destinada a resolver las controversias entre consumidor y vendedor.

Este proyecto explora el potencial de las tecnologías para la resolución de conflictos de baja intensidad, disminuyendo los gastos y los tiempos de espera para obtener una solución a los conflictos (32). Se trata de una plataforma que empezó a funcionar en noviembre de 2016 y cuyo funcionamiento es simple para los utilizadores, rápida, gratuita, totalmente automatizada y en código abierto. Todos los mediadores que participan en la misma están acreditados, poseen gran experiencia en materia de Derecho del consumidor y pertenecen al Colegio de Abogados o a la Cámara de los Notarios de Quebec. Las cifras de las que se dispone en el momento actual son contundentes y demuestran claramente la eficacia de la plataforma, dejando claro que los resultados positivos que derivan de su utilización son muy reales.

---

(29) https://webgate.ec.europa.eu/odr

(30) Reglamento (UE) n° 524/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, sobre resolución de litigios en línea en materia de consumo y por el que se modifica el Reglamento (CE) n° 2006/2004 y la Directiva 2009/22/CE. OJ L 165, 18.6.2013, p. 1-1.

Reglamento de Ejecución (UE) 2015/1051 de la Comisión, de 1 de julio de 2015, sobre las modalidades para el ejercicio de las funciones de la plataforma de resolución de litigios en línea, sobre las modalidades del impreso electrónico de reclamación y sobre las modalidades de cooperación entre los puntos de contacto previstos en el Reglamento (UE) n° 524/2013 del Parlamento Europeo y del Consejo sobre resolución de litigios en línea en materia de consumo. OJ L 171, 2.7.2015, p. 1–4.

(31) Directiva 2013/11/UE del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, relativa a la resolución alternativa de litigios en materia de consumo y por la que se modifica el Reglamento (CE) n° 2006/2004 y la Directiva 2009/22/CE (Directiva sobre resolución alternativa de litigios en materia de consumo). OJ L 165, 18.6.2013, pp. 63–79.

(32) Para conocer más: http://www.cyberjustice.ca/actualites/2014/08/22/presentation-de-parle/

Así, se han iniciado unos 2.000 procedimientos por esta vía, de los cuales el 67,3 % han sido resueltos. El 45 % de éstos han sido resueltos mediante la negociación y el 25 % gracias a la mediación. El porcentaje de consumidores satisfechos tras la resolución de la controversia es del 88 % y el de los comerciantes alcanza el 89,2 %. La negociación o la mediación dura una media de 29 días, lo que indica que es doce veces más rápida que la media de lo que dura un procedimiento ante el tribunal competente, la *Cour du Québec*. Lo que resulta muy interesante es que si finalmente las partes no llegan a una solución gracias a PARLe durante esta etapa «prejudicial», por vía de la negociación o mediación en línea, las informaciones pertinentes relativas a este caso podrán ser reutilizadas si el caso se judicializa ante la *Cour du Québec*. Estos datos dejan entrever todo el potencial de esta herramienta y auguran el aumento de la confianza en este tipo de mecanismos que como hemos visto, ya están sirviendo de ayuda a consumidores y vendedores mediante la mediación y la negociación en línea.

Identificamos por lo tanto en el momento actual, tanto en el ámbito judicial como en el extrajudicial, iniciativas que ofrecen herramientas tecnológicas que inciden en un mayor acceso a la justicia y que tienen por objetivo el responder satisfactoriamente a las necesidades de los litigantes y de los profesionales del mundo de la justicia. Analizaremos a continuación cómo la innovación tecnológica presenta un potencial importante en el ámbito de la justicia, pudiendo transformar el sector en los próximos años.

3. EL POTENCIAL DE LA INNOVACIÓN AL SERVICIO DE LA JUSTICIA

Hemos podido observar en los últimos años cómo la ciberjusticia trae consigo un mejor acceso a la justicia y una justicia más cercana a los ciudadanos y que responde más y mejor a sus necesidades y expectativas (33). Constatamos fácilmente que la innovación tecnológica tiene el potencial de transformar un sector como el de la justicia, siendo el factor clave del éxito de esta evolución digital el que las políticas que la motivan se orienten hacia las necesidades del usuario o utilizador (34) en lo relativo al uso de las herramientas que la ciberjusticia ofrece.

Se puede ya identificar cuáles son algunas de las funcionalidades que la tecnología puede ofrecer, pudiendo mencionar cómo ciertos desarrollos

(33) Ver en este sentido este informe en el que se examina la situación de la ciberjusticia en diferentes países: Benyekhlef Karim y Iavarone-Turcotte Cléa, «Rapport général. Procédure et immatériel» en *Travaux de l'Association Henri-Capitan, Journées espagnoles, L'immatériel*, Bruxelles, Bruylant et LBSV, 2016, 681-697.

(34) Esta es la idea que sostiene la CEPEJ, ver: Comisión Europea para la Eficacia de la Justicia del Consejo de Europa (CEPEJ), *op. cit.*

concretos en el ámbito judicial pueden tener un claro impacto en lo relativo a la reducción sustancial de las barreras tradicionales que impiden o dificultan el acceso a la justicia. Por otro lado, cabe mencionar igualmente cómo la innovación en el ámbito judicial y extrajudicial puede ser definitiva a la hora de reducir ciertas dificultades que puedan tener su origen en el alejamiento geográfico (35)de ciudadanos que viven en zonas aisladas, lejos de las cortes y tribunales, situados normalmente en grandes núcleos urbanos. La barrera del idioma (36) no puede ser ignorada en algunos casos, pudiendo verse superada por la implementación de herramientas tecnológicas capaces de ofrecer servicios de traducción simultánea tanto en los tribunales como gracias a su integración en las plataformas de ODR.

Expertos en la materia no han dudado en establecer recomendaciones para responder con éxito a las expectativas derivadas de la justicia y gracias a la innovación tecnológica. Inciden en la importante cuestión de «reformar» el acceso a la justicia, poniendo el acento en la siguiente proposición: «reforzar los servicios de acogida de los usuarios y mejorar la información que reciben sobre el desarrollo del proceso, poner a su disposición nuevas herramientas de inteligencia artificial capaces de llevar a cabo la utilización de datos legales y judiciales y dando indicaciones provisionales sobre las posibles soluciones al proceso» (37).

Tendremos la oportunidad en las líneas que siguen de poder examinar cuáles pueden ser los beneficios del uso de herramientas de este tipo, que sin duda pueden hacer evolucionar el ámbito de la justicia, gracias al uso de grandes cantidades de datos de naturaleza legal y judicial. Observamos igualmente que el acceso que hace posible un medio como Internet a todo tipo de información de carácter jurídico relativo a la legislación, al procedimiento o a la jurisprudencia, puede reducir indudablemente muchas de las barreras existentes a causa de la falta de conocimiento de un proceso judicial complejo o de cualquier tipo de información de tipo judicial que exista o haya existido en el pasado para ciertos colectivos (38). Sin embargo, observamos cómo la cuestión del acceso a la información judicial en formato digital y en ocasiones, como resultado de políticas de difusión proactiva de información en la red, no está exenta de complejidad, lo cual es inherente al propio proceso judicial «a la luz del principio de publicidad» (39).

---

(35) Reiling Dory, *Technology for Justice, How Information Technology can support Judicial Reform*, Leiden University Press, 2009, p. 167.

(36) *Ibid.*

(37) Institut Montaigne, *op. cit.*, p. 43. Traducción libre del francés.

(38) Reiling Dory, *Technology, op. cit.* p. 168.

(39) Caballero José Antonio, «Acceso a la información Judicial», en *Buenas prácticas para la implementación de soluciones tecnológicas en la administración de la justicia*, J. A. Caballero, C. Gregorio de Gràcia y L. Hammergen (Compil.), IIJusticia, Buenos Aires, 2011, p. 147-160, p. 158.

Al analizar el ámbito de la publicidad y el acceso a todo lo relativo a los procesos judiciales podemos preguntarnos sobre el verdadero impacto tecnológico y más concretamente sobre si los «signos distintivos» del poder judicial se ven en cierto modo transformados: «se puede constatar por ejemplo que la cuestión del acceso al público de las informaciones de naturaleza judicial, lo cual era algo que se daba por supuesto, adquiere un nuevo aspecto en el contexto de la consulta a distancia y a gran escala que es posible gracias a la informatización de las informaciones ligada a Internet» (40).

Ya podemos afirmar que la respuesta tecnológica que conlleva la implantación de los proyectos de ciberjusticia puede ser definitiva para acortar los tiempos de obtención de una sentencia gracias a una mayor celeridad en los trámites que conlleva el proceso judicial. Sin embargo, éste no debería ser el único beneficio derivado de la virtualización del ámbito judicial, puesto que la llamada revolución digital puede suponer una oportunidad única para reflexionar sobre la verdadera adecuación del procedimiento judicial a los objetivos que se persiguen, así como para revisar la pertinencia de ciertos usos y costumbres en un campo claramente caracterizado por el apego a formalismos y tradiciones (41).

La idea que se avanza en este sentido es que la transformación de la justicia tradicional gracias al uso de la tecnología y de Internet permitiría «repensar» el propio proceso judicial, evitando «replicar» al ámbito de lo digital, sin antes evaluar si sería posible prescindir en un futuro de ciertos elementos que pueden resultar superfluos y que sin embargo pueden incidir en la lentitud de la justicia. A simple vista, en un ámbito esencialmente formalista como es el judicial, el nuevo escenario propiciado por la ciberjusticia sería el óptimo para que la innovación tecnológica se vea acompañada de una reflexión más profunda a este nivel. Algunos autores van incluso más lejos, al mantener que esta modernización de la justicia puede ir acompañada de una reflexión encaminada a repensar el propio derecho procesal mediante la revisión de ciertas prácticas judiciales y extrajudiciales, siempre desde el respeto de los derechos fundamentales, «elaborando nuevos modelos procesales fundamentados en la integración de las tecnologías de la información y de la comunicación» (42). Por otro lado, esta revolución digital debe ser respetuosa de muchos de los signos distintivos que podemos identificar en el ámbito judicial, ya que precisamente se ha podido observar que en el campo de la justicia perduran especialmente ciertos «rituales». Expertos en la materia trabajan con el ob-

(40) Gélinas Fabien, «État de droit et justice virtuelle», en *État de droit et virtualité*, K. Benyekhlef y P. Trudel (Dir.), Éd. Thémis, Montréal, 2009, p. 309. Traducción libre del francés.

(41) *Ibid.*

(42) En este sentido avanzan los trabajos del Cyberjustice *Laboratory* de la Universidad de Montreal. Ver sobre esta cuestión: http://www.cyberjustice.ca/projets/vers-la-cyberjustice/

jetivo de identificar de qué modo puede lograrse que la irrupción de medios tecnológicos en el ámbito de la justicia se pueda realizar en el respeto de estos rituales (43). Otra cuestión que llama nuestra atención en este contexto de nuevas prácticas que podrían instalarse en el ámbito de lo judicial impulsadas por la innovación, es la del necesario reconocimiento a nivel legislativo de los medios tecnológicos y de la equivalencia entre diferentes formatos. Podemos citar por ejemplo el «principio de equivalencia funcional» (44) entre un documento papel y un documento electrónico. Algunos autores no dudan en afirmar que poder presentar electrónicamente ciertos documentos en un procedimiento judicial va a contribuir a agilizar la resolución de los casos (45). Por esta razón todas aquellas disposiciones legislativas encaminadas a permitir que los ciudadanos puedan recurrir al uso de las tecnologías en sus relaciones en el ámbito judicial no hacen más que incidir positivamente en la implantación de las soluciones que la ciberjusticia ofrece.

Resulta esencial que podamos analizar igualmente el impacto real que puede tener el factor tecnológico en el ámbito de las ODR y en particular qué consecuencias puede tener la implementación de ciertas innovaciones que son susceptibles de transformar este ámbito.

4. TECNOLOGÍA Y MÉTODOS ALTERNATIVOS DE RESOLUCIÓN DE CONTROVERSIAS: ODR INTELIGENTES Y DERECHOS DIGITALES

Resulta realmente interesante observar como desde hace algunos años se está otorgando una cierta legitimidad a los actores que ofrecen servicios de ODR para resolver controversias de baja intensidad, con independencia de si éstas se han originado o no en línea (46). Para contribuir al éxito de estos medios alternativos sustentados e impulsados por la propia tecnología, resulta realmente fundamental que juzgados, tribunales y ministerios de justicia continúen en el camino del reconocimiento de la legi-

(43) Es sobre esta cuestión sobre la que los trabajos del *Cyberjustice Laboratory* de la Universidad de Montreal también están encaminados, pues el componente tecnológico se ve confrontado a adaptarse a este contexto esencialmente ritual y formalista.

(44) Entre otros textos cabe destacar la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, CNUDMI, sobre Comercio electrónico que ya en 1996 reconocía este principio con el objetivo de equiparar las comunicaciones electrónicas a las comunicaciones papel en los casos en que cumplan con ciertos requisitos.

Ver: Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, CNUDMI, sobre Comercio Electrónico del 12 de junio de 1996, junto con su nuevo artículo 5 bis aprobado en 1998.

http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/1996Model.html

(45) Walsh Barry, «Proyectos de e-justicia: distinguiendo entre mitos y realidades», en *Buenas prácticas para la implementación de soluciones tecnológicas en la administración de la justicia*, J. A. Caballero, C. Gregorio de Gràcia y L. Hammergen (Compil.), IIJusticia, Buenos Aires, 2011, p. 55-80, p. 59

(46) Benyekhlef, Karim: *Some Reflections on the Future of Online Dispute resolution. From e-platform to Algorithms*, 2018 (próxima publicación), p. 10.

timidad de las ODR (47), ya que sin duda estos medios presentan una manera de desarrollar soluciones eficientes para mejorar el acceso a la justicia.

Al afirmar que las ODR representan un medio óptimo para la resolución de controversias de baja intensidad, conviene precisar a qué se hace referencia al hablar de «*low intensity*» en este contexto: «low-intensity disputes cover issues where the amount claimed is low, issues where the object is not problematic and legal issues that are not complex. Low-intensity conflicts are sufficiently important to warrant resolution» (48).

Podríamos pensar en un primer momento en que el hecho de que en este tipo de controversias de baja intensidad las cuestiones jurídicas que entran en juego estén desprovistas en muchos casos de complejidad, haría posible la automatización de alguna parte del proceso. Cabe recordar que las plataformas que ofrecen servicios de ODR podrían estar basadas en lo que podemos denominar un intermediario humano o pueden únicamente poner frente a frente a las dos partes en un procedimiento totalmente automatizado (49). Si bien las ODR están adquiriendo un papel cada vez más importante en un mundo digital y global, es en el ámbito del comercio electrónico en el que se adivina que las ODR, por las características propias a las controversias de baja intensidad que acabamos de enumerar, podrían tener una importancia creciente.

Suponen por lo tanto una herramienta de acceso a la justicia realmente óptima para los consumidores (50), que recurriendo a esta vía extrajudicial para resolver sus controversias con las empresas de *e-commerce*, siempre pueden acudir con posterioridad a los tribunales en el caso en que no haya sido posible encontrar una solución al conflicto en cuestión (51). Expertos en este campo subrayan que las ODR, surgían en un primer momento de la necesidad de resolver los conflictos que se originaban en el ciberespacio y su desarrollo se basó en la idea de que estos medios de resolución de controversias que también se desarrollaban en el mismo entorno digital, resultaban necesarios y apropiados en dicho con-

(47) *Ibid.*, p. 13.

(48) *Ibid.* p. 4.

(49) Council of Europe, Committee on Legal Affairs and Human Rights, *Access to Justice and the Internet: potential and challenges*, Parliamentary Assembly, Doc. 13918, 10 de noviembre de 2015, p. 5. http://website-pace.net/documents/19838/1085720/20151026-InternetAccess-FR.pdf/8d3c44d4-da6c-4dac-ab15-94dc1fcc5d48

(50) Ver sobre esta cuestión: Benyekhlef Karim, «La résolution en ligne des différends de consommation: un récit autour (et un exemple) du droit postmoderne», en Pierre-Claude LAFOND (dir.), *L'accès des consommateurs à la justice*, Yvon Blais, Cowansville, 2010, p. 89-117.

(51) Las ODR también pueden encontrar su lugar en otros ámbitos relacionados con las interacciones en el contexto de la red, como en el ámbito de los nombres de dominio, en el de las cuestiones relacionadas con el derecho de propiedad intelectual y de los derechos de autor o en el de las subastas.

texto (52). El desarrollo y el éxito de las ODR, como medio que permita resolver de forma fácil, rápida, segura y económica los conflictos originados en línea, podrán sin dudad contribuir a acrecentar la confianza del utilizador de las diferentes plataformas que ofrece Internet hoy en día.

Lo que resulta interesante respecto a las ODR, es que se pueda acceder a estos medios electrónicos extrajudiciales, como una primera etapa antes de acudir a los tribunales, como recurso si las partes no han obtenido un resultado satisfactorio por este medio. Por otra parte, las plataformas que ofrecen servicios de ODR, pueden plantear al utilizador múltiples modalidades como son la negociación y la mediación, pudiendo en el caso necesario proceder a transferir por medio electrónico la totalidad del dossier generado al tribunal competente que podría resolver finalmente la controversia si fuera necesario.

Lo que realmente caracteriza a las ODR y las hace únicas frente a las ADR ó los medios de resolución de controversias clásicos es la posibilidad de poder comunicarse a distancia y las innegables ventajas que ofrece lo que podemos denominar la «inteligencia de la máquina» (53). Por otro lado, cabe señalar que uno de los objetivos que podemos observar en la actualidad en el ámbito de las reformas judiciales llevadas a cabo en diferentes países de nuestro entorno, es el empoderamiento de las partes y en este sentido, las tecnologías de la información y de la comunicación pueden jugar un papel esencial para lograr dicho empoderamiento (54).

Resulta de vital importancia mencionar el gran potencial que ofrece la llamada «justicia predictiva», que gracias a herramientas basadas en la inteligencia artificial puede tener un gran impacto en el desarrollo futuro de las ODR. Dicha justicia predictiva permitiría identificar potenciales resultados o soluciones derivadas de un procedimiento o controversia gracias al uso de medios matemáticos, predictivos y analíticos en el ámbito del derecho (55). Es decir, produciendo estadísticas y probabilidades en lo relativo a la solución que se pueda dar a diferentes cuestiones jurídicas que se planteen en el contexto de un conflicto.

En el ámbito de esta justicia predictiva, se puede identificar igualmente otra sub-categoría de la inteligencia artificial que resulta igualmente interesante en el campo de las ODR, como es lo que en inglés se denomina *computational law* y que tendría por objetivo «to develop tools for automating all or part of the legal reasoning and the decision-making process, which we will refer to as decision-helping tools» (56). Tal y como hemos

(52) Rabinovich-Einy Orna y Katsh Ethan, «Technology and the Future of Dispute Systems Design», *Harvard Negotiation Law Review*, Vol. 17, Spring, 151-1999, 2012, p. 164.
(53) Benyekhlef Karim, «*Some Reflections*», *op. cit.* p. 3.
(54) *Ibid.*, p. 13.
(55) *Ibid.*, p. 14.
(56) *Ibid.*, p. 14.

mencionado en las líneas anteriores, estas herramientas podrían claramente resultar de aplicación en el contexto de las ODR, lo cual tendría un impacto claro en cómo podrían resolverse las controversias en línea, gracias a un cierto grado de automatización de la decisión, con todo lo que ello implicaría.

Pero la llamada justicia predictiva también hace referencia al concepto de *machine learning*, tecnología de aprendizaje automatizado que, sustentada igualmente en la inteligencia artificial, permite a la máquina aprender sin que ésta haya sido programada de forma específica para ello (57). En el ámbito de las plataformas de ODR, se adivinan claramente los beneficios que la aplicación de esta tecnología puede tener para conseguir que las herramientas utilizadas puedan ofrecer cada vez mejores soluciones a los usuarios de las mismas.

Dentro de unos años se podrá evaluar efectivamente cual será el impacto de la aplicación de estas innovaciones tecnológicas al campo de las ODR, incluyendo el *deep learning* como subcategoría del *machine learning*, que permitiría superar muchas de las limitaciones a las que se enfrenta la inteligencia artificial desde años por su capacidad para conocer estructuras complejas en el ámbito de grandes cantidades de datos (58).

La innovación este campo, basada en los algoritmos y en la inteligencia artificial puede dar lugar a lo que algunos denominan «*Intelligent ODR Services*». Cuando se desarrollan aplicaciones *on line* para mejorar el ámbito de la justicia en general, dichas aplicaciones deberían ser prácticas, intuitivas y de fácil uso para todos, incluyendo a los que no son expertos en este campo. Una de las maneras de lograr dichos objetivos sería la integración de elementos de inteligencia artificial, lo cual también resulta posible gracias a los importantes desarrollos en el campo del *Big Data*, enfocados a saber interpretar los datos. De todo esto, podemos predecir igualmente que estos datos que nunca han sido tratados o examinados en el pasado, pueden tener un gran potencial en el ámbito de la resolución de controversias (59).

Claramente, el desarrollo de estas plataformas inteligentes de ODR debe estar guiado por una reflexión que lleve a determinar qué aspectos de la resolución de controversias en línea deben siempre estar sujetas a la decisión o al razonamiento humano y cuáles pueden depender de la decisión automatizada o de la «máquina». Únicamente en el caso en que los

(57) *Ibid.*
(58) *Ibid.*, p. 17.
(59) *Ibid.*, p. 23. En este sentido y dentro del ámbito de los trabajos del *Cyberjustice Laboratory* de la Universidad de Montreal, se trabaja en la concepción de una plataforma inteligente de ODR, que permitiría explotar datos de naturaleza judicial y que daría la posibilidad igualmente al utilizador de poder hablar directamente a la plataforma para explicar todos los aspectos relativos a la controversia y ser guiado durante todas las etapas del proceso.

criterios de justicia y los criterios éticos guíen esta reflexión, se podrá asegurar que el empoderamiento de las partes y que un mejor acceso a la justicia queden garantizados (60).

La implantación de todas estas innovaciones en el ámbito de la ciberjusticia va a tener sin duda un impacto en cómo los derechos de los ciudadanos en un contexto digital van a ir dibujándose en el futuro. Si bien hemos podido a lo largo de este texto comprobar que las aplicaciones de ciberjusticia inciden directamente en el derecho de acceso a la justicia, hay otros derechos sobre los que podemos ya identificar un posible impacto.

En un escenario como el que acabamos de exponer, en el que muchas de las aplicaciones y soluciones tecnológicas van a estar basadas en lo que se denomina *Data-Driven Innovation*, es evidente que el derecho a la protección de los datos personales de todos los actores que puedan intervenir en el marco de una ODR, ha de ser protegido en consecuencia. El riesgo asociado al tratamiento de datos personales por las plataformas de ODR no existía en el marco de las ADR tradicionales y por tanto ciertas medidas técnicas deben ser adoptadas en este contexto. El Grupo de Trabajo III de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, que lleva a cabo los trabajos relativas a la «Solución de Controversias en Línea», ha expresado «la importancia de las normas de seguridad del intercambio de datos para los proveedores de servicios ODR» ya que la seguridad de los datos es un elemento importante de la confidencialidad (61).

A nivel internacional, se han identificado los temores relativos a la seguridad técnica y a la protección del derecho a la vida privada, como uno de los desafíos que ralentizan el desarrollo pleno en materia de ciberjusticia (62). Desde hace un tiempo se han podido identificar en el ámbito de la ciberjusticia riesgos respecto a la confidencialidad de los datos, en el contexto de las ODR, del uso de las tecnologías en los juzgados y tribunales o en el del acceso a la información judicial gracias a Internet. En el ámbito concreto del acceso a bases de datos de jurisprudencia y en el de la posibilidad de acceder de forma telemática a información de carácter judicial, se han identificado los riesgos inherentes a la difusión por Internet de información sensible que en el pasado era consultada en formato papel y en un escenario en el que no existía el recurso a motores de búsqueda cada vez más perfeccionados.

(60) *Ibid.*

(61) Grupo de Trabajo III (Solución de Controversias en Línea) de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, A/CN.9/868 – Informe sobre la labor realizada en su 33.º periodo de sesiones, Nueva York, 29 de febrero a 4 de marzo de 2016. p. 5.

(62) Ver sobre esta cuestión: Benyekhlef Karim y Iavarone-Turcotte Cléa, *op. cit.*

Son precisamente las posibilidades que derivan de las funcionalidades de los motores de búsqueda, las que han incidido directamente en el concepto clásico de publicidad de la justicia, fundamentalmente por el acceso permanente y durante un período de tiempo indefinido de los datos personales que las sentencias judiciales pueden contener (63). Ciertas medidas técnicas como puedan ser la anonimización de las sentencias o el recurso a herramientas tecnológicas que impiden la indexación por los motores de búsqueda son utilizadas desde hace años para mitigar los potenciales riesgos en materia de privacidad. El uso de las diferentes tecnologías en el ámbito de los juzgados y tribunales o el acceso por Internet a documentos en el marco de un proceso judicial, deberían ir acompañados de medidas encaminadas a que las informaciones que pueden ser de carácter especialmente sensible, sean protegidas en conformidad a los principios de protección de datos (64). Con el objetivo de crear el necesario sentimiento de confianza en las aplicaciones de ciberjusticia en todos los actores llamados a estar implicados en el desarrollo y el uso de las mismas, como puedan ser los ciudadanos, los abogados, los jueces y en general todos los actores que actúen en el ámbito judicial y extrajudicial, los datos personales deben ser protegidos desde el momento inicial de su tratamiento y durante todo su ciclo de vida.

Ciertas disposiciones recogidas en el Reglamento general europeo de protección datos (65) pueden tener una aplicación fundamental en el contexto de la ciberjusticia. En efecto, este texto europeo, basado en el *risk-based approach*, se convierte en un instrumento cuya aplicación puede ayudar a minimizar los riesgos que hemos identificado en las líneas anteriores, gracias a principios como el de la protección de datos por el diseño y el de la protección de datos por defecto (66). Todo ello con el objetivo de que la privacidad esté integrada desde el momento de la concepción de toda innovación de carácter tecnológico y de que toda aplicación utilizada en el ámbito de la justicia proteja «por defecto» los datos personales. La Evaluaciones de Impacto en la Protección de los Datos Personales (EIPD) que también recoge este reglamento pueden sin duda resultar una herra-

(63) Duaso Calés Rosario, «Regulación europea sobre difusión de la jurisprudencia en Internet», en Carlos G. Gregorio y Sonia Navarro Solano (coord.), *Internet y sistema judicial en América Latina, Reglas de Heredia*, Ad-Hoc, Buenos Aires, 2004, pp. 251-278.

(64) Ver sobre esta cuestión: Duaso Calés Rosario, «Justicia electrónica y Privacidad: nuevas pistas de reflexión sobre la cuestión de la protección de los datos personales y la publicación de las sentencias judiciales en Internet», en *Buenas Prácticas para la implementación de soluciones tecnológicas en la administración de justicia*, J. A. Caballero, C. Gregorio de Gràcia y L. Hammergren (comp.), II Justicia, Buenos Aires, 2011, pp. 181-195.

(65) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE.

(66) Ver sobre estos principios contenidos en el citado Reglamento: Duaso Calés Rosario, «Los principios de protección de datos desde el diseño y protección de datos por defecto» en José Luis Piñar Mañas (Dir.), *El Reglamento general de protección de datos*, Ed. Reus, Madrid, pp. 295-321.

mienta indispensable para identificar los riesgos que toda aplicación de ciberjusticia pueda presentar y adoptar en consecuencia las medidas de protección necesarias (67).

Para finalizar y teniendo en cuenta la aplicación de soluciones basadas en la inteligencia artificial en el ámbito de la ciberjusticia, es importante subrayar cómo en el futuro podría ser necesario reforzar el derecho a conocer por parte de los ciudadanos cómo estas tecnologías son utilizadas, en virtud del principio de transparencia de la justicia. Algunos autores plantean que sería indispensable que los litigantes pudieran conocer lo que el juez ha decidido en los casos en los que haya recurrido al uso de este tipo de herramientas (68). Podríamos imaginar que la misma exigencia sería igualmente necesaria en el ámbito de las ODR, en el que sería importante conocer en qué se basa la resolución de cada una de las controversias. Por esta razón, estos autores recomiendan que en un futuro se pueda regular el funcionamiento de los sistemas que permiten el análisis de datos masivos de naturaleza jurídica, con el objetivo de verificar la necesaria «neutralidad» de los tratamientos realizados gracias a algoritmos. Comprobamos así cómo son muchas las cuestiones relativas a los derechos digitales que plantearán desafíos importantes a la hora de establecer los límites del uso de las aplicaciones ofertadas al ciudadano en el marco de la ciberjusticia.

5. CONCLUSIÓN

La revolución digital puede contribuir a una transformación de la justicia en el que las innovaciones tecnológicas jueguen un papel esencial en la modernización de los servicios que se ofrecen a los ciudadanos. Las soluciones tecnológicas que operan en el ámbito de la ciberjusticia van a conocer en el futuro desarrollos que sin duda van a facilitar el acceso a la justicia y van a permitir que se pueda encontrar de una forma más rápida, eficaz y económica una solución a las controversias. Tal y como hemos podido comprobar, tanto en el ámbito judicial, como en el de los métodos alternativos de resolución de controversias, las tecnologías basadas en la inteligencia artificial pudiendo ser conjugadas al *Big Data*, van a tener una incidencia importante en el desarrollo de la ciberjusticia.

Si las políticas que acompañan a la implantación de las innovaciones tecnológicas en la carrera por la digitalización de la justicia están orientadas a responder a las necesidades del ciudadano como utilizador de estos sistemas, este ámbito puede verse realmente transformado profundamen-

(67) Este documento ofrece detallada información para llevar a cabo estas EIPD: Agencia Española de Protección de Datos, *Guía para una Evaluación de Impacto en la Protección de Datos Personales*, 2014.

(68) Institut Montaigne, *op. cit.*, p. 46.

te y en beneficio de todos. La legitimidad que están adquiriendo en los últimos años las ADR y más recientemente las ODR, van a contribuir sin duda a que muchas controversias que en ocasiones tienen su origen en línea puedan encontrar una solución satisfactoria. En este escenario, tal y como algunos autores nos recuerdan en las líneas anteriores, para asegurar el éxito de las soluciones que ofrece la ciberjusticia, es necesario que las reformas no estén guiadas por criterios puramente tecnológicos, siendo necesaria una visión sustentada en los objetivos de naturaleza judicial y siguiendo una estrategia «modular» que pueda ir dando respuesta a las necesidades que toda plataforma vaya generando. Si la justicia predictiva, así como varias de las tecnologías «inteligentes» que hemos analizado pueden tener un impacto en cuanto al papel que jugarán la máquina y el ser humano en el futuro, en todos casos los derechos de los ciudadanos deben ser respetados en el marco de una justicia digital.

CAPÍTULO 39

AUTONOMÍA PRIVADA Y AUTOTUTELA: OPORTUNIDADES Y RIESGOS DE LOS *SMART CONTRACTS*

JORGE FELIU REY
Profesor Lector Doctor de Derecho Mercantil
Universidad Carlos III de Madrid

1. INTRODUCCIÓN

Uno de los fenómenos que actualmente está más presente en los medios de comunicación y la prensa económica y que está despertando cada vez mayor interés en la doctrina jurídica es la genéricamente denominada tecnología *Blockchain* y los llamados *Smart Contracts* («contratos inteligentes» en una traducción literal poco frecuente, sin embargo).

Sobre la primera, la tecnología Blockchain, su aplicación más conocida en los Bitcoin, y otras variantes de *distributed ledgers*, ya existen trabajos numerosos sobre las posibilidades de aplicación y las promesas de futuro. Sobre los segundos, aunque el término se usa ya con frecuencia y existen algunos trabajos sobre la materia, su aparente novedad implica que no exista aún una literatura consolidada sobre este fenómeno. De modo que, las definiciones son diversas, dependiendo de la aproximación de cada disciplina, y los pronósticos sobre sus efectos y aplicaciones difieren según aproximaciones más o menos realistas.

Como expondremos en los siguientes apartados, los *Smart Contract* son en términos muy generales un conjunto de protocolos informáticos, que permite a un dispositivo por sí mismo procesarlos y ejecutarlos de forma autónoma, sin necesidad de intervención humana. Si esta tecnología la utilizamos para transacciones entre personas, permitiría, junto a la tecnología genéricamente denominada blockchain, en principio, que la verificación de las condiciones para ejecutar una operación y la propia realización de la operación, como prestación acordada, no requiere intermediarios, y que la gestión, la concreción y la ejecución de las prestaciones mediante las operaciones programadas no precisen de intervención humana.

La ausencia de intervención humana y su sustitución por un proceso (conjunto de protocolos) que permite la automatización de operaciones; la concreción automática de las prestaciones en las transacciones; el cumplimiento automático de las mismas; y la utilización de otras tecnologías que permiten la verificación de la información y de la identidad de los sujetos implicados en la transacción, conduce a un elevado ahorro de cos-

tes (1). Efectivamente, imaginemos, ante la cancelación o el retraso de un vuelo, la operativa para atender reclamaciones, gestionar compensaciones y permitir el ejercicio de los derechos de los que son titulares los pasajeros de ese vuelo para tal supuesto. Frente al empleo de la vía de reclamación tradicional, el tiempo y los recursos necesarios para la gestión de las reclamaciones se reducirían drásticamente si un sistema automático verifica el retraso del vuelo, identifica a los pasajeros afectados, acredita el reconocimiento y efectividad de los derechos, y tramita las reclamaciones masivas y las compensaciones. O imaginemos el supuesto de un incumplimiento contractual de una transacción específica. Normalmente, los gastos en que incurre la parte que quiere hacer cumplir el contrato son elevados (pruebas, verificaciones, auditorías, conciliación previa, intentos de negociación, contratación de abogado, procurador, costas), más los costes que se imputan a la sociedad en general por la resolución de las disputas. Si el contrato se puede cumplir en sus propios términos de forma automática y/o predeterminar las consecuencias del incumplimiento del contrato y permitir su ejecución de forma automática, sin posibilidad de injerencia humana, los costes de transacción se reducirían en gran medida (2), y las expectativas de las partes para la satisfacción de sus intereses conforme a lo establecido en el contrato se verían ampliamente protegidas. Rapidez, previsibilidad y automatización marcarían las coordenadas del ejercicio de la autonomía de la voluntad y facilitarían una creciente y efectiva autotutela.

No obstante estas evidentes ventajas, esta figura presenta limitaciones y desventajas y plantea posibles problemas a los que el Derecho debe hacer frente. En este trabajo explicaremos primero brevemente el fenómeno de los *Smart Contracts* (infra 2), y los enmarcaremos en su particular ecosistema (infra 3), para, a continuación, abordar algunas cuestiones jurídicas de los *Smart Contracts* desde dos perspectivas: la autonomía de la voluntad de las partes para acordar lo que estimen adecuado para satisfacer sus intereses, y la posibilidad de uso y el alcance de los mecanismos de autotutela (infra 4).

En este marco, podremos pronunciarnos brevemente sobre el impacto que la generalización de los *Smart Contracts* pueda tener sobre la función futura del Juez o del abogado, y sobre la progresiva conformación de

(1) Sobre este aspecto es interesante el documento elaborado por Capgemini Consulting, *Smart Contracts in Financial Services: Getting from Hype to Reality.* Del mismo modo el documento elaborado por Smart Contracts Alliance, *Smart Contracts: 12 Use Cases for Business & Beyond. A Technology, Legal & Regulatory Introduction*, Chamber Digital Commerce, December 2016.

(2) Freeman, Edward H., «Software Repossession: Electronic Self-Help», *Information Systems Security*, vol. 12:6, 2004, p. 3.

un ordenamiento jurídico paralelo, de base contractual y que opera sobre la infraestructura tecnológica.

2. *SMART CONTRACT*

2.1 **Definición**

Formular una definición de *Smart Contract* no resulta una tarea sencilla, y así lo demuestra la variedad de definiciones diferentes que proponen los trabajos sobre la materia, o la total elusión de una definición con la que otros abordan el fenómeno sin definirlo. Más aún, su complejidad se agudiza por la diversidad de disciplinas que convergen en el estudio de esta figura (p. ej. jurídica, matemática, informática). Por tanto, dependiendo de la disciplina desde la que se trabaje, así como de la función primordial que debe cumplir o que se le atribuye a esta figura, las definiciones y sus características varían.

Una de las primeras definiciones conocidas es la formulada por Nick Szabo, que fue quien acuñó este término, y que definió *Smart Contract* como *a set of promises, specified in digital form, including protocols within which the parties perform on these promises* (3). Partiendo de esta definición germinal, las ulteriores definiciones se podrían clasificar en varios grupos. Un primer grupo de definiciones se centra en el automatismo de su ejecución sin intervención humana, pero haciendo referencia a la figura de «contrato», «acuerdo» o «promesas» (4). En esta misma línea, otras, aun haciendo referencia a la dimensión contractual, sin embargo, centran la descripción en la función del código informático (5). Por otro lado, se encuentran también aquellas otras propuestas que son más neutras y genéricas y eluden toda referencia a los términos «contrato»,

(3) Szabo, Nick, *Smart Contract: Building Blocks for Digital Markets*, 1996, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html.

(4) Así, algunos autores, Wright, Aaron; De Filippi, Primavera, «Decentralized blockchain technology and the rise of lex cryptographia», pp. 10 y 11. https://ssrn.com/abstract=2580664, los han definido como «digital, computable contracts where the perfomance and enforcement of contractual conditions occur automatically, without the need for human intervention». Otros, Werbach, Kevin; Cornell, Nicolas, «Contracts ex machina», *Duke Law Journal*, vol. 67, 2, 2017, p. 320, como un «agreement in digital form that is self-executing and self-enforcing». Y, en similar sentido, Raskin, Max, «The law and legality of Smart Contracts», *Georgetown Law Technology Review*, vol. 1, 2017, p. 309, «is an agreement whose execution is automated (…) often effected through a computer running code that has translated legal prose into an executable program».

(5) *Are software codes that embed the terms and conditions of a contract and that run on a network leading to a partial or full automated self-execution and self-enforcement of the contract* Hourani, Sara, «Cross-Border Smart Contracts: Boosting International Digital Trade through Trust and Adequate Remedies», en *Modernizing International Trade Law to Support Innovation and Sustainable Development, Proceedings of the Congress of the United Nations Commission on International Trade Law*, Vienna, 2017, en http://www.uncitral.org/pdf/english/congress/Papers_for_Programme/11-HOURANI-Cross-Border_Smart_Contracts.pdf.en.

«acuerdo» o «promesas», definiendo *Smart Contract* como un simple programa informático que ejecuta órdenes predefinidas cuando se verifican ciertas condiciones dentro del sistema (6), o, las que se centran en esta idea, pero en relación con la tecnología *blockchain* o *decentralized ledgers* (7) como base.

Desde una perspectiva técnica, se califica de *Smart Contract* tanto un contrato de opción de compra de acciones cuyo ejercicio se ejecuta automáticamente cuando se produce determinado hito (plazo y/o valor de cotización), como simples archivos que gozan de las cualidades de inmutabilidad o integridad del contenido, pero sin valor contractual en un sentido jurídico. En todos ellos suele concurrir un importante elemento de automatismo en la ejecución de instrucciones (o prestaciones) o incluso en la remediación de un incumplimiento de lo programado. Pero, ciertamente, no todas las situaciones que se describen ampliamente con este término responden a un negocio jurídico autoejecutable.

Por tal motivo, y para abarcar con la mayoría de los supuestos, la definición de un *Smart Contract* tiene que ser neutra, recogiendo sus características principales, sin perjuicio de que, en alguno de los supuestos, los *Smart Contract*, puedan tener naturaleza contractual cuando reúna los requisitos que establece cada ordenamiento jurídico.

En este trabajo abordamos precisamente los supuestos en los que el *Smart Contract* tiene naturaleza contractual representando el acuerdo íntegro o incorporándose como parte de un contrato.

2.2 **Forma y lenguaje**

El *Smart Contract* deberá estar redactado en un lenguaje específico, lo que implica a su vez que debe revestir una forma determinada para la obtención de determinados efectos. Por tanto, en la comprensión jurídica de los *Smart Contracts*, hay dos componentes esenciales: el lenguaje y la forma.

---

(6) Definición facilitada en el curso edX: *Blockchain for Business –An introduction to Hyperledger Technologies*. LinuxFoundationX /LFS171x/.

(7) *Computer programs that can be consistently executed by a network of mutually distrusting nodes, without the arbitration of a trusted authority,* Bartoletti, Massimo; Pompianu, Livio, «An empirical analysis of smart contracts: platforms, applications, and design patterns», 2017, https://arxiv.org/abs/1703.06322v1, p. 1. En esta misma línea, Greenspan, Gideon, *Beware of the Imposible Smart Contract*, http://www.the-blockchain.com/2016/04/12/beware-of-the-impossible-smart-contract define *Smart contract* como «a piece of code which is store on an Blockchain, triggered by Blockchain transactions, and which reads and writes data in that Blockchain´s database». O la que resulta más común en los distintos foros, que la define como «una herramienta de código computacional programable (*scripts*) que se almacenan en una red de *blockchain* y se ejecuta de forma autónoma. Una tecnología que permite que se realicen uno o varios términos contractuales entre varios agentes que responden a una lógica booleana (si esto, entonces esto). https://www.elderecho.com/actualidad/blockchain-smarts-contracts-ESADE-Lefebvre-tecnologia-jornada_0_1192875033.html.

2.2.1 La importancia del lenguaje y sus implicaciones

Un componente esencial para la existencia y la consecución de los efectos inherentes a los *Smart Contracts* es el lenguaje, que es lo que obliga, en definitiva, a la existencia de una forma determinada. Para lograr los efectos de automatismo y autoejecución, es necesario que el dispositivo pueda ejecutar las acciones deseadas para el cumplimiento de las obligaciones. A tal fin, estas acciones deben programarse mediante protocolos o instrucciones incorporadas en el lenguaje código, el lenguaje máquina, ya que el lenguaje humano no es capaz de procesarlo (8). En este sentido, debemos advertir que, en el estado actual de la tecnología, el dispositivo, en realidad, no entiende conceptos, sino que ejecuta instrucciones tal y como están programadas. Es decir, cuando presionamos la tecla de impresión, para imprimir un documento, el dispositivo no entiende el concepto de impresión ni la orden, ejecuta sencillamente un protocolo que consigue la finalidad querida, es decir, la obtención en soporte papel de un contenido que estaba en soporte digital. Otro ejemplo algo más sofisticado, en el que ya comenzamos a incorporar nociones de tecnología más avanzada con soluciones de inteligencia artificial, sería el caso de un coche autónomo ante el que se cruza una pelota. Con seguridad, el vehículo se detendrá o aminorará la marcha ante la identificación de un obstáculo, porque así se ha programado antes, pero difícilmente, en el estado actual de la técnica, será capaz, por sí solo de intuir, que tras la pelota pueda aparecer corriendo un niño intentando recuperarla.

Asumir que la programación del *Smart Contract* debe ser en lenguaje máquina tiene significativas implicaciones. Frente al lenguaje humano que juega con matices y ambigüedades, es indeterminado, en ocasiones, desestructurado, el lenguaje máquina, que debe ser leído y procesado correctamente por un dispositivo, es restringido, estructurado, predefinido.

Por tanto, el lenguaje máquina no permite ambigüedades ni imprecisiones. Las decisiones se estructuran en instrucciones condicionales, *si A entonces B, si C entonces D*. Esto implica, como expondremos más adelante en otro apartado, que, actualmente, dado el estado actual de la técnica, no será posible codificar cualquier obligación en un *Smart Contract*, por las propias limitaciones del lenguaje para describir la obligación, «comprenderla», comprobar o verificar su cumplimiento y, en su caso,

(8) Surden Harry, «Computable Contracts», *U.C. Davis L. Rev.*, Vol. 46, 2012, pp. 633 y ss., quien afirma que «(…) contemporary computer algorithms cannot read or understand even basic written language texts anywhere near the sophistication exhibited by a person of ordinary literacy». A nota a pie (n.º 10) explica que el estudio de los algoritmos que permitan a los ordenadores comprender el lenguaje humano es conocido como «procesamiento del lenguaje natural» [*natural language processing* (NLP)].

llevar a cabo las actuaciones programadas, en caso de incumplimiento, o al menos no será posible plantearla en los mismos términos y con la misma extensión.

2.2.2 La forma

Como hemos mencionado anteriormente, para la consecución de los efectos inherentes a los *Smart Contracts* es necesario el empleo de un lenguaje determinado que permite la ejecución autónoma de las órdenes y que determina, a su vez, el recurso a una forma específica para el acuerdo. La necesidad de que revista una forma determinada en un lenguaje específico cumple además y, sobre todo, una función de eficacia, y su ausencia puede implicar perder sus efectos consustanciales (p. ej. el automatismo en su ejecución, en la concreción de las prestaciones o en la aplicación de las consecuencias del incumplimiento).

Sobre esta cuestión deben añadirse dos consideraciones, principalmente, cuando entendemos el *Smart Contract* tiene efectos jurídico-obligacionales. La primera, la constatación de que la forma, entendida en un sentido amplio, ya no tiene una mera función de soporte o documentación, de mera exteriorización y concreción de la voluntad de las partes, sino que adquiere además una singular función como componente dinámico esencial para la eficacia del *Smart Contract*. Más allá del tradicional papel estático de la forma como repositorio, documentación o prueba o requisito de validez, proponemos así nuestra tesis de la forma como componente dinámico del *Smart Contract* para asegurar su cualidad de autoejecutable.

Esto puede implicar que las partes quieran que el contrato revista la forma específica de *Smart Contract* con eficacia constitutiva. Lo que significaría que las partes han acordado, en el ejercicio de su autonomía de la voluntad, que sus declaraciones de voluntad no sean válidas y eficaces hasta la conclusión del *Smart Contract* (9). O bien, dejando a un lado este caso particular, y por el principio espiritualista que rige nuestro derecho respecto a la forma de los contratos (art. 1.278 CC), perfeccionado el

(9) En este sentido, el artículo 2.1.13 de los Principios Unidroit 2016 sobre los contratos comerciales internacionales (en adelante PICC2016) contempla este supuesto al establecer que «cuando en el curso de las negociaciones una de las partes insiste en que el contrato no se entenderá perfeccionado hasta lograr (…) una forma en particular, el contrato no se considerará perfeccionado mientras no se (…)» alcance tal forma. Conforme a los comentarios explicativos del citado artículo, una o ambas partes pueden manifestar de forma clara que no quedarán vinculados a menos que se haya redactado en un documento formal, por lo que no existirá contrato hasta dicho momento, independientemente de que las partes hayan concretado todos los aspectos relevantes de la operación. Por tanto, en este supuesto, no sólo el *Smart Contract* es un contrato, sino que además será su conclusión como tal, en el lenguaje máquina y en la forma de que le dota la programación en ese código para su posterior ejecución, cuando se considere perfeccionado el acuerdo entre las partes.

contrato y acordando buscar los efectos propios de los *Smart Contract* (v.gr. verificación, confianza y automatismo), las partes podrían compelerse recíprocamente a que se cumpla la forma acordada para obtener la citada finalidad.

La segunda consideración se proyecta sobre lo que consideramos un estadio más en la evolución de la forma en los contratos. La forma, en un sentido amplio y genérico, o la documentación de los contratos, en un sentido concreto, ha evolucionado de forma visible a lo largo de la historia de la humanidad. La evolución de la forma ha estado relacionada, al menos parcialmente, con el soporte. Desde los soportes más antiguos como la piedra, la madera, el papiro o el aún contemporáneo papel, hasta los soportes más actuales como el electrónico. La aparición de cada uno de ellos supuso un cambio más o menos disruptivo en la forma de comunicar declaraciones, transmitir conocimiento, documentar acuerdos y hacer memoria.

Esta evolución y el tratamiento legal del soporte digital revelan el mantenimiento de un elemento común en todos esos soportes, su función básicamente pasiva o de documentación, como repositorios. Es decir, actúan todos ellos como un mero soporte donde se recogía lo acordado por las partes, de modo que el cumplimiento de las obligaciones y su posible exigibilidad exigían una actividad o, en su caso, en las obligaciones de no hacer, la pasividad, de las partes o de un tercero. Por tanto, estos soportes (10) cumplían la función de documentar el contrato, entendido como *la operación o conjunto de operaciones necesarias para plasmar o recoger documentalmente las declaraciones de voluntad que forman la esencia del contrato* (11), pero, en definitiva, dependían del ser humano para cumplir con sus términos.

Pero el desarrollo de la tecnología ha permitido que el dispositivo pase a formar parte activa del proceso transaccional, bien en la concreción o determinación de las obligaciones, o bien en su ejecución. Así, nuestra propuesta se concreta en afirmar que en los *Smart Contract* la forma, soporte, código y lenguaje combinados, además de esa función de mero soporte cumple también una función activa en el desarrollo y consumación del contrato. Por tanto, el *Smart contract* no puede calificarse meramente como un contrato electrónico. Si bien la concurrencia del soporte digital parecería facilitar esta definición, es claro que no resulta suficiente para definir la cualidad de automatismo ni la capacidad de autoejecución.

(10) En este sentido, Werbach, Kevin; Cornell, Nicolas, «Contracts ex machina», cit., pp. 6 y 7.
(11) Díez-Picazo y Ponce de León, Luis, *Fundamentos de Derecho civil patrimonial*, cit., vol. I.

3. EL ECOSISTEMA DE LOS *SMART CONTRACTS*

3.1 **La importancia de la confianza y la seguridad: *Decentralized ledgers Technology***

Si bien los *Smart Contracts* no constituyen un fenómeno nuevo, pues ya existían aplicaciones conocidas en algunos sectores, su relación con la ya frecuentemente mencionada y bien conocida tecnología Blockchain o *Decentralized ledgers* les ha permitido adquirir una dimensión y un protagonismo realmente destacables. En efecto, estas estructuras descentralizadas representan un elemento clave del ecosistema de los *Smart Contracts* que les permite lograr determinados efectos.

Efectivamente, los *Smart Contracts,* para que sean eficaces en el sentido de autoejecutables, necesitan operar en o en relación con uno o varios dispositivos que ejecutan las operaciones reflejadas en el código programado. Esta relación de dependencia nos conduce a plantear la cuestión sobre la necesidad de que este dispositivo sea de confianza para las partes del contrato y de fiabilidad suficiente para que ejecute los protocolos. De igual modo, desearán asegurar las partes que no se puede realizar ninguna modificación o alteración del código, así como, y esto es muy importante, que no puedan resultan interrumpidos los procesos de acción y ejecución autónomos.

En definitiva, la eficacia automática de los *Smart Contracts* requiere un marco de confianza y seguridad adecuado a la finalidad que se pretende. Para ello hay que buscar una tecnología que permita la inmutabilidad del código, que acredite el cumplimiento de las prestaciones y facilite la ejecución de las mismas. Tradicionalmente, esta confianza y seguridad se ha logrado mediante la intervención de intermediarios, pero con la irrupción de la tecnología *blockchain,* así como, en general de los denominados *Decentralized ledgers*, se podría reemplazar el recurso a estos intermediarios como tercero de confianza por una solución tecnológica que, en principio, parece dar respuesta a estas necesidades con una interesante transformación de la geometría de las relaciones (12).

(12) El funcionamiento de esta tecnología se basa en la combinación de tres elementos: cadenas de bloques, criptografía y mecanismos descentralizados de consenso. Utilizaremos un símil para ilustrar su operativa y los resultados esperados. Imaginemos una mesa de reuniones alrededor de la cual se sienta un número significativo de personas. Cada una de estas personas (ordenadores o nodos conectados) tiene un libro de registro en blanco donde realiza anotaciones (sistema descentralizado). La primera anotación, sigamos con el ejemplo, es que A tiene 50 acciones y se las quiere transmitir a B. Primero se verifica que A tiene 50 acciones que puede transmitir (bloque con información), y se comprueba que todos los miembros de la mesa están de acuerdo con esta anotación inicial (sistema de verificación por consenso descentralizado). Luego se transmite a B. Como todos tienen en su libro que A es el titular y las puede transmitir, proceden a anotar la transmisión a B. Si A quiere volver a transmitir esas acciones, no podría porque ya no consta en el

Se entiende así que la necesaria fiabilidad que los *Smart Contracts* precisan en la autoejecución, la inmutabilidad de las anotaciones, y el reconocimiento de los derechos para actuar en las transacciones subsiguientes viene conferida por esta tecnología. Si bien la tecnología de los *Decentralized ledgers* opera como uno de los elementos operacionales de los *Smart Contracts,* sin embargo, está impactando en su propia sustancia, de modo que llega a incorporarse en la definición misma de esta figura y su tratamiento legal. Así, en efecto, algunos autores formulan la definición de *Smart Contract* en relación con esta tecnología. Del mismo modo, algunas legislaciones que han abordado la regulación de los *Smart Contracts*, definen esta figura en estrecha relación con esta tecnología. La reciente legislación de Arizona ofrece un ilustrativo ejemplo al definir *Smart Contract* como «an event-driven program, with state, that run on a distributed, decentralized, shared and replicated ledger and that can take custody over and instruct transfer of assets on that ledger» (13). Pero también es cierto que han comenzado con ciertas limitaciones respecto a su ámbito de aplicación. Es el caso del Estado de Arizona donde una nueva Ley considera ilegal requerir que una persona que use o esté sujeta a una tecnología electrónica de trazabilidad de armas de fuego (*electronic firearm tracking technology*) (14) o que revele cualquier información identificable sobre la persona o el arma de fuego de la persona con el propósito de usar la tecnología electrónica de seguimiento de este tipo de armas (15).

---

registro como titular y los miembros de la mesa al verificar tal información rechazarían la anotación, por lo que no permitirían esa transacción. Sólo B podría transmitir las acciones ulteriormente. Intentar una alteración de los registros, aunque no es imposible, exigiría un consenso de todos los miembros de la mesa y una modificación en todos los nodos de cadenas de bloques que recogen un tracto sucesivo, lo que resultaría, sin duda, altamente improbable.

(13) El 31 de marzo de 2017, el Senado de Arizona aprobó la *bill* HB 2417 reconociendo *blockchain signature* y los *Smart contracts*. Conforme a la citada aprobación se modifica la *Arizona Electronic Transactions Act* (AETA), incluyendo el artículo 5 (§44-7061). En el caso del Estado de Delaware, con la iniciativa iniciada en el año 2016 denominada *Delaware Blockchain Initiative*, cuyos objetivos son, alguno ya alcanzado, el uso de la tecnología de los *Distributed ledger* en los Registros Públicos; el uso de las «Smart UCC fillings» en los sistemas de registro de notificaciones en los secured trasnsactions y, el uso de la tecnología de los *Distributed ledger* en las acciones, para de esta manera llevar a cabo la trazabilidad de las emisión y transferencia de acciones. Tinianow, Andrea, «Delaware Blockchain Initiative: Transforming the Foundational Infrastructure of Corporate Finance», en https://corpgov.law.harvard.edu/2017/03/16/delaware-blockchain-initiative-transforming-the-foundational-infrastructure-of-corporate-finance/.

(14) A los efectos de la citada Ley por «electronic firearm tracking technology» significa a platform, system or device or a group of systems or devices that uses a shared ledger, distributed ledger or block chain technology or any other similar form of technology or electronic database for the purpose of storing information in a decentralized or centralized way, that is not owned or controlled by any single person or entity and that is used to locate or control the use of a firearm. Electronic firearm tracking technology does not include a law enforcement database, including the adult probation enterprise tracking system, the juvenile on-line tracking system, the justice web interface, the Arizona criminal justice information system, the national crime information center, the national integrated ballistic information network and a local records management system that is used to manage or process stolen, lost, found, stored or evidentiary firearms.

(15) https://legiscan.com/AZ/text/HB2216/2017

3.2 **Los oráculos**

Por otro lado, es posible que determinados *Smart Contracts* necesiten obtener información del exterior con el fin de, bien concretar las prestaciones, bien proceder a su cumplimiento. A tal fin, el funcionamiento de los *Smart Contracts* depende de otro importante componente de su ecosistema: los oráculos.

Pensemos, por ejemplo, que se concluye un *Smart Contract* en que se deja para una ulterior determinación el precio conforme al valor de cotización de las acciones de una empresa en una fecha concreta o conforme a un determinado índice. Para completar la ejecución el *Smart Contract* deberá conocer en esa fecha determinada cuál es el valor de cotización o del índice y tal información deberá integrarse en el *Smart Contract* para la ejecución automática de las acciones programadas correspondientes. O pensemos en otro caso en el que la cuota pagadera cada mes por el uso de un vehículo durante un año depende del tiempo de uso efectivo. El *Smart Contract* necesitará obtener esta información para poder calcular la cuota correspondiente y llevar a cabo el efectivo cobro.

Esas fuentes de información que suministran datos a un *Smart Contract* son los denominadas *oráculos*. Al igual que en la Antigüedad grecorromana, las personas solían acudir a un lugar sagrado, donde la deidad correspondiente, a través de un intermediario, transmitía un pronóstico o predicción. Hoy, en el caso de los *Smart Contract*s, el dispositivo debe acudir a un tercero para que le suministre la información necesaria para poder continuar con la ejecución de las prestaciones. Cuando el *Smart Contract* funciona sobre un sistema *blockchain* uno de los problemas que generaría el recurso a fuentes externas para recabar datos es que tal información debería ser recibida de forma idéntica por todos los nodos relevantes. Por ello, el recurso a los oráculos resolvería los problemas técnicos porque es el oráculo el que inserta la información como transacción en la cadena y, de ese modo, está disponible y se mantiene inmutable para todos los nodos implicados.

La determinación del oráculo o de los oráculos por las partes será uno de los elementos, como expondremos en un epígrafe posterior, que debemos tener en cuenta en la elaboración de un *Smart Contract*. Del mismo modo, el empleo de oráculos implica el riesgo de abrir una vía indirecta para «hackear» *el Smart Contract*.

3.3 *Contractware* e internet de las cosas

Por último, también es posible que para la obtención de la finalidad que se pretende, el cumplimiento automático de las prestaciones (16), sea preciso contar con otras tecnologías, que en conjunción con los *Distributed ledgers,* forman parte del ecosistema de los *Smart Contracts*. Si el *Smart Contract* no tiene control sobre la ejecución de las prestaciones o sobre las consecuencias del incumplimiento, el automatismo y la autonomía en la ejecución no pueden lograrse. Para ello es necesario que el *Smart Contract* pueda ejecutar esas decisiones en cumplimiento de los términos contractuales con acciones en el entorno físico (p.ej., ante el impago de la cuota de leasing de un coche, se desactiva el dispositivo de arranque y no puede circular) sin necesidad de la intervención de las partes o de otros sujetos.

La capacidad de realizar estas tareas depende de lo que la doctrina ha denominado *contractware* (17), definidos como la plasmación física o digital de los términos del contrato mediante dispositivos que realizan una acción derivada de la ejecución de un *Smart Contract*. Según Raskin, esta plasmación no necesita ser una pieza o activo físico (p. ej. Hardware) sino que puede requerir la intervención de otro código que realice la acción convenida (p.ej. la desactivación de una clave de acceso o la inhabilitación de una cuenta).

4. CUESTIONES RELATIVAS A LA FORMACIÓN DEL CONTRATO

Si partimos de la asunción de que el *Smart Contract* está escrito, total o parcialmente, en lenguaje formal o máquina, surgen inmediatamente cuestiones vinculadas a la formación del contrato de enorme transcendencia, que pueden, de hecho, afectar tanto a la validez del contrato como a su eficacia.

4.1 Consentimiento

En primer lugar, la conclusión del contrato como acuerdo de voluntades pivota alrededor de la válida emisión del consentimiento. Sobre el

(16) Conforme a Raskin, Max («The law and legality of Smart Contracts», *Georgetown Law Technology Review*, vol. 1, 2017, p. 308), «the combination of these components –contractware and blockchains– has made smart contracts that are enforced by a decentralized, third-party network possible».

(17) Según *Ibid.*, pp. 307 y ss., «contractware can be defined as the physical or digital instantiations of contract terms onto machines or other property involved in the performance of the contract. By instantiation, we mean taking the terms of the agreement and either writing them into previously existing software or writing them into software that is connected in some way to a machine that implements the contract». Este autor aclara (nota al pie n.º 4) que este término de «contractware» «has appeared elsewhere to refer to commercial software offerings that facilitate the workflow and writing of traditional contracts».

consentimiento en los *Smart Contracts* hay que realizar varias consideraciones. Primera, se plantea la cuestión de la comprensibilidad. Con carácter general, es preciso distinguir entre el acuerdo de voluntades entre las partes para quedar obligados y la expresión de este acuerdo en una forma concreta o determinada. En un *Smart Contract* esta expresión del acuerdo ha de realizarse mediante lenguaje máquina adecuado para su ejecución. Por tanto, resulta pertinente plantearse cómo asegurar la comprensión del clausulado y así la emisión consciente del consentimiento sobre las prestaciones cuando el acuerdo sólo se elabora en lenguaje máquina sin «transcripción» en lenguaje humano.

Esto resulta más complicado cuando estos tipos de contratos además se estandarizan y se ofrecen a una pluralidad de destinatarios, porque entonces entramos en el ámbito de las condiciones generales de contratación que activan los controles de incorporación, interpretación y contenido a las que están sometidos. Más aún, aun en el caso en que no tuvieran la consideración de condiciones generales, cuando una de las partes tenga condición de consumidor, le serán aplicables todas las normas de tutela y protección que correspondan, en particular, respecto a la abusividad de determinadas cláusulas.

4.2 **Diferencias entre lo acordado y el código**

Otra de las cuestiones relacionadas con la formación y derivada de la dualidad lenguaje máquina-lenguaje humano es la que podría surgir si los términos redactados en lenguaje máquina difieren de lo acordado efectivamente por las partes o si el código no es correcto para lograr la finalidad acordada. Es posible que lo acordado entre las partes al programarse en lenguaje máquina, que por su propia configuración no permite ambigüedades ni conceptos indeterminados, implique un cambio en el sentido original de la prestación o en su alcance.

En este sentido, se pueden presentar, con carácter general, tres escenarios distintos. Primero, que la diferencia entre la prestación querida y la obtenida sea insignificante, por lo que dependiendo el caso y en atención a las expectativas de las partes podríamos entender que ha existido un cumplimiento del contrato y que los intereses de las partes se han satisfecho. Segundo, que la diferencia entre lo querido y lo logrado sea apreciable y, por tanto, que podamos estar ante situaciones de cumplimiento parcial de la prestación. Por último, que la prestación realizada sea diametralmente distinta a la pactada, caso en el que podríamos encontrarnos ante el supuesto de incumplimiento esencial o de *aliud pro alio*.

Como expondremos más adelante en el apartado dedicado a la ejecución, es posible que el desarrollo en la ejecución del contrato sea imparable y el contenido del mismo inmutable, con las consecuencias que de ello

se derivan. Por otro lado, y en el mismo sentido, se deben analizar la cuestión de la responsabilidad, ya que el cumplimiento de la prestación, en algunos supuestos, no lo realiza el ser humano sino la máquina, que cumple con los protocolos que han sido programados. Por tanto, se deberá determinar quién es el responsable de la inadecuada o insatisfactoria ejecución de las instrucciones de la prestación, a efectos de la responsabilidad y la determinación del incumplimiento.

4.3 **Posibles soluciones**

Para evitar, o mitigar en la medida de lo posible, las posibles controversias o conflictos que puedan surgir en relación con estos aspectos relacionados con la formación del contrato, en definitiva, con los problemas de comprensibilidad del código, y sus consecuencias, la práctica contractual (18) y la doctrina (19) plantean varias soluciones.

La primera de ellas es que las partes suscriban previamente un contrato en lenguaje natural donde se establezca todo el contenido del contrato y, a su vez, se determine el código del *Smart Contract* y su interpretación (*data-meaning threshold agreement*). Variante de esta solución, porque no necesita de la suscripción anterior de un contrato previo, es someterse a algún estándar de datos existente. De esta forma, las partes al adherirse al mismo ya conocen, por ser común y compartido, los formatos de datos, sus interpretaciones, etc. De esta forma, como bien afirma Surden (20), los beneficios de adherirse a estos estándares son, primero, que las partes no necesitan dedicar recursos a crear sus propias definiciones; segundo, que permite que múltiples partes puedan interactuar unas con otras usando un sistema común de datos compartidos. Esta solución es muy utilizada en los mercados financieros

La segunda solución es el uso de interfaces para la contratación electrónica, diseñados y facilitados por determinadas empresas, los cuales permiten a las personas que quieren contratar utilizarlas e introducir las prestaciones en lenguaje natural que la propia interface traduce en lenguaje máquina.

Por último, las partes puede suscribir un acuerdo marco (*procedural agreements*) (21), donde acuerdan y determinan todas las condiciones que se aplicarán a los sucesivos *Smart Contracts*.

---

(18) Clack, Christopher D.; Bakshi, Vikram A.; Braine, Lee, «Smart Contract Templates: foundations, design landscape and research directions», *The Computing Research Repository*, 2016.
(19) Surden, Harry, «Computable Contracts», *U. C. Davis L. Rev.*, vol. 46, 2012., pp. 615 y ss.
(20) *Ibid.*, p. 653
(21) Ejemplo de ello es el ISDA (*International Swaps and Derivates Association, Inc.*) *Master Agreement.*

5. CUESTIONES SOBRE EL CUMPLIMIENTO

5.1 **Determinación de las obligaciones y su cumplimiento**

La primera está relacionada con la formación, pero la recogemos aquí por su incidencia directa y significativa en la fase de cumplimiento. Es la relativa a la determinación de las obligaciones y la comprobación de su cumplimiento. Como sabemos, los *Smart Contracts* no permiten una configuración abierta e indeterminada, mediante el uso del código tienen que especificarse y describirse las prestaciones de un modo que sean fácilmente ejecutables, es decir, concretas y determinadas. Por tanto, permiten con facilidad determinar de modo efectivo ciertas obligaciones, p. ej. pagar en una fecha determinada, ejecutar una opción de compra en las que la concreción es muy elevada, la prestación se define de forma completa, y no es preciso recurrir a la interpretación para confirmar la ejecución o proceder a ella.

De hecho, se han identificado como características comunes de los *computable contracts,* que se podría aplicar por extensión a los *Smart Contracts* (22), primero, la necesidad de que las obligaciones sean fácilmente identificables (el día del ejercicio de la opción, la fecha de mayoría de edad, el valor de una acción de una sociedad cotizada); segundo, que el cumplimiento de las obligaciones no esté sujeto a interpretaciones, a excepciones o variables de difícil determinación.

De ahí que determinadas obligaciones genéricas como mantener en buen estado un bien, exigir determinadas conductas conforme al principio de razonabilidad o buena fe, resulten, en cierta medida de difícil reflejo en el *Smart Contract* ya que llevan implícito un juicio humano (23). Aunque ello no es óbice para intentar buscar por otras vías parecidos resultados. Por ejemplo, si la obligación es mantener en buen uso un vehículo industrial, se podría sustituir tal obligación indeterminada por la obligación de ir al taller o a un tercero conforme a un calendario de revisiones, para determinar el estado de la máquina y suministrar esa información al *Smart Contract*, mediante un dispositivo instalado en el vehículo que suministre igualmente los datos relevantes sobre el estado del mantenimiento y/o las condiciones de uso. En definitiva, la idea es intentar determinar lo indeterminado, es decir, objetivarlo y transformarlo en obligacio-

(22) Surden, Harry, «Computable Contracts», cit., pp. 682 y 683.

(23) En este sentido, Werbach, Kevin; Cornell, Nicolas, «Contracts ex machina», *Duke Law Journal*, vol. 67, 2, 2017, p. 43, quien afirma que «some contractual terms simply cannot be expressed through formal logic, because they imply human judgment. A machine has no precise way to assess whether a party used "best efforts", for example». En el mismo sentido, Cuccuru, Pierluigi, «Beyond bitcoin: an early overview on smart contracts», *International Journal of Law and Information Technology*, vol. 25, 2017, p. 190.

nes específicas, verificables, y susceptibles de control por un sistema automático. El problema es que la determinación implica inevitablemente que se pierda la amplitud del abanico de supuestos y matices que abarcan esos principios o estándares de conductas.

Además, y en relación con lo anterior, los contratos deben ser completos, en el sentido que la máquina no podrá interpretarlos ni contextualizarlos en un marco jurídico –sin perjuicio de los avances de la inteligencia artificial esperados en este sentido–, por lo que limita aún más su ámbito de aplicación. Por ejemplo, y con carácter general, una prestación de servicios es, por un lado, de difícil determinación a los efectos de posibles incumplimientos, pero también la dificultad de contextualizar la prestación de servicios bajo determinadas condiciones en un marco normativo.

5.2 **Legalidad del contenido y en su ejecución**

Se ha afirmado en determinados foros tecnológicos que los *Smart Contracts* junto con la tecnología *Blockchain* crea o permite la creación de un ecosistema propio, en cierta medida, ajeno al legal. Entendemos que esta afirmación no es del todo cierta, si el *Smart Contract* es un contrato, redactado en lenguaje máquina, esto no implica que quede ajeno a los requisitos que el ordenamiento jurídico exige al contenido de las prestaciones. Por tanto, deberá pasar también el filtro de la legalidad sustantiva. Cuestión esta que no resulta del todo sencilla si pretendemos que esta labor de contraste sea también automatizada.

Por otro lado, podemos encontrarnos ante un *Smart Contract* cuyo contenido sea válido pero su ejecución en un momento determinado o en una orientación específica despierte dudas sobre su legalidad. Ejemplo de ello lo encontramos en el ámbito no digital con determinados pactos parasociales, donde su contenido puede ser lícito (un sindicato de voto) pero su ejecución puede tener efectos ilícitos (ejercicio de voto con abuso de la minoría).

5.3 **Determinación de los oráculos y posibles consecuencias**

Por otro lado, y no menos importante, hay que retomar la necesidad de acordar previamente los oráculos. Ya que el *Smart Contract* se suministra de la información que recibe de esos oráculos resulta de enorme importancia que los mismos sean confiables dotando la información de certeza y fiabilidad.

A este respecto, podemos diferenciar entre oráculos que se suministran de la misma fuente de información, como ocurre en el sector financiero, al canalizar datos de los mercados regulados, de otros que al no tener la misma fuente de información pueden diferir en los datos que

comunican. Efectivamente, los datos que suministra un determinado mercado (p. ej. la Bolsa de Madrid) son utilizados también por otros suministradores de información, por lo que usar uno u otro oráculo es, en principio, indiferente. Distinto es cuando la información varía, por ejemplo, respecto a la temperatura que hay en un determinado lugar. No es lo mismo obtener la información facilitada por la Agencia Estatal de Meteorología de un territorio concreto que de los canales generales internacionales de meteorología, donde posiblemente reciban la información de canales distintos.

Como se puede intuir, el uso o la introducción de los oráculos puede introducir dentro del sistema cierto grado de incertidumbre, y exponer así la relación contractual al riesgo de depender de fuentes externas de información (24). Entramos de nuevo en el ámbito de los terceros de confianza (25). En este sentido, es interesante observar cómo en contraste con la creciente descentralización que a la que parece conducir la incorporación de las tecnologías de *distributed ledgers*, la fiabilidad y la consistencia del *Smart Contract* vuelve a residir, en este sentido, en terceros de confianza.

6. CUESTIONES SOBRE LA EJECUCIÓN

La doctrina comparte, en principio, la premisa sobre la reducción de costes de transacción y ejecución que supone tanto el automatismo en la ejecución de las prestaciones, como en la posibilidad de ejecutar automáticamente las consecuencias del incumplimiento, y ello por la ausencia de la necesidad de acudir a la autoridad judicial para exigir el cumplimiento del contrato. Pero si bien es cierto, como principio, que los beneficios que acarrearía esa reducción de costes son importantes, no es menos cierto que también se plantean, actualmente, determinados problemas, no sólo legales, sino también prácticos, en relación con la ejecución.

En los siguientes apartados vamos a exponer los que consideramos más relevante. Pero antes de adentrarnos en el análisis de estos problemas, queríamos dejar apuntado la cuestión de la posible admisión por un Tribunal de un *Smart Contract*, no en el sentido de su validez, o el reconocimiento de su firma o integridad, sino en el sentido de que como está escrito en un lenguaje que desconoce el Tribunal se plantea la cuestión de

(24) Cuccuru, Pierluigi, «Beyond bitcoin: an early overview on smart contracts», cit., pp. 185 y 186.

(25) Sobre este tema los trabajos de Rodriguez de las Heras Ballell, Teresa, «El tercero de confianza en el suministro de información. Propuesta de un modelo contractual para la sociedad de la información», *Anuario de Derecho Civil*, 2010, pp. 1245 y ss.; «Intermediación electrónica y generación de confianza en la red: escenarios de riesgos y responsabilidad», *Revista española de seguros*, n.º 153-154, 2013, pp. 43 y ss.

si por sí sólo puede representar la voluntad de las partes sobre lo acordado o es necesario su interpretación o traducción al lenguaje natural para que el Tribunal pueda valorarlo (26).

6.1 **Inmodificabilidad, automatismo en la ejecución e irreversibilidad**

Con carácter general, el uso de *Smart Contracts* con la tecnología que suministran determinados *Decentralized ledgers* implica que una vez activado, su ejecución no puede detenerse. Su finalidad es clara, evitar precisamente uno de los principales problemas que surge en la contratación tradicional, el riesgo de que una de las partes incumpla. Por otro lado, el automatismo en su ejecución permite, en principio, la sustitución de los mecanismos tradicionales legales de tutela para el cumplimiento de las obligaciones contractuales.

Efectivamente, el uso en las redes descentralizadas de la tecnología denominada *Tamper-proof* implica que las acciones son imparables en su ejecución y, en un sentido tecnológico, no pueden fallar independientemente de posibles actos maliciosos, cortes de energía, interrupción de la red, catástrofes naturales o cualquier otro evento de esta naturaleza (27). En este sentido se ha afirmado que cualquier operación llevada a cabo es inmodificable, potencialmente irreversible (absoluta certeza sobre el cumplimiento de la obligación) e impermeable (la imposibilidad para intervenir en los términos establecidos una vez formalizado en la plataforma) (28). Aunque es obvio que esto acarrea beneficios, también es cierto que puede implicar la aparición de varios problemas, relacionados principalmente con aquellas cuestiones legales que puede afectar a la ejecución de las prestaciones, v. gr., y en general, a supuestos de validez o eficacia del contrato.

Efectivamente, puede ocurrir que el contrato sea inválido bien por faltar el consentimiento, bien por un vicio en el mismo, o bien porque algunas de las obligaciones sean contrarias a la Ley, a la moral o al orden público. Utilizando los mecanismos tradicionales de tutela, el Juez, en su caso, determinaría la nulidad del contrato con las consecuencias jurídicas que conlleva. Si partimos de la premisa que *un Smart Contract* no puede detenerse en su ejecución, deberíamos esperar a que este se ejecutara y, posteriormente, que se produjeran los efectos propios de la nulidad o anu-

(26) Clack, Christopher D. y otros, «Smart Contract Templates: foundations, design landscape and research directions», cit., p. 11.

(27) Conforme a *ibid.*, p. 4.

(28) Cuccuru, Pierluigi, «Beyond bitcoin: an early overview on smart contracts», cit., p. 190. Conforme a este autor, «the absolute stability of the instructions embedded in a fully decentralized blockchain does not allow a direct intervention on the terms set out, but at most a compensatory protection of the parties».

labilidad. Por tanto, siempre, *ex post* y de forma restitutiva. Del mismo modo, es posible que las circunstancias que llevaron a las partes a contratar hayan cambiado radicalmente. Aunque si bien es cierto que posiblemente algunos de los supuestos se podrían contemplar en lenguaje máquina modificando el contenido de las prestaciones iniciales, el contrato suele ser incompleto por naturaleza, resultando casi imposible prever y concretar en lenguaje máquina la posible ocurrencia de los eventos.

Estas modificaciones de las circunstancias del contrato, en el caso de los *Smart Contract*, implicaría que las partes no podrían modificar el contenido del contrato ni, por tanto, sus consecuencias. Igualmente, en los supuestos de resolución o rescisión del contrato, resultaría bastante difícil poder conseguir los efectos legales y materiales de un contrato resuelto. Entraríamos en el absurdo y en la contradicción de un contrato declarado resuelto pero que sigue vigente.

Por tanto, la posibilidad de paralizar la ejecución o exigir el cumplimiento de las prestaciones, bien por cuestiones de validez, bien de eficacia, o simplemente porque así lo quieren las partes, resultaría en general, si bien no imposible, altamente improbable, si partimos de la premisa de la inmodificabilidad del contenido y de la imposibilidad de detener la ejecución.

Por ese motivo, actualmente, existen soluciones tanto para poder paralizar el automatismo en la ejecución de los *Smart Contracts* como para efectuar posibles modificaciones en el código que permitan subsanar los errores o limitar el automatismo. En primer lugar, como no es posible llevar a cabo, con carácter general, una paralización en la ejecución o una modificación del código una vez activado, lo que se hace en la práctica es la inclusión de un código adicional en el *Smart Contract* que provoca la inhabilitación o desactivación del mismo, llamado código auto destructivo o suicida (29). En segundo lugar, adoptando soluciones estructurales que atenúen precisamente el rasgo definitorio de los *distributed ledger* que es la descentralización. De este modo, se barajan modelos alternativos como los sistemas híbridos o las plataformas de blockchain privadas. Estos modelos permitirían identificar usuarios o nodos «cualificados» que mitigaran los efectos propios de los sistemas propios de los sistemas descentralizados, bien corrigiendo los errores, o bien permitiendo de algún otro modo la reversibilidad de la operación (30). Pero en este último supuesto, la autorización o la posibilidad de que se pueda «intervenir» en el código implicaría una pérdida de las funciones que le son propias a este sistema (31).

---

(29) Bartoletti, Massimo; Pompianu, Livio, «An empirical analysis of smart contracts: platforms, applications, and design patterns», cit., p. 11.

(30) Cuccuru, Pierluigi, «Beyond bitcoin: an early overview on smart contracts», cit., pp. 190 y ss.

(31) En este sentido *Ibid.*, p. 192, «efficiency and decentralization should not result in a kind of "oppression by code" hindering any legitimate review or correction of the instructions programmed

En este sentido, sería interesante pensar en la posibilidad de que la autoridad judicial pudiera convertirse en un Oráculo de los *Smart Contract*, de manera que, bien durante la vigencia del *Smart Contract*, bien en el momento de ejecutar las prestaciones, aquel tuviera que acudir al citado Oráculo para que le informe si debe o no ejecutar las prestaciones o debe proceder a modificar su contenido.

6.2 **Ejecución extrajudicial**

Con carácter general, el uso de los Smart Contract implica la ausencia de la intervención judicial en relación a la exigencia en el cumplimiento de las prestaciones o a las consecuencias que derivan de su incumplimiento. Aunque es cierto que cada vez más se permite el uso de mecanismos de tutela extrajudiciales, como puede ser la mediación o el arbitraje, o la intervención cada vez más frecuente de notarios y registradores, todos ellos tienen una habilitación legal que permite su intervención, todo ello en aras de salvaguardar los intereses y derechos de las partes.

Lo que se plantea no es tanto la posibilidad de acudir a los medios extrajudiciales de tutela descritos en el párrafo anterior, los cuales están reconocidos y cuyo ámbito competencial está definido legalmente, sino a la posibilidad de que las partes puedan convencionalmente determinar mecanismos de tutela distintos.

A este respecto debemos distinguir entre las consecuencias pactadas que se derivan de un incumplimiento (p.ej. una cláusula penal) y la posibilidad de ejecutar esa consecuencia de forma unilateral sin beneplácito del deudor. Pero ambas tienen que ser también medidas y ejecutadas conforme al rasero de la legalidad. Efectivamente, si se establece en el *Smart Contract* que, si una de las partes incumple una prestación, se le transfiere la propiedad de un bien mueble dado en garantía, estaríamos ante un supuesto de pacto comisorio, por tanto, nulo. Pero si en vez de un pacto comisorio estamos ante un pacto marciano, la respuesta tiene que ser diferente.

Del mismo modo, podría ser contrario para los derechos fundamentales la obligatoriedad de incorporar determinados dispositivos en los seres humanos con la finalidad de obtener determinada información a los efectos de determinar las prestaciones (p. ej. chips injertos en el cuerpo) o para coaccionar el cumplimiento de las prestaciones (p. ej. que afecte a determinadas capacidades motoras o psicomotrices del deudor; o el esta-

---

in the blockchain. At the same time, however, opening the doors to external control downplays the advantages decentralized ledgers can offer». Otras posibles soluciones son las contempladas por Raskin, Max, «The law and legality of Smart Contracts», cit., pp. 327 y 328.

blecimiento de alarmas sonoras en su vivienda para coaccionarle al cumplimiento).

Por otro lado, y en relación con la ejecución de las consecuencias del incumplimiento de la prestación, debemos acudir a cada ordenamiento jurídico para comprobar si se permite o no de los mecanismos de autotutela y en que ámbito. Ejemplo de ello lo encontramos en Estados Unidos con el régimen de las garantías mobiliarias (art. 9 *Uniform Commercial Code*, en adelante UCC). Conforme a la §9-609 un acreedor garantizado puede adquirir la posesión del bien garantizado sin procedimiento judicial, si procede sin romper la paz (*procedes without breach of the peace*) (32). Pues bien, este artículo ha abierto la posibilidad de los denominados *started interrupted devices* que permite desde la distancia, a través de un dispositivo incorporado a un automóvil, impedir el encendido del vehículo. Por tanto, si una persona deja de pagar las cuotas del coche, el acreedor podría, desde la distancia, impedir que el deudor o cualquier otra persona pueda encender el vehículo y, por tanto, utilizarlo. Ya inmovilizado e inaccesible para el deudor, el acreedor puede recogerlo.

Pero las consecuencias que puede implicar utilizar arbitraria, excesiva o abusivamente este mecanismo para los intereses propios y de terceros (p. ej. que se pare en un lugar indebido con grave riesgo para la vida de los ocupantes o terceros; que no funcione ante una emergencia, etc.), es lo que ha llevado a que algunos Estados hayan comenzado a regular estos mecanismos de autotutela, recociendo su legalidad, pero también estableciendo ciertas restricciones en su aplicación (33).

Por tanto, entendemos que la mera existencia de Smart Contract no justifica por sí mismo la utilización de mecanismos de auto tutela de cualquier naturaleza ni en toda su extensión. Es necesario que esté amparado legalmente.

6.3 **Los remedios**

Partiendo de la idea de principio que los *Smart Contracts,* con la tecnología de los *distributed ledger,* permite un proceso de ejecución automático del contrato imparable e inmodificable, logrando así su finalidad de cumplir el contrato en sus propios términos, se podría pensar que, gracias

(32) «§ 9-609. Secured Party's Right to Take Possession After Default.

(a) [Possession; rendering equipment unusable; disposition on debtor's premises.] After default, a secured party: (1) may take possession of the collateral; and (2) without removal, may render equipment unusable and dispose of collateral on a debtor's premises under Section 9– 610.

(b) [Judicial and nonjudicial process.] A secured party may proceed under subsection (a): (1) pursuant to judicial process; or (2) without judicial process, if it proceeds without breach of the peace».

(33) Sobre estas cuestiones, Raskin, Max, «The law and legality of Smart Contracts», cit., pp. 329 y ss.

a ello, desaparecerían los supuestos de conflicto, se reduciría drásticamente la litigiosidad y el ejercicio de la acción de cumplimiento en forma específica.

De todas las cuestiones expuestas en los párrafos anteriores, y del estado actual de la técnica, podríamos afirmar que la litigiosidad no queda eliminada, pero el remedio principal, por lógica, tendería a ser más el restitutorio/indemnizatorio que el de cumplimiento en forma específica (34). Efectivamente, si el contrato se cumple en sus propios términos, cuando no debería por alguna causa legal o contractual que lo justificara, las prestaciones llevadas a cabo tendrían, en su caso, que restituirse. De ahí que el remedio sería restitutorio. Cuestión más compleja sería el ejercicio de la acción indemnizatoria, ya que primero se debería determinar el sujeto que ha causado el daño y la relación de causalidad.

Por último, podríamos encontrarnos ante el supuesto en que lo ejecutado no sea lo querido por las partes como consecuencia de un error en el código o una mala determinación de las prestaciones. Aquí volveríamos a un remedio restitutorio y, ahora sí, un cumplimiento del contrato en sus propios términos.

7. LA FUNCIÓN DEL ABOGADO Y DEL JUEZ

Queríamos terminar este trabajo con algunas consideraciones respecto a la función de los abogados y de los Jueces en un ecosistema de *Smart Contracts*, puesto que en algunos foros se anuncia ya irremediablemente su desaparición.

Respecto a los abogados entendemos que, en el ámbito de los *Smart Contract,* al igual que en la contratación tradicional, su función no es meramente la de un ejecutor autómata de los deseos de su cliente que transcribe en un papel su voluntad. Es un filtro de la legalidad como expresa el aforismo latino, *mihi factum, dabo tibi ius*. Por tanto, al igual que en los contratos en soporte tradicional, deberá redactar adecuadamente y cotejar los términos del *Smart Contract* y las posibles consecuencias que se deriven del mismo, bien por sus propios medios porque haya adquirido los conocimientos informáticos suficientes para llevar a cabo tal tarea, bien en compañía de una persona que tenga los conocimientos de programación. No será nada infrecuente que las futuras generaciones de abogados ya tengan conocimiento de programación, ya sea porque algunas Universidades están estableciendo dentro de sus programas de estudios una

(34) En este sentido, Werbach, Kevin; Cornell, Nicolas, «Contracts ex machina», cit., p. 376 quienes afirman que «it would be a grave mistake to think that smart contract will truly eliminate litigation. (…) Litigation persist, but it will be shifted from claims of breach to claims of restitution».

asignatura *ad hoc*, bien porque *motu propio* están realizando cursos externos sobre la materia.

En relación con los Jueces se podría predicar algo parecido. No es un mero autómata que ejecuta la voluntad de las partes. Es una figura indispensable en la impartición de la justicia, que valora, estima, interpreta la conducta de las partes y la legitimidad de sus intereses, al igual que defiende determinados intereses susceptibles de especial protección.

Por tanto, creemos que ambas figuras son insustituibles. Cuestión distinta es que el estado de la técnica avance de tal modo que la persona física sí pueda ser sustituida por una máquina que pueda cumplir tanto la función de abogado como la de Juez. Efectivamente, como ocurrió en la revolución industrial la función meramente mecánica del ser humano en los procesos industriales fue sustituido por máquinas, ya que el estado de técnica en ese momento y en los posteriores, permitió la automatización de sus funciones. En el mismo sentido, entonces, cuando las máquinas tengan capacidad de entender y comprender como hace un ser humano, y no solo a través de probabilidades o variables estadísticas, y, por ende, cumplir con la función de abogados y jueces, entonces quizá debamos replantear este pronóstico y asumir un progresivo reemplazo de funciones de ambas figuras por sistemas cada vez más complejos, sofisticados y adaptables.

CAPÍTULO 40

INNOVACIÓN Y TECNOLOGÍA EN LA ADMINISTRACIÓN DE JUSTICIA. ELEMENTOS PARA UN PARADIGMA DE LOS DERECHOS JUDICIALES DIGITALES*

MANUEL FERNÁNDEZ SALMERÓN
Universidad de Murcia

* El presente trabajo es resultado del proyecto de investigación sobre *El uso de las tecnologías de la información y la comunicación en el ámbito judicial: de la modernización a la innovación y la Justicia Abierta* [DER2015-67352-P (MINECO/FEDER)], financiado por el Ministerio de Economía y Competitividad y el Fondo Europeo de Desarrollo Regional (FEDER).

1. INTRODUCCIÓN. *INNOVACIÓN* PARA EL CIUDADANO O *LA NADA*

Hablar de innovación y de progreso tecnológico en el funcionamiento de cualquier complejo institucional, integrado en el aparato público, conlleva un riesgo nada desdeñable. En efecto, aunque parece ir de suyo que el diseño de soluciones modernizadoras para la actividad de los poderes públicos debe encontrar, fundamental e invariablemente, su razón de ser en el fortalecimiento de los derechos de los ciudadanos, resulta asimismo cierta la existencia de una, a veces frecuente, «inercia tecnológica» en las decisiones políticas, que puede ceder a la tentación de convertir las medidas modernizadoras en un fin en sí mismo; riesgo sin duda mayor en las organizaciones públicas que en las privadas, por ser aquellas más proclives a la autorreferencialidad y a los peligros de la instrumentalización en favor del logro de objetivos de rentabilidad política. La proyección de esta idea sobre la puesta en marcha de ambiciosos programas de modernización de la Administración de Justicia nos parece, asimismo, incuestionable.

La Administración de Justicia española –se he repetido en diversas ocasiones, porque es muy cierto– ha llegado comparativamente tarde al proceso de adaptación de su funcionamiento al contexto tecnológico que vive la sociedad, si tomamos como referencia la relativamente pronta previsión del nuevo escenario en el funcionamiento de sus poderes públicos *hermanos,* las Administraciones Públicas. Las razones diferenciadoras invocadas para tal retraso han sido controvertidas entre los autores, habiéndose expuesto, entre ellas, las relativas al especial estatuto personal de los titulares de órganos judiciales; la tradicional resistencia al cambio del estamento judicial; las interferencias competenciales fruto de un escenario, en este sentido, demasiado *laberíntico* o, en fin, que se trate de un servicio de alta intangibilidad, que no comporta una actividad recaudatoria considerable (1) y que, por ello, es capaz de generar menores incentivos para el impulso *inversor* en modernización (2).

(1) Con cifras de 2013, la actividad del aparato judicial importaba a los presupuestos públicos anuales alrededor de 4.000 millones de euros. La implantación, en plena crisis económica, de un sistema de tasas para el acceso a los tribunales con el que, sin embargo, se pretendía hacer frente únicamente al 8 por 100 de ese gasto total, suscitó viva polémica, a pesar de experimentar una sensible edulcoración en 2013, hasta su virtual desactivación por la STC 140/2016, de 21 de julio. Sobre el tema, resulta muy ilustrativo el análisis de Doménech Pascual, G., «Las tasas judiciales a juicio. Comentario crítico de la Sentencia del Tribunal Constitucional 140/2016, de 21 de julio», *Indret*, enero de 2017; accesible en: http://www.indret.com/pdf/1276.pdf. Todos los enlaces hipertexto aportados en este trabajo han sido consultados por última vez el 21 de junio de 2018.

(2) Puede que la explicación sea, como se muestra con frecuencia, multifactorial. Entre otros análisis, resulta de interés el de un magistrado, manifestado en el inicio del proceso de adaptación: Roas Martín, P.L., «La magistratura ante la Administración electrónica de la Justicia», en Gamero Casado, E. y Valero Torrijos, J. (Coords.), *Las tecnologías de la información y la comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio*, Aranzadi, Cizur Menor, 2012, pp. 806-809.

Pero, una vez superado ese retraso y activada, en mayor o menor medida, la transformación de este sector, en coherencia con el contexto social innovador que lo circunda, a nuestro juicio existe tal vez un peligro mayor que el de la mera intempestividad. En efecto, desencadenar un activismo hueco a la hora de diseñar de políticas innovadoras en el ámbito judicial, presenta importantes inconvenientes, comenzando por la generación de un peligroso espejismo. Así es, la simple yuxtaposición de soluciones legales e, incluso, de medidas efectivas, en el ámbito de la tecnificación de la actividad judicial, sin un impulso político robusto que las sustente y, lo que es más importante todavía, sin una aproximación concienzuda a los efectos que las mismas producirán sobre los derechos individuales, supone un rotundo fracaso y, aun más, un fraude en el más pleno sentido de la expresión. Tras años de experiencias frustradas en el ámbito de las Administraciones Públicas, este diagnóstico nos parece indiscutible (3).

En el ámbito de la Justicia nada impide que se incurra en similares riesgos de inadecuación entre prescripciones normativas y medidas efectivas; o, dicho de otro modo, entre los *deseos* del legislador y la *realidad* de los derechos ciudadanos. En este sentido y valorando ambos vectores (deseo y realidad), comprobamos que es cierto que nuestro país emprendió con entusiasmo, a finales de la primera década de los 2000, la senda de la transformación tecnológica de la Justicia, que culminó en la célebre Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia (4). Pero es asimismo cierto que, con el transcurso del tiem-

(3) Ignoramos si existe un estudio más reciente, pero el «Sondeo sobre el estado de implantación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas», realizado por el *Laboratorio Iberoamericano de Gobierno para la Innovación Pública* (*Novagob.lab*), de mayo de 2016 –esto es, seis meses después de la entrada en vigor de la norma–, resultaba muy elocuente. En efecto, en esa fecha, de todos los organismos sujetos a ella, «el 86,7 por 100 no dispone de sistemas de identificación de clave concertada, más fácil de usar para un porcentaje alto de procedimientos. El 67,7 por 100 no dispone del registro de funcionarios habilitados para actuar en nombre de los ciudadanos, derecho ya reconocido en la Ley 11/2007 y fácil de implantar, solo es necesario regularlo normativamente y es la solución a los ciudadanos no adaptados a la administración electrónica. En coherencia con lo anterior, el 64,5 por 100 no dispone de oficinas de asistencia al registro. El 62,9 por 100 no han comenzado aún con la digitalización de los documentos que llegan en soporte papel para luego continuar su tramitación de forma electrónica. El 62,9 100 no puede realizar copias auténticas mediante funcionario habilitado o sistema automático. El 61,7 por 100 declara que sus expedientes no reúnen todos los requisitos para ser considerados como expedientes electrónicos. El 51,6 por 100 no tiene publicado su catálogo de procedimientos con la información básica y descriptiva de los mismos, otro derecho básico desde 2007. El 49,2 por 100 no está utilizando los sistemas de interoperabilidad para recabar datos» (p. 4). El informe se encuentra accesible en: https://lab.novagob.org/wp-content/uploads/2017/05/NovaGob-Estudios-3-2016-Sonde-Ley-392015.pdf. Y ello sin entrar en ámbitos sectoriales, como el trascendental de la contratación pública, recientemente «removido» con la aprobación de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, pero al que ya se imponía la licitación electrónica en el paquete de Directivas de 2014.

(4) En adelante, LTICAJ. Este planteamiento optimista, seguramente justificado entonces, puede encontrarse en Mata de Bueno, F., «E-justicia: Hacia una nueva forma de entender la justicia», *Revista Internacional de Estudios de Derecho Procesal y Arbitraje*, núm. 1, 2010, p. 3, accesible en: http://www.riedpa.com/COMU/documentos/RIEDPA1102.pdf.

po, ni su funcionamiento e interoperabilidad están siendo todo lo efectivos que cabría esperar, ni la incorporación de soluciones tecnológicas parece que esté teniendo un impacto tan considerable sobre los parámetros fundamentales de satisfacción de los usuarios (justiciables, abogados, procuradores).

Así es. Por un lado, el contraste entre los principales indicadores de funcionamiento de la Administración de Justicia española y los de sus homólogos del resto de la Unión Europea, arroja, en una evaluación reciente y seria, un resultado moderadamente satisfactorio (5). Pero, por otro lado, nos encontramos con que la valoración ciudadana de la Justicia en España no ha evolucionado en la misma progresión en que lo han hecho todos esos –incuestionables– avances. Parece como si por entre los resquicios del entramado de esa supuesta modernización, fluyera sin remisión la escorrentía de la frustración y de la incapacidad para superar muy graves problemas, cuando no la sospecha del abuso, algo sobre lo que volveremos, al analizar algunas manifestaciones del avance tecnológico, como la videoconferencia o el uso de drones (6).

Las estadísticas españolas vienen mostrando desde hace años, invariablemente, que una de las instituciones públicas peor valoradas por los ciudadanos es la Justicia. Dejando de lado aspectos como los de la independencia o similares –nucleares, sin duda, pero impertinentes seguramente para la perspectiva afrontada en este trabajo–, resulta muy interesante contrastar la opinión de los destinatarios directos de las decisiones judiciales, los abogados, y advertir el porqué de ese –en principio incomprensible– desajuste entre la pretendida y progresiva tendencia innovadora de nuestro sistema de Justicia y las importantes taras que lo afligen.

Es cierto que se constata recientemente alguna leve mejoría. Con datos de 2016, es el Gobierno la institución pública peor valorada, aun-

(5) En *The 2018 EU Justice Scoreboard* [(Comunicación de la Comisión al Parlamento Europeo, el Consejo, el Banco Central Europeo, el Comité Económico y Social Europeo y el Comité de las Regiones COM(2018) 364 final] se acredita no solo que la litigiosidad en España es, comparativamente, similar a la de nuestros socios, sino que en determinados asuntos es incluso más baja. Pero en los parámetros más directamente relacionados con lo aquí tratado, como la duración de los procesos en primera instancia, aunque esta es superior a la media, se encuentra por debajo (en 2015) de la de países homologables, como Francia e Italia. En el caso de los procesos administrativos, la duración es comparativamente muy razonable, vuelve a situarse sensiblemente por debajo de la de Italia y es muy similar a la de Alemania y Francia. En otros parámetros, como la *ratio* de asuntos resueltos o los litigios pendientes ante las diversas jurisdicciones, la posición de España varía, aunque es siempre bastante competitiva. En lo que respecta directamente con la transparencia y el empleo de medios electrónicos, en campos como «Servicios de información al público en línea sobre el sistema judicial», «Disponibilidad de medios electrónicos» o «Empleo de tecnologías de la información y la comunicación entre órganos judiciales y abogados», los resultados arrojados por nuestro país –dejando de lado las dificultades para obtener datos muy precisos en un entorno tan heterogéneo–, son incuestionablemente altos. El documento es accesible en: http://ec.europa.eu/info/sites/info/files/justice_scoreboard_2018_en.pdf.

(6) *Vid. infra*, 2.2.

que inmediatamente detrás se encuentra la Administración de Justicia (7). Pero podría muy bien señalarse que el disfavor ciudadano sobre esta –aminorado respecto de años anteriores– se fundamenta, muy probablemente, en la gran oleada de politización que han experimentado muchos conflictos judiciales, ante la incapacidad de las instancias políticas para su satisfactoria elucidación. Por ello, resulta, como decíamos, elocuente acudir a un estudio realizado entre abogados, aunque el mismo se desarrollara en 2009, pues muestra algunas de las problemáticas que lastran nuestro sistema de Justicia y que no parecen haber quedado resueltas (8).

Los abogados arrojan datos reveladores. Así, consideran mayoritariamente (el 71 por 100) que la Justicia es *ineficiente,* que funciona mal, e incluso un pequeño porcentaje estima que la situación había empeorado en 2009. Su problema esencial es, pues, para los abogados el del diseño de su dinámica interna, de sus procedimientos de funcionamiento. Y si, sobre ese planteamiento deficiente, se yuxtaponen las soluciones tecnológicas, el problema persistirá, que es en buena medida lo que todavía sucede. Los abogados, de hecho, consideran mayoritariamente (76 por 100) que los jueces son competentes y que los contratiempos que aquejan a la Justicia «no dependen fundamentalmente de las personas que la componen, sino de la forma en que está organizada». Y ese modo de organización solo parcialmente ha sido revertido, y donde lo ha sido, como veremos que

(7) Los datos son analizados aquí: http://metroscopia.org/sistema-educativo-sindicatos-bancos-y-grandes-empresas-pierden-la-batalla-de-la-confianza-de-los-espanoles/. La demoscopia es, sin embargo, compleja en su manejo. Así, en el *10.º Barómetro del CGPJ. Encuesta General sobre la Administración de Justicia* (septiembre de 2008), la opinión ciudadana en relación con que la Administración de Justicia funciona mal en España se había incrementado respecto del año anterior, pasando de un 44 por 100 a un 57 por 100 (accesible en http://www.poderjudicial.es/stfls/ESTADISTICA%20JUDICIAL%20NUEVO/FICHEROS/9003%20Barometro%20CGPJ/Barometro%202008.pdf). Con una medición proveniente de otra fuente, aunque más actualizada (2015), la mejora había sido, en efecto, muy leve y pasaba a un 53 por 100. *Vid. La imagen de los Abogados y de la Justicia en la sociedad española. Barómetro externo del Consejo General de la Abogacía Española 2015*, p. 11; accesible en: http://www.abogacia.es/wp-content/uploads/2015/07/INFORME-V-BAROMETRO-EXTERNO-CGAE-NOVIEMBRE-2015.pdf. En cambio, en el *Barómetro del CIS*, con datos de enero de 2018, solo un 2,5 por 100 de la población consideraba que la Administración de Justicia se situaba entre los tres principales problemas del país, frente a la violencia contra la mujer (4,6 por 100); la corrupción y el fraude, tan ligada sin embargo a una cierta percepción de impunidad de judicial (35,1 por 100) o la inseguridad ciudadana (2,9 por 100). Solo el funcionamiento de los servicios públicos (0,9 por 100) preocupa en menor medida a la ciudadanía. Los datos en: http://www.poderjudicial.es/stfls/ESTADISTICA%20JUDICIAL%20NUEVO/FICHEROS/9001E%20Barometro%20del%20Centro%20de%20Investigaciones%20Sociologicas/BAROMETRO%20MENSUAL%20CIS.xls.

(8) Se trata del interesante estudio «La Justicia española evaluada por los abogados», realizado por «Metroscopia» para el *Consejo General de la Abogacía Española*, y fechado en mayo de 2009. El documento está accesible aquí: http://www.abogacia.es/wp-content/uploads/2012/05/La-Justicia-Espanola-evaluada-por-los-abogados.pdf. Ciertamente, se trata de una fecha ya lejana, pero, como se verá seguidamente en el texto, no parece que las principales taras alegadas por los letrados se hayan aminorado drásticamente a día de hoy.

sucede con los llamados *sistemas de gestión procesal* (9), las dificultades de fondo no parece que hayan sido resueltas del todo (10).

Conviene, en todo caso, aclarar que este trabajo no es de ninguna forma una condena a la innovación en la justicia, en la que firmemente creemos (11). Antes bien, el mismo pretende ahondar, en alguna medida, en las posibles razones de algunos de estos inconvenientes, los cuales pueden deberse no tanto a una falta de tecnificación, cuanto a la incorporación ineficiente o errada de los medios tecnológicos, unas veces, o a la ausencia de garantías suficientes para los ciudadanos, otras. De esta manera procuraremos aportar nuestro grano de arena a una puesta en marcha, realmente eficaz, de soluciones innovadoras y avances tecnológicos que, en múltiples ámbitos, pueda contribuir a garantizar, en mayor y mejor medida, los derechos de los justiciables y, en definitiva, la calidad de nuestro Estado de Derecho.

2. *¿JUSTICIA ELECTRÓNICA?* EL EMPLEO DE MEDIOS ELECTRÓNICOS EN LA ADMINISTRACIÓN DE JUSTICIA Y EN LA ACTIVIDAD JURISDICCIONAL

El fomento del empleo de medios electrónicos en el ámbito de la actividad judicial constituye una tendencia generalizada en Occidente, a pesar de que los ritmos de implantación sean desiguales y heterogéneo el alcance de las medidas adoptadas (12). En esta materia cabe, no obstante y a

(9) En adelante, SGP, en singular o plural según el contexto.

(10) El estudio es enormemente ilustrativo y la mayor parte de las consideraciones de los letrados se orientan hacia la conclusión de que los problemas son estructurales y difícilmente reformables mediante un simple cambio tecnológico, por muy profundo y paradigmático que este haya sido o pueda ser. Incluso, algunos de los inconvenientes invocados quedan seguramente agravados con esta modernización. Así, el 89 por 100 de los abogados encuestados consideró que los posibles medios alternativos de resolución de conflictos que podrían descargar a los tribunales y agilizar su funcionamiento siguen sin estar adecuadamente establecidos y potenciados. El 87 por 100 señala que los gobiernos, del signo que sean, muestran por lo general más interés en tratar de controlar a la Justicia o de influir sobre ella que por emprender una mejora a fondo de su funcionamiento que la modernice y la haga plenamente eficiente. El 82 por 100 señala que la oficina judicial no suele estar organizada, por lo general, del modo más adecuado para su mayor eficiencia. Muchos asuntos que ahora han de ser resueltos o controlados por un juez podrían tener otro tipo de tratamiento procesal más ágil e informal sin merma alguna de las garantías jurídicas de las partes implicadas. El 74 por 100 señala que la legislación procesal necesita una profunda revisión que agilice el funcionamiento de la Justicia. El 70 por 100 que, en gran medida, los problemas de funcionamiento de la Justicia se deben a que los diversos cuerpos que la integran dependen de organismos distintos y por ello no están adecuadamente coordinados. El 63 por 100, en fin, piensa que la Justicia ha tendido siempre a organizarse y funcionar de la forma que resultaba más conveniente para jueces y juristas y no del modo en que podía resultar más cercana y útil a la ciudadanía.

(11) Opinión, por cierto, compartida con vehemencia por los propios abogados, que en el *Barómetro Interno de Opinión de la Abogacía Española 2013*, ante preguntas relativas a su uso de las nuevas tecnologías para el ejercicio de su profesión, un 80 por 100 consideró que era muy importante. Sobre esto, puede consultarse la URL: https://www.abogacia.es/wp-content/uploads/2012/05/INFORME-GENERAL-Barometro-Interno-de-Opinion-Enero-2013.pdf.

(12) Aunque el análisis adopta un enfoque limitado acerca de las posibilidades de utilización de los medios electrónicos en la actividad judicial, el ya citado *EU Justice Scoreboard 2018* muestra indicadores relativamente satisfactorios para España en diversos campos relacionados con el

nuestro juicio, una relevante partición en el enfoque, de modo que se pueden individualizar seguramente dos campos claramente delimitados de implantación de las TIC, sin perjuicio de que ambas vertientes converjan en el metafenómeno que se ha dado en denominar *Justicia abierta* (13).

Las perspectivas que, como decimos, se localizan en esta materia son, a nuestro juicio, esencialmente dos. Por una parte, la implementación de las TIC en el funcionamiento de las estructuras de soporte de la actividad judicial, incluyendo los canales de interactuación con las partes y la gestión del expediente judicial. Por otra parte, debe atenderse asimismo al empleo de medios tecnológicos en la actividad propiamente jurisdiccional, destacando su aplicación al *proceso* y sus aledaños. Dentro de este segundo enfoque, conviene, a su vez, subdistinguir la modernización de la actividad jurisdiccional enderezada más directamente al incremento de la celeridad y de la *eficiencia* de la Administración de justicia (14), de aquella otra que trata de ordenar el proceso, haciéndolo más *eficaz*, en orden a una averiguación más certera y precisa de la verdad, en consonancia con el avance tecnológico general de la sociedad(15).

De un modo u otro, abordaremos en este trabajo todos los enfoques, pero debido a requerimientos insoslayables de espacio, por una parte, enfrentaremos una visión panorámica, aunque crítica, del proceso de implantación de los SGP; mientras que, por otra parte y en relación con la aplicación de avances en la actividad estrictamente jurisdiccional, limitaremos el examen a dos herramientas en las que, a partir de un análisis

---

empleo de las TIC en la actividad judicial. Ya se trate de la «disponibilidad de medios electrónicos» (para iniciar procesos; hacer un seguimiento al estado de tramitación del caso y para practicar citaciones y emplazamientos), ya del «uso de las TIC en la relaciones entre órganos jurisdiccionales y abogados» (para comunicaciones entre juzgados y abogados; firma electrónica de documentos y presentación de solicitudes), la posición relativa de nuestro país no es ciertamente la mejor, pero suele alcanzar mejor ubicación en los indicadores que los restantes grandes Estados europeos. *Vid.* las pp. 25 y 26 del citado documento.

(13) Sobre una idea parecida –por lo demás, ya antigua y bien conocida en el ámbito de las Administraciones Públicas–, esto es, la de que la mera tecnificación de la actividad no desemboca *per se* en un auténtico cambio de paradigma, según ya hemos adelantado en el texto, *supra* 1, *vid*. las reflexiones de Cortés, O., «Justicia abierta en España: situación, retos y barreras», p. 7 (accesible en: http://www.gigapp.org/index.php/mis-publicaciones-gigapp/publication/show/2323), quien distingue entre *e-Justicia* y *Justicia abierta* como escalones distintos y de tránsito sucesivo.

(14) Como puede ser el caso de las grabaciones de voz e imagen de las vistas y comparecencias, generalizada en todos los órdenes jurisdiccionales en España, a partir de la Ley 13/2009, de 3 de noviembre, de reforma de la legislación procesal para la implantación de la nueva Oficina judicial. También la interactuación entre las partes y el órgano jurisdiccional mediante videoconferencia, posibilidad prevista, con carácter general, en el artículo 229.3 LOPJ, que contiene, como veremos con detalle sucesivamente, una interpretación actualizadora del principio de inmediación; o, en fin, la previsión del llamado *Punto Neutro Judicial*, como herramienta de apoyo a la función jurisdiccional. Cierto es que estas medidas están íntimamente relacionadas, al mismo tiempo, con la tecnificación de la oficina y del expediente judiciales, al contribuir decisivamente a su constancia y gestión digitales.

(15) En este grupo se incluirían, entre otras, herramientas de investigación prueba como los virus espía, el uso de VANT *(Vehículos Aéreos No Tripulados)* con fines de investigación y, en general, de cualquier instrumento que encaje en la cláusula de medios de prueba innominados, prevista en el artículo 299.3 LEC.

detenido –por cuanto sabemos, ausente en nuestro Derecho a día de hoy–, se han detectado buena cantidad de problemas jurídicos sin resolver: la videoconferencia y el empleo de dispositivos de seguimiento, captación y registro de imagen, o, lo que es igual, de drones. La resolución de tales cuestiones problemáticas ha tratado de afrontarse desde la experiencia del Derecho norteamericano, cuyo análisis crítico puede resultar sin duda fructífero, a pesar de las insalvables diferencias culturales.

2.1 **La modernización tecnológica en la gestión procesal: balance y perspectivas**

La generalización de la tramitación electrónica de los procedimientos judiciales, al menos sobre el plano legal, se ha intensificado en época reciente (16), con lo que ello conlleva de tendencia a la eliminación del papel en el despacho de los expedientes y en la práctica de los actos de comunicación procesal. A pesar de que el avance es, en hipótesis, positivo, lo cierto es que la gestión procesal electrónica en España presenta un recorrido algo desalentador desde su implantación definitiva con la LTICAJ y la puesta en funcionamiento del aplicativo *Lex-Net*. Es cierto que, en descargo del sistema español, conviene recordar que en algunos de los países vecinos que han establecido herramientas semejantes, estas han sido objeto de críticas o, en su caso, se han advertido deficiencias, seguramente inevitables, en su funcionamiento (17).

Tal vez lo primero que convenga aclarar al respecto sea la arquitectura de las herramientas para la gestión de la Administración de Justicia en España, empresa nada sencilla, como se comprobará seguidamente. Desde el punto de vista interno de la organización judicial, cada colectivo profesional interviniente en los distintos expedientes judiciales está dotado de una herramienta informática, a través de la cual lleva a cabo los trámites que le son propias. Junto a ellos, existe un aplicativo de comunicaciones cuyo objetivo esencial es el de hacer llegar a los mediadores procesales (abogados y procuradores) las comunicaciones y recibir de ellos la documentación procesalmente pertinente. En principio, ambas herramientas

(16) Fundamentalmente, a partir de la reforma de la LEC operada por la Ley 42/2015, de 5 de octubre, y el Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema *LexNET*.

(17) Es el caso de los sistemas belga o francés. El primero *(Phenix)*, objeto de elogios, ha experimentado dificultades de implantación *(cfr.* Rosa, J., Teixeira, C. y Sousa Pinto, J., «Risk factors in e-justice information systems», *Government Information Quarterly*, núm. 30, 2013, pp. 245-246). En cuanto al sistema francés *(e-Barreau)*, los problemas tampoco han estado ausentes, comenzando por su precio de suscripción. *Vid*. el clarificador estudio de Velicogna, M., Errera, A. y Derlange, S., «e-Justice in France: the *e-Barreau* experience», *Utrecht Law Review*, vol. 7, núm. 1, 2011, pp. 163 y ss.

(la de gestión procesal interna y la de comunicación) han de estar, naturalmente, interconectadas, ser compatibles e interoperables (18).

Pero la operatividad real de estos sistemas se ha complicado irremediablemente en nuestro Estado compuesto. En efecto, la transferencia de las competencias en materia de justicia –entendidas como las relativas a los medios personales y materiales para el sostenimiento de la estructura judicial– a ciertas Comunidades Autónomas, ha conducido a una paradoja, consistente en la perturbadora convivencia de diversos aplicativos de comunicación y distintos SGP (19). Las dificultades no terminan aquí, pues, por una parte, no todos los colectivos profesionales emplean el mismo sistema de gestión, sino que, cualificadamente, el Ministerio Fiscal utiliza uno propio, denominado *Fortuny*. Y, por otra parte y lo que resulta más grave, existen serios problemas de compatibilidad e interoperabilidad entre la mayor parte de tales sistemas. Esta última circunstancia presenta una incuestionable incidencia sobre los derechos fundamentales de los justiciables y, especialmente, sobre el de tutela judicial efectiva, en la medida en que entorpece, alza obstáculos (en este caso técnicos), a la impetración del auxilio judicial de los ciudadanos (20).

Ante la alarma que esta visión –puramente *estática*– del sistema seguramente ha ido acumulando, parece existir la intención de revertir tal estado de cosas, probablemente mediante la generalización de una versión mejorada de *Minerva* en todo el territorio nacional (21). Pero, además de las resistencias que, desde la perspectiva competencial, arrastraría esta pretensión, la misma se enfrenta a ciertas dinámicas que la obs-

---

(18) Para ello, inspirándose en los Esquemas Nacionales de Interoperabilidad y de Seguridad aprobados al amparo de la hoy derogada Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, se confeccionaron por parte de un organismo técnico (el *Comité Técnico Estatal de la Administración Judicial Electrónica)* las Bases del EJIS *(Esquema Judicial de Interoperabilidad y Seguridad). Vid.* los arts. 45 y 47 LTICAJ.

(19) A modo de *Torre de Babel* judicial, el mapa es realmente complejo y causa cierto estupor. En el llamado «Territorio Ministerio de Justicia» (Comunidades Autónomas con competencias no transferidas), el aplicativo de comunicación es *LexNET* y el SGP es *Minerva*. De entre el resto de Comunidades Autónomas, algunas conservan ambas herramientas estatales (Aragón, Principado de Asturias, Galicia o La Rioja); otras solo emplean *LexNET*, pero adoptan su propio SGP (Andalucía –*Adriano–;* Canarias –*Atlante II–;* Cataluña –*eJusticia–;* Comunidad Valenciana –*Cicerone–;* Madrid –*IUSMadrid–)* y un último grupo adopta sistemas autónomos para ambas finalidades (País Vasco –*JustiziaSip-JustiziaBat–;* Navarra –*Avantius-Sistema PSP–* y Cantabria –*Vereda–)*.

(20) El problema ha calado en la opinión pública: https://elpais.com/diario/2008/12/23/sociedad/1229986801_850215.amp.html.

(21) Así se avanzaba en prensa antes del verano de 2017: http://www.abogacia.es/2017/07/27/catala-propone-a-las-ccaa-crear-un-sistema-de-gestion-procesal-comun-en-toda-espana/. Repárese en que la pretensión del Ministerio consiste en *acordar* esa extensión, dado que, según una interpretación, no podría *imponerla* a las Comunidades Autónomas con competencias transferidas. No obstante, resultaría seguramente interesante una reflexión acerca de esta posibilidad, al amparo de la habilitación contenida en el artículo 149.1.1.ª CE, toda vez que resulta claro que del mismo se deriva un auténtico título competencial a favor del Estado y que la jurisprudencia constitucional ha encajado en su seno la determinación estatal unilateral del marco organizativo para el ejercicio de ciertos derechos, así como la fijación de requisitos mínimos de calidad de los servicios, por ejemplo. Un análisis pormenorizado sobre el alcance de este precepto constitucional puede encontrarse en Pemán Gavín, J., *Igualdad de los ciudadanos y autonomías territoriales*, Civitas, Madrid, 1992, pp. 228 y ss.).

taculizan. De hecho, en buena medida, la tónica viene consistiendo hasta ahora más bien en el fenómeno contrario, esto es, en un reforzamiento de la posición de algunos SGP autonómicos. Así es, paralelamente a los intentos ministeriales por difundir Minerva en todo el territorio nacional, se han producido expansiones parciales de algunos de los sistemas autonómicos (22), con el consiguiente afianzamiento de las resistencias de tales Comunidades Autónomas a abandonar sus plataformas domésticas, dada la generación de economías de escala a causa de la difusión de sus propias herramientas en otros territorios (23). La complejidad de la situación es ya, pues, mayúscula y parece que la debilidad de *Minerva* en el panorama nacional prosigue, a pesar de las propuestas ministeriales (24).

Pero, al margen de amenazas externas, puede afirmarse que, en muy buena medida, el relativo fracaso de *Minerva* se encuentra también en la concepción y ejecución del sistema mismo. En efecto, las competencias en materia de puesta en marcha de aplicaciones para la actividad judicial están –de modo ciertamente inverosímil– compartidas entre el CGPJ, el Ministerio de Justicia y algunas Comunidades Autónomas. En este entramado, conviene ahora destacar el papel del primero de ellos. El CGPJ no dispone en esta materia de facultades presupuestarias (25) –que descansan, pues, en el Ministerio y en las Comunidades Autónomas, en función del ámbito concernido–, pero sí goza de una trascendental e inexpropiable potestad, a saber, la de certificar la compatibilidad de las aplicaciones y de los distintos SGP que pretendan implementarse en España (26). Y lo cierto es que, muy probablemente por razones

(22) Así, el sistema cántabro *Vereda* está basado en el navarro *Avantius*. Asimismo, la Comunidad Autónoma de Aragón ha decidido adoptar el sistema foral a partir de 2018.

(23) Pensamos que la resistencia de las Comunidades Autónomas a sumarse a la propuesta del Estado de uniformar los SGP, extendiendo *Minerva*, es, hasta cierto punto, lógica. Entendemos que se trata en mayor medida, como veremos sucesivamente en el texto, de un problema de liderazgo por parte de las instituciones estatales implicadas.

(24) La debilidad es también económica. La cantidad invertida en *LexNet* entre 2010 y 2016 ha sido de 7,3 millones de euros (http://denuncialexnet.es/archivos/2016-04-20_resolucion-transparencia.pdf; fuente: https://www.elconfidencial.com/tecnologia/2017-08-03/desastre-lexnet-justicia-ciberseguridad-orfilia-rafael-catala_1424504/). A esta cantidad se sumaría un gasto ministerial de otros 6 millones de euros, destinado a crear las estructuras necesarias para emprender esa labor de uniformización, en las Comunidades Autónomas con competencias en materia de Justicia *(vid.* al respecto el enlace de la nota 21).

(25) Arnáiz Serrano, A., «El Consejo General del Poder Judicial y las tecnologías de la información y la comunicación aplicadas a la Justicia», en Gamero Casado, E. y Valero Torrijos, J. (Coords.), *Las tecnologías de la información y la comunicación en la Administración de Justicia*, cit., p. 773.

(26) Con el auxilio, en su caso, del *Centro de Documentación Judicial (CENDOJ)* y del *Comité Técnico Estatal de la Administración Judicial Electrónica*. Así se desprende del artículo 619.2 LOPJ y, sobre todo, de lo dispuesto en los artículos 230.6 («Los programas y aplicaciones informáticos que se utilicen en la Administración de Justicia deberán ser previamente informados por el Consejo General del Poder Judicial […] Los sistemas informáticos que se utilicen en la Administración de Justicia deberán ser compatibles entre sí para facilitar su comunicación e integración, en los términos que determine el Comité Técnico Estatal de la Administración de Justicia Electrónica»)

de conveniencia política, basadas en las motivaciones ya apuntadas, este órgano parece haber hecho dejación de tan estratégica y esencial función. De este modo, insistimos, las grandes sumas invertidas en el desarrollo e implantación de los sistemas autóctonos de las Comunidades Autónomas se está erigiendo en un indudable freno político para la ya inaplazable integración de los SGP.

Y, aunque parecía que el panorama era susceptible de pocas complicaciones adicionales, lo cierto es que se viene enrevesando en extremo, especialmente en el último año. En efecto, no solo el CGPJ parece haber hecho una dejación total de funciones, en materia de compatibilidad e interoperabilidad entre las aplicaciones de comunicación y gestión procesal de las Comunidades Autónomas con competencias propias, y las de aquellas otras integradas en el territorio del Ministerio de Justicia, sino que los propios sistemas estatales –y, destacadamente, el aplicativo de comunicaciones *LexNet*– suma un preocupante historial de fallos de seguridad (27).

No se trata, ciertamente, de construir un discurso reduccionista y alarmista sobre problemas complejos, pero da la impresión de que la incorporación de soluciones tecnológicas en la actividad judicial se encuentra a merced de la coyuntura o la ocurrencia políticas, en la medida en que o bien tal incorporación sobreviene a un acontecimiento crítico (28), bien se erige en herramienta para decisiones inquietantes de los poderes públicos (29), o bien, sencillamente y lo que resulta mucho más ordinario y aceptable, no termina de dotarse de un marco regulador del todo cohe-

---

y 560 LOPJ («1. El Consejo General del Poder Judicial tiene las siguientes atribuciones: […] 16.ª Ejercer la potestad reglamentaria, en el marco estricto de desarrollo de las previsiones de la Ley Orgánica del Poder Judicial, en las siguientes materias: […] l. Establecimiento de las bases y estándares de compatibilidad de los sistemas informáticos que se utilicen en la Administración de Justicia»).

(27) La vulnerabilidad de la herramienta ha supuesto la exposición indiscriminada de enormes cantidades de datos relativos a actuaciones procesales. *Cfr.* http://www.elmundo.es/espana/2017/07/27/597a2341268e3e1b698b45e3.html; tratándose, al parecer, de un claro defecto de programación *(cfr.* http://www.pafsaez.com/archivos/3101).

(28) Es el caso del *Sistema de Registros Administrativos de apoyo a la Administración de Justicia (SIRAJ)*, regulado en el Real Decreto 95/2009, de 6 de febrero, que integra y pone al servicio de los órganos jurisdiccionales la información obrante en importantes registros administrativos de relevancia judicial (como el Registro Central de Penados y Rebeldes o el Registro Central para la Protección de las Víctimas de Violencia Doméstica, y otros). Su creación se produjo en esa fecha, fundamentalmente, como respuesta a las deficiencias detectadas durante la instrucción del caso *Mari Luz,* en el que órgano el competente para la instrucción de la causa no pudo disponer de información relativa a una condena pendiente del encausado, por ilícitos similares cometidos sobre su propia hija, así como afectante a procesos en curso que comprometían al detenido, tramitados ante otros órganos jurisdiccionales.

(29) Es el caso del acuerdo suscrito entre el CGPJ y la AEAT, enderezado al suministro por parte del primero de información, con trascendencia tributaria, relativa a la participación de abogados y procuradores en todos los procedimientos judiciales durante los años 2014, 2015 y 2016, salvo en el dato relativo a la «identificación del cliente». Se puede acceder aquí a la nota de prensa sobre este controvertido acuerdo: https://confilegal.com/wp-content/uploads/2017/09/Acuerdo-CGPJ-20-7-2017.pdf.

rente (30), patología que, como comprobaremos sucesivamente, afecta a diversas herramientas tecnológicas.

2.2 **El uso de dispositivos y aplicaciones en el marco de la actividad jurisdiccional. Algunos desarrollos sobre el empleo de la videoconferencia y los Vehículos Aéreos no Tripulados a la luz de la experiencia jurídica norteamericana**

En la línea ya expuesta en precedencia, dentro del segundo bloque de medidas modernizadoras debe incluirse la realización de actuaciones procesales mediante el empleo de medios electrónicos y, en general, de cualesquiera tecnologías avanzadas. En este sentido, si bien en términos muy generales, el camino recorrido por España es, debe decirse, encomiable, de modo que las previsiones relativas al uso de tales instrumentos para cualesquiera actuaciones con relevancia judicial –incluyendo, como se verá, las de investigación– son diversas y generosas en sus planteamientos.

Bajo un principio general contenido en su legislación judicial orgánica (31), nuestro ordenamiento jurídico ha ido incorporando disposiciones sobre la tecnificación de las actuaciones judiciales. Así, también desde fecha temprana, se prevé la obligación de registro –con correlativa prohibición de transcripción– en soporte apto para la grabación y reproducción del sonido y la imagen, de todas aquellas «actuaciones orales en vistas, audiencias y comparecencias celebradas ante los jueces o magistrados o, en su caso, ante los secretarios judiciales» (32). Más específicamente, la realización de actuaciones probatorias empleando herramientas telemáticas recibió un impulso definitivo en nuestro Derecho, sobre todo, a partir de 2003 (33).

---

(30) Es, seguramente, el caso de las comunicaciones y notificaciones electrónicas en el ámbito judicial, practicadas bien a través de *Sede judicial electrónica*, bien de la herramienta *LexNet*, ya examinada. No podemos detenernos en la disciplina y las vicisitudes de estas actuaciones, pero los problemas no son de escasa entidad. Entre ellos se encuentra el de las comunicaciones practicadas a partes aún no personadas en un proceso o no representadas en él. *Cfr.*, sobre este particular, el trabajo de Cerdá Meseguer, J.I., «Las notificaciones electrónicas en el proceso judicial», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 46, 2018, sobre todo epígrafe V.

(31) El artículo 230 LOPJ dispone que «1. Los Juzgados y Tribunales y las Fiscalías están obligados a utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, puestos a su disposición para el desarrollo de su actividad y ejercicio de sus funciones, con las limitaciones que a la utilización de tales medios establecen el Capítulo I bis de este Título, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y las demás leyes que resulten de aplicación». Previsión introducida, prácticamente en los términos vigentes, nada menos que en 1994.

(32) Artículo 147 LEC. Se trata, como decíamos, de una previsión anterior a la de muchos otros ordenamientos jurídicos, como se ha destacado oportunamente (así, en Gómez Martínez, C., «La grabación del sonido y de la imagen en los juicios civiles. Del juez lector al juez espectador», p. 2; accesible en: http://www.juecesdemocracia.es/publicaciones/revista/articulosinteres/lagrabaciondesonido.pdf).

(33) El artículo 229 LOPJ dispone hoy que «2. Las declaraciones, interrogatorios, testimonios, careos, exploraciones, informes, ratificación de los periciales y vistas, se llevarán a efecto ante juez o tribunal con presencia o intervención, en su caso, de las partes y en audiencia pública, salvo lo dispuesto en la ley. 3. Estas actuaciones podrán realizarse a través de videoconferencia u otro sistema similar que

Ahora bien, por su especial capilaridad en cuanto a la afectación de derechos fundamentales de los justiciables y de los restantes sujetos implicados en la actividad jurisdiccional, procedemos a continuación a un examen más detenido de algunas de las soluciones tecnológicas previstas, con especial incidencia en el ámbito de la justicia criminal. Así, de un lado, abordamos seguidamente los pormenores derivados de la implantación de la videoconferencia como herramienta garantizadora de la tan traída y llevada *eficiencia,* prevista para vehicular las declaraciones, testimonios y pruebas en general, pero cuyo respaldo, casi sin fisuras, no consigue ocultar del todo los muchos óbices que contra su implantación global e indiscriminada pueden formularse. De otro lado, ahondaremos en los efectos reales que el empleo de sistemas de seguimiento y captación de imagen por medios aéreos (drones), en tanto que herramientas de investigación criminal, puede ocasionar para la integridad de los derechos fundamentales de los ciudadanos implicados. En ambos casos, tomaremos la experiencia del ordenamiento jurídico norteamericano, como punto de partida para la formulación de los necesarios correctivos a nivel jurídico interno.

2.2.1 La videoconferencia o «no es oro todo lo que reluce». Una herramienta tan necesaria como necesitada de ajustes en su configuración

Al margen de la disciplina general contenida en la LOPJ, la implantación de la videoconferencia recibió un nuevo impulso normativo en el ámbito de la justicia criminal, también en 2003 (34), disponiéndose con claridad, a partir de entonces, que la comunicación entablada debía reunir los requisitos de *simultaneidad* o *desarrollo en tiempo real;* había de comprender *imagen y sonido;* con una *implicación completa de los sentidos comprometidos, de modo equivalente, en una comunicación presencial,* lo que incluía, lógicamente, la bidireccionalidad. Tales condiciones son de suma importancia para garantizar una homologación de la videoconferencia a las declaraciones practicadas por comparecencia física, siendo, a su vez, garantía de protección de los derechos fundamentales implicados en la verificación de tales diligencias. Como bien se ha conclui-

---

permita la comunicación bidireccional y simultánea de la imagen y el sonido y la interacción visual, auditiva y verbal entre dos personas o grupos de personas geográficamente distantes, asegurando en todo caso la posibilidad de contradicción de las partes y la salvaguarda del derecho de defensa, cuando así lo acuerde el juez o tribunal. En estos casos, el secretario judicial del juzgado o tribunal que haya acordado la medida acreditará desde la propia sede judicial la identidad de las personas que intervengan a través de la videoconferencia mediante la previa remisión o la exhibición directa de documentación, por conocimiento personal o por cualquier otro medio procesal idóneo».

(34) Lo que no impidió que ya en 2001 tuviera lugar la primera utilización de videoconferencia en un juicio oral en España, entre la Audiencia Provincial de Sevilla y ciertos testigos y peritos de la Universidad de las Islas Baleares (el dato en Nevado, M.T., «Reflexión sobre la actualidad de la declaración electrónica en el proceso penal español. Especial consideración del proceso con menores», *Revue Droit International, Commerce, Innovations & Développement*, núm. 1, 2012, p. 9).

do, estas características excluyen el empleo de sistemas que carezcan de tales requisitos, como el correo electrónico, pero también de la mensajería instantánea o los chats de texto (35). No obstante, algún precepto legal resulta algo insuficiente a este respecto, a pesar de que sus carencias puedan salvarse finalmente por vía de interpretación sistemática (36).

Como medio de defensa y, en general, de aportación de elementos de juicio por parte de justiciables y ciudadanos, en la videoconferencia conviene ser especialmente esmerados por lo que se refiere a la protección de colectivos vulnerables. Desde este punto de vista, destaca el caso de los menores, contemplados expresamente en nuestro Derecho a estos efectos. De este modo, si las razones generales que pueden justificar la práctica de una diligencia, probatoria o no, mediante esta herramienta se concretan en «utilidad, seguridad y orden público», su práctica con menores encaja en el supuesto de que la comparecencia física pueda resultarles «gravosa o perjudicial» (37).

De hecho y precisamente, el discurso relativo a la práctica de videoconferencias procesales en relación con determinados procedimientos especialmente sensibles, fundamentalmente debido a la naturaleza de los sujetos implicados, permanece por el momento enmarcado en el debate sobre los pros y contras generales de la herramienta. Las ventajas parecen unánimemente claras: eficacia de las actuaciones, eficiencia o abaratamiento de costes y simplificación en el acceso a la justicia. Pero también se han puesto de manifiesto problemas de adaptación del sistema a las garantías judiciales, entre las que destaca el omnipresente *principio de inmediación* (38). En cualquier caso, desde la perspectiva de sujetos vulnerables, los inconvenientes pueden atender al estatuto jurídico de la persona en cuestión, en cuyo caso resulta conveniente una armonización normativa, que podría operarse, no obstante y hasta cierto límite, por vía interpretativa (39). Pero se han localizado otras desventajas en el plano

(35) En igual sentido, Nevado, M.T., *ibídem*, p. 10.

(36) En efecto, el artículo 707 LECr señala, en sede de prueba de testigos, que «con este fin podrá ser utilizado cualquier medio técnico que haga posible la práctica de esta prueba, incluyéndose la posibilidad de que los testigos puedan *ser oídos* sin estar presentes en la sala *mediante la utilización de tecnologías de la comunicación»;* las cursivas son nuestras.

(37) Artículos 325 para las diligencias sumariales y 731 bis LECr para la práctica de pruebas. Es solo este último el que, sin embargo, hace referencia expresa a los menores.

(38) Recogidos sumariamente por Simón Castellano, P., «La modernización tecnológica de la Administración de Justicia», *Revista Vasca de Administración Pública*, núm. 92, 2012, pp. 310-311. Incluso de algún precepto de nuestro ordenamiento jurídico puede todavía derivarse la idea de una identificación del principio con una inmediación exclusivamente *física*. Así, el artículo 268 LOPJ dispone que «1. Las actuaciones judiciales deberán practicarse en la sede del órgano jurisdiccional».

(39) Pensemos, precisamente, en la protección que nuestra Justicia criminal dispensa a los propios menores o a los incapacitados, sea cual sea la calidad en la que deban comparecer en las actuaciones judiciales. Así, por ejemplo, «en el caso de los testigos menores de edad o personas con la capacidad judicialmente modificada, el Juez de Instrucción podrá acordar, cuando a la vista de la falta de madurez de la víctima resulte necesario para evitar causarles graves perjuicios, que se les tome declaración mediante la intervención de expertos y con intervención del Ministerio Fiscal»

propiamente técnico, tanto desde la perspectiva del desenvolvimiento psicológico de los comparecientes como, incluso, de la apreciación judicial de las declaraciones y el comportamiento –cuando sea relevante– del declarante, a partir del peculiar contexto en que se realizan, todo ello con una clara repercusión jurídica sobre la licitud de este instrumento.

En USA son frecuentes, desde hace al menos una década, los debates judiciales y doctrinales acerca de la procedencia de practicar videoconferencias, tanto desde la perspectiva constitucional como de la relativa a las garantías previstas en las leyes procesales, en determinados tipos de juicios (40). Desde el punto de vista –decisivo– de la interacción del juez con el acusado, existen posicionamientos críticos con la aplicación de esta solución tecnológica a litigios criminales en los que se encuentre en juego su libertad, aunque, a tales efectos, pueden distinguirse, a su vez, dos itinerarios. Por un lado, el de los procedimientos criminales iniciales, en los que existe una extendida consideración judicial –sin posicionamiento, hasta el momento, del Tribunal Supremo– acerca de que la videoconferencia es incompatible con el derecho constitucional al proceso debido y a un juicio justo *(due process* y *fair trail),* así como con el legal del acusado a estar *presente* en todas las actuaciones del juicio, desde la comparecencia inicial hasta la sentencia (41). La legislación procesal criminal, que instauró en 2002 la posibilidad de videoconferencias, reconoce hoy su práctica, pero limitadamente a determinadas fases y siempre bajo consentimiento del acusado (42).

Pero, por otro lado, resulta seguramente menos consensuada la verificación de videoconferencias en los procedimientos tramitados sobre excarcelados, a través de alguna de las instituciones presentes en el ordenamiento jurídico norteamericano, a través de las cuales el condenado disfruta de una libertad *tutelada* o *supervisada* (43), y que ha sido también judicialmente cuestionada, aunque a partir de parámetros de mera legalidad ordinaria (44). Asimismo, se ha estudiado en el Derecho estadouni-

---

(art. 433 LECr). En tales circunstancias la videoconferencia puede no resultar viable, pues esos dos ejes de protección del menor o incapacitado (la que se brinda mediante la asistencia de técnicos y mediante el recurso a la videoconferencia) pueden no parecer a primera vista conciliables, de modo que uno de los dos, supuestamente, habrá de ceder en muchos casos.

(40) Uno de esos estudios críticos es el de Garofano, A., «Avoiding Virtual Justice: Video-Teleconference Testimony in Federal Criminal Trials», *Catholic University Law Review*, núm. 56, 2007, pp. 683 y ss.; accesible en: http://scholarship.law.edu/lawreview/vol56/iss2/10.

(41) *Rule* 43 de las *Federal Rules of Criminal Procedure*, que exige que «the defendant must be present at: (1) the initial appearance, the initial arraignment, and the plea; (2) every trial Stage, including jury impanelment and the return of the verdict; and (3) Sentencing».

(42) *Vid.* «Developments in the Law – Access to Courts», *Harvard Law Review*, núm. 122, 2009, p. 1183.

(43) *Parole*, *probation* y *supervised release.*

(44) Sobre este particular, puede consultarse, entre otros, el estudio de Marr, K., «The Right to «Skype»: The Due Process Concerns of Videoconferencing at Parole Revocation Hearings», *University of Cincinnati Law Review*, núm. 81-4, 2013; accesible en: http://scholarship.law.uc.edu/uclr/vol81/iss4/6.

dense la compatibilidad legal del empleo de la videoconferencia en los juicios en materia de extranjería y asilo, en los que este mecanismo de comunicación se prevé como cauce sustitutivo integral para toda declaración procesal del demandado *(Respondant)* (45).

Aunque aplicables a los ámbitos colacionados con anterioridad y a otros, en general, al hilo de esta problemática se han desplegado análisis fructíferos sobre las posibles distorsiones derivadas de la práctica de videoconferencias. Así, por lo que se refiere a los de naturaleza estrictamente jurídica, se ha señalado que, en los procedimientos relativos a la libertad condicional y similares, la videoconferencia viola los derechos vinculados al *due process,* tales como el derecho del acusado a ser asistido de consejo *(Right to Effective Assistance of Counsel)* (46); o el de contradecir testimonios adversos *(Right to Confront Adverse Witnesses)* (47). En definitiva, como ha sido reconocido judicialmente, los encausados disponen de algunas garantías procesales que solo se satisfacen si se posibilita su derecho a estar físicamente presentes (48), lo que, en muy buena medida, convierte la videoconferencia en materia criminal en un mecanismo excepcional y no en una solución *por defecto* (49).

Pero el fundamento de muchos de los argumentos formulados en Derecho contra la videoconferencia encuentra –como es habitual– su sopor-

---

(45) «Developments in the Law – Access to Courts», cit., p. 1182. Los jueces de inmigración tienen una importante sobrecarga y medios escasos, lo que, unido a la reclusión de los sujetos afectados, ha inducido al regulador a admitir con gran generosidad la práctica de videoconferencias. Aunque dotada de poderes decisorios muy severos, esta «jurisdicción» depende, no obstante, del Departamento de Justicia, lo que le ha granjeado sombras de parcialidad y de constituir un atentado al principio de separación de poderes.

(46) Se argumenta que este derecho se pone en peligro desde el momento en que el abogado debe decidir si estar físicamente presente con su patrocinado, de modo que no padezca la relación comunicativa abogado-cliente, o en la sede del órgano judicial, junto al acusador, de modo que no se resienta la correcta comunicación con el tribunal (Marr, K., «The Right to «Skype»: The Due Process Concerns of Videoconferencing at Parole Revocation Hearings», *cit.*, pp. 1532-1533).

(47) Por razones muy parecidas a las señaladas en relación con el derecho a ser asistido. Derechos ambos frente a los que no procedería la alegación eficaz de razones de conveniencia, eficiencia o ahorro de costes o tiempo, que son, por cierto, igualmente invocadas en el Derecho español (Marr, K., *ibidem*, pp. 1535-1537). En el supuesto de los testigos, existe una cláusula (la llamada *Confrontation Clause)*, derivada de la Sexta Enmienda de la Constitución norteamericana, en virtud de la cual «In all criminal prosecutions, the accused shall enjoy the right […] to be confronted with the witnesses against him», cuya integridad podría peligrar con la ausencia de un enfrentamiento real y presencial. Sobre este particular aspecto, *vid*. Tokson, M.J., «Virtual Confrontation: Is Videoconference Testimony by an Unavailable Witness Constitutional?», *The University of Chicago Law Review*, núm. 74, 2007, pp. 1581 y ss. De hecho, en 2002 se modificó la *rule* 26 de las *Federal Rules of Criminal Procedure*, admitiendo el testimonio remoto de testigos solo «en circunstancias excepcionales», cuya concreción ha sido remitida a la casuística de los tribunales (sobre esto, puede consultarse el interesante estudio de McAllister, M.C., «Two-Way Video Trial Testimony and the *Confrontation Clause:* Fashioning a Better *Craig Test* in Light of *Crawford*», *Florida State University Law Review*, núm. 34, 2007, pp. 835 y ss.).

(48) *«If the right to be physically present is fulfilled».* Así se declara, por ejemplo, en *United States v. Thompson*, 599 F.3d 595, 599 (7th Cir. 2010).

(49) *United States v. Thompson*, *cit.* En 1996, se permitió el uso de esta herramienta, a día de hoy globalmente aceptada, en el ámbito civil, aunque solo *«for good cause in compelling circumstances»* («Developments in the Law – Access to Courts», *cit.*, p. 1183).

te en constataciones técnico-científicas. En efecto, aunque la investigación sobre estos fenómenos es escasa y muy reciente, estudios realizados en el campo de la psicología y las ciencias del comportamiento parecen acreditar algunas fallas de la videoconferencia, a la vista de las garantías jurídicas que deben proporcionarse a las partes procesales. Así, existen algunas evidencias acerca de que la falta de contacto visual directo o el papel del lenguaje no verbal –intensificado en casos en los que la *conducta* del encausado, percibida por el tribunal, es determinante para el resultado del juicio, como sucede en los procesos por inmigración–, tienen alcances distintos cuando la comunicación inter-personal es real y cuando se produce por mediación de herramientas tecnológicas (50). Convendrá seguramente esperar a que se amplíen y contrasten estos resultados, de cara a la consolidación de una cierta prudencia regulatoria y aplicativa en la materia (51).

2.2.2 Vehículos Aéreos no Tripulados e investigación criminal: ¿hacia un *panóptico digital?*

El empleo de vehículos aéreos no tripulados o drones (52), aun en buena medida huérfano de una regulación exhaustiva que los contemple como herramienta de aprovechamiento económico masivo –muy alejado, pues, del lúdico y minoritario *aeromodelismo*–, se ha convertido en los últimos años en una clara preocupación para el Derecho, a la que no podía ser ajeno el vinculado con las garantías ciudadanas ínsitas al funciona-

(50) No podemos extendernos en detalle sobre los resultados de estos estudios, pero conviene tenerlos muy en cuenta para una aproximación menos idealista a la videoconferencia. Algunos de ellos son claramente expuestos en un *paper:* Hass, A.S., «Videoconferencing in Immigration Proceedings», *Harvard Law School Student Scholarship Series*, Paper 3, 2006; accesible en: http://lsr.nellco.org/harvard_students/3. Consideraciones sobre los mismos pueden encontrarse, asimismo, en Poulin, A.B., «Criminal Justice and Videoconferencing Technology: The Remote Defendant», *Tulane Law Review*, núm. 78, 2004, pp. 1089 y ss., especialmente 1104 y ss.

(51) La videoconferencia está experimentando, por el contrario, una imparable expansión, incluyendo su difusión como mecanismo de cooperación judicial entre los Estados de la UE, en la que concurren, sin embargo, elementos de singular complejidad, como el idioma. A pesar de ello, la fe en la herramienta parece inquebrantable, sin que, por cuanto nos alcanza, se haya profundizado en Europa en ninguna de las problemáticas expuestas. Desde 2014 existe un grupo de expertos sobre videoconferencia transfronteriza, en el seno del *«EU Council Working Party on e-Law (e-Justice)»* y, de hecho, la videoconferencia es una de las iniciativas incluidas en el *Plan de acción plurianual 2014-2018 relativo a la Justicia en red europea* (2014/C 182/02). Para unas pautas, muy simples, sobre el tema, puede consultarse este documento: https://e-justice.europa.eu/content_taking_evidence_by_videoconferencing-405-AT-en.do?clang=en.

(52) Creemos que no procede entrar aquí en una disección detallada sobre el alcance preciso de los términos empleados hoy día en la regulación técnica, la práctica administrativa o el lenguaje común, por lo demás, aún no consolidado. Se vienen usando como sinónimos –y así lo hacemos nosotros– los términos «drone», «Vehículo Aéreo no Tripulado» (UAV, *Unmanned Aerial Vehicle)*, RPA *(Remotely Piloted Aircraft)*, RPAS *(Remotely Piloted Aerial System)* o UAS *(Unmanned Aerial System)*, aunque algunos de ellos tienen más implantación en el ámbito civil y otros en el militar. Nosotros emplearemos el término «drone» como omnicomprensivo.

miento de la Justicia (53). Esos dispositivos presentan especial relevancia en diversos ordenamientos jurídicos, comenzando por el español, en el que su uso ha sido específicamente avalado a partir de 2015 (54), así como, nuevamente, en el Derecho norteamericano, en el que, por comprometer garantías amparadas por la Cuarta Enmienda de la Constitución (55), ha suscitado algunas polémicas académicas (56).

En nuestro Derecho, la previsión sobre el uso de estos instrumentos en el ámbito de la Justicia criminal (57) ha recibido, por autorizada doctrina, un claro aval en relación con su conformidad a las garantías constitucionales relativas a la intimidad de los individuos. En efecto, a partir de las coordenadas espaciales –«lugar o espacio público»– en las que se permite su uso, parece excluirse el amparo legal de una utilización potencialmente lesiva para los investigados, desde este concreto punto de vista (58). Pero lo cierto es que los peligros existen. En primer lugar, conviene recordar que, al contrario de lo que sucede con la mayor parte de las restantes

(53) Existen incursiones doctrinales patrias sobre el fenómeno. Así y sin ánimo alguno de exhaustividad, desde la óptica de la intervención administrativa, destacan las de Brufao Curiel, P., «El régimen jurídico internacional, europeo y español de las aeronaves no tripuladas o drones y su influencia en el mercado, la gestión y el derecho aeronáutico», *Revista Aranzadi Doctrinal*, núm. 6, 2015, pp. 223-254 o Mora Ruiz, M., «La ordenación jurídico-administrativa de los *drones* en el Derecho español: entre la libre competencia y la protección del interés general». Desde la óptica de los derechos reconocidos en el artículo 20 CE, téngase en cuenta el trabajo de Escribano Tartajada, P., «Drones y derecho a la intimidad y la propia imagen: estado de la cuestión y problemas que se plantean en la actualidad». Los dos últimos en Guerrero Lebrón, M.J./Peinado Gracia, J.I. (Dirs.) y Contreras de la Rosa, I. (Coord.), *El Derecho aéreo entre lo público y lo privado. Aeropuertos, acceso al mercado, drones y responsabilidad*, Universidad Internacional de Andalucía, Sevilla, 2017, pp. 210-237 y 238-259, respectivamente. Con una perspectiva más general, que comprende el estudio de ilícitos penales cometidos mediante estos artefactos, *vid*. Nadal Gómez, I., «La litigiosidad que se nos viene encima: cuestiones procesales al hilo de la aparición de «drones» en nuestros cielos», *Diario La Ley*, núm. 8507, 25 de marzo de 2015.

(54) Mediante la Ley Orgánica 13/2015, de 5 de octubre, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica.

(55) Dicha enmienda reconoce «The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized».

(56) En Estados Unidos el debate sobre la problemática de fondo parece haberse iniciado hace ya años, a partir de la vigilancia mediante satélites. *Cfr.*, entre otros, el temprano trabajo de Steele, L. J., «The View from on High: Satellite Remote Sensing Technology and the Fourth Amendment», *Berkeley Technology Law Journal*, núm. 6, 1991, pp. 317 y ss.; asimismo, también los trabajos de Korodi, P., «Satellite Surveillance Within U.S. Borders», *Ohio State Law Journal*, núm. 65, 2004, pp. 1627 y ss. o Craig, B., «Online satellite and aerial images: issues and analysis», *North Dakota Law Review*, núm. 83, 2007, pp. 547 y ss.

(57) Dicha previsión se contiene, en esencia, en el artículo 588 *quinquies a)* LECr *(Captación de imágenes en lugares o espacios públicos)*, del siguiente tenor: «1. La Policía Judicial podrá obtener y grabar por cualquier medio técnico imágenes de la persona investigada cuando se encuentre en un lugar o espacio público, si ello fuera necesario para facilitar su identificación, para localizar los instrumentos o efectos del delito u obtener datos relevantes para el esclarecimiento de los hechos».

(58) Es, en esencia, la opinión de Bueno de Mata, F., «Comentarios y reflexiones sobre la Ley Orgánica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica», *Diario La Ley*, núm. 8627, 19 de octubre de 2015, apartado III.

medidas «tecnológicas» de investigación introducidas en 2015, el uso de drones u otros dispositivos de captación y registro de imágenes contemplados en el precepto citado de la LECr, no está sujeto a plazo, lo que presenta, como veremos, notable incidencia desde la perspectiva de los derechos afectados. En segundo lugar, el uso de drones se cualifica, asimismo, frente a otras medidas por el hecho de que, en principio, no requiere de una autorización judicial específica (59).

En este contexto, conviene, sin embargo, aportar dos reflexiones. La primera es la relativa a la afectación de estas medidas a la *intimidad* o *privacidad* de los investigados. Esta afectación parece no concurrir en todos los casos, pero la razón de ello, reside, seguramente, en que partimos de un concepto podríamos decir que «analógico» de esta garantía, cuando lo que realmente demanda el uso masivo de dispositivos de vigilancia y captación de imagen, como los drones es, tal vez, una reconstrucción de los derechos relacionados con la privacidad del individuo o, al menos, un enfoque «pluralista» de los mismos frente a las interferencias del aparato público, en conjunción con el principio general de libertad y sus manifestaciones sobre la locomoción humana (60). Sobre ello ahondamos en las consideraciones que siguen.

En efecto, cierta doctrina norteamericana ha indagado en la necesaria adaptación de la vigilancia mediante drones a los requerimientos que la jurisprudencia de aquel país ha venido exigiendo para considerar la concurrencia de una «indagación» *(search)* en la privacidad, en la precisa signi-

(59) En el Derecho norteamericano, la doctrina judicial evacuada en relación con la Cuarta Enmienda parece partir del principio contrario: when a «search» occurs it «is presumptively unreasonable without a warrant» se señala en *Kyllo v. United States*, 533 U.S. 27, 40 (2001), *apud* Talai, A.B., «Drones and *Jones:* The Fourth Amendment and Police Discretion in the Digital Age», *California Law Review*, núm. 102, 2014, p. 751. Cuestión distinta –clave, como se verá– es la relativa a cuándo puede decirse que concurre una observación mediante drones que constituya una *pesquisa* (search), en el preciso sentido derivado de la Cuarta Enmienda.

En cuanto a nuestro Derecho, conviene recordar que nosotros examinamos aquí la sola captación de imagen mediante los dispositivos a que se refiere el citado artículo 588 *quinquies a)* LECr, lo que remite a una obtención *dinámica* y *selectiva* de la imagen de los investigados. La captación *estática* y *general* de imágenes, mediante la instalación de videocámaras por las fuerza de seguridad, tiene presupuestos y alcance distintos, muy vinculados a la garantía prevista en el artículo 18.4 CE, en los que no podemos detenernos. Su principal manifestación tal vez sea la extrajudicial, mediante la instalación de videocámaras en vías públicas, todavía regulada en la Ley Orgánica 4/1997, de 4 de agosto. En el ámbito judicial su alcance es, en cambio, mayor (vuelve a ser una captación *selectiva* o *discriminada)*, de modo que, previa la oportuna autorización del juez, la LECr consiente la grabación de imagen y su sonido asociado en el interior de un domicilio. *Vid.* un posicionamiento muy crítico al respecto en Richard González, M., «Conductas susceptibles de ser intervenidas por medidas de investigación electrónica. Presupuestos para su autorización», *Diario La Ley*, núm. 8808, 21 de julio de 2016, apartado *C*.

(60) La preocupación que el uso general de drones (no solo, pues, con fines de investigación policial) supone para la *privacidad* es bastante patente. Remitimos ahora a los análisis realizados en los trabajos citados en nota 53. Una evaluación de su impacto en la opinión pública puede obtenerse aquí: https://elpais.com/tecnologia/2016/04/19/actualidad/1461068413_955128.html. En cuanto que, en esta sociedad vigilada, parece inaplazable una redefinición de la privacidad, resultan interesantes las reflexiones de Calo, M.R., «The Drone as Privacy Catalyst», ensayo publicado en *Stanford Law Review*, December 2011; accesible en: https://www.stanfordlawreview.org/online/the-drone-as-privacy-catalyst/.

ficación proscrita por la Cuarta Enmienda. En tal sentido, son tres los *tests* ensayados. El primero es el *Trespass test* o «test de la intrusión», en virtud del cual una búsqueda o indagación, a los efectos de la Cuarta Enmienda, no concurre si la autoridad no realiza una acción de *perturbación física* –en el tradicional sentido que adquiere esta expresión en la legislación civil patrimonial– sobre ciertos elementos prohibidos (personas, viviendas, documentos, etc.). La adaptación del uso de drones a los requerimientos de este test es muy compleja, pues parece no concurrir intromisión propiamente dicha por parte de un ingenio que sobrevuela –incluso propiedad privada–, en ocasiones, a miles de metros de altitud (61).

En defecto de intromisión física, un segundo escalón viene integrado por el «test de la expectativa razonable de privacidad» *(Reasonable Expectation of Privacy Test),* sentado, con su fisonomía actual, en una conocida sentencia del Tribunal Supremo (62). El mismo parte de un axioma, de gran interés para la moderna invasividad tecnológica, consistente en que «la Cuarta Enmienda protege personas, no lugares» *(the Fourth Amendment protects people, not places),* de modo que, al margen del espacio en que se practique, la indagación o la búsqueda proscrita concurrirá o no en función de la frustración de las legítimas expectativas de privacidad –objetivamente razonables– que el individuo posea. Ello conduce, como ha sido expresamente reconocido por el Tribunal, a que el concepto general de privacidad (63) sea distinto del aplicable a efectos de la Cuarta Enmienda. No obstante, tal distinción se ha ido diluyendo con la evolución tecnológica (64) y con algún otro correctivo, como la «Teoría del Mosaico», que analizamos seguidamente.

El test de la expectativa de privacidad no ha experimentado actualizaciones provenientes directamente de la experiencia con drones, pero las conclusiones que han ido incorporándose a esta doctrina han intentado serle aplicadas por analogía y, en tal sentido, su análisis puede ser fructífero de cara al ordenamiento jurídico español, que, como vimos, habilita a las fuerzas de seguridad dependientes de la autoridad judicial para el empleo de estos ingenios volantes, siempre que se produzca en «lugar o es-

(61) Talai, A.B., «Drones and *Jones:* The Fourth Amendment and Police Discretion in the Digital Age», cit., pp. 761-762.

(62) *Katz v. United States*, 389 U.S. 347, 361 (1967).

(63) Nacido a partir del célebre trabajo de Warren, S.D. y Brandeis, L.D., «The Right to Privacy», *Harvard Law Review*, vol. 4, núm. 5., 15 de diciembre de 1890, pp. 193-220.

(64) Un ejemplo es el de la información divulgada o de dominio público, que no entra dentro del ámbito de cobertura de la Cuarta Enmienda. En su fisonomía tradicional, esta exclusión tiene tal vez sentido, pero resulta más problemática, al menos de modo tajante, en el moderno contexto tecnológico, en el que, voluntariamente, los ciudadanos proporcionamos cotidianamente cantidades ingentes de datos. *Vid.* sobre esto Talai, A.B., «Drones and *Jones:* The Fourth Amendment and Police Discretion in the Digital Age», *cit.*, pp. 754-756.

pacio público» (65). En tal sentido y, en principio, al igual que en el Derecho patrio, ha sido declarado en USA que la Cuarta Enmienda no protege frente a investigaciones realizadas en espacios públicos, centrando su ámbito de protección en el domicilio y su perímetro.

Es más, la jurisprudencia también ha señalado que no es suficiente con que la pesquisa o investigación se realice sobre el domicilio para que nos encontremos amparados por la Cuarta Enmienda, sino que son necesarios requisitos adicionales. Por una parte, resulta determinante de su licitud el hecho de que la búsqueda se realice desde una vía pública (66). En tal sentido y a partir de resoluciones judiciales evacuadas en relación con casos de vigilancia aérea policial sobre sospechosos, se ha declarado que, si bien existe una expectativa *subjetiva* razonable de privacidad en relación con el espacio aéreo situado sobre el domicilio de una sospechosa, no resulta admisible, en cambio, una expectativa *objetiva* razonable en relación con la vigilancia aérea policial (67).

Por otra parte, un escalón adicional para concretar la concurrencia de una intromisión proscrita por la Cuarta Enmienda consiste en acreditar que los elementos observados dentro del domicilio –inaccesibles, en principio, en ausencia de una injerencia física– lo han sido mediante el empleo de una tecnología de acceso no público o generalizado. Esta reflexión es, asimismo, muy reveladora para la realización de un escrutinio sobre la constitucionalidad del uso de drones para fines de investigación, a la vista de que muchos de ellos pueden ir dotados de dispositivos muy invasivos (68). Así, se ha declarado, por ejemplo, que requiere orden judicial la

---

(65) Salvo mejor opinión, no alcanzamos a concretar la carga semántica adicional que aporta el empleo de dos sustantivos («lugar» y «espacio»), adjetivados con la condición de «público», en vez de uno solo.

(66) En *California v. Ciraolo*, 476 U.S. 207, 213 (1986) se afirmó ya que «la protección que brinda la Cuarta Enmienda sobre el domicilio nunca se ha extendido a la exigencia de que los agentes de la ley se protejan los ojos al pasar por un hogar situado junto a vías públicas» (Talai, A.B., «Drones and *Jones:* The Fourth Amendment and Police Discretion in the Digital Age», *cit.*, p. 762).

(67) Talai, A.B., *ibidem*, pp. 762-763. Los pronunciamientos en este sentido y similares son varios, a partir de la citada *California v. Ciraolo*. Los casos son muy explicativos y todos parten de que la observación visual realizada por agentes de policía desde el éter público *(public airwaves)* o espacio aéreo legalmente navegable *(legally navigable airspace)* no requiere orden judicial específica *(search warrant)*. Así, en *Florida v. Riley*, 488 U.S. 445 (1989) se sostiene que «la Cuarta Enmienda no estaba implicada cuando la policía voló en helicóptero, a cuatrocientos pies, sobre el invernadero parcialmente cubierto del acusado, ubicado al lado de su casa móvil, y observó, a simple vista, plantas de marihuana en su interior, porque cualquiera podría haberse posicionado de manera similar en un avión y haber hecho las mismas observaciones, a través de las secciones descubiertas del techo»; en *Dow Chem. Co. v. United States*, 476 U.S. 227 (1986) se afirma que «cuando se utilizó una cámara de vigilancia para observar las áreas abiertas de una instalación industrial, no se realizó ninguna *pesquisa»;* o en la citada *California v. Ciraolo*, en la que se mantiene que las observaciones a simple vista, desde un avión situado a mil pies, sobre un patio trasero cercado que se considera dentro del perímetro de la casa, no constituyeron una *pesquisa*, porque «en una época en la que el vuelo privado y comercial en las vías aéreas públicas es rutinario, no es razonable que el encausado confíe en que sus plantas de marihuana estén constitucionalmente protegidas frente a tal observación».

(68) Sobre estos aspectos técnicos puede consultarse, asimismo, el completo trabajo, tantas veces citado, de Talai, A.B., *ibidem*, pp. 744-751.

observación de un domicilio, desde un apostadero público, pero empleando una cámara térmica (69). De este modo, la Cuarta Enmienda puede proteger casos en los que la observación ha sido realizada desde un lugar público, pero empleando una tecnología generalmente indisponible o, de otro modo, que permite observar elementos inicialmente solo accesibles mediante la comentada perturbación física.

Por último, desde el punto de vista de la protección de la privacidad, a modo de correctivo del *Reasonable Expectation of Privacy Test,* se encuentra, destacadamente, el tercer y último constructo doctrinal: The *Mosaic Theory o «*Teoría del mosaico». A partir de ella se afirma, con carácter general, que, si bien es cierto que la vigilancia realizada sobre un individuo en espacios públicos no es ilícita desde la perspectiva de la Cuarta Enmienda, un seguimiento permanente y continuado en el tiempo, aun desplegado en tales vías o espacios públicos, puede atentar contra la comentada garantía de la «expectativa razonable de privacidad». En efecto, cualquiera tiene una estimación razonable, objetiva y socialmente protegida, de que no va a ser observado, incluso fuera de las zonas protegidas (domicilio, etc.) con esa intensidad, continua y permanentemente, pues lo así observado no es accesible al común de los ciudadanos, por su integralidad, prolongación y alcance (70).

No obstante, la teoría del mosaico ha sido profundamente contestada, padeciendo una crónica inestabilidad debido a la renuncia de los jueces a fijar un límite temporal preciso a partir del cual entraría en juego la cobertura de la Cuarta Enmienda y, en consecuencia, la necesidad de una orden judicial. No obstante, puede servir de pauta en relación con el uso de drones en ordenamientos jurídicos que, como es español, no han determinado límites temporales precisos a estas prácticas investigadoras.

En cualquier caso, toda esta construcción doctrinal enderezada a proteger la privacidad, en el sentido derivado de la Cuarta Enmienda, presenta evidentes fallas en su aplicación a la investigación mediante drones, según lo ya visto: aunque en buena parte de las sentencias se presentan casos de observación ocular directa por agentes de la autoridad –y no de monitorización mediante cámaras accionadas por control remoto, que es

(69) Decidido en *Kyllo v. United States,* 533 U.S. 27, 34 (2001).

(70) La teoría fue sentada en una conocida sentencia de apelación *[United States v. Maynard*, 615 F.3d 544, 555-56 (D.C. Cir. 2010)]. En ella se declaró contrario a la Cuarta Enmienda el rastreo GPS desplegado sobre un individuo las 24 horas del día, durante 28 días consecutivos. No obstante, la sentencia fue en buena medida corregida en *United States v. Jones*, 132 S. Ct. 945, 954 (2012). Los argumentos se basaban en las consideraciones realizadas en el texto: «el todo es algo diferente de la suma de sus partes». «Una persona razonable no espera que nadie monitoree y conserve un registro de cada uno de sus movimientos»; por el contrario, «lo que espera es que la imagen de conjunto de sus movimientos permanezca desconectada y anónima». *Cfr.* Talai, A.B., «Drones and *Jones:* The Fourth Amendment and Police Discretion in the Digital Age», *cit.*, pp. 757-760 y 765-766.

lo característico de los drones–, es cierto que estos artefactos no suponen una invasión física de espacios protegidos *(Trespass Test)*; solo algunos de estos artilugios pueden considerarse «fuera del mercado» por su nivel tecnológico, mientras que un buen número de ellos, con un gran potencial de invasividad, son generalmente accesibles *(Reasonable Expectation of Privacy Test);* etcétera.

Pues bien, la segunda de las reflexiones que anunciábamos al inicio de este apartado consiste precisamente en esto: que todas esas deficiencias surgidas en la proyección sobre el uso de drones de la doctrina construida en torno a la privacidad protegida por la Cuarta Enmienda, han conducido a postular que, en definitiva, el problema de la *intimidad* no es el único implicado en el uso de estos dispositivos, sino que en igual o mayor medida lo es el de la *discrecionalidad gubernamental*. Para una mejor adaptación a las amenazas –actuales y previsibles– que la vigilancia tecnológica mediante este tipo de ingenios puede llegar a suponer para las libertades ciudadanas, se han propuesto dos vías de argumentación. Primordialmente, la reformulación de la teoría del mosaico, pues es ella la que verdaderamente sostiene la posibilidad de proteger a los ciudadanos de indagaciones policiales incluso en la vía pública. Pero, a su vez, para ello resulta imprescindible «huir», por así decir, de la *privacidad,* como único bien jurídico protegido por la Cuarta Enmienda (71).

En efecto, según Talai, la Cuarta Enmienda protege, incluso en mayor medida que el bien *privacidad* de los ciudadanos, su *libertad de locomoción* o *deambulatoria,* que hunde sus raíces en la libertad y seguridad personales del individuo y su derecho a desplazarse (72). En tal sentido, existe una clara sintonía entre la problemática que puede derivarse del uso de drones con fines de investigación o prevención criminales y la jurisprudencia, evacuada en USA, en relación con las «retenciones y cacheos» masivos, permanentes y continuos (73). Así –se afirma–, hoy día los agentes de la autoridad no necesitan parar y registrar a los viandantes para poder limitar arbitrariamente su libertad de locomoción, sino que tal limitación puede operarse, en su sentido más literal, de modo «telemático». De esta manera, la identidad de razón entre, por una parte, la vigilan-

(71) Apoyándose en precedentes judiciales y análisis doctrinales, Talai considera la Cuarta Enmienda «as a general liberty amendment» (Talai, A.B., *ibidem*, p. 767).

(72) Derechos de libertad que, aun desde perspectivas distintas, reconocen los artículos 17 y 19 CE, pudiendo extraerse de ellos consecuencias también útiles a los efectos de lo aquí examinado, como se verá a continuación.

(73) *Stop-and-frisk policies*. También denominados «*Terry* stops», pues los límites de tales conductas policiales fueron establecidos, de modo muy controvertido, en una conocida sentencia: *Terry v. Ohio* 392 U.S. 1 (1968), evacuada en el contexto de una práctica habitual en muchas grandes ciudades norteamericanas en los años 60, consistente en el ejercicio continuado y masivo de controles policiales para reducir la criminalidad en las calles.

cia en el sentido de la Cuarta Enmienda *(search)* y, por otra, la retención y el cacheo, sería clara: se puede vigilar a alguien por motivos varios, pero la vigilancia policial tiene el mismo fundamento que la práctica de retenciones y cacheos: la persona concernida se considera sospechosa de alguna conducta antisocial (74). Las consecuencias de estos planteamientos para el ordenamiento jurídico español podrían ser, como decíamos, muy fructíferas, conduciendo a fortalecer los derechos comprometidos en el empleo de estos dispositivos, superando con ello las magras referencias legales (75).

El principal obstáculo para esta asimilación, a partir de la teoría del mosaico, consiste en que la misma exigía una duración prolongada de la vigilancia para caer en el ámbito de relevancia constitucional, mientras que parece razonable señalar que seguimientos con drones de no muy larga duración pueden resultar, asimismo, contrarios a las garantías protegidas por la Cuarta Enmienda (76). Para ello, el último y definitivo bastión de cara al control en el uso de estos dispositivos, consiste en aplicar las limitaciones elaboradas en torno al ejercicio de la *discrecionalidad policial,* con mayor motivo toda vez que, al igual que sucede en el caso

(74) En cambio, diferencia esencial entre la retención y el cacheo en las calles y la vigilancia masiva mediante drones, consistiría en que la primera sería, en principio, más selectiva por más perceptible. Como prueba, Talai señala que entre 2004 y 2012 el Departamento de Policía de la ciudad de Nueva York (NYPD) realizó 4,4 millones de «*Terry* stops» y en el 80 por 100 de ellos el sujeto afectado fue una persona de color (Talai, A.B., «Drones and *Jones:* The Fourth Amendment and Police Discretion in the Digital Age», *cit*., p. 772).

(75) En efecto, como es sabido, tanto nuestro TC como el TS han construido un importante y detallado cuerpo de doctrina acerca de los límites para el ejercicio de la potestad de retención por parte de las fuerzas y cuerpos de seguridad. En tal sentido, el TC ha llegado a señalar –en un sentido que nos recuerda, con intenso eco, las ideas que venimos expresando en el texto– que: «el sometimiento de la detención a plazos *persigue la finalidad de ofrecer una mayor seguridad de los afectados por la medida*, evitando así que existan privaciones de libertad de duración *indefinida*, *incierta o ilimitada* (SSTC 341/1993, de 18 de noviembre; 174/1999, de 27 de septiembre y 179/2000, de 26 de junio); la cursiva es nuestra. En cuanto a la doctrina del TS, puede verse un resumen de la misma, entre tantas, en la STS (Sala 2.ª), de 7 de marzo de 2013 (Res: 156/2013). Tal doctrina podría progresivamente adaptarse al uso policial de drones, a partir tanto de argumentos esgrimidos en este trabajo, como de otros. Sobre la jurisprudencia en relación con los derechos del artículo 17 y concordantes de la CE puede consultarse, *ex plurimis*, el trabajo de Pomed Sánchez, L., «Algunos aspectos de la jurisprudencia constitucional sobre el derecho a la libertad y a la seguridad», *Revista Catalana de Seguretat Publica*, núm. 16, 2006, pp. 165 y ss., sobre todo 170 y ss.

(76) Sin embargo, como herramienta de política general de seguridad, la potencialidad del uso de drones sobre la psicología y el control social de la población es realmente asombrosa, sobre todo a partir de la posibilidad de considerar estos ingenios como plataformas para usar conjuntamente con –o incluso integrar– otras tecnologías, señaladamente cámaras con diversas funcionalidades y GPS (para designación de objetivos, característicamente), llegando incluso a concebir la posibilidad de artilugios volantes con capacidad de interactuación física (captura) con humanos, como ya muestra un experimento llevado a cabo por la Universidad de Pennsylvania. Esta idea da lugar al empleo de la expresión «*Digital Panoptic*» o Tercer Panóptico, en el sentido de la culminación de los sistemas de vigilancia y control social integral, que habrían transitado desde el primer Panóptico, el arquitectónico de Bentham, pasando por el segundo, encarnado en el orwelliano empleo masivo de circuitos cerrados de televisión. *Vid.* Talai, A.B., «Drones and *Jones:* The Fourth Amendment and Police Discretion in the Digital Age», cit., pp. 775-778.

de los *«Terry stops»,* el uso de drones no requiere, inicialmente, una previa orden judicial (77).

En tal sentido, se ha propuesto un esquema analítico para determinar la posible ilicitud del empleo de drones con fines de vigilancia criminal, por incurrir en abuso en el ejercicio de la discrecionalidad policial, con relevancia desde el punto de vista de la Cuarta Enmienda. Así, desde la óptica de los *costes,* si el ejercicio del poder empleado por la autoridad puede imponer un alto costo en términos políticos para los ciudadanos, a pesar de que el impacto económico para el erario derivado del empleo de tal poder sea bajo, existen indicios de abuso. Desde el prisma de la *cobertura,* si el ejercicio del poder puede extenderse indefinidamente, existen indicios de abuso. En cuanto al cálculo *riesgo-beneficio,* si el argumentario empleado para el ejercicio de ese poder es seductor e incluso irresistible, existe un claro indicio de uso abusivo. «Es decir, desconfíe de las justificaciones basadas en el bien público, que se utilizan para acallar la disidencia y sofocar el debate». Por último, el *sigilo:* si el ejercicio del poder es extrañamente clandestino, alimentando así la falta crónica de atención y la aquiescencia, existen indicios de ejercicio abusivo de tal poder (78). Por lo demás, España no se ha visto libre de casos en los que una, previsión normativa ha dejado excesivamente abierta la discrecionalidad administrativa, en el empleo de herramientas tecnológicas esencialmente volcadas hacia la actividad jurisdiccional (79).

---

(77) No obstante, el abuso puede producirse, como es natural, incluso mediando tal orden. Es el caso, en buena medida «piloto» en la materia, enjuiciado en la sentencia *State of North Dakota v. Brossart*, No. 32-2011-CR-0049 (Dist. Ct. N. D. July 31, 2012). Resumidamente: las fuerzas del orden obtuvieron orden judicial para vigilar, mediante un drone cualificadamente avanzado y penetrante [un *Predator* MQ-1, fabricado por *General Atomics Aeronautical Systems, Inc.* y dotado de un avanzadísimo sistema: *Autonomous Real-Time Ground Ubiquitous Surveillance* (ARGUS)], las condiciones en que debía producirse, y finalmente se produjo, el arresto de un granjero acusado por su vecino de finca de robarle unas cabezas de ganado. Sobre este supuesto, además del trabajo de Talai, ya citado (Talai, A.B., *ibidem*, pp. 737-739, fundamentalmente), puede consultarse Bryan, T., «*State v. Brossart:* Adapting the Fourth Amendment for a Future With Drones», *Catholic University Law Review*, núm. 63, 2015, pp. 465 y ss.

(78) El análisis en Talai, A.B., *ibidem*, pp. 778-780.

(79) Seguramente SITEL (*Sistema Integral de Interceptación de Comunicaciones Electrónicas*) sea el caso más célebre. Este sistema gubernamental permitió, desde sus inicios, a las fuerzas y cuerpos de seguridad y al Centro Nacional de Inteligencia tratar, al margen de los jueces, ciertas informaciones muy relevantes (los llamados *datos asociados)*, como la identificación de las personas, su domicilio, los números del titular y de cuenta asignados por el proveedor de servicios de acceso, la dirección de correo electrónico o la situación geográfica de la terminal. Su involucración en algunos sonados procesos judiciales, como el relativo a la denominada «Trama *Gürtel»*, terminaron de disparar las alarmas sobre el posible abuso gubernamental en el empleo de esta herramienta. En términos jurídicos pueden consultarse, entre otros: Martínez Ferríz, J.L.J., «La operatividad de SITEL: su discutida legalidad dentro de un Estado de derecho que actúa bajo el imperio de la ley (A intención de la polémica suscitada sobre la licitud constitucional de las escuchas del caso *Gürtel)»*, *Diario La Ley*, núm. 7434, martes, 29 de junio de 2010; o Rodríguez Laínz, J.L., «Consideraciones jurídicas en torno a la licitud constitucional de SITEL», *Diario La Ley*, núm. 7344, miércoles 10 de febrero de 2010. Sin embargo, la legitimidad del sistema fue finalmente avalada. Por un lado, la STS (Sala Tercera) de 5 de febrero de 2008 confirmó la posibilidad de una disciplina, aun

3. ALGUNAS CONCLUSIONES DE ORDEN GENERAL

El análisis desplegado en este trabajo –apegado necesariamente, como se ha visto, a unos pocos aunque relevantes fenómenos–, arroja, a nuestro juicio, algunas esclarecedoras conclusiones. La primera consiste en la *necesidad* de un replanteamiento muy serio sobre el orden y el modo de operar de las distintas instituciones implicadas en la promoción y materialización, normativa y ejecutiva, de las soluciones innovadoras y tecnológicas en la Justicia de nuestro país. El orden y la coordinación en la actuación de los poderes públicos resulta insustituible de cara al logro de los principios comprometidos en el Estado de Derecho, incluido el tan valorado de la *eficiencia* (80) y, desde luego, en mucha mayor medida, para la garantía de los derechos fundamentales de los ciudadanos (81).

En segundo lugar, los análisis desplegados nos refuerzan en la consideración de que la simple implantación de soluciones tecnológicas no solo no resulta suficiente para un mejoramiento efectivo en el ejercicio de la función jurisdiccional, sino que puede conllevar un deterioro significativo de la misma, incluyendo preocupantes exposiciones de los derechos fundamentales de los ciudadanos. Esta realidad no solamente se ha constatado en los aspectos de gestión procesal, con resultados creemos que suficientemente contrastados, sino que adquiere una relevancia, a nuestro juicio incluso superior, en el caso de la modernización de las actuaciones procesales y de investigación judicial.

En efecto, en este ámbito, el examen crítico que hemos desplegado sobre la implantación, en nuestro ordenamiento jurídico procesal, de herramientas como la videoconferencia o la generalización de medios digitales de seguimiento, captación y registro de imagen, como los drones, ha revelado, según los casos, dos aspectos sobre los que convendrá seguir reflexionando. Por una parte, que la disponibilidad y regulación acabada de este tipo de instrumentos tecnológicos no solo ha de verse precedida, sino con certeza continuamente avalada, por estudios e investigaciones jurídicos profundos (académicos, especialmente) que aporten perspectivas, cuando no soluciones, a los complejos problemas que los mismos hacen aflorar, según ha podido comprobarse en este trabajo. Por otra parte,

---

parcial, del sistema mediante norma reglamentaria. Por otro, la Sala Segunda lo respaldó igualmente, aunque con la concurrencia de dos importantes votos particulares, en la STS de 30 de diciembre de 2009. A pesar de ello, al menos durante un tiempo, se extendió en la opinión pública una creciente sombra de duda sobre las posibles manipulaciones de que podía ser objeto la herramienta en manos del Gobierno, al margen de su control judicial.

(80) Resulta seguramente ridículo que se invoque este principio como motor para la generalización de la videoconferencia, cuando el despliegue de los SGP en España está suponiendo un auténtico dispendio de recursos.

(81) Por insistir en los SGP, la descoordinación ya comentada sobre su elección e implantación afecta al derecho a la tutela judicial efectiva de los concretos justiciables.

la necesidad apenas expresada queda reforzada, a nuestro juicio, si partimos de que, en muchas ocasiones, los derechos que pueden verse afectados en su implementación exceden con mucho de los meramente procesales, comprometiendo estas aún novedosas herramientas, como ha podido también comprobarse en este estudio, derechos constitucionales sustantivos de primer orden.

XI

SALUD Y MUNDO DIGITAL

CAPÍTULO 41

ROBOTS Y SANIDAD

MIGLE LAUKYTE
Conex-Marie Curie Fellow (1)
Departamento de Derecho Privado
Universidad Carlos III de Madrid

(1) Este proyecto ha recibido fondos de la Universidad Carlos III de Madrid, del Séptimo programa marco de Investigación y Desarrollo Europeo bajo el acuerdo de subvención n.º 600371, del Ministerio de Economía, Industria y competitividad (COFUND2014-51509), del Ministerio de Educación, cultura y Deporte (CEI 15-17) y del banco Santander.

1. INTRODUCCIÓN: POR QUÉ ES IMPORTANTE HABLAR DE ROBÓTICA EN EL ÁMBITO MÉDICO-SANITARIO

La importancia de la discusión relativa al robot y la sanidad no es negociable, y ello por distintas razones.

La primera razón es que estamos hablando de uno de los derechos humanos, el derecho a la salud, que se encuentra en el listado de los derechos humanos sociales. Los derechos sociales, según Bobbio (2004), existen por una razón igualitaria: el derecho a la salud, así como los demás derechos sociales, reducen la desigualdad entre ricos y pobres. De hecho, Navarro (1998, 139) dice claramente que la «atención sanitaria pública tiene un efecto redistribuidor y equilibrador más fuerte que las transferencias sociales y la educación». Por eso, con o sin robots, estamos ante un derecho (salud) con un gran potencial de impacto en nuestras sociedades.

En según lugar, además de ser un derecho humano, la salud es un tema de una importancia enorme desde el punto de vista económico. Según Lema Añón (2010), el gasto público en sanidad continúa creciendo desde la Segunda Guerra Mundial (2), de forma que la inversión en la robótica médico-sanitaria puede llegar a ser insostenible para el sistema público sanitario. Pero si bien es cierto que en la actualidad este gasto en continuo crecimiento parece imposible sostenerlo, también es verdad que dicho mayor gasto puede ser amortizado con la prestación de servicios mejores a través de una tecnología avanzada más extendida, mediante una mayor competencia entre proveedores y, consecuentemente, con una tecnología posiblemente más asequible (más barata). Precisamente, gracias a esta tecnología y su extensión y difusión (democratización tecnológica) los médicos humanos podrán centrar sus esfuerzos más específicamente en aquellos casos particulares donde el factor humano reviste una especial relevancia. De esta forma, al final, resulta difícil saber si el gasto que supone la robótica médica va a tener solo consideración de gasto o podrá ser contemplado también como inversión. De ahí la conveniencia de discutir con profundidad las distintas opciones y los posibles escenarios de su desarrollo.

La robótica en la sanidad puede ser también vista desde la dialéctica propia entre los sectores público y (versus) privado en el ámbito médico-sanitario, así como la lucha de los intereses contrapuestos entre la protec-

(2) Al mismo tiempo, el autor también nos invita a «mirar con precaución los informes que periódicamente se publican sobre la voracidad infinita e insostenibilidad de los sistemas sanitarios que las más de las veces parten de unos presupuestos políticos no explicitados y se presentan con pretendida asepsia científica» (Lema Añón 2010, 201). Como en muchos casos, quizás la verdad se encuentre en el término medio y tengamos que recoger los datos de distintas fuentes para entender como es la situación en la realidad.

ción de propiedad intelectual de la industria farmacéutica del mundo desarrollado y el derecho al acceso a los medicamentos por parte (también) de los sectores más vulnerables del hemisferio pobre. Es más, se puede enfocar este discurso sobre la sanidad pública versus sanidad privada desde una perspectiva más general al considerar la sanidad y salud como auténticos «bienes comunes», pues «curar a los necesitados es un deber de civismo y de solidaridad de todo médico» (Mattei 2013, 75). Si estamos de acuerdo con está visión de la realidad, tenemos que encuadrar la cuestión de la robotización de la sanidad en manos del sector privado en términos mucho más alarmantes de lo que estamos haciendo hasta ahora.

Conectado con este discurso, cabe señalar el siguiente argumento: necesitamos a los robots, o mejor aún, lo necesita el sistema sanitario nacional. Nuestra sociedad occidental tiene graves problemas demográficos: pocos nacimientos, envejecimiento poblacional creciente, mayor número de enfermedades, significativos colectivos de personas que necesitan atención continua, asistencia, ayuda, y supervisión. Y no es una novedad de los últimos años: Navarro (1998, 141) ya nos ha advertido que en todo el mundo desarrollado «[…] la mayoría de enfermos son enfermos crónicos», y que el reto principal para la medicina es «la prevención y tomar cuidado de la morbilidad crónica». Para cualquier sistema médico-sociosanitario se trata de un reto muy serio e importante y quizás los robots asistenciales, si bien no pueden solucionarlo del todo, al menos pueden ofrecer algunas opciones más, sobre todo para las personas de la tercera edad, de movilidad reducida o incapacitados (3).

En cuarto lugar y en línea con lo expuesto, la robótica en la sanidad tiene conexiones con otras áreas de fundamental importancia como, por ejemplo, la vertiente laboral: un gran número de trabajadores del ámbito o sector sanitario pueden llegar a encontrarse sin trabajo (o con una reducción significativa del mismo) porque serán sustituidos por robots. No obstante, se señala que estas personas afectadas en su ámbito laboral podrán dedicarse a otros sectores (sanitarios y asistenciales) en los que el factor humano tiene una especial relevancia e importancia precisamente por el hecho de que determinados trabajos actuales van a ser realizados por los robots: los humanos nos concentraremos en aquello que no se puede robotizar y donde ninguna inteligencia artificial puede sustituirnos (4).

(3) Es verdad que las soluciones robóticas no carecen de problemas. Hablamos más adelante sobre ello.

(4) En este sentido ya en el 1966, Mumford nos proponía ver la mecanización y la automación (de robótica aun no se hablaba) no como la liberación del trabajo sino como la liberación por el trabajo, entendido el trabajo como auto-gratificante, educativo y estimulante. Esta visión no solo nos protegía del aburrimiento y desesperación, sino que creaba espacios para nuestra creatividad, autonomía y sentimientos de utilidad. Más sobre este tema, ver Mumford 1966.

Además, debemos tener en cuenta que, a fecha de hoy, no tenemos ninguna legislación específica para los robots, si bien existen algunos indicios significativos de que no faltarán importantes menciones al derecho a la salud en una legislación futura, cuando ésta sea eventualmente desarrollada. Así se refleja en el Informe de Comisión de Asuntos Jurídicos con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica [2015/2103(INL)]. En tanto, mientras esperamos a ver dónde nos lleva la evolución tecnológica, resulta oportuno y aconsejable continuar debatiendo sobre el tema: sólo el debate permitirá encontrar las mejores soluciones a los posibles problemas con los robots en la sanidad, pero también, quizás, a prevenir y evitar anticipadamente la llegada de estos problemas.

2. ESTADO DEL ARTE DE LA ROBÓTICA EN LA MEDICINA

Las nuevas (que ya no lo son tanto) tecnologías en el ámbito médico-sanitario nos ha cambiado el modo de ver la medicina: quizás tiene razón Capurro (2014) quien considera la medicina, entendida como ciencia y técnica terapéutica, como parte de la relación entre el hombre, el mundo y las tecnologías digitales. Hoy tiene sentido añadir a esta relación la inteligencia artificial y la robótica. Pero, al mismo tiempo, esta aplicación de las tecnologías de punta a la medicina ha generado diversos interrogantes en los ámbitos jurídicos, sociales, y filosóficos: cuanto más avanzamos tecnológicamente, más veces observamos que si bien gracias a estas tecnologías podemos solucionar un mayor número de problemas de salud y ayudar siempre a más gente, por el contrario, debemos ser conscientes que no todos podemos acceder a esta medicina avanzada: la ampliación de su acceso a todos los sectores de población es demasiado lenta y compleja, de forma que la tecnología por sí sola no cuenta y, por el contrario, que el factor humano y sobre todo el calor humano –la cual resulta imposible de recrear en la máquina o programar en el ordenador–, también tienen poderes curativos, quizás mayores que algunos medicamentos.

Uno de los avances tecnológicos de los últimos años es la inteligencia artificial y sobre todo la robótica que está revolucionando la medicina y todo el ámbito de los servicios médico-sanitarios: tenemos o estamos desarrollando (¡aun en este momento!) nuevas máquinas para tratar enfermedades, operar los cuerpos tanto desde fuera (cirugía externa o invasiva) como desde dentro (5), ayudar a los médicos y enfermeros a tener un mejor cuidado de los pacientes, y muchas más posibilidades, tantas e in-

(5) Hablando de la cirugía desde exterior, me refiero al robot cirujano tal vez más famoso, el robot *Da Vinci*, que ayuda a efectuar las operaciones cirujanas torácicas con la invasión mínima, mientras que hablando sobre la cirugía interior, me refiero al robot *Origami*, es decir, un robot en miniatura que una vez tragado puede arreglar las perforaciones causadas en el estómago

numerables son que tan realizar una simple enumeración de las mismas supondría un desafío tal que demandaría más espacio de lo que ocupa este escrito (6).

La verdad es que los robots están entrando en el sistema sanitario a todos los niveles: en las emergencias, en los ambulatorios, en la rehabilitación, en las salas operatorias, farmacias y en muchos otros lugares. Hay muchas clasificaciones y distintos modos de organizar estas enormes cantidades de robots para entenderlos: la clasificación que expongo a continuación es solo uno de los numerosos ejemplos que podemos encontrar en el mundo de la robótica médico-sanitaria: así podemos distinguir los ya mencionados (i) mínimamente invasivos aparatos de cirugía, (ii) aparatos diagnósticos, (iii) prótesis avanzadas (hablamos de seguida de un ejemplo de tal prótesis ósea: el exoesqueleto), (iv) aparatos de tele-presencia, (v) robots asistentes personales y (vi) aparatos para gestión de sanidad publica como, por ejemplo, los drones que ayudan a proporcionar servicios médicos en las áreas no accesibles o bien de difícil acceso (sobre ellos también vamos de hablar en seguida) (7).

Esta clasificación resalta una particularidad de la robótica médico-sanitaria que quizás no percibamos inmediatamente, y es que la robótica médico-sanitaria tiene que ser entendida en un sentido amplio y no en su sentido literal: por ejemplo, el robot que desinfecta un hospital no es en sentido estricto un robot médico, pero lo es en sentido amplio porque permite a los médicos no solo adoptar mejores cuidados a los pacientes, sino que también asegura que los pacientes puedan tener mejores curas (8). Tampoco un robot médico en este sentido estricto es:

> Tug es un robot que trabaja en un hospital pero no sabe nada de medicina. A lo mejor Tug se parece a un personaje de *Star Wars*, porque además de parecer físicamente a *R2-T2,* tiene una función muy importante: distribuir las medicinas, llevar sábanas limpias de cama y recoger las sucias, servir la comida, portar los instrumentos médicos, quitar la basura sanitaria, y hacer muchas otras cosas que ahora mismo en los hospitales las hacen los humanos. Así, mientras Tug hace todo esto, los enfermeros y el resto del personal

humano. Para más información sobre este robot, ver «http://news.mit.edu/2016/ingestible-origami-robot-0512)».

(6) El desarrollo de la medicina y de las nuevas tecnologías puede ser visto a través del desarrollo desde la medicina 1.0 (medicina sin antibióticos y rayos X) a la medicina 2.0 (con antibióticos y rayos X) y a la medicina 3.0 empoderada por robótica entre otras tecnologías para llegar a la medicina 4.0 definida por la combinación de microelectrónica y las tecnologías de punta (Wolf y Scholze 2017).

(7) Más sobre esa clasificación, ver *Addressing Regulatory Considerations for Medical Robotic Devices* (2017) de Underwriters Laboratories (UL), disponible en «https://library.ul.com/wp-content/uploads/sites/40/2017/08/BNG-UL17-Medical-Robots-White-Paper-080117-1.pdf».

(8) Es el caso del robot XENEX que desinfecta los hospitales de la infección nosocomial o intrahospitalaria las cuales causan cada año muchas muertes en nuestros hospitales y ambulatorios. Más sobre XENEX, ver «https://www.xenex.com».

médico-sanitario pueden dedicar más tiempo a los pacientes y Tug contribuye a una mayor eficacia y eficiencia (9).

El mismo discurso podemos aplicar a los robots asistenciales o a los drones-transportadores de medicamentos: desde el punto de vista estrictamente médico-jurídico no son herramientas medicas, pero lo son en el sentido más inclusivo adoptado en este escrito donde los robots son médicos si de alguna manera, directamente o indirectamente mejoran la salud, ayudan a solucionar los problemas médico-sanitarios y facilitan el proceso de curación.

Es verdad que no hay actualmente ninguna área de servicios de sanidad donde los robots no podrían ayudar, facilitar, soportar, acelerar los tiempos o mejorar la calidad de los servicios sanitarios: en efecto, encontramos la robótica y inteligencia artificial en las tecnologías con el gran potencial de «disruptar» la industria médica de EE. UU. en la próxima década (10), y quizás la europea también. La naturaleza de tal disrupción aun no resulta tan obvia y deja muchos interrogantes: mientras tanto nuestro papel es anticipar los problemas que pueden surgir.

Quizás, pensando en esta naturaleza posiblemente disruptiva, la Comisión de Asuntos Jurídicos en el ya mencionado informe [2015/2103(INL)] dedica una gran atención no solo a los robots médicos, sino también a los robots asistenciales y de rehabilitación e intervención en el cuerpo humano, a través de las prótesis robóticas y otras tecnologías. Parece que la robótica médica está siendo una cuestión urgente y los ciudadanos, los consumidores y los pacientes, todos ellos, queremos y necesitamos una mayor certidumbre por parte del legislador.

Antes de continuar hablando de los concretos desafíos y posibilidades de la robótica médico-sanitaria, en la siguiente sección voy a plantear brevemente el derecho a la salud como uno de los derechos humanos que va a verse aún más afectado por la robótica.

3. SANIDAD Y DERECHO A LA SALUD

El derecho a la salud o a su protección, como establece la Constitución española, es reconocido a todos los ciudadanos en casi todos los países del mundo. En este sentido, aunque con una redacción diferente, dicho derecho es contemplado en el artículo 35 de la Carta de los Derechos Fundamentales de la Unión Europea (2007/C303/01), donde podemos leer que el derecho a la protección de la salud es uno de los derechos humanos de

(9) Tug es un robot real producido por Aethon. Más sobre Tug, ver «http://www.aethon.com/tug/tughealthcare/».

(10) Por lo menos esta es la previsión de *Health Research Institute* di PwC (2016) en su informe sobre los asuntos de industria sanitaria.

carácter social: «toda persona tiene derecho a acceder a la prevención sanitaria y a beneficiarse de la atención sanitaria en las condiciones establecidas por las legislaciones y prácticas nacionales». Siempre en la misma línea hay muchísimos otros tratados internacionales que lo reconocen como la Constitución de la Organización Mundial de la Salud (OMS) (1946), Declaración Universal de Derechos Humanos (1948), y las constituciones de numerosos países democráticos.

Como ya hemos visto en la discusión efectuada hasta ahora, hay una tendencia natural a confundir el derecho a la asistencia sanitaria y el derecho a la salud, que no son la misma cosa ni tampoco el mismo derecho. Probablemente, el primero es parte fundamental del segundo, que incluye y está vinculado a su vez a otros derechos y libertades, así como a diversos factores tales como el desarrollo socioeconómico en general (lo que aclara muy bien entre muchos Navarro 1998, y Lema Añón 2010). La siguiente explicación es muy ilustrativa: «[…] el derecho a la salud exige el acceso universal e igualitario a la asistencia sanitaria […] pero al mismo tiempo, […] el derecho a la salud no es equivalente al acceso universal e igualitario a la asistencia sanitaria» (Lema Añón 2010, 201). Entonces, el derecho a la asistencia sanitaria es *conditio sine qua non* del derecho a la salud, pero no lo agota: desde este punto de vista, el derecho a la salud es mucho más amplio, incluyente y extendido.

Está claro que el derecho a la salud es y va a seguir siendo un derecho fundamental para el bienestar de las personas porque no podemos imaginar un estado del bienestar sin garantías de que, ante una concreta contingencia, no podamos contar con la asistencia sanitaria. Al mismo tiempo la inversión en el desarrollo de la tecnología médica de punta está creciendo y los propios médicos no siempre están seguros de que toda esta tecnología sea absolutamente beneficiosa para los pacientes: por ejemplo, Fred (2009) denomina la tendencia de los médicos hacia una total adición a la tecnología «el tenesmo tecnológico» describiéndolo como un ansia incontrolable de confiar los diagnósticos en los más recientes aparatos. Este mismo discurso se podría ampliar no solo a la diagnosis sino también a otros procedimientos o protocolos, de ahí que debamos ser conscientes de que la confianza en la tecnología tiene un cierto lado obscuro que hace a los médicos dudar en la toma de sus decisiones, depender totalmente de la tecnología, y perder sus capacidades y habilidades.

La pregunta que me planteo en este escrito, por el contrario, es distinta y más concreta, ya que son preguntas referidas no a la tecnología en general sino a una tecnología en particular: ¿los robots representan una ventaja o un peligro para nosotros? ¿La robótica puede asegurar que más personas podrán satisfacer su derecho a la salud y a la asistencia sanitaria? ¿Es posible que, paradójicamente, experimentemos un empeora-

miento en el ejercicio de este derecho? En lo que sigue de este escrito, voy a concentrarme en la próxima sección en la vertiente más prometedora de la robótica médico-sanitaria, mientras que en la sección 5 voy a analizar la robótica médico-sanitaria con un enfoque más crítico, subrayando los aspectos que podrían ser perjudiciales.

4. POSIBILIDADES OFRECIDAS POR LA ROBÓTICA MÉDICO-SANITARIA: ¿NOS VAN A TRAER ALGO BUENO LOS ROBOTS?

Si observamos el derecho a la salud desde la perspectiva del Derecho internacional de los derechos humanos, descubrimos cuatro parámetros que nos ayudan a establecer en qué estado se encuentra tal derecho en un país (*Fact Sheet 31* de OMU y de la Oficina del Alto Comisionado de Derechos Humanos de las Naciones Unidas; Lema Añón 2010). Estos parámetros son disponibilidad, accesibilidad, aceptabilidad y calidad. La pregunta que surge es la siguiente: si influye, y en el caso de respuesta positiva a esta primera pregunta, cómo influye la robótica en estos parámetros. En otras palabras, ¿puede tener la robótica un impacto positivo al garantizar el derecho a la salud? Además, si observamos el panorama creciente y extenso de las aplicaciones robóticas en el ámbito medico-sanitario a través de estos parámetros, podemos descubrir una metodología para una mejor comprensión de las posibilidades que ofrecen tales tecnologías, y evitar los riesgos que supone una incorrecta o incompleta compresión de las mismas.

4.1 **El parámetro de la disponibilidad**

En primer lugar, desde el parámetro de la disponibilidad de instalaciones, servicios y productos médicos dentro de un país, la robótica podría aportar muchas mejorías en este sentido: por ejemplo, actualmente el gobierno de Malawi está testando el dron para poder efectuar la diagnósis precoz de los niños afectados por VIH que se encuentran lejos de los centros médicos (11) (o bien a aquellos que no puedan para llegar a los mismos). El mismo problema, pero desde una óptica distinta, es el objeto perseguido por el proyecto europeo *Remote Medical Diagnostician* (ReMeDi) (12): no solo hay lugares de difícil acceso para la población, sino que aun en el caso de poder acceder, existe el riesgo de que no se encuentre en dicho lugar el médico por falta de personal u otras causas. Este sistema robótico es una de

(11) La noticia ha sido publicada por el Centro de Prensa de UNICEF del año 2016. Para más información sobre este dron, léase este enlace: «https://www.unicef.org/media/media_90462.html». Una de las empresas que está desarrollando los drones para transportes de medicinas, muestras de laboratorio y otro soporte médico-sanitario en las áreas poco accesibles es Matternet (mas sobre esta empresa, ver enlace «https://mttr.net/»).

(12) Más sobre REMEDI, ver enlace «http://www.remedi-project.eu».

las posibles soluciones a este problema: el robot sustituye al personal médico efectuando el examen físico y de ultrasonografía del paciente, informando de la situación al doctor que se encuentra en otro hospital.

4.2 **El parámetro de la accesibilidad**

El parámetro de la accesibilidad significa que las estructuras médico-sanitarias tienen que ser accesibles físicamente, financieramente, y sin discriminación ninguna. Para el problema de accesibilidad física, hay muchos ejemplos de exoesqueletos robóticos (13) que podrían marcar la diferencia para las personas con movilidad reducida. Pero el problema verdadero es la accesibilidad desde el punto de vista económico: los robots no son baratos, al contrario. No obstante, hay una esperanza en que el aumento de las ventas, difusión e incremento de la demanda de este producto conlleve la consiguiente bajada de precios, haciendo los robots más accesibles tanto a los individuos como a los hospitales, clínicas de rehabilitación, residencias de mayores u otros establecimientos médico-sanitarios (14).

4.3 **El parámetro de aceptabilidad**

La aceptabilidad requiere que las infraestructuras, productos y servicios respeten la ética médica, los aspectos de género y la cultura del país. Son requisitos demasiado complejos e invitan a muchas interpretaciones: sobre todo respecto a la ética médica que se ocupa de los problemas que hasta ahora nos hacen discutir sin encontrar una solución única en muchos casos. Son pocas las cuestiones referidas a la ética médica, como la protección de la privacidad, las que estamos transfiriendo al día de hoy con un cierto nivel de éxito en el mundo tecnológico (estamos hablando, en particular, de privacidad por diseño y por defecto).

Por lo que concierne a los robots y la consideración de la cuestión de género, actualmente parece que somos nosotros (los humanos) los que tenemos un comportamiento distinto con los robots varones y robots mujeres, y no al contrario. Parece que cuando estamos relacionándonos con los objetos, tenemos una necesidad de asignar un género a este objeto y el género que lo asignamos, condiciona nuestro comportamiento con el robot reforzando los estereotipos existentes contra los cuales estamos luchando (Nomura 2017).

---

(13) Por ejemplo, el sistema ReWalk, primer exoesqueleto aprobado por la *FDA* (Administración de Alimentos y Medicamentos Nord americana) que permite a las personas con los traumas a la médula espinal caminar, subir y bajar las escaleras, y hacer otros movimientos («http://www.rewalk.com/»).

(14) Según Coren (2017), los ingresos de los exoesqueletos en EE. UU. han subido desde menos de 100 millones de dólares en 2015 hasta casi 200 millones en el 2017. No tenemos ninguna causa para no esperar ulteriores subidas en los próximos años con consiguientes bajadas de precios.

La cuestión cultural es un ulterior desafío para la robótica, si bien la necesidad de tener en cuenta los aspectos culturales en el desarrollo tecnológico no es algo nuevo: Capurro (2014) por ejemplo, hablando de la sociedad de información, nos invita a «enculturar» (*enculture*) la técnica digital en distintas sociedades, adaptando en consecuencia las estructuras y servicios médicos. No tenemos que mirar muy lejos para ver esta realidad a través de la robótica medica: por ejemplo, los experimentos realizados han demostrado que los ciudadanos de EE. UU. tienen más confianza y se sienten más a gusto con un robot asistente que los ciudadanos chinos (Evers *et alii* 2008). Eso nos ayuda a entender que probablemente la robótica asistencial va a tener más éxito en EE. UU. que en este país asiático. Estas distinciones van a ser aún más evidentes en el ámbito médico-sanitario gracias a la globalización y movilidad de las personas.

4.4 **El parámetro de la calidad**

El último parámetro, la calidad, supone la cualificación adecuada del personal médico-sanitario, los medicamentos e instrumentos médicos aprobados e instalaciones sanitarias adecuadas. No podemos ignorar la importancia de este parámetro en el campo de la robótica médico-sanitaria: el ya mencionado exoesqueleto *ReWalk* no está disponible en España porque no hay personal que sepa manejarlo ni poder enseñar, a su vez, a los enfermos a utilizarlo. En otras palabras, aunque pudiéramos permitirnos adquirir un *ReWalk*, no tendríamos médicos ni enfermeros para ayudarnos a manejarlo con seguridad. Por eso el parámetro de la calidad puede mostrarnos cuán importante es el contexto –profesional, normativo, e institucional– para poder ejercer el derecho a la salud y a la asistencia sanitaria.

4.5 **Otras oportunidades**

Hablando de las posibilidades ofrecidas por la robótica médico-sanitaria, hay muchas cuestiones abiertas como por ejemplo, si tenemos derecho a elegir quien nos opera: ¿un robot cirujano o un cirujano humano? Si las estadísticas nos muestran que los robots cirujanos cometen menos errores, ¿tengo derecho a pedir que me opere el robot y no un ser humano? Porque los robots cirujanos no se cansan físicamente ni mentalmente, como tampoco tienen un día malo en el que todo se les cae de las manos (¡metafóricamente hablando, claro!) ni se afligen con las debilidades propias de los humanos como las dudas o las incertidumbres. Aún más: los robots pueden conocer y manejar más información que nosotros al no sufrir sobrecarga informativa la cual nos debilita desde el punto de vista cognitivo. Un ejemplo es el sistema inteligente *Watson* de *IBM* que acon-

seja a los médicos elegir la mejor estrategia del tratamiento, y a diferencia de los humanos, *Watson* tiene acceso y puede procesar tales cantidades de datos que los humanos nunca podremos procesar (15).

Además, hay situaciones en la vida, aunque raras y excepcionales, en las que los robots pueden dar solución a un problema no solo médico sino también ético:

> Jorge, paciente y testigo de Jehová, se encuentra con el dilema de no poder autorizar para que le hagan transfusión de sangre alguna, sea su propia sangre como de un tercero, porque su religión no lo permite. Los cirujanos han explicado a Jorge que la medida consistente en la transfusión de sangre es muy común en las operaciones invasivas, de forma que si Jorge no da permiso, puede haber riesgo de muerte. Jorge pregunta si su operación puede ser menos invasiva, pero en su caso –cáncer de próstata– la operación lo es. Jorge se informa más y descubre que hay un hospital donde los cirujanos utilizan los robots para este tipo de operaciones. Jorge solicita poder operarse allí, siendo operado con el sistema robótico Da Vinci que lleva a cabo la operación casi sin perder una gota de sangre de Jorge (16).

En este ejemplo vemos como los robots médicos ofrecen la posibilidad, a los cirujanos y a los pacientes, de encontrar una solución mejor para ambas partes, sin que ninguna de ellas tenga que ir contra sus convicciones y creencias, y además refuerza la idea de que quizás no se trata de la cuestión de quien es mejor médico, si el robot o el ser humano. Por el contrario, la respuesta más adecuada es que cada uno de ellos tiene sus puntos fuertes, si bien lo mejor de ambos lo vemos cuando robot y humano trabajan juntos.

5. LOS RIESGOS CAUSADOS POR LA ROBÓTICA MÉDICO-SANITARIA: ¿QUÉ ARRIESGAMOS?

Una vez visto el elemento positivo que los robots podrían aportar al sector médico-sanitario, vamos a ver la otra cara de la moneda e intentar entender cuáles pueden ser los riesgos existentes para las personas humanas desde la robotización del sector de sanidad.

Antes de entrar en algunos riesgos específicos para el área de la sanidad, hay siempre la certidumbre (ya no es riesgo sino certidumbre) de que la robótica médico-sanitaria antes de ser para todos, va a ser para unos pocos elegidos que van a poder permitírsela. Así sucede ya con los medicamentos más avanzados, con los cuidados más sofisticados, con las

(15) Últimamente Watson ha causado mucha desilusión y criticas (ver por ejemplo, Ross y Swetlitz 2017) pero tampoco le faltan seguidores, como por ejemplo, Johnson 2017.

(16) Este ejemplo es inspirado en un caso real de hospital *St. Joseph's Healthcare* en Hamilton (Canadá) (Kent 2017).

técnicas cirujanas más innovadoras, y no hay porque pensar que va a ser distinto con la robótica médica más revolucionaria.

Sin ninguna duda, y como ya he apuntado en la introducción, uno de los riesgos más discutidos en relación a la automatización, la robótica y la inteligencia artificial es la de la pérdida de trabajo, y en nuestro caso, la pérdida de trabajo de gran responsabilidad, calificación y dificultad como el del cirujano o del médico en general, así como el del enfermero que, aún no es calificado al mismo nivel que el cirujano, aunque tiene una importancia enorme para la curación y bienestar de los pacientes. Desde esta óptica, ¿qué tal la relación médico/enfermero-paciente? ¿Somos nuestro cuerpo, que cada vez es más una colección de datos que se debe digitalizar, como dice Capurro (2014), o somos algo más y este algo más necesita interaccionar con otros humanos, sobre todo en las situaciones de vulnerabilidad extrema como las que concierne a nuestra salud? ¿Curar es saber leer correctamente los síntomas del cuerpo o también saber entender el alma? ¿Los robots son capaces de hacerlo? Parece que aún no, ni tampoco es algo factible para el actual nivel de desarrollo tecnológico, pero ¿y el día de mañana? Actualmente se habla mucho de aislamiento y soledad causadas o soportadas por la tecnología: ¿los robots van a contribuir a aumentar estos fenómenos?

Tengamos en cuenta aún otra cosa: como ya hemos observado en el principio de este escrito, el robot médico-sanitario es algo más que solo un robot con una función medica predefinida, y es que los robots médico-sanitarios también tienen una función no tan médica, como distribuir la ropa de la cama o desinfectar los espacios hospitalarios. Siguiendo este razonamiento, la robótica va a eliminar no solo el trabajo cualificado, sino también el trabajo sencillo y no cualificado: ¿estamos ante el riesgo de dejar de ser animales que utilizan las herramientas activamente para pasar a ser animales pasivos, esclavos de las maquinas (Mumford 1966)?

5.1 **Los riesgos conectados con el parámetro de accesibilidad: discriminación y privacidad**

Dejando aparte el riesgo general de deshumanizar la sanidad, recordemos uno de los parámetros expuestos en sección anterior, en particular el parámetro de accesibilidad a la sanidad. Hemos visto que uno de sus aspectos es entenderlo como accesibilidad sin discriminación alguna, o sea los robots tienen que comportarse e interaccionar de la misma manera con todas las personas, sean estas personas hombres, mujeres, niños, personas con discapacidades físicas o intelectuales, de cualquier raza, religión, creencias, etc. Pero lo cierto es que hemos constatado cómo un sistema inteligente utilizado para predecir los crímenes resulta ser racista al sugerir que el color de piel nos hace más o menos inclines a violar la

ley (17) u otros ejemplos de los programas inteligentes que claramente han reflejado no sus sino nuestros prejuicios y estereotipos. El problema es que no solo expresamos nuestros prejuicios, sino que también los estamos programando en los robots y otros sistemas inteligentes, como si el prejuicio transferido en lenguaje de programación dejara de ser una práctica ilegal, inmoral e inaceptable. Resulta notorio que ello supone un impacto muy importante en el ámbito medico-sanitario donde somos todos iguales ante la enfermedad, muerte y sufrimiento.

Volviendo al parámetro de accesibilidad, dicho parámetro establece que tenemos el derecho a buscar, recibir e impartir la información médica a todos, y también al mismo tiempo, exigir que los datos personales sean tratados con confidencialidad. En este sentido, la robótica médico-sanitaria aporta unos riesgos enormes: estamos hablando no solo de nuestros datos personales accesibles para los robots (y las personas que los manejan, lo han desarrollado, lo actualizan, etc.), sino también de los datos personales sensibles, es decir, los datos con mayor protección y más importantes para cada uno de nosotros.

Y en este sentido, estamos solo hablando de la gente que de una u otra manera tienen acceso legítimo al robot: ¿qué decir de los *hackers* y el riesgo cierto y real de que entren en «la mente» de robot para tener acceso a lo que «sabe» («datos») la máquina?

Como si esto no fuera ya suficientemente grave, debemos entender que los robots médico-sanitarios van a tener acceso a una gran cantidad información personal no de una sola persona, sino de muchas personas y colectivos (por ejemplo, todas las personas de una planta o sección específica de un hospital). En este sentido no resulta errónea la posible visión del robot como un depósito ambulante de datos personales sensibles.

Además, el nuevo Reglamento General de Protección de Datos (Reglamento 2016/679) introduce el derecho a la portabilidad de los datos, que en el sentido de este escrito, se trata en la mayoría de los casos de datos personales sensibles pero no solo. Por ejemplo, tenemos que garantizar a los pacientes cuidados por robots, el poder pedir al hospital u otra institución médica o médico-comercial –que tiene el robot en propiedad o en alquiler, etc.– la protección de los datos que el paciente mismo ha cedido y los robots han recogido observando y atendiendo al citado paciente. Es una cuestión que interesa no solo a los robots: lo importante es que la interoperabilidad y estándar compartidos entre los distintos sistemas que

(17) Estamos hablando de un sistema utilizado en EE. UU. y producido por *Northpointe*. La investigación hecha por organización sin ánimo de lucro *ProPublica* ha evidenciado que, según el sistema, las personas de piel blanca tenían más posibilidades de obtener un bajo marcador de cometer un crimen y después violar la ley, mientras la gente de piel negra obtenían este marcador alto, pero cometían menos crímenes en la vida real de lo que predecía el sistema. Para saber más, ver «http://www.businessinsider.com/software-that-predicts-criminal-behavior-could-be-biased-2016-5».

procesan los datos –sean estos sistemas robóticos o no– es algo que podría no solo contribuir a promover la cultura de protección de datos, sino que también dar un impulso positivo a la competitividad entre empresas.

6. CONCLUSIONES

La considerable cantidad de robots utilizados en el sector sanitario, y que cada vez con mayor frecuencia sustituyen a los operadores sanitarios humanos (desde el cirujano hasta la enfermera, desde la persona que nos recibe a la entrada en hospital hasta el fisioterapista que nos asiste después de una operación) nos hace preguntarnos como queremos que sea la sanidad del siglo XXI y qué papel juega el factor humano en los servicios sanitarios. Lo cierto es que los robots no pueden responder a todos los problemas de la sanidad que tenemos hoy en día, ya porque el mayor problema de la sanidad no es de carácter tecnológico, de recursos o de financiación. El mayor problema es la falta de igualdad social, el bajo nivel de calidad de vida, y, entre muchas otras cosas, las dificultades para acceder a los bienes comunes, o bienes de la colectividad como agua potable, aire limpio (y de calidad), y la información crítica (Mattei 2013). En este paisaje, y a pesar de los medios que tenemos, «[…] el abismo entre el derecho proclamado [derecho a la salud] y los hechos es seguramente uno de los más amplios que podemos encontrar en el catálogo de derechos humanos» (Lema Añón 2010, 62): guardamos la esperanza de que los robots nos ayudarán a reducirlo.

XII

RELACIONES INTERNACIONALES Y MUNDO DIGITAL

CAPÍTULO 42

LAS RELACIONES INTERNACIONALES EN EL MUNDO DIGITAL

SANTIAGO RIPOL CARULLA
Catedrático de Derecho internacional público. Universidad Pompeu Fabra

1. ESTADO Y SOBERANÍA, EL MARCO TEÓRICO TRADICIONAL DE LAS RELACIONES INTERNACIONALES

Tradicionalmente, las Relaciones internacionales –entendidas como el juego de los actores en el sistema internacional– han tenido como sujeto principal al Estado-Nación y a la soberanía como concepto teórico funda-

mental. Podría afirmarse que así ha sido desde que en 1513 N. Maquiavelo empleara por primera vez el término Estado en la primera frase de su obra *El Príncipe*.

Sin duda, el Estado, como forma de organización de las sociedades políticas, es el actor que mayor número de prerrogativas y de funciones desempeña a nivel internacional. Con razón, por lo tanto, ha dicho M. Merle que es «el actor privilegiado de la vida internacional» (1). En efecto, una rápida ojeada a los acontecimientos que jalonan las relaciones internacionales –intercambios comerciales, acciones diplomáticas, hechos militares, decisiones políticas...– permite apreciar con facilidad que el Estado participa directa o indirectamente en todas ellas: en unos casos como sujeto activo, esto es, realizando o absteniéndose de realizar una acción concreta; en otras como sujeto pasivo, es decir, como destinatario de esas mismas acciones.

Por otra parte, la soberanía o independencia, como atributo de la autoridad suprema del poder estatal, es el rasgo definitorio del Estado como actor internacional. La soberanía o *suprema potestas* significa que un Estado no está sometido a la autoridad de ningún otro Estado o grupo de Estados e implica el derecho del Estado a ejercer en su territorio y sobre su población las funciones estatales con exclusión de cualquier otro Estado. Desde este punto de vista la noción de soberanía se define por su contenido: un conjunto de competencias territoriales y personales que corresponde desarrollar en exclusiva a los Estados.

Pero este doble eje Estado/soberanía parece haberse truncado a raíz de los importantes cambios vividos durante los últimos años en la Comunidad internacional.

2. CAMBIOS EN LA COMUNIDAD INTERNACIONAL

2.1 **Profundización en los avances científicos y técnicos**

Por una parte, se ha producido una profundización en los avances científicos y técnicos. En rigor, el desarrollo científico y técnico no es un aspecto novedoso en sí mismo; tal desarrollo está en la naturaleza misma de la ciencia y de la técnica. Sí es novedoso y remarcable, en cambio, la rapidez y la profundidad de estos avances, y el marcado carácter ambivalente con el que se presenta actualmente el progreso tecnológico.

En conexión con este extremo se halla la noción de sociedad del riesgo, desarrollada por el sociólogo alemán Ulrich Bech quien, en 1986, coincidiendo con el accidente de la central nuclear de Chernóbil, publicó una

(1) Merle, M., *Sociología de las relaciones internacionales*, Alianza Editorial, Madrid, 2000 (3.ª ed.), p. 165.

obra llamada a ejercer una gran influencia. El libro, titulado *La sociedad del riesgo. Hacia una nueva modernidad* (1998), parte de la constatación de que en las sociedades más industrializadas ha sido posible «reducir objetivamente y excluir socialmente la miseria material auténtica». Pero en la medida que esta superación de la cuestión del reparto de la riqueza se ha producido mediante el recurso a la tecnología, las sociedades posindustriales han debido enfrentarse a una nueva cuestión acaso más acuciante que la anterior: el reparto de los riesgos, de los efectos secundarios provocados por un recurso masivo a la tecnología.

A diferencia de los peligros que debía afrontar la sociedad industrial, los riesgos a los que ahora debe hacerse frente se caracterizan por su dimensión universal, por su gran complejidad científica y tecnológica que dificulta enormemente la determinación de sus causas, por la producción de «daños sistemáticos y a menudo irreversibles que suelen permanecer invisibles» y, como consecuencia de todo lo anterior, porque la definición, medición y gestión del riesgo es una tarea que, en la medida que interesa a todos, corresponde al poder político, el cual se ve compelido con frecuencia a decidir sobre muy complejas cuestiones técnicas, que le obligan a recurrir de nuevo a las valoraciones de quienes poseen el saber científico que ha hecho posible la tecnología que inicialmente generó los riesgos sobre los que debe decidirse.

El desarrollo científico y técnico ha generado nuevos elementos de solidaridad internacional en la medida que se han evidenciado los negativos efectos potenciales que dicho desarrollo puede tener sobre la sociedad. Esta circunstancia ha provocado, por ejemplo, la aparición del derecho internacional del medio ambiente.

En otro orden de cosas, el desarrollo y la consolidación de internet han superado cualquier expectativa de cambio y de progreso que pudiera haberse hecho hace 10 años sobre la sociedad tecnológica. El derecho (también el derecho internacional) se ve afectado intensamente por el fenómeno internet que, en sí mismo, supuso un nuevo reto, entre otras cosas porque nació como una realidad ajena a las fronteras estatales y al margen de la ley (2).

2.2 **Mundialización económica, globalización y crisis financiera de carácter global**

La mundialización económica es el segundo gran cambio vivido en la comunidad internacional de finales del siglo XX y principios del siglo XXI. En cierto modo se trata de una circunstancia que resulta también de la

(2) TSAGOURIAS, N.; BUCHAN, R., *Research handbook on IL and Cyberspace*, Edward Elgar Publishing, Cheltenham, UK; Northampton, MA, USA, 2015.

revolución científica y tecnológica pues esta (junto a otros factores) ha permitido que la unificación del espacio económico mundial sea, hoy por hoy, un hecho.

El modelo de crecimiento capitalista seguido desde el final de la Segunda Guerra Mundial mostró sus límites a consecuencia de la crisis del petróleo de 1973 y 1979. La incapacidad para gestionar tal crisis llevó a los gobiernos a emprender un proceso de desregulación de los mercados, mediante el cual pretendían afianzar el peso relativo de sus economías frente a la de los otros Estados. Esta dinámica de desregulación, liberalización y privatizaciones, propia de los años ochenta, fue hábilmente aprovechada por las empresas (principalmente por las empresas relacionadas con las tecnologías de la información y los mercados financieros) que, mediante aquellas medidas, vieron una potencial ampliación de sus mercados. Finalmente, la caída del muro de Berlín y la consiguiente incorporación de los países de Europa central y oriental al sistema de economía capitalista, terminó por cuajar el salto de una economía internacionalizada a una economía mundial. Tras Europa central y oriental han entrado en la onda globalizadora las naciones de la antigua Unión Soviética, los países emergentes del sudeste asiático o América Latina, India y China.

En esta economía globalizada, «la producción, el consumo, la circulación, así como sus componentes (capital, mano de obra, materias primas, gestión, información, tecnología, mercados) están organizados a escala global, bien de forma directa, bien mediante una red de vínculos entre los agentes económicos». Pero la globalización, cuyo motor han sido los procesos económicos, ya no es un fenómeno exclusivamente económico puesto que tiene consecuencias sobre todos los ámbitos de las relaciones sociales, las cuales han resultado también globalizadas (3).

La globalización alcanzó su cénit en 1997, año en que se produjo la crisis asiática iniciada en Tailandia en ese mismo año y que se extendió durante 1998 a Corea, Indonesia e incluso a Japón y a Rusia, que en 1998 no pudo hacer frente al pago de su deuda. Esta crisis puso en evidencia que la globalización no garantizaba por sí misma la estabilidad económica ni bastaba para erradicar la pobreza, de la que en ocasiones (como ocurrió en Rusia), se hizo portadora, generalizando así una sensación de malestar respecto de la globalización y sus manifestaciones.

Pero el problema de mayor envergadura que ha acompañado a la globalización ha sido su gestión (4), de la que la crisis financiera y económica internacional iniciada en 2008 es muestra.

---

(3) García Segura C., «La globalización en la sociedad internacional contemporánea: dimensiones y problemas desde la perspectiva de las relaciones internacionales», *Curso de derecho internacional de Vitoria/Gasteiz, 1998*, Tecnos / UPV, Madrid, 1999, pp. 315-350.

(4) En las manos de quienes sostienen una visión concreta de la economía –el fundamentalismo de mercado, según expresión de G. Soros– sobre todas las demás visiones. Lo escribió E. Stiglitz,

Enfrentados a la misma, los gobiernos nacionales, incapaces de ofrecer una respuesta individual, recurrieron desde los primeros compases de la crisis a mecanismos de concertación internacional (G-20), así como a las organizaciones internacionales [Fondo Monetario Internacional (FMI) y Unión Europea].

2.3 **La proliferación de los actores de la comunidad internacional**

Esta última constatación conduce ya a dar una primera respuesta al primero de los interrogantes formulados: el Estado no es ya el actor privilegiado que tradicionalmente ha sido; otros actores comparten con él un destacado protagonismo. Pongamos algunos ejemplos.

En el marco de la lucha contra el terrorismo internacional de carácter global, el Consejo de Seguridad ha adoptado sanciones dirigidas expresamente a Daesh (Estado Islámico), Al-Qaida y las personas, grupos, empresas y entidades asociadas con ellos. En efecto, algunas resoluciones del Consejo de Seguridad imponen a los Estados la obligación de: 1) Congelar los fondos y otros activos financieros o recursos económicos de las personas y entidades designadas en las resoluciones. 2) Impedir la entrada en su territorio o el tránsito por él de las personas designadas. 3) Impedir el suministro, la venta y la transferencia en forma directa o indirecta, desde su territorio o por sus nacionales fuera de su territorio, o utilizando buques o aeronaves de su pabellón, armamento y material conexo de todo tipo, piezas de repuesto y el suministro de asesoramiento técnico, asistencia o adiestramiento relacionados con actividades militares a las personas y entidades designadas.

En la página web del Grupo del Banco Mundial puede encontrarse la ventana *El Banco Mundial y la sociedad civil*, que, entre otros aspectos, constata la importancia de lo que denomina Organizaciones de la Sociedad Civil (OSC), «una gran variedad de instancias: grupos comunitarios, ONG, sindicatos, grupos indígenas, instituciones de caridad, organizaciones religiosas, asociaciones profesionales y fundaciones». El Banco Mundial reconoce que las OSC se han convertido en importantes canales de prestación de servicios sociales que complementan la acción gubernamental y destaca también su «influencia en cuanto a la formulación de políticas públicas a nivel mundial». De ahí su interés por establecer canales de cooperación con las OSC. También la ONU recurre a este mismo concepto de sociedad civil.

---

premio Nobel de Economía en 2001 y antiguo vicepresidente senior del Banco Mundial: «En muchos lugares del mundo la oposición no es a la globalización *per se* (…) sino al conjunto particular de doctrinas, las políticas del consenso de Washington, que han impuesto las instituciones financieras internacionales» (Stiglitz, J. E., *El malestar de la globalización*, Taurus, Madrid, 2002).

El «World Court Project» es un ejemplo de esta influencia. El 15 de diciembre de 1994, la Asamblea General de la ONU aprobó la Resolución 49/75 K, mediante la que solicitó de la Corte Internacional de Justicia (CIJ) que emitiera una opinión consultiva sobre la siguiente cuestión: «¿autoriza el derecho internacional en alguna circunstancia la amenaza o el empleo de las armas nucleares?» (CIJ. Opinión consultiva sobre la legalidad de la amenaza o el empleo de armas nucleares, 8 de julio de 1996). Pues bien, en la opinión separada que el juez G. Guillaume formuló a la opinión consultiva finalmente adoptada por la Corte, puede leerse que la aprobación de la Resolución 49/75 K tuvo «su origen en una iniciativa de una asociación llamada International Association of Lawyers Against Nuclear Arms (IALANA) que, de consuno con otras agrupaciones, emprendió en 1992, un proyecto titulado «World Court Project» encaminado a que la Corte proclamara la ilicitud del empleo o la amenaza del empleo de las armas nucleares». «Estas asociaciones –continúa G. Guillaume– desplegaron intensa actividad para que se sometieran a votación las resoluciones por las que se pedía la opinión de la Corte y hacer que comparecieran ante esta los Estados hostiles a las armas nucleares», e hicieron llegar su presión hasta los magistrados de la Corte por vía de millones de cartas en las que se hacía «un llamamiento tanto a su conciencia como a la conciencia pública» (epígrafe 2. Véase también la opinión disidente del magistrado Oda: párrafos 6-14).

Del mismo modo, la globalización ha supuesto un incremento del peso de las empresas multinacionales en la vida internacional; incremento que ha sido expresamente reconocido por el consejo de administración de la Oficina Internacional del Trabajo que en 2006 adoptó la *Declaración tripartita de principios sobre las empresas multinacionales y la política social* (que enmendaba dos Declaraciones sobre el tema adoptadas en 1977 y 2000) (5).

(5) Según esta Declaración «las empresas multinacionales desempeñan un papel muy importante en las economías de la mayor parte de los países y en las relaciones económicas internacionales, que es de interés creciente para los gobiernos, así como para los empleadores, los trabajadores y sus respectivas organizaciones. Mediante las inversiones directas internacionales y otros medios, estas empresas pueden aportar ventajas sustanciales al país de acogida y los países de origen, contribuyendo a una utilización más eficaz del capital, la tecnología y el trabajo. En el marco de las políticas de desarrollo establecidas por los gobiernos, pueden aportar también una contribución muy importante a la promoción del bienestar económico y social; a la mejora del nivel de vida y la satisfacción de las necesidades básicas; a la creación de oportunidades de empleo, tanto directa como indirectamente; y a la promoción de los derechos humanos básicos, incluida la libertad sindical, en todo el mundo. Por otra parte, los progresos realizados por las empresas multinacionales en la organización de sus operaciones que trascienden el marco nacional pueden dar lugar a una concentración abusiva de poder económico y a conflictos con los objetivos de la política nacional y los intereses de los trabajadores. La complejidad de estas empresas y la dificultad de percibir claramente sus estructuras, operaciones y planes son también motivo de preocupación en el país de acogida, en el país de origen o en ambos».

Sirvan estos ejemplos para poner de manifiesto la importante presencia de actores distintos al Estado en la comunidad internacional contemporánea (6). Según se ha podido apreciar, las instituciones internacionales reconocen la progresiva incorporación de estos actores a la vida internacional, constatan su importancia como detonantes de los procesos políticos internacionales, y aprueban declaraciones y normas que les tienen como destinatarios.

3. DEFINIENDO LA ESTRUCTURA DE LA GOBERNANZA DEL MUNDO DIGITAL

3.1 **El reto de la globalización: la incorporación de la sociedad civil a los procesos de creación y aplicación del derecho internacional**

En efecto, las organizaciones internacionales han permitido resolver otra de las grandes cuestiones a las que se enfrenta el derecho internacional en la era de la globalización: la incorporación de la sociedad civil a los procesos de creación y aplicación del derecho internacional (7).

K. Anan lo planteó como un reto. Para el antiguo secretario general de la ONU es imprescindible fortalecer los vínculos entre las ONG y otros agentes de la sociedad civil, por una parte, y las Naciones Unidas, por otra,

(6) Sobre esta cuestión han teorizado, entre otros muchos autores, S. Strange y D. Held. Mientras la primera pone el acento en el hecho de que el Estado debe compartir espacio económico y financiero internacional con estos nuevos actores (*La retirada del Estado*, Intermon-Oxfam-Icaria, Barcelona, 2001), el segundo percibe la ocasión para vertebrar un «marco de instituciones y procedimientos democráticos en el sistema internacional» (*La democracia y el orden global: del Estado moderno al gobierno cosmopolita*, Paidós, Barcelona, 1997, p. 317).

Y, sin embargo, en la Teoría de las Relaciones internacionales y del Derecho internacional, esta presencia de actores distintos al Estado en la comunidad internacional no tiene todavía el debido reflejo. Como ha puesto de manifiesto Ph. Alston, suele agruparse a estos actores bajo el término «actores no estatales». Al hacerlo así, se refuerza la idea de que el Estado no es sólo el actor principal, sino el actor indispensable y central alrededor del que pivota la vida internacional. Haciendo uso de una imagen muy potente (el síndrome del «no es un gato»: al igual que su hija de 18 meses cuando comenzaba a hablar se refería a todo animal que no fuera un gato como un no gato), Alston denuncia la limitación que implica agrupar todos estos actores bajo el término «actores no estatales» (Alston, Ph., «*The "Not-a-Cat" Syndrome*: Can the International Human Rights Regime Accommodate *Non*-State Actors?», en Alston, Ph. (Ed.), *Non-State-Actors and Human Rights*, Oxford University Press, Oxford, 2005, pp. 15-20).

(7) En este orden de cosas es obligado mencionar que autores tan significados como D. Kennedy, profesor de Derecho internacional de la Universidad de Harvard y presidente del Consejo asesor del Foro de Davos, consideran que una caracterización de la comunidad internacional centrada en las actuaciones públicas de los Estados no se corresponde ya con la realidad, en la que el poder privado ocupa áreas de influencia y de poder muy relevantes. En su obra *A World of Struggle: How Power, Law, and Expertise Shape Global Political Economy* (Princeton University Press, Oxford, 2016) reclama que el Derecho internacional incorpore a la gobernanza mundial la experiencia de los expertos (abogados internacionalistas, abogados de derechos humanos, asesores jurídicos de los ejércitos, profesionales de la política, especialistas en desarrollo económico…) que diariamente prestan su consejo a las instituciones privadas.

y a tal fin propuso a los Estados diversas medidas de reforma institucional que permitan la actuación tripartita ONU-Gobiernos-sociedad civil (8).

Es claro que una comunidad internacional más plural precisa de un derecho internacional abierto a todos. Los actores de la vida internacional (Estados, organizaciones internacionales, ONG, empresas transnacionales, minorías, pueblos, individuos) son destinatarios de las normas jurídicas internacionales, de ahí que la eficacia de las mismas pase por haber atendido a dichos actores en el momento de su elaboración. Y también por atenderles en la fase de aplicación del derecho internacional.

Son interesantes en este sentido las Comisiones de Estudio creadas en la Unión Internacional de Telecomunicaciones (UIT) para que las organizaciones y administraciones de telecomunicaciones y TIC (Tecnología de la Información y de la Comunicación) de todo el mundo le asistan en la preparación de las bases técnicas para las Conferencias de Radiocomunicaciones y en la elaboración de Recomendaciones UIT-R (normas de radiocomunicaciones) e Informes y la recopilación de manuales de radiocomunicación. Asimismo, la UIT ha desarrollado un mecanismo de participación directa de los «fabricantes y operadores del mundo hasta los pequeños actores innovadores que trabajan con las tecnologías nuevas y emergentes, pasando por las principales instituciones de I+D (Investigación y Desarrollo) e instituciones académicas» en la aprobación de sus normas de armonización técnica. Es el llamado proceso de aprobación alternativo, caracterizado por la brevedad del tiempo invertido (entre el 80 y el 90 % más rápido) y porque puede iniciarse a partir de la presentación de una propuesta de reglamentación por los referidos fabricantes, operadores y expertos.

En el ámbito de la aplicación del derecho es reseñable el rol asumido por el Órgano de Solución de Diferencias de la Organización Mundial de la Propiedad Industrial (OMPI) respecto de las controversias en materia de nombres de dominio en internet. La Corporación para la Asignación de Nombres y Números en Internet, más conocida por sus siglas en inglés ICANN (Internet Corporation for Assigned Names and Numbers) es una entidad regida por el derecho de California sin ánimo de lucro responsable de la coordinación global del sistema de identificadores únicos de internet y de su funcionamiento estable y seguro. El 24 de octubre de 1999 aprobó la Política uniforme para la resolución de conflictos en materia de nombres

(8) *Renovación de las Naciones Unidas. Un programa de reforma.* Informe del secretario general, Doc. A/51/1950, de 14 de julio de 1997, párrafos 207-216. El secretario general presentó un proyecto similar a la sociedad económica mundial del Banco Mundial (al que se ha hecho referencia). El proyecto, conocido como el Pacto Mundial, fue presentado en enero de 1999 ante el Foro de Davos como un esfuerzo por comprometer a las grandes empresas internacionales y a los directivos de las principales organizaciones laborales en la asunción de nueve principios relativos a la defensa de los derechos humanos, de los derechos colectivos de los trabajadores y de la protección medioambiental.

de dominio, que establece el marco jurídico para la solución de controversias existentes entre el titular de un nombre de dominio y un tercero (es decir, entre dos particulares) por el registro y utilización abusivos de un nombre de dominio de internet en los dominios genéricos de nivel superior o gTLD (por ejemplo, .biz, .com, .info, .mobi, .name, .net, .org). El ICANN adoptó esta Política basándose en un informe preparado por el Centro de Arbitraje y Mediación de la OMPI (Centro de la OMPI) que actualmente actúa como órgano de resolución de controversias en esta materia.

3.2 **La imposible gobernanza unitaria de la red**

Sin embargo, no ha resultado posible que la gobernanza de la infraestructura técnica de la red pasara a ser responsabilidad de la UIT, en detrimento de ICANN. El enfrentamiento sobre esta cuestión entre la UIT e ICANN y entre los Estados es importante y halla reflejo en las ratificaciones recibidas por el Reglamento de las Telecomunicaciones Internacionales que la UIT actualizó en 2012 –mientras que Brasil, Rusia, India, China y Sudáfrica (BRICS) sí lo han firmado, Estados Unidos, Canadá, Japón y los países de Europa, no lo han hecho–, y en el texto de la Resolución 101 (REV. BUSAN, 2014) *Internet Protocol-based networks*. A falta de una organización internacional que regule las cuestiones de política pública internacional relacionadas con Internet y la gestión de recursos esenciales de Internet, disponemos por el momento, del Foro para la Gobernanza de Internet –«un espacio abierto y descentralizado para el debate sobre políticas que favorecen la sostenibilidad y solidez de Internet que reúne a los gobiernos, sector privado, comunidad técnica, academia y sociedad civil»– que la ONU contribuyó a crear.

Ante la inexistencia de una organización internacional universal reconocida por todos los Estados como responsable de la regulación de la sociedad digital, cobra importancia la tarea que en este ámbito viene desarrollando la Unión Europea.

En la UE, la regulación de la economía digital se plantea expresamente en términos de mercado y de crecimiento, como una oportunidad para relanzar la economía de la UE (9) –la economía digital «crece siete veces más deprisa que el resto de la economía»– y los Estados miembros «van a la zaga de otros países en cuanto a redes digitales veloces, fiables y conectadas, que sustenten nuestras economías y estén presentes en cada momento de nuestra vida privada y profesional. A la hora de comunicarse entre países, los ciudadanos europeos se encuentran hoy en día con costes diferentes, sistemas incompatibles y una conectividad irregular en

(9) Así, el folleto explicativo de la *Agenda digital para Europa* (de la serie Comprender las políticas de la Unión Europea) lleva el siguiente subtítulo: Relanzar la economía europea (2014).

todo el continente. Esto perjudica a todos los ciudadanos, empresas e innovadores de Europa» (10).

Es preciso, por lo tanto, construir un mercado único digital, siguiendo el modelo normativo europeo –basado, entre otros principios, en la privacidad y la neutralidad de la red– que hagan de la UE un firme punto de referencia para muchos fuera de Europa, «que ven que es necesario un marco jurídico estable y previsible para abordar las complejidades de la economía y la sociedad digitales» (11). El 6 de mayo de 2015, la Comisión lanzó la *Estrategia para un mercado único digital* (12), que presenta dieciséis acciones específicas que conllevan el compromiso de hacer inversiones sustanciales en infraestructuras y que, en el campo jurídico, comprenden la revisión de la normativa para la protección de los consumidores, el derecho de la propiedad intelectual, las normas sobre telecomunicaciones, el marco de la comunicación audiovisual y sobre protección de los datos personales… (13).

4. EL PODER DE LOS ESTADOS EN EL MUNDO DIGITAL

4.1 **Diplomacia digital y diplomacia pública**

En otro orden de cosas, los Estados y las Organizaciones internacionales tratan de adaptarse a la nueva realidad del mundo. Como indica el Ministerio de Asuntos Exteriores y de Cooperación de España, junto a los «tradicionales instrumentos diplomáticos como el intercambio de visitas, los contactos políticos bilaterales o las reuniones multilaterales», la política exterior española debe recurrir a otros de carácter transversal, ligados a la nueva realidad de las relaciones internacionales, por lo que aportan un valor añadido adicional. La Estrategia de Acción Exterior 2015-2018 se refiere como nuevos instrumentos a la diplomacia digital y la diplomacia pública (14).

La primera consiste simplemente en el recurso a internet y a las tecnologías de la información para comunicar los contenidos de la política exterior española, «haciendo pública nuestra valoración de actuaciones internacionales que así lo merezcan; dar una ágil respuesta que facilite a

(10) *Ibid.*

(11) Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: *Revisión intermedia de la aplicación de la estrategia para el mercado único digital. Un mercado único digital conectado para todos*, COM(2017) 228 final, 10 de mayo de 2017.

(12) Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: *Una Estrategia para el Mercado Único Digital de Europa* [COM(2015) 192 final].

(13) *Revisión intermedia…*, *op.cit*

(14) Ministerio de Asuntos Exteriores y de Cooperación, *Estrategia de acción exterior*, febrero de 2015, Apartado 8: Instrumentos, pp. 132 y ss.

nuestros socios y aliados saber en qué asuntos nos posicionamos públicamente y cuál es el contenido de esa posición; y proporcionar una información extensa y detallada a los ciudadanos que la precisen sobre temas diversos que atañen a su vida profesional o seguridad en sus viajes». La diplomacia digital –añade– «entraña grandes oportunidades de influencia, permite hablar directamente y con mayor frecuencia con amplias audiencias, escuchar opiniones, sugerencias y recibir información que antes no estaba al alcance de los responsables de la política exterior» (15). Finalmente, a través de la diplomacia digital se ofrece una mejor atención al ciudadano (16).

Se puso en marcha, así, el Plan de Diplomacia Digital, del que el MAEC destaca los tres aspectos siguientes: 1) El despliegue de la Diplomacia Digital en redes sociales «se ha articulado en torno a un esquema de 28 hubs, subregionales, multilaterales y por idioma (17); y la presencia de todas las Embajadas y Consulados en, al menos, una red social (…) Actualmente, el Ministerio de Asuntos Exteriores y de Cooperación está presente en Twitter, con dos cuentas una en español @MAECgob y otra en inglés @SpainMFA, en Facebook, en Youtube y en Instagram. A esta presencia, se une también la de nuestras Embajadas y Consulados, lo que hace un total de más de un millón de seguidores y amigos en nuestras redes». 2) La elaboración de un Atlas de Redes Sociales del Ministerio. Este Atlas se ha confirmado como el principal instrumento de verificación de nuestras cuentas, pues permite identificar las webs y las cuentas en redes sociales de las representaciones en el exterior. 3) La realización de campañas digitales, como #ViajaSeguroMAEC y #RecomendacionesErasmus y el lanzamiento de multitud de infografías explicativas y vídeos sobre temas de relaciones internacionales y política exterior de España, por ejemplo sobre la candidatura de España a un puesto en el Consejo de Derechos Humanos de la ONU para el periodo 2018-2021; sobre asuntos consulares, como la solicitud del voto electoral desde el extranjero; y so-

(15) *Ibid.*, pp. 136-137.

(16) En efecto, «en las páginas webs del ministerio y de las representaciones en el exterior, se ofrece información sobre las actividades de los altos cargos del ministerio y las noticias de actualidad de la política exterior española. Accediendo a la pestaña Servicios al Ciudadano, podrá obtener toda la información consular para realizar ciertos trámites como inscripciones en el Registro Civil, legalización de documentos o renovación del pasaporte. En las webs de las misiones diplomáticas y consulares en el extranjero, están disponibles los datos de contacto y contenidos específicos consulares e informativos para cada país. Por último, a través de la propia página web, se ha habilitado un registro de quejas y sugerencias, gracias al cual «se recogen, tramitan y responden tanto las iniciativas que presentan los usuarios para mejorar la calidad de los servicios del Ministerio de Asuntos Exteriores y de Cooperación, como las manifestaciones de insatisfacción respecto a los mismos». http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/DiplomaciasigloXXI/Paginas/default.aspx

(17) Los 28 hubs o puntos focales son Embajadas españolas elegidas con criterios de equilibrio geográfico, de idiomas y de grandes temas horizontales. A los hubs se les pide un mayor esfuerzo comunicativo y una coordinación con las oficinas de su zona, con el fin de dinamizar la información disponible sobre nuestro país hacia terceros.

bre otros temas como las oportunidades de empleo en Organizaciones Internacionales.

Lo anterior es aplicable a otros Estados y organizaciones internacionales, como la Unión Europea, por ejemplo. Su página web –https://europa.eu/european-union/index_es– presenta sus contenidos con un claro sentido explicativo y de facilitación de acceso al ciudadano. Además de las ventanas *Acerca de la UE* y *La UE por temas*, la página de bienvenida recoge otras dos: *Vivir, trabajar y viajar en la UE* y *Hacer negocios*. Esta página da cuenta también de los medios para contactar con la UE y sus oficinas, entre los que la propia web destaca Europe Direct y Cuentas de las instituciones, organismos y agencias de la UE en las redes sociales. Por su parte, la página web de la Secretaría de Estado de los Estados Unidos recoge los mismos planteamientos e instrumentos. Como aspecto novedoso cabe mencionar el Bureau of International Information Programs (IIP), un instrumento para las conversaciones people-to-people con funcionarios sobre las prioridades de la política exterior (https://www.state.gov/r/iip/).

Gracias a la diplomacia digital es posible una diplomacia pública, «entendida como aquella dirigida a la opinión pública, al mundo empresarial y a la sociedad civil en general» y que permita estar en contacto con el creciente número de actores en la escena internacional: «empresas, instituciones culturales y científicas, grupos sociales y particulares deben ser tenidos cada vez más en cuenta en el contexto actual. Gracias a la diplomacia pública, se logra dar a conocer y proyectar con mayor eficacia y alcance la realidad de nuestro país y explicar a tan vastos destinatarios nuestras posiciones en relación con las principales cuestiones internacionales y las razones en las que se sustentan nuestras principales iniciativas de política exterior» (18).

El ejercicio del poder en la sociedad digital requiere la imposición de esa determinada visión de las cuestiones internacionales. Lo explica bien el MAEC cuando se refiere al papel de los centros de pensamiento o *think-tanks*: «El mundo al que nos dirigimos se configura, más que nunca, como una sociedad del conocimiento en la que la capacidad de influir se nutre del poder de las ideas. España tiene una visión del mundo, propia y elaborada, y por ello debe aportar una contribución fundamental al debate estratégico internacional» (19). Se trata, en fin, del *thought leadership*, el

(18) El MAEC enmarca en este contexto la actividad de diversas instituciones vinculadas con el mismo: Real Academia de España en Roma, Acción Cultural Española (AC/E), Agencia Española de Cooperación Internacional para el Desarrollo (AECID), la red de Casas creadas por MAEC a partir de 1990, Escuela Diplomática, Fundación Carolina, Instituto Cervantes, Instituto Europeo del Mediterráneo, entre otras. http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/DiplomaciasigloXXI/Paginas/Diplomaciapublica.aspx

(19) http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/DiplomaciasigloXXI/Paginas/centrospensamiento.aspx

liderazgo a través de las ideas, que consiste en «la capacidad de ocupar el espacio de la conversación y generar impactos en la vida pública, no solo en la academia. Los nuevos medios y las redes producen un efecto multiplicador» (20).

4.2 **Nuevos retos**

J. Nye ha puesto de manifiesto que actores distintos a los Estados están utilizando la revolución de la información para acumular legitimación moral e influir en el comportamiento de los estados (21), los cuales, como expuso hace años J. R. Capella, «han perdido poder frente a mutadas instituciones privadas que le están subordinadas –en términos de poder– hasta esta fase de la historia» (22). Entre estos actores –señala R. Rubio–, encontramos, sin duda, «las grandes compañías transnacionales, con implantación e intereses económicos en un gran número de países, lo que las convierte en un sujeto indispensable para la adopción de determinadas medidas, cuya ejecución sin su colaboración es prácticamente imposible» (23). En claro reconocimiento de esta importancia, cabe señalar que, en el marco de la reforma de su servicio exterior, Dinamarca prevé el nombramiento de un Embajador para la digitalización que salvaguarde y promueva los intereses daneses ante las grandes compañías del sector digital (24).

Por lo demás, han surgido nuevos ámbitos de preocupación para la seguridad de los Estados. En primer lugar, la ciberseguridad o garantía de la seguridad en el ciberespacio, «nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información –incluida Internet–, las redes y los sistemas de información y de telecomunicaciones». El conjunto de estas infraestructuras, redes y sistemas es en la actualidad la base para la prestación por las Administraciones Públicas, las empresas y los ciudadanos presten unos servicios esenciales para la sociedad y economía de todo

(20) Powell, Ch.; Manfredi, J. L., «Innovación, diplomacia y think tanks», *La Diplomacia Pública como reto de la política exterior*, MAEC; Escuela Diplomática; Real Instituto Elcano, Madrid, 2014, pp. 59-67.

(21) Nye, J., *La paradoja del poder norteamericano*, Taurus, Madrid, 2003, p. 85, donde cita el papel desarrollado por Al Jazeera.

(22) Capella, J. R., «Estado y derecho ante la mundialización: aspectos y problemáticas generales», en Capella, J. R. (Coord.), *Transformaciones del derecho de la mundialización*, Madrid: CGPJ, 1999, pp. 85-121 (pág. 106). Tras la afirmación anterior, Capella se refiere a la progresiva formación de un soberano privado supraestatal, «constituido por el poder estratégico conjunto de las grandes compañías transnacionales y, sobre todo, hoy, de los conglomerados financieros». Ver, también, Castells, M., *La era de la información: Economía, sociedad y cultura (vol. 2. El poder de la identidad*, Siglo XXI, Madrid, 2003, p. 282.

(23) Rubio, R. «La diplomacia pública: nuevos actores en un escenario nuevo», en *La Diplomacia Pública… op.cit.*, pp. 10-19, en particular, p. 16

(24) Anders Samuelsen, announces digitisation ambassador, 27 de enero de 2017; www.http://um.dk/en/news

país, y resulta esencial la articulación de una adecuada capacidad de prevención, defensa, detección, respuesta y recuperación frente a las amenazas y ataques al mismo (25). En segundo lugar, se ha puesto de relieve a partir de las elecciones presidenciales en Estados Unidos (2016) y Francia (2017), la posibilidad de que un Estado (Rusia) realice ciertas acciones para influir en el desarrollo de los procesos electorales y en los debates políticos (Cataluña, 2017) de otros países (26). En este orden de cosas, las filtraciones de documentos oficiales de acceso restringido por parte de la organización Wikileaks ponen de manifiesto la vulnerabilidad del Estado ante la red –como antes se puso de manifiesto la pérdida de la privacidad individual– y han abierto un debate sobre los límites de la transparencia en la red (27).

Esta cuestión conduce a la última consideración que quiero realizar. el debate sobre el respeto de los derechos fundamentales por internet. A. E. Pérez Luño ha expuesto con su claridad proverbial los términos de esta cuestión: «Internet implica, por tanto, el riesgo de un efecto multiplicador de los atentados contra derechos, bienes e intereses jurídicos (…). Su potencialidad en la difusión ilimitada de imágenes e informaciones la hace un vehículo especialmente poderoso para perpetrar atentados criminales contra bienes jurídicos básicos: la intimidad, la imagen, la dignidad y el honor de las personas, la libertad sexual, la propiedad intelectual e industrial, el mercado y los consumidores, la seguridad nacional y el orden público (…). El carácter internacional e ilimitado de esas conductas hacen más difícil su descubrimiento, prevención y castigo, ya que incluso en los casos en que puedan ser detectadas pueden plantearse conflictos sobre la jurisdicción sancionadora competente» (28).

---

(25) Presidencia del Gobierno, *Estrategia de ciberseguridad nacional 2013*. Son características de los ciberataques: 1) Bajo Coste muchas de las herramientas utilizadas por los atacantes pueden obtenerse de forma gratuita o a un coste muy reducido. 2) Ubicuidad y fácil ejecución la ejecución de los ataques es independiente de la localización de los agresores, no siendo imprescindible, en muchos casos, grandes conocimientos técnicos. 3) Efectividad e impacto si el ataque está bien diseñado, es posible que alcance los objetivos perseguidos. 4) La ausencia de políticas de ciberseguridad, la insuficiencia de recursos y la falta de sensibilización y formación pueden facilitar este adverso resultado. 5) Reducido riesgo para el atacante la facilidad de ocultación hace que no sea fácil atribuir la comisión de un ciberataque a su verdadero autor o autores, lo que, unido a un marco legal dispar o inexistente, dificulta la persecución de la acción. 6) La multiplicidad de potenciales atacantes (página 10). En IFG Spain, *La gobernanza de Internet en España 2015*, Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones, Madrid, junio de 2015, pp. 66-68, donde se recoge una relación de los ciberataques habidos en 2014.

(26) Torres Soriano, M. R., *Hackeando la democracia: operaciones de influencia en el ciberespacio*, Instituto Español de Estudios Estratégicos, Documento de opinión 66/2017, www.ieee.es.

(27) Ver al respecto, Eco, U., «Reflexiones sobre Wikileaks», y A. Abruzzesse, «Wikileaks; opacidad y transparencia», publicados en el número 374-375 de *Revista de Occidente* (2012), dedicado al secreto. pp. 173-180 y 181-196, respectivamente. Lozano, J. (Ed.), *Secretos en red. Intervenciones semióticas en el tiempo presente*, Sequitur, Madrid, 2014.

(28) Internet y los derechos humanos, *Anuario de Derechos humanos*. Nueva época vol. 12, 2011, pp. 287-330.

Y concluye: «Internet plantea una preocupante paradoja, que deriva de su eficacia global e ilimitada para atentar contra bienes y derechos, mientras que la capacidad de respuesta jurídica se halla fraccionada por las fronteras nacionales. Por ello, la reglamentación jurídica del flujo interno e internacional de datos es uno de los principales retos que hoy se plantean a los ordenamientos jurídicos nacionales y al orden jurídico internacional». Ya se ha expuesto que la UE ha emprendido esta labor normativa, de la que es expresión destacada el Reglamento General de Protección de Datos, que será aplicable a partir del próximo 25 de mayo (29).

(29) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Para un comentario al mismo, ver Piñar Mañas, J. L. (Dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de protección de datos*, Ed. Reus, Madrid, 2016.

XIII

SOSTENIBILIDAD Y REVOLUCIÓN DIGITAL

CAPÍTULO 43

CIUDADES INTELIGENTES Y DERECHO: DE LA E-ADMINISTRACIÓN A LA CIUDAD INTELIGENTE

Rubén Martínez Gutiérrez
Profesor Titular de Derecho Administrativo
Universidad de Alicante

1. PLANTEAMIENTO GENERAL

En el último año he tenido la oportunidad de participar (e incluso dirigir) algunos Seminarios y publicaciones de interés que han analizado en profundidad, desde diferentes posicionamientos y con un carácter interdisci-

plinar las Ciudades Inteligentes, conocidas por el público en general como *Smart Cities* (1).

Mi aproximación y acercamiento a este nuevo campo de estudio ha provenido de mi línea de investigación más sólida y a la que he dedicado más tiempo: el régimen jurídico de la Administración pública electrónica (y dentro de ella, también, de la contratación pública electrónica).

A pesar de esta circunstancia, nunca me había detenido a sentar las bases de una idea que en mi interior he tenido siempre consolidada: la implantación de la e-Administración debe entenderse como presupuesto inexcusable de la correcta articulación de los modelos de gestión de las Ciudades basados en las TIC, es decir, de las Ciudades Inteligentes. En la misma línea, también soy consciente, y así intentaré defenderlo en el apartado 3, que sin interoperabilidad en los servicios de las Administraciones Locales no pueden articularse modelos exitosos de Ciudades Inteligentes. Al conocer la amable invitación de los profesores Tomás de la Quadra y José Luis Piñar a participar en este Libro centrado en el análisis de los Retos Digitales, encargándoseme tratar el tema de la relación entre Derecho y Ciudades Inteligentes, pensé que esta sería una buena oportunidad para establecer estos presupuestos, sin renunciar a apuntar también otros elementos de análisis que me parecen altamente interesantes y que aunque lo he trabajado previamente, su análisis doctrinal ha sido tan escaso que me gustaría también resaltarlos en este trabajo, con la esperanza de que futuras investigaciones académicas profundicen y diseccionen, seguramente con más acierto que yo en estos momentos, estas ideas que me parecen esenciales para justificar por qué debemos avanzar hacia modelos de Ciudad Inteligente.

Con este presupuesto, el presente Capítulo también incidirá en las formas de participación de las personas en la generación de los datos a gestionar por las Ciudades Inteligentes, en la prestación eficaz de los servicios públicos, en la necesidad de modernizar la normativa de régimen local y en la propuesta de diseñar la ciudad en base a la gestión de los datos de las Ciudades Inteligentes a la que he denominado urbanismo tecnológico. También nos referiremos a los aspectos metodológicos que la administración deberá seguir para culminar correctamente el proyecto de im-

(1) Especialmente interesantes resultan los Seminarios celebrados en la Universidad de Alicante: Seminario sobre Gestión Inteligente y Sostenible de las Ciudades: *open data* y modelos *Smart City*, celebrado el 13 y 14 de octubre de 2016, y, el II Seminario sobre Gestión Inteligente y Sostenible de las Ciudades: Gobernanza, *Smart Cities* y Turismo, celebrado los días 6 y 7 de julio de 2017, organizados ambos por la UA y la Conselleria de Transparència, Responsabilitat Social, Participació i Cooperació. Asimismo, interesa destacar las siguientes publicaciones, en buena medida cimentadas en dichas investigaciones: Piñar Mañas, J.L. (Dir.): *Smart Cities. Derecho y Técnica para una ciudad más habitable*, Reus, Madrid, 2017, y, Cantó López, M.T., Ivars Baidal, J., y Martínez Gutiérrez, R., (Dirs.): *Gestión inteligente y sostenible de las ciudades: Regulación y Destinos Inteligentes*, Tirant Lo Blanch, Valencia, en prensa.

plantación de los sistemas de Ciudad Inteligente. El Capítulo terminará con una conclusión general de los retos digitales que se tendrán que afrontar en la relación entre Derecho y Ciudades Inteligentes, a modo de conclusiones de los apartados analizados.

2. LA IMPLANTACIÓN DE LA E-ADMINISTRACIÓN COMO REQUISITO PREVIO INEXCUSABLE

La aprobación en los últimos años de las Leyes que podrían conformar el nuevo Derecho Administrativo *electrónico* básico, cuya clave de bóveda está formada esencialmente por 4 Leyes: 1. La Ley 19/2013, de Transparencia, Acceso a la Información Pública y Buen Gobierno, 2. La Ley 39/2015, de Procedimiento Administrativo Común de las Administraciones Públicas, 3. La Ley 40/2015, de Régimen Jurídico del Sector Público, y, 4. La Ley 9/2017, de Contratos del Sector Público; ha determinado que podamos afirmar sin miedo a equivocarnos que la tramitación de los procedimientos administrativos será ya, desde la entrada en vigor con plena eficacia de las Leyes llamadas «Siamesas» de 2018 (2 de octubre de 2018), única y exclusivamente electrónica (2). Esta realidad será aplicable también a ámbitos específicos de tramitación procedimental y, en particular, y dada su importancia, también en el sector de la contratación pública, que como se sabrá, tiene un alto índice de impacto en la gestión administrativa (3).

A pesar de esta realidad, establecida con carácter preceptivo, son muchas las Administraciones que se resisten a la llegada del nuevo modelo de e-Administración, bien sea por pura resistencia, en menor medida ya, o por las dificultades, el desconocimiento del nuevo procedimiento de tramitación procedimental electrónico y la escasez de medios materiales y humanos, en la mayoría de los casos. Precisamente en esta problemática, se encuentran nuestras Administraciones Locales, que desafortunadamente se han encontrado en este proceso de transformación digital ante grandes retos y un desamparo de la Administración General del Estado, las Comunidades Autónomas y las Diputaciones (salvo contadas excepciones) diametralmente opuesto y proporcional al reto que legalmente se les ha exigido.

Pues bien, en este contexto, el desarrollo y articulación plena de la e-Administración (4) y con ella de los nuevos procedimientos de e-Contra-

(2) Martínez Gutiérrez, R.: *El Régimen Jurídico del Nuevo Procedimiento Administrativo Común*, Thomson Reuters Aranzadi, Navarra, 2016, pp. 87 y siguientes.

(3) Martínez Gutiérrez, R.: *La contratación pública electrónica. Análisis y propuesta de transposición de las Directivas Comunitarias de 2014*, Tirant Lo Blanch, Valencia, 2015.

(4) Con respecto al concepto de e-Administración, véase Martínez Gutiérrez, R.: *El procedimiento electrónico en las Administraciones Locales. Aspectos metodológicos y normativos del proceso de implantación*, CEMCI, Granada, 2018.

tación (5) (exigibles con la Ley 9/2017, de Contratos del Sector Público) se presenta como requisito inexcusable y previo a la implantación de las Ciudades Inteligentes. No tendría sentido que el camino hacia las Ciudades Inteligentes discurriera al margen de la previa implantación, tanto a nivel interno como a nivel externo, de las técnicas de Administración pública electrónica, y, dentro de las mismas, adquiere especial interés por lo que al ámbito de objeto de estudio de este Capítulo se refiere, la plena articulación de redes intranet de gestión e intercambio electrónico de datos y documentos que cumplan adecuadamente con las exigencias de los Reales Decretos 3 y 4 de 2010 en base a los cuales se promulgaron los Esquemas Nacionales de Seguridad y de Interoperabilidad, a los que prestaré la necesaria atención en el siguiente apartado. Difícilmente se podrá conseguir una adecuada gestión de la información, datos y documentos de la actividad administrativa, del desarrollo de procedimientos y de la prestación de servicios públicos si no disponemos de un sólido proyecto de e-Administración en nuestra Administración Local.

Finalmente, y en esta misma línea argumental, aunque estableciendo importantes obligaciones adicionales, Piñar Mañas ha defendido recientemente que la efectiva implantación de Ciudades Inteligentes requiere la previa puesta en funcionamiento del modelo de Gobierno Abierto municipal, siendo esta circunstancia clave para cimentar el éxito de cualquier proyecto tecnológico (6). El Gobierno Abierto parte de la necesaria previa implementación de sistemas de tramitación electrónica de procedimientos o de Administración pública electrónica, con unas obligaciones adicionales de transparencia y participación ciudadana a través de medios tecnológicos para la toma de decisiones gubernamentales. Como veremos más adelante, en el ADN del concepto de «urbanismo tecnológico» que se abordará en el apartado 7 de este Capítulo radica precisamente la idea de que los ciudadanos participen en la motivación y justificación de las decisiones discrecionales urbanísticas, cuestión que estaría inserta dentro de las acciones de Gobierno Abierto municipal.

3. LA IMPORTANCIA ESTRUCTURAL DE LA INTEROPERABILIDAD EN LA OBTENCIÓN Y GESTIÓN DE LOS DATOS

La interoperabilidad como principio de funcionamiento básico y estructural de las plataformas de tramitación electrónica de cualquier tipo de procedimientos administrativos ha quedado patente no solo en España

(5) En relación a la noción de e-Contratación tanto en sentido amplio como estricto, véase Martínez Gutiérrez, R.: *La contratación pública electrónica…*, *op. cit.*, pp. 45 y siguientes.

(6) Piñar Mañas, J.L.: «Derecho, técnica e innovación en las llamadas Ciudades Inteligentes. Privacidad y Gobierno Abierto», en Piñar Mañas, J.L. (Dir.): *Smart Cities. Derecho y Técnica para una ciudad más habitable*, Reus, Madrid, 2017, pp. 21 y siguientes.

sino también en la mayoría de normas y documentos institucionales comunitarios. En estos documentos se justifica la importancia de la interoperabilidad en una idea global: sin interoperabilidad y por ende sin interconexión de sistemas, aplicaciones y plataformas de gestión de datos, documentos y procedimientos no es posible implantar de manera efectiva proyectos de e-Administración ni otros derivados de éstos como por ejemplo la implantación de Ciudades Inteligentes. De esta forma, existe una coincidencia a la hora de reconocer la interoperabilidad como objetivo prioritario y a la vez insalvable si se pretende alcanzar el pleno desarrollo del nuevo modelo de Administración electrónica en Europa y en España. Precisamente como consecuencia del carácter transversal de la interoperabilidad, y su importancia capital para la consecución de la Administración electrónica, en algunos trabajos previos he considerado la interoperabilidad como un nuevo principio jurídico del modelo de e-Administración (7). La consideración como principio de la interoperabilidad proviene directamente de la extrapolación al denominado Derecho Administrativo Electrónico de la definición jurídica de principios elaborada por García de Enterría y Fernández Rodríguez, en base a la cual puede afirmarse que los principios se identifican con aquellos elementos esenciales e indispensables para la consecución y desarrollo de una determinada actividad, y precisamente su calificación como principios hace referencia a su carácter básico como soportes primarios estructurales del sistema (8).

Pues bien, como ya he advertido a propósito de esta consideración, «si algo puede ser catalogado como soporte primario estructural del nuevo modelo de administrar y de las plataformas electrónicas del nuevo procedimiento administrativo común a tenor de lo establecido por las nuevas Leyes 39 y 40 de 2015 es, desde luego, la interoperabilidad. Tanto es así, que sin interoperabilidad no hay posibilidad de comunicación electrónica entre las plataformas y aplicaciones que las Administraciones y administrados utilizan para realizar procedimientos electrónicos por lo que la regulación jurídica de la interoperabilidad y su garantía, a pesar de las dificultades interpretativas que puedan plantear estas normas y de las rigideces que se desprenden de las mismas en su diseño, es fundamental para el correcto desarrollo del modelo de gestión documental electrónico del nuevo procedimiento (especialmente en relación a la interacción e inter-

(7) Véase espacialmente, Martínez Gutiérrez, R.: «Relaciones interadministrativas por medios electrónicos. Interoperabilidad», en Gamero Casado, E., (Dir.): *Tratado de Procedimiento Administrativo Común y Régimen Jurídico Básico del Sector Público*, Tomo II, Tirant Lo Blanch, Valencia, 2017, pp. 2899 y siguientes.

(8) García de Enterría, E. y Fernández Rodríguez, T.R.: *Curso de Derecho Administrativo*, Tomo I, 11.ª ed., Civitas, Madrid, 2002, p. 83.

conexión de archivos para el intercambio electrónico de datos y documentos entre Administraciones)» (9).

La principal consecuencia de esta realidad es el necesario cumplimiento por las Administraciones Locales, también en el camino hacia la migración a su modalidad de Ciudades Inteligentes, de las normas establecidas del Real Decreto 4/2010, por el que se regula el Esquema Nacional de Interoperabilidad (y también del Real Decreto 3/2010, por el que se aprueba el Esquema Nacional de Seguridad) y sus normas técnicas de desarrollo. El cumplimiento del Esquema Nacional de Interoperabilidad se predica necesariamente de cualquier archivo, aplicación o plataforma electrónica que vaya a ser utilizada en el ámbito de las Administraciones y ello incluye inexorablemente los sistemas de gestión de las Ciudades Inteligentes.

En consecuencia, y de conformidad con el significado y alcance de la interoperabilidad, podemos afirmar que dicho principio también es estructural en la creación e implantación de las Ciudades Inteligentes ya que de lo contrario, sería altamente costoso tanto desde el punto de vista económico como de inversión de tiempo, conseguir el necesario enlace y cruce de gestión de datos públicos que es la base de las plataformas de gestión municipal basadas en modelos *Smart City.*

4. LA PARTICIPACIÓN ACTIVA Y LA PARTICIPACIÓN INSCONSCIENTE. EL DERECHO AL ANONIMATO Y AL ACCESO AL DATO MÍNIMO NECESARIO

La gestión de las Ciudades Inteligentes parte de la premisa de la obtención de datos e información para identificar las necesidades sociales de la población y así prestar servicios o adoptar decisiones más adecuadas a la realidad social. Esta obtención de datos se realiza bien mediante la toma de datos de manera indirecta (y anónima) de los ciudadanos y ciudadanas, o bien mediante la participación directa de los mismos en procesos participativos que puedan facilitarse por la Administración. A este respecto, y como ha analizado Cantó López, las personas que habitan una ciudad se convierten en los denominados «ciudadanos sensor» (10), siendo elementos clave en el buen desarrollo de proyectos de Ciudad Inteligente. En esta línea, es necesario plantearnos si en pleno siglo XXI y con las potencialidades tecnológicas que permiten los modelos de Ciudades Inteligentes «no sería recomendable, e incluso obligatorio vistos los pro-

(9) Martínez Gutiérrez, R.: «Relaciones interadministrativas por medios electrónicos. Interoperabilidad», *op. cit.*, p. 2899.

(10) Cantó López, M.T.: «Administración pública y participación activa del ciudadano en la gestión de la ciudad inteligente», en Piñar Mañas, J.L. (Dir.): *Smart Cities. Derecho y Técnica para una ciudad más habitable,* Reus, Madrid, 2017, p. 49.

pósitos de las nuevas normas legales como la Ley 39/2015, de Procedimiento Administrativo Común, que los conceptos jurídicos indeterminados y las situaciones complejas que se plantean en la adopción de decisiones discrecionales (…) deban necesariamente completarse, total o parcialmente, con los datos basados en las técnicas de *open data* que puedan obtenerse total o parcialmente de la ciudadanía y de las personas que utilizan y «pisan» las ciudades cada día, y que en base a ellos se pueda al menos valorar las opciones de planificación urbanística sostenible más ajustada a las necesidades reales, completándose así el margen de discrecionalidad legítimo de la Administración» (11) (12).

De esta manera, las plataformas de gestión de datos e informaciones en las Ciudades Inteligentes pueden ayudar a la adopción de decisiones administrativas y de Gobierno, ahora bien, de las dos modalidades existentes para la obtención de datos: de un lado, la participación activa y plenamente consciente de los ciudadanos, y, de otro lado, la participación inconsciente de las personas en la obtención de datos; será necesario cumplir en todo caso con la normativa reguladora de la protección de datos de carácter personal, tanto el Reglamento de la Unión Europea de 2016 como la Ley Orgánica española de protección de datos (ya sea la actual o la que se atisba en el horizonte jurídico próximo). En todo caso, y especialmente, se debería garantizar el cumplimiento de la normativa de protección de datos en el supuesto de la obtención de datos inconsciente de los mismos, en base al denominado acceso al dato mínimo necesario y a los nuevos principios de protección de datos por diseño de las aplicaciones de gestión y anonimización y segregación de datos para garantizar su privacidad.

En esta línea, me gustaría traer a colación una reflexión que realicé en un trabajo previo y en la que señalé que «debe mencionarse muy positivamente la nueva regulación comunitaria de protección de datos publicada en el DOCE el 4 de mayo de 2016 mediante el Reglamento General de UE Protección de Datos (de aplicación directa en España a partir de 25 de mayo de 2018), ya que establece el denominado principio de minimización de datos (artículo 5.1.c) y lo desarrolla en su artículo 25 sobre la base de la «protección de datos desde el diseño y por defecto», cuya finalidad parece ser que en las transmisiones de datos no se obtenga más información y datos que los absolutamente necesarios para lo cual los archivos y

(11) Martínez Gutiérrez, R.: «Introducción. Gestión inteligente y sostenible de las ciudades: Gobernanza, *Smart Cities* y Turismo», en Cantó López, M.T., Ivars Baidal, J., y Martínez Gutiérrez, R., (Dirs.): *Gestión inteligente y sostenible de las ciudades:…*, *op. cit.*

(12) La idea de utilizar el *open data* para este propósito me surge en la lectura del trabajo de Valero Torrijos, J.: «Sostenibilidad y gestión de la información en las ciudades inteligentes *(Smart Cities):* apuntes para un debate desde la perspectiva jurídica», en Bustillo Bolado, Roberto, y Gómez Manresa, M.F., (Dirs.): *Desarrollo sostenible: análisis jurisprudencial y de políticas públicas*, Thomson Reuters Aranzadi, Navarra, 2014, pp. 493 a 495.

bases de datos deberán diseñarse con ciertos parámetros técnicos que permitan dichas posibilidades técnicas, es decir, lo que aquí hemos denominado como acceso al dato mínimo necesario. Esta nueva vía, sin duda más garantista y adecuada al derecho a la protección de datos de carácter personal, junto con la posibilidad de que las Administraciones puedan intercambiar ciertos datos en los procedimientos iniciados de oficio sin necesidad de consentimiento del interesado cuando nos encontremos ante el cumplimiento de una finalidad pública o una obligación legal vinculada al ejercicio de potestades públicas del órgano a la que parece habilitar la combinación de los artículos 5.1.b), 6.1.c) y e), 6.3, 9.2.g), 23.1.e) y h), y 89.1 del Reglamento General UE de Protección de Datos, es posible que permita un sistema mucho más coherente, seguro y ágil de transmisiones electrónicas de datos que facilite la simplificación administrativa y el desarrollo de procedimientos administrativos más acordes a las posibilidades tecnológicas actuales, redundando todo ello en beneficio de las personas interesadas y de las Administraciones en el cumplimiento y ejercicio de sus funciones y/o misiones de interés público normativamente atribuidas por el ordenamiento jurídico» (13).

Las plataformas de gestión de datos e informaciones de las Ciudades Inteligentes deberán diseñarse conforme a los principios de funcionamiento que hemos señalado en el presente apartado y que garantizan plenamente el derecho fundamental a la protección de datos de carácter personal de los ciudadanos que participen, ya sea activamente o de forma inconsciente, en la obtención de datos y documentos que vayan a ser empleados en los sistemas de gestión de las Ciudades Inteligentes.

5. LA CIUDAD INTELIGENTE Y LA PRESTACIÓN EFICAZ DE SERVICIOS PÚBLICOS

Una de las razones que siempre se argumentan para justificar la necesidad de que nuestras ciudades se transformen a su modalidad de gestión Inteligente es conseguir una prestación más eficaz de los servicios públicos municipales. En otros trabajos previos, he podido analizar el impacto y también la conveniencia de que nuestros municipios asuman el reto digital de transformarse a Ciudades Inteligentes, para conseguir una prestación más eficaz de los servicios públicos (14). Una buena gestión de los datos en la prestación de los servicios públicos (en particular, en la gestión de las aguas, la recogida de residuos, la gestión del tráfico, la raciona-

(13) Martínez Gutiérrez, R.: «Relaciones interadministrativas por medios electrónicos. Interoperabilidad», *op. cit.*, p. 2921.

(14) Martínez Gutiérrez, R.: «El impacto de las *Smart Cities* en la tutela ambiental y en la planificación urbana», en Piñar Mañas, J.L. (Dir.): *Smart Cities. Derecho y Técnica para una ciudad más habitable*, Reus, Madrid, 2017, pp. 57 a 64.

lización de la iluminación pública, etc.) puede conseguir que los servicios se cumplan de una manera más eficiente, y por tanto, con un importante ahorro de costes manteniendo la prestación eficaz de los servicios.

En este contexto, sería conveniente advertir de la necesidad de que los pliegos de los contratos que rigen la prestación de estos servicios incorporen cláusulas para asegurar que las herramientas tecnológicas de gestión de datos de prestación del servicio cumplen adecuadamente con los parámetros establecidos en los Reales Decretos 3 y 4 de 2010 reguladores de los Esquemas Nacionales de Interoperabilidad y de Seguridad (a los que nos hemos referido en el apartado 3), de manera que los Ayuntamientos se aseguren la utilización de estos datos y su integración en las plataformas de gestión electrónica de procedimientos propias del modelo de e-Administración, y de ahí, a su volcado y utilización en las plataformas de gestión de Ciudades Inteligentes.

Además, el carácter básico y la aplicación directa a los Ayuntamientos de las normas de interoperabilidad y seguridad contenidas en el ENI y el ENS no se circunscriben únicamente a las herramientas de e-Administración o de e-Contratación, sino que se predican de cualquier herramienta tecnológica que vaya a ser implantada y utilizada por las Administraciones. He de reconocer que esta realidad es un tanto desconocida y quizá por ello sea necesario incidir en esta problemática, de forma que los pliegos que vayan a regir la prestación de estos servicios se confeccionen de conformidad al ordenamiento legal y normativamente establecido.

Finalmente, también es importante que se garantice la plena integración de las herramientas de gestión y prestación de los servicios con las plataformas municipales de gestión de los procedimientos administrativos electrónicos que se hayan puesto en funcionamiento de conformidad a las Leyes 39 y 40 de 2015, reguladoras del procedimiento administrativo común y del régimen jurídico del sector público. Esta interconexión es necesaria y debe permitir integrar en la misma red de la Administración Local cualquier trámite administrativo asociado al mismo: la solicitud de prestación del servicio, las reclamaciones, el pago de las tasas, etc.

6. LA NECESIDAD DE MODERNIZAR LA NORMATIVA DE RÉGIMEN LOCAL

Si analizamos detenidamente todos los retos y pasos previos necesarios para conseguir una adecuada implantación de los modelos de Ciudades Inteligentes a los que hemos ido haciendo referencia durante el presente Capítulo, observaremos que muchos de ellos requieren la actualización constante de la manera de actuar de nuestras Administraciones Locales, ajustando los cambios tecnológicos propios de la era actual a la forma de tramitar y de desarrollar actuaciones y procedimientos adminis-

trativos. La necesidad de acometer dichos cambios no solo es meramente organizacional o procedimental, es también normativa. Es preciso reflexionar sobre la necesaria adaptación de la normativa legal de régimen local y su necesaria y progresiva actualización y reforma. La Ley 7/1985, Reguladora de las Bases de Régimen Local, la normativa reglamentaria básica de régimen local (en particular el Reglamento de Organización y Funcionamiento de las Administraciones Locales de 1986), etc., son normas totalmente desactualizadas desde el punto de vista de su actualización a las necesidades derivadas de la implantación de la e-Administración y también de los modelos de Ciudad Inteligente.

En la sociedad actual del siglo XXI, el uso intensivo de las TIC es ya una constante en el ámbito privado y cada vez más en el ámbito público gracias al impulso fundamental de la normativa comunitaria, piénsese por ejemplo en la normativa relativa a la contratación pública electrónica, a la facturación electrónica o a la protección de datos de carácter personal, sin hablar del impulso y análisis que desde la Unión Europea se está realizando en los últimos años con el objetivo de determinar una normativa europea común en materia de procedimiento administrativo. Pues bien, en este contexto de cambios, la normativa reguladora de régimen local ha permanecido impasible, y por ello sería necesaria su modernización y adaptación a las nuevas realidades: e-Administración, e-Contratación, *Smart Cities,* etc., de forma que el Derecho deje de convertirse en un obstáculo para la puesta en funcionamiento de proyectos de modernización y pase a ser un auténtico canalizador, mediante una regulación adecuada y adaptada a las necesidades de las AALL, del potencial que las TIC pueden generar en nuestras Administraciones.

El reto de reformar y adaptar a la era tecnológica todo el elenco de normas básicas que son de aplicación primaria a las Administraciones Locales no es menor, y resulta imprescindible para afrontar con garantías la modernización de nuestros Ayuntamientos. No sería razonable la articulación de modelos de gestión de datos e informaciones propios de las Ciudades Inteligentes sin una base normativa sólida y que dotase de seguridad jurídica a la gestión de la actividad administrativa propia de estos modelos.

Por tanto, es preciso que el legislador proceda a modernizar de inmediato la normativa básica de régimen local, dando cobertura jurídica a las modalidades de gestión de la información, datos y actuación administrativa basados en las TIC, y especialmente al establecimiento de modelos de gestión de Ciudades Inteligentes.

7. EL DISEÑO URBANÍSTICO DE LAS CIUDADES INTELIGENTES: HACIA UN NUEVO URBANISMO *TECNOLÓGICO*

La manera en la que justificar y motivar de mejor forma las decisiones discrecionales propias de algunos ámbitos de la actuación administrativa es un reto que los investigadores del Derecho Administrativo debemos afrontar. El urbanismo es uno de los ámbitos de la actuación municipal más polémicos y en los que el ejercicio de potestades discrecionales resulta más evidente, y en este ámbito, gracias a los datos obtenidos de manera directa, tanto voluntaria como inconsciente (cuestión que hemos analizado en el apartado 4 de este Capítulo), se pueden motivar las decisiones que se adoptan en el planeamiento urbanístico o en los rediseños urbanos gracias a la información que aporten los propios habitantes de las ciudades. Las plataformas de gestión de datos e información propios de las Ciudades Inteligentes pueden ayudar a los gobiernos a adoptar mejores decisiones, basando las mismas en los datos que se obtengan de los propios ciudadanos.

Dentro de las competencias propias de las Corporaciones Locales se encuentra la «promoción en su término municipal de la participación de los ciudadanos en el uso eficiente y sostenible de las tecnologías de la información y las comunicaciones» (artículo 25.2.ñ) de la Ley 7/1985, Reguladora de las Bases de Régimen Local), y también las siguientes: «Urbanismo: planeamiento, gestión, ejecución y disciplina urbanística. Protección y gestión del Patrimonio histórico. Promoción y gestión de la vivienda de protección pública con criterios de sostenibilidad financiera. Conservación y rehabilitación de la edificación» [artículo 25.2.a) de la LRBRL]; «Medio ambiente urbano: en particular, parques y jardines públicos, gestión de los residuos sólidos urbanos y protección contra la contaminación acústica, lumínica y atmosférica en las zonas urbanas» [artículo 25.2.b) de la LRBRL]; «Infraestructura viaria y otros equipamientos de su titularidad» [artículo 25.2.d) de la LRBRL]; y, «Tráfico, estacionamiento de vehículos y movilidad. Transporte colectivo urbano» [artículo 25.2.g) de la LRBRL], entre otras cuestiones que también tienen incidencia en el urbanismo. La interrelación de todas estas competencias locales, con la determinación de la Ley 39/2015, de Procedimiento Administrativo Común, que exige que en el proceso de elaboración de los reglamentos (y el planeamiento urbanístico tiene este carácter) se potencie la participación ciudadana, debe llevarnos a considerar seriamente la necesidad de que en la adopción de decisiones urbanísticas se utilicen los datos obtenidos de las plataformas de gestión de las Ciudades Inteligentes (15).

(15) En esta línea, con carácter previo, y en conexión con la legislación urbanística de la Comunidad Valenciana, véase, Martínez Gutiérrez, R.: «El impacto de las *Smart Cities* en la tutela ambiental y en la planificación urbana», *op. cit.*, p. 64 a 67.

Esta nueva realidad proviene directamente de los objetivos de la estrategia de la Unión Europea *EUROPA 2020: Una estrategia para un crecimiento inteligente, sostenible e integrador* (Documento COM/2010/2020 final) (16), y creo que es necesario contemplar la posibilidad de instaurar legalmente, o al menos de analizar la conveniencia de articular el concepto o noción de urbanismo tecnológico, entendido como la necesaria integración de los datos e informaciones obtenidas gracias a la aplicación de plataformas de gestión TIC y, en particular de los proyectos *Smart City,* en la motivación y justificación de las decisiones discrecionales que se adoptan en el ámbito urbanístico, con la finalidad de completar de mejor manera los conceptos jurídicos indeterminados que se presentan en la normativa legal urbanística y de solucionar de forma más certera las denominadas situaciones complejas propias de la gestión del planeamiento urbanístico.

En este sentido, no se trata de coartar el legítimo margen de discrecionalidad de los órganos municipales con competencias en el urbanismo, sino de que utilicen, incluso preceptivamente, datos e informaciones suficientes y precisas como para que adopten la decisión que estimen pertinente en base a la mejor información disponible, proporcionada de manera directa o indirecta por las personas que habitan la ciudad.

Las plataformas de gestión de datos de las Ciudades Inteligentes pueden aportar en este punto una valiosa fuente de información que permita a los órganos con competencia en la aprobación de la normativa urbanística obtener un mejor conocimiento de la situación de partida, de forma que puedan adoptar las soluciones más certeras, teniendo además en cuenta la participación directa (voluntaria o incluso inconsciente) de los vecinos y vecinas (a la que nos hemos referido en el apartado 4 de este Capítulo). En línea con lo que apunta Piñar Mañas, llegará el momento en el que legalmente se nos exija a los órganos de las Administraciones que actuemos de esta manera, empleando los datos e informaciones obtenidos de las plataformas de gestión de Ciudades Inteligentes, de manera que el diálogo entre Derecho y técnica es imprescindible (17) en la implantación de los nuevos modelos de gestión de las ciudades.

Siempre que un órgano administrativo deba adoptar una decisión de carácter discrecional, y en particular una decisión de planeamiento urbanístico o de rediseño urbano, sería conveniente que pudiese contar con los datos e informaciones de que disponga la plataforma de gestión de la Ciudad Inteligente, ya que resulta una manera más adecuada de justificar y motivar su decisión que centrarse única y exclusivamente en su subjeti-

(16) Documento disponible en:

http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52010DC2020. Fecha de consulta: 18.02.2018.

(17) Piñar Mañas, J.L.: «Derecho, técnica e innovación en las llamadas Ciudades Inteligentes. Privacidad y Gobierno Abierto», *op. cit.*, p. 31.

vo criterio o en informes técnicos que puedan emitir un juicio subjetivo de los técnicos municipales. En este sentido, propuestas como las aquí señaladas del urbanismo tecnológico pueden abrir el camino hacia un ejercicio más razonado de la discrecionalidad administrativa, que evite la producción de decisiones arbitrarias enmascaradas en el ejercicio de potestades discrecionales.

8. ASPECTOS METODOLÓGICOS DEL PROCESO DE IMPLANTACIÓN DE LAS CIUDADES INTELIGENTES EN NUESTRAS ADMINISTRACIONES LOCALES

Como ya he advertido en una monografía reciente, «todo proceso de reforma o de adaptación en la Administración implica tener que cumplir con una serie de aspectos metodológicos que permitan planificar el proceso de implantación y lograr los objetivos marcados con la reforma que se emprende» (18). El análisis estratégico de los procesos de reforma administrativa y la determinación de fórmulas adecuadas para llevarlos a buen término es esencial, y ciertamente, cuando nos encontramos ante nuevas modas, la planificación real suele brillar por su ausencia.

En los procesos de implantación de sistemas TIC en las Administraciones Locales deben tenerse en consideración al menos los siguientes aspectos: «1. Liderazgo político e institucional. 2. Planificación de la implantación. 3. Implicación de los órganos administrativos fundamentales de la organización en el proceso en un primer momento, para posteriormente conseguir la implicación del máximo número posible de empleados de la Administración. 4. Modificación de la organización administrativa y su adaptación al modelo de gestión electrónico gracias a vencer el miedo al cambio mediante una adecuada formación. 5. Implantación de las modificaciones primero a nivel interno, dentro de la organización administrativa, y posteriormente a nivel externo, ofertando procedimientos y servicios a los ciudadanos. Y, 6. Inversión económica inicial y apuesta por la reutilización y transferencia de tecnología. Pasemos a analizar cada uno de ellos» (19).

Cuando un Ayuntamiento se disponga a convertir su ciudad en una Ciudad Inteligente, el reto y la inversión económica serán elevados. Precisamente por esta razón, no puede dejarse de lado la planificación estratégica del proceso de implantación, que permita involucrar en este nuevo reto digital a toda la organización administrativa. Que el proyecto de implantación de un modelo de Ciudad Inteligente culmine adecuadamente

(18) Martínez Gutiérrez, R.: *El procedimiento electrónico en las Administraciones Locales…*, *op. cit.*

(19) Martínez Gutiérrez, R.: *El procedimiento electrónico en las Administraciones Locales…*, *op. cit.*

dependerá de múltiples factores, tal y como hemos analizado a lo largo de este Capítulo, pero lo que es claro es que uno de los elementos cruciales será el establecimiento de cauces metodológicos para asegurar el correcto desenvolvimiento del proyecto, razón por la cual, me ha parecido necesario llamar la atención sobre este aspecto que en los análisis jurídicos de los procesos de implantación de la tecnología en las Administraciones muchas veces se suelen pasar por alto.

9. CONCLUSIÓN. EL RETO *DIGITAL* DEL DERECHO PÚBLICO PARA GOBERNAR LAS CIUDADES INTELIGENTES

En el presente Capítulo hemos podido reflexionar sobre la relación entre Ciudades Inteligentes y Derecho. Es necesario ser conscientes de que las Ciudades Digitales son la nueva moda TIC en nuestras Administraciones Locales y quizá por ello resulta altamente conveniente cimentar jurídicamente las bases de esta nueva aplicación de la tecnología a la gestión municipal. Con el objetivo de fundamentar y razonar los retos digitales de las Ciudades Inteligentes y de su regulación por el Derecho, el presente trabajo ha realizado una serie de propuestas, en base a las cuales podemos concluir:

1. Como paso previo al establecimiento de sistemas de gestión de información y datos de Ciudad Inteligente resulta inexcusable que internamente la Administración Local haya procedido a implantar de manera adecuada su plataforma de gestión electrónica de procedimientos administrativos o sistema de Administración pública electrónica. Sin esta realidad administrativa previa, difícilmente se podrá instaurar un modelo de gestión exitoso de Ciudad Inteligente.

2. Los modelos de Ciudad Inteligente se basan en la gestión y obtención de datos e informaciones, y por ende, en la interconexión de aplicaciones, sistemas, plataformas, etc., centrada en la aplicación de las TIC a la gestión administrativa. En este contexto, la interoperabilidad, entendida como la «capacidad de los sistemas de tecnologías de la información y las comunicaciones (TIC), y de los procesos (…) a los que apoyan, de intercambiar datos y posibilitar la puesta en común de información y conocimientos» (artículo 3.º apartado f) de su Decisión 2004/387/CE del Parlamento Europeo y del Consejo, de 21 de abril de 2004, relativa a la prestación interoperable de servicios paneuropeos de administración electrónica al sector público, las empresas y los ciudadanos (IDABC), debe considerarse como un elemento estructural de la implantación de los modelos de gestión de Ciudades Inteligentes. Sin interoperabilidad no habrá interconexión de datos e información, de archivos y plataformas,

con lo que el desarrollo de un exitoso modelo de ciudad *Smart City* será altamente complicado.

3. El Derecho debe velar porque las plataformas de gestión de datos e informaciones de las Ciudades Inteligentes se diseñen conforme a los principios modernos que garantizan el derecho fundamental a la protección de datos de carácter personal de los ciudadanos que participen en el proceso de obtención de datos, ya sea cuando su participación se produzca activamente o también cuando dicha participación se realice de forma inconsciente. En este reto, explorar fórmulas como la anonimización de datos y principios de funcionamiento como el acceso al dato mínimo necesario para la realización de la concreta actuación administrativa pueden resultar claves para una adecuada gestión de la información y datos cubriendo los derechos fundamentales de las personas que participan en estos procesos.

4. La migración hacia Ciudad Inteligente debe tener como uno de sus polos principales de atracción la mejora de la prestación de servicios públicos, siendo más eficaz y eficiente gracias a la utilización de los datos e informaciones y a la adopción de decisiones más acertadas en la prestación de los servicios. Para poder obtener estas ventajas de gestión, los pliegos que rijan los procesos de contratación pública de los servicios públicos deberán garantizar la utilización por la Administración Local de los datos que obtengan las concesionarias y también que los sistemas de información y gestión de datos que implanten cumplan con la normativa reguladora de los Esquemas Nacionales de Interoperabilidad y Seguridad, de forma que el trasvase de datos y el tratamiento de la información pueda desarrollarse con éxito, de forma sencilla y si realizar grandes inversiones económicas para permitir el uso de la información y datos que obtengan las concesionarias en la prestación de los servicios públicos.

5. La aplicación de las plataformas de gestión de datos e informaciones de las Ciudades Inteligentes reviste especial interés cuando nos encontramos ante situaciones complejas, en las que los órganos administrativos deben adoptar decisiones discrecionales y motivar y justificar las mismas, muchas veces, además, completando gran cantidad de conceptos jurídicos indeterminados. Uno de los ámbitos en los que esta problemática se presenta como más aguda es el urbanismo, razón por la cual, de la mano de las Ciudades Inteligentes se debería profundizar en nuevas propuestas como el urbanismo tecnológico, entendido como la necesaria integración de los datos e informaciones obtenidas gracias a la aplicación de plataformas de gestión TIC y, en particular de los proyectos *Smart City,* en la motivación y justificación de las decisiones discrecionales que se adoptan en el ámbito urbanístico, con la finalidad de completar de mejor manera los conceptos jurídicos indeterminados que se presentan en la

normativa legal urbanística y de solucionar de forma más certera las denominadas situaciones complejas propias de la gestión del planeamiento urbanístico.

6. A la hora de proceder a la implantación de un sistema de gestión de Ciudad Inteligente es preciso seguir una metodología y planificación común a todo proceso de implantación de la tecnología en las Administraciones Locales. La implicación del personal y de los órganos esenciales de cualquier Administración resulta necesario para culminar adecuadamente cualquier proyecto TIC, y en este sentido, la implantación de un modelo de gestión de Ciudad Inteligente deberá atenerse a una metodología y planificación que permita conseguir los objetivos marcados.

Estos seis retos digitales de la implantación de los modelos de Ciudades Inteligentes deben analizarse cuidadosamente, y al menos, deben tenerse como referencia en el momento en el que nuestros Ayuntamientos se decidan a contratar a empresas para la implantación de modelos de gestión de la ciudad basados en plataformas *Smart City.* Las nuevas modas TIC en la gestión municipal pueden conllevar consecuencias indeseables en cuanto a costes económicos y a adopción de decisiones equivocadas que impliquen que los proyectos no tengan finalmente el retorno de gestión y económico deseado para nuestros Ayuntamientos. El reto digital último al que se enfrentarán nuestros Ayuntamientos que pretendan implantar un modelo de gestión de Ciudad Inteligente no será intentar lograrlo, sino conseguirlo con las cotas más elevadas de eficacia y éxito. Con la idea de ayudar a conseguir este reto se ha elaborado el presente trabajo, que espero que haya servido de ayuda a aquellos que lo hayan podido leer.

CAPÍTULO 44
SMART CITIES, SMART VILLAGES Y ACCIÓN PÚBLICA

MAGDALENA SUÁREZ OJEDA
Profesora Derecho Administrativo
Universidad Complutense de Madrid
Miembro grupo UNE CTN 178 *Smart Cities*

1. LAS CIUDADES INTELIGENTES Y LA INTELIGENCIA APLICADA A LAS CIUDADES

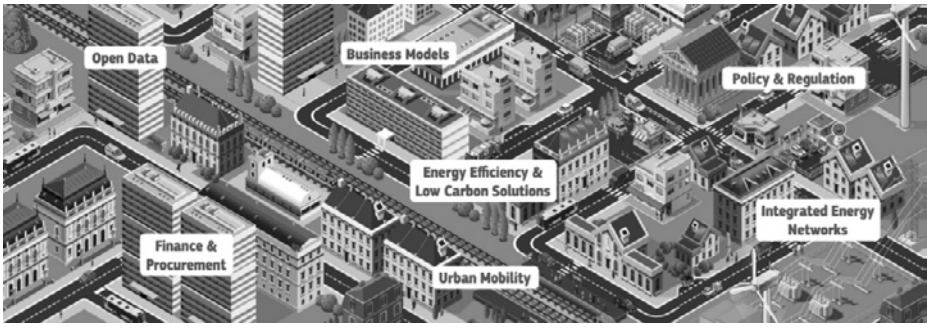
1.1 Concepto de ciudades inteligentes

La discusión sobre cuál debería ser la definición de la ciudad inteligente ha provocado ríos de tinta e intensos debates. La cuestiones eran varias: si una ciudad podía ser inteligente o lo eran verdaderamente sus autoridades y habitantes; si las ciudades no digitalmente adaptadas no podían ser inteligentes; si los diseños de ciudades clásicas (Atenas, Roma, París, Londres…) o las «ciudades ideales» no eran vivos ejemplos de ta-

lento a pesar de haber introducido las nuevas tecnologías, porque obviamente no existían.

Indudablemente todo ello tiene gran sentido y cuanto menos merece una detenida reflexión. Lo que resulta evidente al día de hoy, es que cuando hablamos de *smart cities* nos referimos a un fenómeno que se produce como consecuencia de la revolución tecnológica (1) que un determinado momento tiene su traducción –como no podía ser de otra manera en la ciudad–. Las TICs salen de sus naturales espacios de la gestión de datos e impulso asombroso de los medios de comunicación y con el devenir del tiempo, el perfeccionamiento y desarrollo tecnovlógico comienzan a dar respuestas a la eventos y servicios que tienen lugar en las ciudades.

Entre las muchas definiciones (2), propongo la ofrecida por el CNT 178 «Ciudad inteligente es la visión holística de una ciudad que aplica las TIC para la mejora de la calidad de vida y accesibilidad de sus habitantes y asegura un desarrollo sostenible económico, social y ambiental en mejora permanente. Permite a los ciudadanos interactuar con ella de forma multidisciplinar y se adapta en tiempo real a sus necesidades, de forma eficiente en calidad y costes, ofreciendo datos abiertos, soluciones y servicios orientados a los ciudadanos como personas».



Fuente: http://ec.europa.eu/eip/smartcities/files/eip-ifc-infographic.pdf

(1) Cualquier invento de la humanidad ha tenido su inmediata aplicación en la vida cotidiana, es más desde la época de los grandes inventos, la tensión de mejora de las ciudades ha sido evidente, así sucedió con el alumbrado público, el abastecimiento de agua corriente en las viviendas, los ferrocarriles por poner un ejemplo.

El impacto de la innovación fomenta un atractivo diálogo entre la tradición y la modernidad muy fecundo. *Vid.* Edgerton, D., Innovación y tradición. Historia de la tecnología moderna. Barcelona, Crítica, 2007.

(2) Otra definición cabal es la que proporciona la UIT: «Una ciudad inteligente y sostenible es una ciudad innovadora que utiliza las tecnologías de la información y la comunicación (TIC) y otros medios para mejorar la calidad de vida, la eficiencia de las operaciones, los servicios urbanos y la competitividad, asegurando que responda a las necesidades de las generaciones presentes y futuras respeto a aspectos económicos, sociales, ambientales y culturales».

De esta manera, lo que buscan las ciudades inteligentes es dar una mejor respuesta a las necesidades sociales valiéndose de los nuevos instrumentos tecnológicos, pero no es una categoría absoluta, dado que las urbes siguen teniendo los mismos compromisos medioambientales, históricos, turísticos, etnográficos o cualquier otros que estuvieran presentes en su realidad cotidiana. Por eso, nos encontramos con puntualizaciones terminológicas como las que realiza UN-HABITAT, introduciendo el concepto de resiliencia *(smart and resilient cities),* es decir las urbes que están preparadas para el cambio y son capaces de superar situaciones de crisis o adversidad (tragedias ambientales o extrema violencia).

En todo caso, las tecnologías aplicadas a las ciudades deben cumplir también un papel integrador y generador de lugares comunes de diálogo social. La utilización del espacio y el tiempo de la vida cotidiana puede amplificarse de modo positivo con la utilización de las TICs. Existen ya numerosos ejemplos de ello (app para personas con discapacidad, plataformas think tanks, etc.) (3). Además de servir de palanca a las iniciativas de economía circular y economía participativa.

1.2 **Los retos actuales de las *smart cities***

Sin duda, las *smart cities* han sido en los últimos tiempos uno de los temas de mayor relevancia pública a nivel político (tal vez no divulgativo). En esta ocasión, el sector privado, las administraciones públicas han impulsado un modelo sustentado en tres pilares fundamentales: normalización, industria y gobernanza. Como consecuencia de ello se produjeron varias convocatorias de subvenciones para ciudades inteligentes dentro de la Agenda Digital y las numerosas normas producidas en el seno de UNE (4). Por todo ello, se entiende que España y Dubai representan los dos modelos conceptuales onmicrompresivos de éxito a efectos de *smart cities*. Cuya influencia parece que puede alcanzar mayor desarrollo (5).

---

(3) Lahoz Palacio, C.F., «La influencia de las tecnologías de la comunicación sobre la sociabilidad en los espacios públicos» III Congreso Ciudades Inteligentes, Madrid, Tecmared, 2017, pp. 47-52. Navarro Cano, Nieves. «Ciudades inteligentes inclusivas y accesibles, diseñar para la diversidad» en Smart cities, derecho y técnica para una ciudad más habitable, Reus, Madrid, 2017.

(4) Suárez Ojeda, M. «De las ciudades inteligentes a los territorios inteligentes. Especial referencia a la discapacidad». Tirant lo Blanch, 2018 (en prensa).

(5) «… también se están desarrollando actualmente normas (futuras recomendaciones UIT) –sobre sistemas externos tipo estación, puerto o aeropuertos inteligentes, edificios inteligentes, sistemas rurales e Inteligencia turística–, lo que permitirá desarrollar soluciones de fuerte impacto en las ciudades y abrir nuevos modelos de negocio. En colaboración con el organismo de normalización nacional, UNE, se ha estado en contacto con las principales entidades representativas que están participando en la generación de interfaces y modelos de datos normalizados, como CENELEC (Comité Europeo para la Estandarización Electrotécnica),

Actualmente la prestación de servicios públicos innovadores han tenido que abordar cuestiones tales como:

— Superar el entendimiento de que los servicios no se pueden entender de modo unívoco, sino que hay una relación entre ellos; hubo que transformar pues, el «concepto vertical» en modelo «plataforma».

— Las ciudades se asemejan a organismos vivos, pero también tienen una dimensión unitaria. El Iot, el internet de las cosas, lleva a mirar a los edificios de forma individualizada siendo posible que la información que estos transmitan sea de gran valor para el conjunto de la ciudad. En la que hay puntos emblemáticos (estadios de futbol, aeropuertos, estaciones de metro, grandes almacenes, por poner un ejemplo).

— Como luego veremos, la problemática actual ha pasado de las ciudades inteligentes a los territorios inteligentes.

— Las islas inteligentes plantean singularidades porque son particularmente atractivas y medioambientalmente frágiles.

— Los destinos turísticos inteligentes ha tenido particular impacto dado que el 12% PIB español proviene de ingresos por turismo. Sin lugar a dudas la tensión entre la población estable y la fluctuación de personas entre 20%-40% en determinados períodos no puede atenderse con un sistema ordinario de gestión local.

La implantación de las nuevas fórmulas propuestas por las *smart cities* obligan, como toda situación de cambio, a transformar también estructuras. En nuestro país en la actualidad, y una vez superadas las fases iniciales (6), nos encontramos antes los siguientes retos:

— Adopción de unos sistemas de información común para que los esfuerzos empleados en la implementación de modelos sirviera de modelo dentro de la estrategia de digital y de investigación.

— Alcanzar consenso en la denominación común de las acciones y objetos para facilitar el flujo de datos.

— Utilización de plataformas de servicios abiertas y normalizadas al objeto de propiciar la interoperabilidad entre las mismas.

— Capacidad de gestión de big data y posibilidad de ofrecer servicios de comunicación enriquecida (RCS).

ETSI (European Telecommunications Standards Institute) y otras.» Red.es: https://www--red--es.insuit.net/redes/es/actualidad/magazin-en-red/espa%C3%B1a-logra-el-consenso-internacional-en-la-estandarizaci%C3%B3n-de-la

(6) Conferencia pronunciada por Enrique Martínez Marín. III Congreso Ciudades Inteligentes, Madrid 26-27 de abril 2017.

2. DE LAS CIUDADES INTELIGENTES A LOS TERRITORIOS INTELIGENTES

2.1 **Evolución de las *smart cities***

El urbanismo siempre ha suscitado encendidas polémicas y sin lugar a dudas un fecundo análisis filosófico, científico y cultural. En la actualidad la superación del análisis de las urbes de modo morfológico ha dado paso a la generación de otros paradigmas como las diferencias sociales, la segregación, la etnicidad o la criminalidad, impulsadas en gran medida por la Escuela de Chicago (7). En el momento vigente, las ciudades cobran importancia por sí mismas, y yo porque hay una clara tendencia a adoptar decisiones vinculantes para la ciudadanía desde un ámbito supranacional o internacional; pero también desde un ámbito infranacional (8). Es evidente, que las decisiones de corte regional configuran en gran medida los derechos de la ciudadanía están conformados de modo decisivo por dichas políticas. Pero no es menor el papel que representan los Municipios en la vida de las personas, su devenir diario y la forma de asumir sus necesidades primarias.

En el asunto de las *smart cities* la cuestión parece plantearse de modo estrictamente local; es decir, en principio la implantación de las TICs viene fuertemente determina por: la propia decisión política, la capacidad técnica y económica, el número de habitantes y la efectiva recepción de señal. Es decir, parece que las candidatas perfectas son las capitales de provincia o las ciudades medianas o grandes.

Es evidente, que con el fenómeno de la globalización se ha planteado una verdadera competitividad entre las ciudades, aupado por la elaboración constante de *rankings*.

De este modo, cuando comienza el impulso de las *smart cities* en lo que se está pensado en urbes, en ciudades. Establecimiento particularidades cuando se trata de municipios turísticos.

Más allá de estas inicitivas las *smart cities* obtienen el impulso gubernamental cuando se incluyen como estrategia dentro de la Agenda Digital y se aprueba el Plan Nacional de Ciudades Inteligentes y se comienzan a subvencionar proyectos para ciudades con determinadas características

(7) Paddison, R. and McCann, E. «Introduction: Encountering the city-Multiple Perspectives on Urban Social Change» pp. 3-14. Cities & Social Change. Encounters with contemporary urbanism. Sage publications, London, 2014.

(8) Harding, A. and Blockland, T., Urban theory. A critical introduction to power, cities and urbanism in the 21st century «From the urban crisis to the «triumph of the city» Sage publications, London, 2014. There is a growing sense, however, that the course of history has moved against nations and nationally based systems of economic and social management and towards arrangements in which what happens, economically and politically, at both supranational and subnational level is assuming greater importance. Whilst there is broad consensus about the growing importance of supranational institutions and decision-making, though, the debate focusing upon the subnational level has been more speculative», p. 57.

de adecuación, por criterios de población o desarrollo tecnológico a través de la entidad pública empresarial Red.es.

Pero ahora mismo las políticas van más allá, detectada la situación de que muchas zonas jamás alcanzarán las ratios suficientes para implementar de modo satisfactorio unas políticas sustentadas en un entorno digital. Por ello el Ministerio de Energía, Turismo y Agenda Digital ha aprobado el Plan Nacional de Territorios Inteligentes, cuyas líneas estratégicas son las siguientes (9):

— Acciones territoriales: integrado por seis áreas: objetos internos de ciudades (edificios, estaciones, puertos y aeropuertos), 5G, Laboratorio Virtual de Interoperabilidad, Territorios Rurales Inteligentes, Turismo Inteligente y Servicios Públicos 4.0 en plataformas de ciudad y mundo rural.

— Acciones de soporte: engloba las acciones facilitadoras de las acciones territoriales: impulso de la Normalización, actuaciones de carácter internacional, gobernanza del Plan Nacional, comunicación, difusión, capacitación y formación.

— Acciones complementarias: Iot para prestación de servicios públicos en Territorios Inteligentes y Movilidad.

Fuente: plan nacional territorios inteligentes 2018

(9) Plan Nacional de Territorios Inteligentes: http://www.agendadigital.gob.es/agenda-digital/noticias/Documents/PNTI/plan-nacional-territorios-inteligentes.pdf

2.2 **Necesidad de encontrar nuevos planteamientos para el mundo rural**

Entre las cuestiones que suscitan mayor preocupación e interés en el momento actual es ofrecer una solución para conseguir que el mundo rural consiga entrar en el mundo digital.

En ocasiones podemos no ser del todo conscientes del peso del mundo rural en el panorama nacional. La situación es la siguiente:

«Utilizando técnicas derivadas de los sistemas de información geográfica (SIG) y en consonancia con la literatura europea reciente, se defiende la necesidad de integrar al menos otras dos dimensiones: la intensidad de la intervención humana sobre el territorio –medida por el tipo de cobertura del suelo prevaleciente– y el grado de accesibilidad desde los municipios rurales a las ciudades.

El resultado es una propuesta tipológica que considera seis tipos distintos de municipios: municipios urbanos e intermedios abiertos y cerrados (según la cobertura del suelo), y municipios rurales accesibles y remotos. La clasificación en función de los usos del suelo no es discriminatoria para los municipios rurales, del mismo modo que, por definición, la dimensión de accesibilidad no afecta a los municipios urbanos.

Los resultados indican que el 77,6% de los municipios son rurales y abiertos, mientras que solo un 2% son urbanos y cerrados, y el 58% de los municipios rurales pueden considerarse accesibles. Los municipios rurales remotos representan el restante 42,2% de los municipios rurales, albergando el 30% de la población total de estos (alrededor de dos millones de personas). La duración del viaje desde ellos a la ciudad más próxima es de 66 minutos. Se ha comprobado que existe un nivel apreciable de heterogeneidad a escala provincial en cuanto al carácter más o menos remoto de las correspondientes áreas rurales.» (10)

Además de esta significativa importancia las medidas que se adopten deberán estar en sintonía con la Ley 45/2007, de 13 de diciembre, para el desarrollo sostenible del medio rural (11). En este entorno se plantean

---

(10) Reig Martínez, Ernest, Guerlich Gisbert, Francisco J., Cantarino Martín, Isidro, «Informe Delimitación de áreas rurales y urbanas a nivel local, demografía, coberturas de suelo y accesibilidad. Informe BBVA», 2016, pp. 97 y ss.

(11) «Artículo 10. Delimitación y calificación de zonas rurales.

1. Para la aplicación del Programa de Desarrollo Rural Sostenible, las Comunidades Autónomas llevarán a cabo la delimitación y calificación de las zonas rurales definidas en el artículo 3.b) en su respectivo territorio, de acuerdo con los siguientes tipos:

a) Zonas rurales a revitalizar: aquellas con escasa densidad de población, elevada significación de la actividad agraria, bajos niveles de renta y un importante aislamiento geográfico o dificultades de vertebración territorial.

diversos retos, entre los que se encuentra alcanzar unas pautas metodológicas adecuadas (12), sustentadas en:

— Establecer un sistema de medición basados en los principios de eficacia, interoperatividad y transferibilidad.

— Determinar uno «mapas de empatía» para conocer las necesidades reales.

— Determinar estrategias en términos de sostenibilidad.

Es muy importante tener en cuanta que el medio rural no es susceptible de aplicación de plano las mismas pautas que las establecidas para las *smart cities.* Las comunidades rurales, sufren –en ocasiones de modo severo– la despoblación y envejecimiento de sus habitantes. Por tanto, el establecimiento de los servicios públicos 4.0 exige forma personalizada por parte de la Administración, acercando la prestación de dichos servicios públicos, en vez de trasladar a muchas personas se desplazan los servicios, dado que las administraciones públicas conocer las circunstancias de esta población porque cuenta con numerosos datos administrativos.

El mundo rural necesita obtener de la aplicación de las TICs a su territorio: posibilidad de fijar la población, atraer el talento y generar oportunidades sin perder la identidad.

El éxito de la política sobre territorios inteligentes parte de un factor determinante, la posibilidad de acceso a banda ancha y la recepción de señal, que como puede verse desciende de modo notorio cuando nos encontramos en lugar de poca densidad de población o muy alejadas de un lugar donde la cobertura de red sea aceptable.

---

b) Zonas rurales intermedias: aquellas de baja o media densidad de población, con un empleo diversificado entre el sector primario, secundario y terciario, bajos o medios niveles de renta y distantes del área directa de influencia de los grandes núcleos urbanos.

c) Zonas rurales periurbanas: aquellas de población creciente, con predominio del empleo en el sector terciario, niveles medios o altos de renta y situadas en el entorno de las áreas urbanas o áreas densamente pobladas» Artículo 10. Delimitación y calificación de zonas rurales. 1. Para la aplicación del Programa de Desarrollo Rural Sostenible, las Comunidades Autónomas llevarán a cabo la delimitación y calificación de las zonas rurales definidas en el artículo 3 b) en su respectivo territorio, de acuerdo con los siguientes tipos: a) Zonas rurales a revitalizar: aquellas con escasa densidad de población, elevada significación de la actividad agraria, bajos niveles de renta y un importante aislamiento geográfico o dificultades de vertebración territorial. b) Zonas rurales intermedias: aquellas de baja o media densidad de población, con un empleo diversificado entre el sector primario, secundario y terciario, bajos o medios niveles de renta y distantes del área directa de influencia de los grandes núcleos urbanos. c) Zonas rurales periurbanas: aquellas de población creciente, con predominio del empleo en el sector terciario, niveles medios o altos de renta y situadas en el entorno de las áreas urbanas o áreas densamente pobladas.

(12) Chapa Monteagudo, C., Casales Moreno, J.A., *et alii*, «La experiencia de los redactores de la norma española de territorios rurales inteligentes en el seno del CTN 178» III Congreso Ciudades Inteligentes, Madrid, Tecmared, 2017 pp. 709-715.

Rango de cobertura	Nº Entidades	Nº de habitantes totales	Nº hogares totales	Hogares cubiertos ADSL ≥ 2 Mbps
90≤x≤100	13.607	35.679.553	13.851.958	13.380.453
80≤x<90	3.959	7.035.637	2.658.986	2.287.332
70≤x<80	1.589	1.430.202	534.008	402.081
60≤x<70	1.308	468.505	175.828	113.711
50≤x<60	1.343	233.385	88.440	48.553
40≤x<50	625	133.238	50.780	23.125
30≤x<40	268	57.584	21.757	7.631
20≤x<30	75	20.462	7.668	1.857
10≤x<20	81	22.690	8.580	1.420
0≤x<10	38.833	1.690.084	653.889	455
Totales	**61.688**	**46.771.341**	**18.051.894**	**16.266.618**

Tabla 9.- Distribución de las entidades singulares por rango de cobertura de ADSL ≥ 2 Mbps en 2016

Fuente: Informe Banda Ancha en España 2016. Secretaria de Estado para la Sociedad de la Información y la Agenda Digital

Indudable esta cuestión comporta la necesidad de aplicar fondos públicos, esperemos que las apuestas de las políticas públicas vayan en este sentido y los nuevos satélites (particularmente el Hispasat 30 W6) puedan satisfacer las demandas de banda ancha en lugares remotos. Junto con ello resulta imperioso establecer unas pautas y criterios adecuados de asistencia y formación en el mundo rural para afrontar estos retos. Parece, no obstante, que hay rayos de esperanza; un ejemplo válido aplicado hasta la fecha son las comunidades digitales de Castilla y León cuyo eje de acción son los convenios con entidades municipales y Diputaciones Provinciales (13).

3. LA UNIÓN EUROPEA: LAS POLÍTICAS TERRITORIALES Y DE COHESIÓN Y LA POLÍTICA MEDIOAMBIENTAL

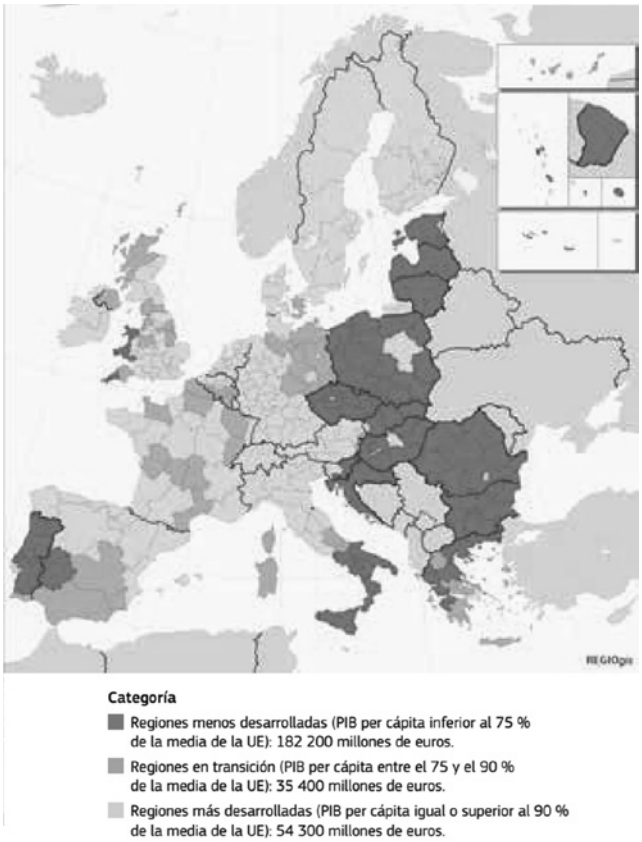
Es muy previsible que la implantación de las *smart village* no tengan un final feliz si no se acompañan de una decisiva toma de posición y aplicación de energías a intentar paliar las diferencias territoriales, económicas y sociales, en el sentido establecido en el Tratado de Lisboa (arts. 174 y ss.), cuyo tenor literal es el siguiente:

> «A fin de promover un desarrollo armonioso del conjunto de la Unión, ésta desarrollará y proseguirá su acción encaminada a reforzar su cohesión económica, social y territorial.
> La Unión se propondrá, en particular, reducir las diferencias entre los niveles de desarrollo de las diversas regiones y el retraso de las regiones menos favorecidas.

(13) Comunidades Digitales de Castilla y León: https://rmd.jcyl.es/web/jcyl/MunicipiosDigitales/es/Plantilla100/1274785626082/_/_/_

Entre las regiones afectadas se prestará especial atención a las zonas rurales, a las zonas afectadas por una transición industrial y a las regiones que padecen desventajas naturales o demográficas graves y permanentes como, por ejemplo, las regiones más septentrionales con una escasa densidad de población y las regiones insulares, transfronterizas y de montaña.»

Por tanto las políticas de la UE se han centrado también en paliar las honda diversidad de renta que se da dentro del territorio de la Unión, ello obedece a diferentes razones, como: mejorar la coordinación de las diferentes políticas, avanzar en el proceso de integración y potenciar el desarrollo de regiones deprimidas al objeto de consolidar y mejorar el funcionamiento del mercado interior (14).



Fuente: Política regional europea https://europa.eu/european-union/topics/regional-policy_es

(14) Bonete Perales, T. «Políticas de cohesión, social y territorial» en Tratado de Derecho y Políticas de la Unión Europea. Tomo VII. Otras políticas horizontales y sectoriales. Maíllo González-Orús y Becerril Atienza, B., Thomsom Reuters, Aranzadi, Cizur Menor, 2015, pp 189-244.

Como puede verse en la imagen las diferencias de renta entre las diversas regiones es notable, por lo que lógicamente la implantación de los territorios inteligentes de modo satisfactorio será más costoso en términos generales en una parte significativa de la Unión Europea.

En el momento actual, se está estudiando la fórmula de poder desplegar políticas públicas adecuadas actuando en los diversos niveles territoriales. Uno de los criterios que se puede seguir es la delimitación empleada por EUROSTAR en la define los territorios de la UE en categorías NUTS 2 (coincidiría con Comunidades Autónomas) y NUTS 3 (Provincias) (15).

Veremos, pues, como se cohonesta esta política territorial con las *smart village,* hasta ahora, el FSE (Fondo Social Europeo de Desarrollo Regional) ha sido un financiador relevante en las subvenciones que España a destinado a la implantación y mejora de las *smart cities.*

Tenemos que tener en cuenta que estas ciudades inteligentes serán en todo caso, unas *green cities,* por lógica imperativa de las políticas comunitarias europeas que estable como objetivos principales del desarrollo urbano que las iniciativas mantengan principios de sostenibilidad ambiental (16), dirigida a tres puntos estratégicos:

1. Movilidad Urbana Sostenible, a través de la utilización de energías alternativas, transporte público, logística eficiente y una correcta planificación.
2. Distritos sostenibles y entorno construido: mejorando la eficiencia energética de los edificios y distritos, aumentando la proporción de fuentes de energía renovables utilizadas y la habitabilidad de las comunidades.
3. Infraestructuras integradas y procesos en Energía, TIC y Transporte, conectando activos de infraestructura para mejorar la eficiencia y la sostenibilidad de las ciudades.

4. EL IMPULSO DIGITAL A NIVEL NACIONAL E INTERNACIONAL

Como ya se ha apuntado, la implantación y uso de la tecnología resulta ineludible si se trata de ciudades inteligentes. No es noticia, que España es líder en el impulso de los sistemas de normalización a través de UNE (17),

(15) Eurostar:

http://ec.europa.eu/eurostat/statistics-explained/index.php/Urban-rural_typology#The_OECD_methodology

(16) Suárez Ojeda, M., «Smart cities: un nuevo reto para el Derecho Público» en Smart cities, derecho y técnica para una ciudad más habitable, Reus, Madrid, 2017, pp. 73-91.

(17) «Ciudades inteligentes. El antiguo Ministerio de Industria, Energía y Turismo puso en marcha en 2015 el Plan Nacional de Ciudades Inteligentes, como parte de la Agenda Digital para España. Lograr que las ciudades y lo asentamientos urbanos sean inclusivos, seguros y sostenibles es uno de los 17 objetivos de desarrollo sostenible de la Agenda 2030 de Naciones Unidas. Las smart cities contribuyen en gran medida a conseguir este objetivo, al permitir optimizar recursos, disminuir emisiones de gases de efecto invernadero y mejorar la movilidad y la vida de las personas.

en la actualidad hay aprobadas 23 normas de todos los ámbitos imaginables que dan respuestas a las diversas necesidades de implantación de sistemas inteligentes en las ciudades (18). Estas normas no son de obligado cumplimiento y la propuesta puede venir del sector privado. En este sentido el CTN 178 de ciudades inteligentes ha sido ciertamente trabajador y vivaz. Este buen hacer ha tenido su eco en el liderazgo nacional a la hora de proponer líneas de actuación en los organismos internacionales.

Recientemente la UIT ha aprobado una serie de documentos entre los que destaca la generación de los KPI, sustentados en tres grandes bloques de análisis: dimensión ambiental, dimensión económica y dimensión social y cultural.

2. Key performance indicators numbering convention

Table 4 – KPI numbering convention

XX -		X(X):		X(X):		Number	C or A
Dimension		Sub-Dimension		Category		1, 2, 3, etc.	C: Core A: Advanced
EC	Economy	E	Energy	AQ	Air Quality		
EN	Environment	EH	Education, Health and Culture	B	Buildings		
SC	Society and Culture	EN	Environment	C	Culture		
		I	Infrastructure	D	Drainage		
		ICT	ICT	E	Energy		
		P	Productivity	ED	Education		
		SH	Safety, Housing and Social Inclusion	EM	Employment		
				EQ	Environmental Quality		
				ES	Electricity Supply		
				FS	Food Security		
				H	Health		
				HO	Housing		
				IN	Innovation		
				ICT	ICT Infrastructure		
				PS	Public Sector		
				PSN	Public Spaces and Nature		
				SA	Safety		
				SI	Social Inclusion		
				T	Transport		
				UP	Urban Planning		
				WA	Waste		
				WS	Water and Sanitation		

Fuente: UIT: https://www.itu.int/en/publications/Documents/tsb/2017-U4SSC-Collection-Methodology/index.html#p=18

La complejidad del entorno urbano exige, para la construcción de ciudades inteligentes, abiertas y accesibles, entre otros factores, un cuerpo normativo sólido. Por este motivo, en abril de 2016, se inició una colaboración entre la entonces Secretaría de Estado de Telecomunicaciones y la Sociedad de la Información, AENOR y la Unión Internacional de las Telecomunicaciones, que ha permitido a España impulsar el desarrollo de una veintena de normas que contribuirán a poner en marcha las recomendaciones de estandarización que publique la UIT. El resultado de todos estos esfuerzos se ha materializado en el reconocimiento del modelo español como referencia internacional en el campo de las ciudades inteligentes, tal y como señala el Informe Anual de la Comisión de Banda Ancha para el Desarrollo Sostenible de la ONU», p. 111.

http://www.minetad.gob.es/es-ES/IndicadoresyEstadisticas/Informes/InformesMITYC/Informe%20Anual%202016.%20S. G.%20de%20Estudios,%20An%C3%A1lisis%20y%20Planes%20de%20Actuaci%C3%B3n/Informe%20Anual%20(SG%20Estudios).pdf

(18) Marcos Paramio, T., «El modelo de normalización español de Ciudades Inteligentes (UNE, CTN 178) y su impacto internacional» https://www.esmartcity.es/comunicaciones/comunicacion-modelo-normalizacion-espanol-ciudades-inteligentes

Más recientemente, España ha sido un referente en la adopción de las Recomendaciones UIT: ITU-T Y.4200: Requerimientos de interoperabilidad para plataformas de Ciudades Inteligentes, y la ITU-T Y.4201: Requerimientos de alto nivel y marco de referencia de las Plataformas de Ciudades Inteligentes, basadas en la Norma UNE 178104 «Ciudades Inteligentes. Infraestructuras. Sistemas integrales de gestión de la Ciudad Inteligente» (19).

CONCLUSIONES

— En España las administraciones públicas, el sector privado y la normalización han sido impulsores de las *smart cities* en un buen escenario de sintonía y colaboración. Lo que ha llevado a la aprobación de numerosas normas UNE que han sido referente mundial y fuente de inspiración de varias recomendaciones publicadas en el seno de la UIT.

— La Agenda Digital cumple un papel importante en el impulso de las *smart cities* y ahora de los territorios inteligentes

— Quedan numerosos retos que atender; aplicación de Iot, aplicación de TICs en las zonas rurales, destinos rurales inteligentes e islas inteligentes principalmente.

(19) AENOR: http://www.aenor.com/revista/pdf/ene18/42ene18.pdf

CAPÍTULO 45

TURISMO SOSTENIBLE E INTELIGENTE EN EL MUNDO DIGITAL (1)

ALEJANDRO CORRAL SASTRE
Profesor Colaborador Doctor de Derecho Administrativo
Universidad San Pablo-CEU de Madrid

(1) El presente trabajo se inscribe en el Proyecto de Investigación sobre Protección de Datos, Seguridad e Innovación: Retos en un mundo global tras el Reglamento Europeo de Protección de Datos, Ref. DER2016-79819-R, del programa I+D+i del Ministerio de Economía y Competitividad del que es investigador principal el Dr. D. JOSÉ LUIS PIÑAR MAÑAS: www.privacidadyacceso.com.

1. INTRODUCCIÓN

En este trabajo se pretende poner de manifiesto la importancia de implementar un modelo turístico basado en las TIC en orden a avanzar hacia un modelo de turismo más sostenible (2), centrado no solo en el incremento de la demanda, sino también en el aumento de la calidad de los servicios que se prestan y, por consiguiente, de la rentabilidad del sector, sin que los destinos se vean sometidos a un excesivo estrés ambiental o social.

No se debe olvidar que el turismo es un sector económico especialmente abonado para el desarrollo de las TIC y de la economía digital. De hecho, la adopción de internet y el crecimiento del comercio electrónico han sido más rápidos en el sector turístico (3). Así, las tecnologías 2.0, las redes sociales y el uso de dispositivos móviles han tenido un impacto muy importante en el turismo en los últimos años.

Pero no debemos quedarnos ahí. Si se quiere mantener los niveles de competitividad turística hay que dar satisfacción a los requerimientos de los nuevos usuarios de servicios turísticos, mucho más informados y más exigentes, es decir, lo que ha venido en llamarse el viajero (o turista) digital.

No obstante, en este sentido, la transformación del modelo turístico, la conversión de destinos turísticos en los denominados «destinos inteligentes», no debe basarse exclusivamente en la utilización de tecnologías

(2) Fullana, P. y Ayuso, S., *Turismo sostenible*, Ed. Rubes, Barcelona, 2002, p. 30, «el desarrollo del turismo sostenible que satisface las necesidades de los turistas y regiones anfitrionas presentes al mismo tiempo que protege y mejora las oportunidades de futuro. Está enfocado hacia una gestión de todos los recursos de tal forma que satisfagan todas las necesidades económicas sociales y estéticas al tiempo que respeta la integridad cultural, los procesos ecológicos esenciales, la diversidad biológica y los sistemas de apoyo a la vida».

(3) *Smart Destination*, SEGITTUR, 2015, p. 19.

avanzadas que permitan una mayor conectividad entre empresas y usuarios, sino que la transformación debe ser más profunda, cultural si se quiere, implicando también a otros agentes protagonistas como pueden ser los residentes en esos destinos o las administraciones públicas competentes. Solo así, con la participación de todos en el proceso, podremos hablar de un turismo sostenible. Y es que este es uno de los principales objetivos de la intervención del Derecho y de la Administración en el sector, alcanzar un nivel de desarrollo turístico adecuado, es decir, rentable, pero sin olvidar que un crecimiento descontrolado puede generar importantes daños al medio ambiente y social que, a la postre, redundan de forma muy negativa en el propio sector (4).

2. EL TURISMO EN ESPAÑA: UN SECTOR ESTRATÉGICO PARA LA ECONOMÍA

Que el turismo es un sector muy relevante, esencial más bien, para la economía de nuestro país no es nada nuevo. Al contrario, ya nos hemos acostumbrado a que las informaciones económicas señalen la importancia de este sector para la buena marcha de la economía.

Los datos publicados no hacen otra cosa que confirmar esta idea. Así, según la Cuenta Satélite del Turismo en España (CSTE) (5) publicada por el Instituto Nacional de Estadística, el sector aporta un 11,2 por ciento del Producto Interior Bruto (PIB), lo que en euros se traduce en 125.529 millones, una cifra nada desdeñable. Por otro lado, la aportación al empleo supone un 13 por ciento del total, es decir, 2,56 millones de puestos de trabajo (6).

---

(4) A esta paradoja parece referirse Fernández Rodríguez, C., en «El valor de lo intangible y armonizado en la calidad turística europea», *Revista de Derecho de la Unión Europea*, núm. 24, 2013, p. 343, cuando manifiesta que «cuando se habla de turismo y desarrollo sostenible se están relacionando dos fenómenos que, en sí mismos, pueden resultar a primera vista, contradictorios: un fenómeno que desde el punto de vista numérico y de calidad puede resultar deteriorante del medio en que se desenvuelve y otro fenómeno que persigue precisamente el efecto inverso: que se mantenga el desarrollo y el medio en un punto tal de equilibrio que exista una perfecta interactuación sostenida en el tiempo y para el disfrute de generaciones futuras».

(5) La Cuenta Satélite del Turismo de España (CSTE) es una estadística de síntesis compuesta por un conjunto de cuentas y tablas, basadas en los principios metodológicos de la contabilidad nacional, y que presenta los distintos parámetros económicos del turismo en España, para una fecha de referencia dada. La base actual es el año 2010. Básicamente comprende tres tipos de elementos:

– Cuentas y tablas de oferta, en las que se trata de caracterizar la estructura de producción y costes de las empresas turísticas.

– Tablas de demanda, en las que se trata de caracterizar, desde el punto de vista económico, los diferentes tipos de turistas, el turismo nacional frente al internacional, el tipo de bienes y servicios demandados, etc.

– Tablas que interrelacionan la oferta con la demanda, que permiten obtener unas mediciones integradas de la aportación del turismo a la economía a través de variables macro como el PIB, la producción o el empleo.

(6) Datos de año 2016, publicados en www.ine.es el 18 de diciembre de 2017.

Por tanto, a la vista de estos datos, y de la posición que ocupa España como destino turístico mundial, debemos mantener este alto nivel de competitividad que pasa, sin duda, por apostar por un cambio de las fórmulas de gestión turística que permita afrontar los nuevos retos con mayor eficacia. En este sentido, la utilización de las TIC se convierte en un elemento estratégico para alcanzar ese objetivo.

Pero no solo debemos tener presente esta dimensión económica, que es muy importante. La utilización de las TIC de forma global no solo debe destinarse a incrementar la oferta y, por tanto, el número de visitantes. Al contrario, puede permitir, por ejemplo, conocer en tiempo real el número de turistas para saber si se ha sobrepasado la capacidad de carga (7) del destino y así, ayudar a adoptar las medidas necesarias para proteger el medio ambiente. En definitiva, puede coadyuvar a alcanzar la sostenibilidad del sector.

El concepto de turismo inteligente que se va a utilizar en este trabajo tiene presente esta idea, es decir, la utilización de las TIC en el sector no solo para incrementar la oferta, sino para gestionar de forma global el destino turístico, mejorar la calidad del producto y crecer de forma sostenible.

3. EL TURISMO INTELIGENTE: HACIA UN TURISMO MÁS SOSTENIBLE

Cuando utilizamos el adjetivo inteligente para referirnos a un sustantivo como ciudad o turismo, debemos intentar aclarar, con carácter previo, a que nos estamos refiriendo. Desde luego, parece que podemos hablar del uso de TIC, no cabe duda, pero para ello ya se ha venido utilizando otro adjetivo que parecía referirse claramente a estas tecnologías: «digital». Así, se ha venido hablando con normalidad de turismo digital o economía digital, y de hecho todavía suele hacerse. ¿Qué ha cambiado, entonces, para utilizar ahora el adjetivo «inteligente»?

Bien, parece que ahora, al referirnos al turismo o a una ciudad como inteligentes, estamos indicando que es algo más que el mero uso de las TIC (8), es decir, que estas aportan un valor que supone una transforma-

(7) Sobre el concepto de capacidad de carga, O`Reilly, A. M., «*Tourism carrying capacity: concept and issues*», *Tourist Management*, vol. 7, 1986, pp., 254-258. Salom Parets, A., «Las limitaciones al crecimiento poblacional y espacial establecidas por la normativa territorial y urbanística», INAP, 2011, pp. 309 y ss. García Saura, P. J., *Desarrollo sostenible y Turismo. Análisis del régimen jurídico medioambiental de la legislación turística española*, Aranzadi, 2007, p. 140, «Es necesario establecer la capacidad de carga para determinar el límite de turistas compatible con una oferta sostenible y acometer la ordenación turística en función de esta variable».

(8) Debemos tener en cuenta, en este sentido, que estas tecnologías están en constante evolución y transformación. Piénsese en este sentido, en el Internet de las Cosas o la propia Inteligencia Artificial, que tienen un potencial que todavía, según estimo, solo somos capaces de intuir.

ción total del sustantivo, un cambio estructural. Y esto es, precisamente, lo que está ocurriendo en el turismo.

Como ya se ha indicado más arriba, el sector turístico ha aprovechado, con especial rendimiento, el uso de estas tecnologías. Las empresas turísticas han sido capaces de transformar, con relativa facilidad, sus modelos de negocio. La adaptación a lo digital ha sido asombrosa. Desde hace ya varios años, es completamente normal reservar un viaje combinado, un billete de avión o una habitación de hotel a través de internet.

Pero esa transformación digital ha beneficiado especialmente a las empresas turísticas y a los consumidores de sus servicios. Se han ajustado los precios y se ha incrementado la demanda. Además, han nacido nuevos modelos de negocio bajo el paraguas de la economía digital: la economía colaborativa, que en el sector turístico ha tenido una especial incidencia. De hecho, si analizamos con detenimiento esta transformación digital, podemos llegar a la conclusión de que el uso de las TIC, que ha facilitado el aumento del número de turistas en algunas zonas de España, está detrás del estrés ambiental y social de algunos destinos concretos. Por consiguiente, el uso de estas tecnologías no ha coadyuvado, precisamente, a alcanzar el objetivo de sostenibilidad que se encuentra en la mayoría de las normas turísticas autonómicas en nuestro país. Tampoco ha ayudado la liberalización a la que ha sido sometido el sector en los últimos años, que ha permitido el incremento de la oferta y la demanda sin un control tan riguroso como el que ha sido tradicional en España (9).

Pues bien, la utilización de las TIC no puede quedarse solo en eso, es decir, en incrementar la oferta y la demanda, sino que debe ser un catalizador para alcanzar un desarrollo turístico sostenible. Un desarrollo del turismo que pase por prever y evitar el deterioro del medio ambiente, por impulsar la participación de visitantes y residentes en la toma de decisiones, por lograr más eficiencia en el uso energético, o por mejorar la movilidad y la integración de infraestructuras, por poner solo algunos ejemplos. En este escenario, que es el que se pretende, sí podremos hablar de turismo inteligente como un concepto amplio, es decir, como algo más que el mero uso de las tecnologías.

(9) La transformación digital de las empresas no ha ido en paralelo al de las administraciones públicas que tiene la obligación de supervisar su actividad (en el inicio y durante el ejercicio de las mismas). Así, normas como la Directiva de Servicios o la Ley 20/2013, de 9 de diciembre, de Garantía de la Unidad de Mercado, han supuesto un cambio enorme en la manera de supervisar la actividad turística por parte de las administraciones competentes, ya que han generalizado el control posterior por medio de declaraciones responsables y comunicaciones previas en perjuicio de las autorizaciones. Véase Corral Sastre, A., *La liberalización del sector turístico ¿Hacia un modelo de turismo sostenible?*, Reus, 2017.

3.1 **El desarrollo de las ciudades inteligentes como paso previo necesario al desarrollo del turismo inteligente**

Según estimo, uno de los principales logros alcanzados por el uso adecuado de las TIC, desde un punto de vista social, es lo que se ha venido denominando como «ciudad inteligente». Pese a ser un concepto un tanto impreciso, podemos definir la ciudad inteligente, siguiendo al profesor José Luis Piñar Mañas, como «aquella que se vale de la innovación tecnológica para ofrecer un entorno más habitable a las personas» (10). Asimismo, el Grupo Técnico de normalización 128 de AENOR (AEN/CTN 178/SC2/GT1 N 003 la define como: «Ciudad Inteligente (Smart City) es la visión holística de una ciudad que aplica las TIC para la mejora de la calidad de vida y la accesibilidad de sus habitantes y asegura un desarrollo sostenible económico, social y ambiental en mejora permanente. Una ciudad inteligente, permite a los ciudadanos interactuar con ella de forma multidisciplinar y se adapta en tiempo real a sus necesidades, de forma eficiente en calidad y costes, ofreciendo datos abiertos, soluciones y servicios orientados a los ciudadanos como personas, para resolver los efectos del crecimiento de las ciudades, en ámbitos públicos y privados, a través de la integración innovadora de infraestructuras con sistemas de gestión inteligente».

De estas definiciones cabe resaltar, según entiendo, una idea que me parece esencial: el uso de las TIC y de los avances tecnológicos para mejorar la calidad de vida de los ciudadanos y lograr un desarrollo sostenible de las ciudades. Desde luego que una ciudad necesita un adecuado tejido empresarial y económico para poder alcanzar estos objetivos, pero el enfoque se centra, fundamentalmente, en los ciudadanos (11).

Este es un buen punto de partida para lo que posteriormente se definirá como Destino turístico inteligente. La idea que sustente este concepto, en mi opinión, debe ser la misma, es decir, utilizar los avances tecnológicos para lograr un desarrollo turístico sostenible, centrado en la calidad de los servicios prestados a los turistas, pero sin olvidar otros intereses que resultan esenciales para el propio desarrollo del turismo, como la protección del medio ambiente y el respeto a la cultura e identidad locales y a sus residentes, entre otros (12).

---

(10) Piñar Mañas, J. L., «Derecho, técnica e innovación en las llamadas ciudades inteligentes», en *Smart Cities. Derecho y técnica para una ciudad más habitable*, Piñar Mañas, J. L. (Dir.), Suárez Ojeda. M (Coord.), Reus, 2017, p. 18.

(11) Cantó López, M.ª T., «Administración Pública y participación activa del ciudadano en la gestión de la ciudad», en *Smart Cities. Derecho y técnica para una ciudad más habitable op. cit.*, p. 39.

(12) Sobre la importancia de las personas en el desarrollo de ciudades inteligentes y destinos turísticos inteligentes, véase, Gómez Oliva A.; Server Gómez, M.; Jara, A. J.,; Parra-Meroño, M.ª C., «Turismo inteligente y patrimonio cultural: un sector a explorar en el desarrollo de las Smart Cities», *International Journal of Scientific Management and Tourism*, núm. 3, 2017, p. 394, «Las ciudades aumentan su población progresivamente y por ello el ritmo de vida en ellas se acelera. La necesidad de interacción entre las personas y los diferentes sectores de la ciudad crece y con

No obstante, debe señalarse que el hecho de que los destinos turísticos inteligentes se basen en el desarrollo de las ciudades inteligentes, no implica que tengan que implementarse en los mismos espacios ni compartir objetivos (13). La ciudad inteligente implica el uso de tecnologías para incrementar el nivel de vida de sus residentes; el destino turístico inteligente, por su parte, centra sus objetivos en los turistas, sin obviar los residentes, por supuesto, pero con una finalidad diferente. En este sentido son conceptos próximos pero con líneas definitorias distintas (14).

3.2 **Los destinos turísticos inteligentes**

Teniendo en cuenta lo manifestado en el epígrafe anterior, el concepto de destino turístico inteligente se basa en los avances de las TIC aplicadas a un territorio determinado y al sector turístico, pero de manera que facilite la toma de decisiones o, incluso, aplicando sistemas de inteligencia artificial, sea capaz de tomarlas por sí mismo. Así, una de las principales características de un destino turístico inteligente es la capacidad para generar inteligencia, es decir: «que sus entes gestores (que pueden ser, repito, sistemas de inteligencia artificial) deben ser capaces de obtener datos en tiempo real, analizarlos y tomar decisiones que les permitan ser más eficientes en la gestión integral del destino: en su promoción y comercialización, en la creación de experiencias únicas y personalizadas para el turista, en la atención a los residentes, en el impulso de un entorno de sostenibilidad, etc.» (15).

En este sentido, el destino turístico inteligente supone ir más allá de la mera adquisición y aplicación de las más avanzadas tecnologías, implica un cambio en todos los niveles y los agentes intervinientes, es decir, «no se trata de hacer lo mismo con nuevas aplicaciones tecnológicas si no de revolucionar la gestión turística de acuerdo con las posibilidades tecnoló-

---

ello aumenta el capital social e intelectual de la población. Esto hace que una Smart City, haciendo uso de tecnologías pioneras, necesite de un núcleo basado en las personas en el que interactúen la educación, la cultura y el comercio. Este factor ha sido el menos desarrollado a pesar de que cualquier cambio o mejora en la infraestructura de una ciudad debe basarse en las comunidades y personas. La transformación de una ciudad en inteligente debe tener como objetivo la mejora de la calidad de vida de los individuos que hacen uso de ella».

(13) Esta idea se deduce de *Big Data, retos y oportunidades para el turismo*, Instituto Valenciano de Tecnologías Turísticas, Agencia Valenciana de Turismo, 2015, pp. 17 a 19.

(14) En este sentido se manifiesta el trabajo *Destinos Turísticos Inteligentes. Manual Operativo para la configuración de Destinos Turísticos Inteligentes*, Agencia Valenciana del Turismo, 2015, p. 11, al manifestar que «El origen de destino turístico inteligente no puede asociarse exclusivamente a la aplicación del paradigma Smart City a los destinos turísticos. Una serie de cambios estructurales en el sector turístico justifican la necesidad de nuevos enfoques en la gestión de los destinos turísticos, una necesidad que confluye con la consolidación del paradigma Smart City y que convierte al destino turístico inteligente en una referencia para la gestión turística.»

(15) *Smart Destination*, *op. cit.*, pp. 204 y 205.

gicas y la capacidad de actuación local (16), y ello con el objetivo de alcanzar un desarrollo turístico sostenible basado en la calidad.

En los siguientes epígrafes, se intentará poner de manifiesto como los avances tecnológicos más vanguardistas pueden coadyuvar a alcanzar el objetivo de un destino turístico inteligente basado en un crecimiento razonable. Así, avances como el *big data*, el Internet de las Cosas, el *cloud computing*, la inteligencia artificial o *blockchain*, solo por señalar los más importantes, tienen un papel determinante en la configuración de destinos turísticos inteligentes.

3.2.1 *Big data* y reutilización de la información turística

Ya no estamos, en realidad, ante una novedad, pues desde hace ya varios años se viene utilizando el concepto de *big data* para referirnos al fenómeno mediante el cual, cantidades ingentes información digital, prácticamente inabarcable por la mente humana, es captada, gestionada y tratada por sistemas de información automatizados. La principal característica de este sistema, no obstante, reside en la potencial capacidad para «descubrir o inferir hechos y tendencias ocultos en esos datos» (17). Se convierte, por consiguiente, en una herramienta idónea para comprender mejor el comportamiento de los ciudadanos ante determinados servicios ofrecidos en el mercado y, además, para intentar deducir comportamientos futuros, de manera que podamos adelantarnos ante posibles tendencias.

Este es, precisamente, el uso principal que puede darse al *big data* en el sector turístico, es decir, entender mejor el comportamiento de los consumidores y deducir posibles cambios de actitud. En definitiva, realizar un análisis predictivo del mercado y adoptar una posición proactiva ante posibles cambios (18). Además, teniendo en cuenta el estado actual de la técnica, esta posibilidad no queda reservada a las grandes empresas y operadores del sector, sino que está al alcance, a un precio razonable, de cualquier pequeña, mediana o micro empresa, aumentado la competitividad de las mismas. No se debe pasar por alto, no obstante, el hecho de que los datos sobre los que actúan estas herramientas proceden de los propios turistas y de los residentes en un determinado destino turístico, por lo que, en buena medida, estos deberían obtener algún tipo de ventaja de aquellas empresas que aprovechan los datos y la información inferida. Solo repercutiendo el beneficio de esa información sobre los residentes y visitantes de los destinos turísticos, estaremos

(16) *Destinos Turísticos Inteligentes. Manual Operativo para la configuración de Destinos Turísticos Inteligentes*, *op. cit.*, p. 12.

(17) Gil, E., *Big data, privacidad y protección de datos*, Agencia Española de Protección de Datos, 2016, p. 16.

(18) *Big Data, retos y oportunidades para el turismo*, *op. cit.*, p. 12.

avanzando hacia un desarrollo turístico sostenible basado en la tecnología. Esta es una idea que, por ahora, solo se puede dejar apuntada, pero que, sin duda, puede resultar, al menos en mi opinión, muy interesante.

Otra cuestión digna de analizar sobre el *big data* se refiere al uso que las empresas y particulares pueden hacer de los datos generados por las propias administraciones públicas con competencia en materia turística. Y es que, de acuerdo con lo establecido en la Ley 19/2013, de 19 de noviembre, de Transparencia, Acceso a la Información y Buen Gobierno (en adelante, LTAIBG), dicha información debe ser pública (publicidad activa, artículos 5 a 11) y, además, puede ser reutilizada por personas físicas y jurídicas del sector privado, con fines comerciales y no comerciales, en los términos establecidos por el artículo 3.1 de la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público (19).

Por otro lado, también ha de tenerse en cuenta el potencial de estas tecnologías para predecir posibles impactos negativos en el medio ambiente o en el ámbito social o cultural de los destinos, de forma que pongan en peligro la sostenibilidad del sector a medio o largo plazo. En este sentido, estas herramientas de análisis de datos a gran escala podrían ser utilizadas por las administraciones públicas competentes (esencialmente las comunidades autónomas) como instrumentos de prevención. Así, podrían anticiparse al daño y, por tanto, minimizar o, incluso, evitar sus consecuencias. Como es lógico, habría de darse la necesaria cobertura legal a dicha actuación administrativa, que estaría relacionada con la actividad de policía, restringiendo determinadas actividades de particulares en determinadas zonas amenazadas (20), entre otras posibles actuaciones que puedan llevarse a cabo.

Por último, no se puede dejar de mencionar que el análisis y tratamiento de esta enorme cantidad de datos, unido a la utilización de sistemas avanzados de inteligencia artificial puede suponer una auténtica revolución en el sector, pues la toma de decisiones no se dejaría ya en manos de los gestores turísticos, sino de «máquinas», con todas las controversias éticas y jurídicas que puede plantear, pero sin dejar de lado, como es lógico, los avances y beneficios que, asimismo, puede conllevar.

3.2.2 Internet de las cosas y conectividad

Una de las características esenciales de los destinos turísticos inteligentes es su alto nivel de conectividad para el desarrollo del Internet de

(19) Bauzá Martorell, F. J., «Big data y open data en la administración turística: acceso y reutilización de la información», *Revista Vasca de Administración Pública*, núm. 108, 2017, p. 24.

(20) *Ibidem*, p. 23, «… habrá que admitir la posibilidad de que particulares accedan a los datos obrantes en poder de la Administración turística para fines comerciales o no comerciales, como también la opción que asiste a la Administración turística de interceptar los datos de usuarios y prestadores de servicios turísticos que circulan en las redes sociales, siendo este un medio idóneo para desplegar la actividad inspectora y consiguientemente la potestad sancionadora».

las cosas y los sistemas M2M (machine to machine). Esta conectividad permite que tanto las empresas como los visitantes puedan estar conectados a internet en todo momento, beneficiándose de múltiples servicios a los que acceden a través de la red. En este sentido, ya no solo se habla del Internet de las Cosas (*Internet of Things* o *IoT*, en sus siglas en inglés), es decir, de la conexión de distintos elementos físicos en una red más amplia, sino del Internet de Servicios (*Internet of Services* o *IoS)* y del Internet de las Personas (*Internet of People* o *IoP*) (21).

En concreto, esa conectividad se basa, entre otros, en los siguientes elementos: Wifi gratuito, como uno de los servicios más demandados por los turistas; aplicaciones para móviles, como consecuencia del uso generalizado de estos dispositivos por parte de los usuarios, códigos QR que facilitan el acceso a determinados servicios web, sistemas de geolocalización, para permitir al visitante saber dónde está en cada momento y qué visitar, sistemas de realidad aumentada u holografía, aplicado a museos, patrimonio histórico o cultural (22), entre otras.

Esta tecnología es, además, esencial para lograr un nivel de datos adecuado que permita un uso inteligente de los mismos basado en el *big data,* tal y como se ha señalado en el epígrafe anterior. Por otro lado, está presente en todo el ciclo del viaje turístico: desde la preparación, es decir, lo que se ha venido llamando la «inspiración asistida», donde se ofrece una gran cantidad de información sobre el destino turístico a los potenciales visitantes; durante el propio viaje, ya que a través de las TIC se hace mucho más intensa la experiencia vivida por los turistas, se facilita su movilidad y la interacción con operadores o con otros viajeros, en definitiva, permite que se tomen decisiones más acertadas; por último, el después, es decir, la posibilidad de medir con gran eficacia el grado de satisfacción de los turistas, incrementando la reputación de los empresarios y profesionales y permitiendo, asimismo, mejorar en aquellos aspectos que no hayan sido del agrado de los usuarios de los servicios turísticos (23).

3.2.3 *Cloud computing*

El *cloud computing* es una tecnología que permite, esencialmente, incrementar la eficacia y eficiencia en el uso de las TIC. En definitiva, permite a cualquier persona, empresa, profesional, etcétera, con independencia del sector económico en el que actúe, acceder, sin restricción geográfica o temporal, y utilizando el dispositivo que se estime más adecuado (móvil, tableta, etc.), a recursos informáticos tales como softwares y pla-

(21) *Destinos Turísticos Inteligentes. Manual Operativo para la configuración de Destinos Turísticos Inteligentes*, *op. cit.*, p. 14.
(22) *Smart Destination*, *op. cit.*, pp. 37 y 38.
(23) *Ibidem*, p. 20.

taformas, dependiendo de las necesidades de cada momento, y todo ello sin necesidad de invertir grandes sumas en recursos e infraestructuras tecnológicas (24). Por otro lado, facilita la posibilidad de desarrollar nuevos productos y servicios tecnológicos. Estamos, por consiguiente, ante «un modelo de prestación de servicios tecnológicos que permite el acceso bajo demanda y a través de la red a un conjunto de recursos compartidos y configurables (como redes, servidores, capacidad de almacenamiento, aplicaciones y servicios) que pueden ser rápidamente asignados y liberados con una mínima gestión por parte del proveedor de servicios.» (25).

Se trata de una tecnología que, como en otros ámbitos, puede aportar grandes beneficios en el sector turístico, pues permite mejorar los servicios y reducir los correspondientes costes. Así, en el subsector hotelero, aumentando la potencia y flexibilidad de la gestión, en el de restauración, permitiendo gestionar desde el suministro de alimentos hasta la ocupación del local, o el de intermediación, con compra de billetes en línea o agencias virtuales, por poner solo algunos ejemplos relevantes (26).

3.2.4 *Blockchain*

En mi opinión, los efectos que esta tecnología puede tener sobre el sector turístico no han sido, por el momento, debidamente estudiados. Y es que se trata de una novedad que puede suponer un cambio revolucionario no solo en la economía, sino también en la cultura y la forma de pensar (27). Una de las características esenciales del *blockchain* pasa por la desaparición de los intermediarios o terceros de confianza, lo que reduce enormemente los costes de transacción y aumenta la transparencia y la integridad de la información (28). Esta circunstancia hace que los desarrollos que pueden darse en la economía en general, y en el turismo en particular, sean muy interesantes. Así, la utilización de «contratos o agentes inteligentes», con capacidad «autoejecutiva» sin necesidad de intermediarios, el uso de aplicaciones descentralizadas (Dapps) que utilizan códigos abiertos, la posibilidad de aprovechar el sistema como plataforma para mejorar la gestión de ciudades inteligentes y destinos turísticos inte-

(24) Casasola, M., Molina, M., Recio Gayo, M., «La nube: nuevos paradigmas de privacidad y seguridad para un entorno innovador y competitivo», CIDE, 2014.

(25) Informe conjunto del Consejo General de la Abogacía Española y la Agencia Española de Protección de Datos sobre *Utilización del Cloud Computing por los despachos de abogados y el derecho a la protección de datos de carácter personal*, 2012.

(26) Guasch Portas, V., y Soler Fuensanta J. R., «*Cloud computing*, turismo y protección de datos», *Revista de Análisis Turístico*, núm. 17, 2014, pp. 63 y 64.

(27) Sobre esta novedosa tecnología Tapscott, D. y Tapscott, A., *La revolución blockchain*, Deusto, 2017; o Cervigni, L. S., *El blockchain en la práctica*, Bidit, 2016.

(28) García González, L. C., Polo Tolón, M. y Molero Manglano, I., «Tecnologías blockchain», en Preukschat, A., (Coord.), *Blockchain: La revolución industrial de internet*, Gestión 2000, 2017, p. 236.

ligentes, en la medida que la información se hace neutral, no jerárquica, accesible y segura (29) y, por consiguiente, permite aumentar la participación de los ciudadanos en la gestión.

Igualmente, esta tecnología puede resultar muy apropiada para mejorar el control que deben realizar las administraciones públicas competentes sobre la actividad de las empresas y profesionales que prestan servicios turísticos, garantizando la calidad y el respeto al medio ambiente y al entorno social, a través, por ejemplo, de la creación de registros de operadores turísticos en un determinado territorio (30).

3.3 **El uso de las TIC para alcanzar mayores cotas de sostenibilidad y calidad turística**

Ya se ha puesto de manifiesto la importancia que tiene el uso de las TIC para mejorar la gestión turística por parte de las empresas y la experiencia del turista en el destino. Pero no nos podemos quedar ahí. El uso de estas tecnologías debe estar presidido, según entiendo, por un objetivo más amplio: alcanzar un desarrollo turístico en el que la idea fundamental sea la calidad y la sostenibilidad turística. En este sentido, la utilización por parte de los destinos turísticos inteligentes de todas las tecnologías mencionadas más arriba permite controlar con mayor eficacia el crecimiento turístico y, por tanto, incrementar la calidad y la sostenibilidad turística. A continuación se mencionan, sin ánimo de ser exhaustivo, los principales beneficios que podemos obtener de estas tecnologías de cara a incrementar los niveles de sostenibilidad.

3.3.1 Control de la capacidad de carga del destino turístico para evitar estrés ambiental y social

Uno de los conceptos esenciales cuando hablamos de sostenibilidad turística es el de capacidad de carga de los destinos, es decir, el número máximo de visitantes que un determinado territorio puede soportar sin que se vea dañado el medio natural o el ambiente social. Y es que, un incremento de la demanda turística sin el debido control administrativo correspondiente puede ser, a medio largo o plazo, contraproducente, pues, en primer lugar, se estará sometiendo a los correspondientes territorios a unos niveles muy altos de estrés ambiental o/y social y, en segundo lugar, porque la calidad del destino percibida por el cliente disminuirá, lo que puede poner en riesgo la pervivencia de ese territorio como destino turís-

(29) Junestrand, S., «Smart Cities en la era blockhain», en Preukschat, A. (Coord.), *Blockchain: La revolución industrial de internet*, *op. cit.*, p. 107.

(30) Fernández Hergueta, R., «El sector público y el uso de la blockchain» en Preukschat, A., (Coord.), *Blockchain: La revolución industrial de internet*, *op. cit.*, p. 94.

tico. Desde luego, tratar de incrementar a cualquier precio el número de turistas sin tener en cuenta otras consideraciones no puede ser considerado un desarrollo turístico sostenible.

En este sentido, las TIC aplicadas a los destinos turísticos pueden servir de herramienta para reducir esos riesgos. Así, puede ayudar a las administraciones públicas competentes a determinar, con menor margen de error, cual es el número de visitantes que un determinado destino puede asumir sin que comience a afectarse de manera negativa otros bienes susceptibles de protección. Además, se puede dotar a esas mismas administraciones públicas, siempre respetando el principio de legalidad, por supuesto, de instrumentos y herramientas de control que mejoren la eficacia de la intervención administrativa sin incrementar, o incluso disminuyendo, las cargas administrativas que deben soportar las empresas y profesionales del sector (31).

3.3.2 Mayor participación de los residentes en la toma de decisiones sobre política turística por parte de las Administraciones públicas

Un desarrollo turístico sostenible, como ya se ha puesto de manifiesto más arriba, requiere de una adecuada participación de los residentes en la toma de decisiones públicas en materia turística (32). En este sentido, la utilización de TIC puede facilitar esta tarea, dado que permite dicha participación a través, por ejemplo, de mecanismos de consulta o información pública en la sede electrónica o portal de internet de la administración correspondiente. Como es fácilmente comprensible, los residentes de un determinado destino turístico son especialmente sensibles con el desarrollo de políticas turísticas que tienen como objetivo único el incremento de la demanda turística y, por tanto, el número de visitantes (33). Es, por consiguiente, especialmente importante, sobre todo en el ámbito

(31) Bauzá Martorell, F. J., «Big data y open data en la administración turística: acceso y reutilización de la información», *op. cit.*, p. 26, «Siendo así que la realidad del sector turístico deriva hacia el mundo digital, la intervención administrativa no puede quedarse anclada en las visitas de inspección y el requerimiento de documentación, porque en ese caso no alcanza la plenitud de la relación jurídico-administrativa. El análisis de las redes se convierte en imprescindible para asegurar el cumplimiento de la normativa turística y el análisis de macro datos desde luego permite realizar comprobaciones masivas y automatizadas de ese cumplimiento o incumplimiento (fraude). En caso contrario nos encontramos con la paradoja de que la normativa aplicable no se exige a un buen número de obligados, porque sencillamente no existen para la Administración turística, porque no hay constancia de su intervención en el mercado como operadores turísticos, y el control sobre los mismos se da exclusivamente en caso de una eventual denuncia».

(32) Fullana, P. y Ayuso, S., Turismo sostenible, *op. cit.*

(33) En los últimos meses han surgido brotes de «*turismofobia*» como consecuencia del incremento de turistas en determinadas ciudades españolas como Barcelona o Madrid. Así, puede verse noticia de diario El País de 28 de mayo de 2017, en el siguiente enlace:

https://elpais.com/economia/2017/05/27/actualidad/1495908161_850351.html

turístico, facilitar la participación de los ciudadanos en la toma de decisiones administrativas que les vayan a afectar (34).

3.3.3 Mejora en la movilidad y en la eficiencia energética de las ciudades

Otros de los aspectos que pueden verse positivamente afectados con el uso de las TIC en los destinos turísticos inteligentes es el que se refiere a la movilidad dentro de las propias ciudades (35). En este sentido, cuando se habla de ciudades inteligentes y destinos turísticos inteligentes nos referimos, igualmente, a una mejora en la movilidad dentro de los correspondientes territorios, de manera que, entre otros aspectos, se optimice la fluidez del tráfico, se aumente la eficacia de los servicios públicos de transportes, evitando atascos, embotellamientos, o las denominadas «horas punta», ahorro de combustible, reducción de la contaminación, etc. (36). Esta mejora en la movilidad, como es lógico, redunda en una mayor calidad de los servicios y en un menor impacto medioambiental y social, por lo que es importante a efectos de alcanzar un desarrollo turístico sostenible.

3.3.4 Aumento de la calidad de los servicios turísticos y de la rentabilidad económica

Uno de los elementos que coadyuvan a la sostenibilidad turística es el de la calidad. Solo si se alcanza un alto nivel de calidad podemos hablar de sostenibilidad, pues aumentará, asimismo, la rentabilidad económica del turismo. Un turismo de calidad es rentable económicamente porque requiere menos consumidores para lograr los mismos rendimientos. Además, no puede considerarse de calidad un destino saturado y abarrotado de turistas, pues genera incomodidad a los residentes y mala imagen de destino a los usuarios.

No hay que confundir, no obstante, turismo de calidad con turismo caro o de élite, pues tampoco podría considerarse socialmente sostenible. El turismo de calidad es, tal y como ha puesto de manifiesto la propia Or-

(34) Sobre la importancia de la participación ciudadana en la planificación de la ordenación territorial, se puede ver a Bouazza Ariño, O., «La participación ciudadana en el proceso planificador: fundamento constitucional y legal», *WPS Review International on Sustainable Housing and Urban Renewal*, núm. 4, 2016, p. 40, «Con ello se pretenderá buscar las herramientas jurídicas que permitan la configuración de un modelo planificación territorial respetuosa con la definición del concepto de justicia social, yendo más allá de las preocupaciones estrictamente económicas. Una planificación elaborada teniendo en cuenta la opinión de la población en relación con el desarrollo urbano permitiendo, de esta manera, el derecho de la población residente a su implicación en los procedimientos democráticos de decisión. Así, podrán manifestar su posición sobre el esquema que se tenga previsto realizar y que va a afectar a sus vidas o, utilizando un concepto de moda, a su calidad de vida».

(35) *Destinos Turísticos Inteligentes. Manual Operativo para la configuración de Destinos Turísticos Inteligentes*, *op. cit.*, p. 22.

(36) Martínez Gutiérrez, R., «El impacto de las Smart Cities en la tutela ambiental y en la planificación urbana», en *Smart Cities. Derecho y técnica para una ciudad más habitable*, *op. cit.*, p. 64.

ganización Mundial del Turismo, «el resultado de un proceso que implica la satisfacción de todas las necesidades y expectativas legitimas del consumidor respecto a los productos y servicios demandados, a un precio aceptable, de conformidad con los determinantes subyacentes de calidad, como la salud y seguridad, higiene, accesibilidad, transparencia, autenticidad y armonía de la actividad turística considerada con su entorno humano y natural», es decir, la satisfacción total del cliente con los servicios recibidos. En el cumplimiento de este objetivo tienen una misión esencial las TIC, pues permiten, por mencionar solo algunos ejemplos, tener acceso a internet desde cualquier lugar, conocer las horas punta para evitar aglomeraciones (estado de ocupación de restaurantes, museos, medios de transporte), acceder a información sobre novedades culturales, entre otros. En definitiva, el uso de las tecnologías mejora la calidad de vida del turista (y, también, del ocio del residente, lo que redunda en una mejora en la percepción del turismo).

4. LOS PRINCIPALES RETOS ANTE EL TURISMO INTELIGENTE

4.1. **Protección de datos y privacidad. La importancia de la privacidad en el diseño y por defecto**

Como es fácilmente comprensible, uno de los retos esenciales a los que debe hacer frente el desarrollo del turismo inteligente es, precisamente, el riesgo que supone para la privacidad (37). Así, el uso masivo de datos que se llevan a cabo a través del *big data*, *cloud computing*, internet de las cosas, etc., implica que cada vez es más complicado garantizar al ciudadano un control total sobre sus datos personales, de manera que se han de arbitrar otras herramientas que aseguren un respeto escrupuloso a este derecho fundamental. En esta línea, resultan especialmente importantes los principios de protección de datos por defecto y en el diseño (38) que se han incluido en el artículo 25 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD). Estos principios van a

(37) Piñar Mañas, J. L., «Derecho, técnica e innovación en las llamadas ciudades inteligentes», en *Smart Cities. Derecho y técnica para una ciudad más habitable*, *op. cit.*, p. 21. En el mismo sentido, Valero Torrijos, J., «Ciudades inteligentes y datos abiertos: implicaciones jurídicas para la protección de los datos de carácter personal», Istituzioni del Federalismo, *Rivista di Studi Giuridici e Politici*, núm. 4, 2015, pp. 1025 y ss.

(38) Un estudio detallado sobre estos dos principios esenciales se puede encontrar en Duaso Cales, R., «Los principios de protección de datos desde el diseño y protección de datos por defecto» en Piñar Mañas, J. L. (Dir.) y Álvarez Caro, M. y Recio Gayo, M., (Coords.) *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad*, Reus, 2016, pp. 295 y ss.

resultar claves en la creación de destinos turísticos inteligentes, pues el desarrollo de la tecnología y las aplicaciones necesarias por parte de empresas y administraciones públicas, así como el uso de las mismas por parte de los turistas, deben tener en cuenta siempre la privacidad de los usuarios, así como la necesidad impuesta en el nuevo RGPD de utilizar siempre los datos mínimos que sean imprescindibles para la prestación de un servicio determinado, no más (minimización). No obstante, esta tensión entre avances tecnológicos y Derecho no es nueva (39), de ahí que se pueda afirmar que, de alguna manera, si se permite la expresión, están condenados a entenderse (40).

4.2 **Desarrollo tecnológico para todos: inclusión**

Al hablar de desarrollo tecnológico aplicado a destinos turísticos, se debe tener en cuenta a todas aquellas personas que, por diferentes motivos, no tienen o no quieren tener acceso a las TIC. Pienso, sobre todo, en personas mayores, discapacitados o personas sin suficientes recursos, pero también en aquellos que voluntariamente han optado por excluirse del desarrollo tecnológico (41). Pues bien, estas personas no pueden quedar al margen del beneficio de esos avances, sino que, lógicamente, deben ser incluidas. En este sentido, cabe indicar que cualquier innovación tecnológica, incluido el turismo digital, debe ser inclusiva, no excluyente (42).

4.3 **Y no olvidemos el encanto de la desconexión: el «turismo digital *detox*» o sin tecnología**

Un reclamo turístico evidente (aunque no exento de cierto esnobismo) en estos tiempos de digitalización total puede ser, precisamente, la ausencia de conexión, es decir, la posibilidad de evadirte durante unos días o, en el mejor de los casos, semanas, de todos los dispositivos tecnológicos que nos mantienen en contacto permanente con el mundo digital. En este sentido, y en contra de lo que se ha venido desarrollando a lo largo de este trabajo, no resulta descabellado pensar que este tipo de destinos turísticos puedan tener éxito. Se podría hablar del turismo desconectado, o como ya se menciona en algunas guías y blog turísticos espe-

(39) Piñar Mañas, J. L., *Derecho e innovación tecnológica. Retos de presente y futuro*, CEU Ediciones, 2018, p. 9.

(40) Recio Gayo, M., *Protección de datos personales e innovación: ¿(In)compatibles?*, Reus, 2016.

(41) El derecho a no ser digitales, que no siempre se respeta, tal y como pone de manifiesto Piñar Mañas, J. L., *Derecho e innovación tecnológica. Retos de presente y futuro*, *op. cit.*, p. 22.

(42) *Ibidem*, p. 23.

cializados, «turismo digital *detox*» (43), es decir, para la desintoxicación digital. Estos destinos se caracterizan por su falta de conexión y la ausencia de tecnología.

Lo más interesante de estos destinos sin tecnologías es que deben ser considerados destinos turísticos de la más alta calidad, pese a su desconexión de las TIC. Una breve reflexión sobre esta circunstancia puede llevar a la conclusión de que los ciudadanos necesitan, en ocasiones, desconectarse. Podría así plantearse la extensión del derecho a la desconexión del que habla la doctrina laboralista (44) a otros ámbitos del Derecho. Reflexión que dejo solamente apuntada por exceder del objeto del presente trabajo.

4.4 **La economía colaborativa en el turismo**

El uso de las TIC ha permitido que surjan en el ámbito turístico nuevos modelos económicos que cuestionan el tradicional. Así, han hecho posible que ciudadanos particulares, no empresas ni profesionales del sector, presten determinados servicios turísticos en lo que se ha venido a denominar, con mayor o menor fortuna, economía colaborativa. Sin entrar en un análisis exhaustivo de este fenómeno económico, pues no es el lugar adecuado para hacerlo, sí se debe manifestar que supone un reto importante para el sector turístico, sobre todo en lo que se refiere a la regulación, pues no queda del todo claro si deben someterse a las mismas reglas que el resto de empresas y profesionales o no (45). Hay dudas, por tanto, de si estamos ante servicios prestados en competencia desleal (46). En cualquier caso, lo que sí está claro, en mi opinión, es que este nuevo modelo ha nacido al albur del desarrollo de las TIC.

---

(43) Un blog de la página web www.lonelyplanet.es, titulado «¿WiFi? No, gracias. Viajes para desconectar», plantea como alternativa al turismo digital o inteligente, la vuelta al turismo analógico, en destinos que se caracterizan por ser «paraísos *free tech*». Así señala que «Algunas islas caribeñas como San Vicente o las Granadinas se ofrecen como vacaciones de desintoxicación digital (Digital Detox). Es su principal atractivo además de unas playas magníficas, aguas transparentes y buenos hoteles, eso si: sin ordenador, sin teléfono, sin wifi, como se hacía antes. La desconexión es total. […] Es una nueva tendencia que va a crecer en los próximos años. Los viajeros ya han probado la experiencia de viajar completamente conectados pero hay muchos que desean volver a los viejos tiempos, cuando viajar era dejar atrás muchas cosa». En el mismo sentido, en la sección de «el viajero» del diario El País, publicado el 6 de abril de 2016, se habla de «Hoteles donde desconectar del mundo». Por su parte, la sociedad estatal Paradores de Turismo ofrece su programa *detox*.

(44) Entre otros, Alemán Páez, F., «El derecho de desconexión digital: una aproximación conceptual, crítica y contextualizadora al hilo de la *Loi Travail* n.º 2016-1088», *Trabajo y derecho: nueva revista de actualidad y relaciones laborales*, núm. 30, 2017, pp. 12 y ss.

(45) Laguna de Paz, J. C., «El papel de la regulación en la llamada economía colaborativa», *Revista de Estudios Europeos*, núm. 70, 2017, pp. 159 y ss.

(46) Miranda Serrano, L. M., «Economía colaborativa y competencia desleal: ¿deslealtad por violación de normas a través de la prestación de servicios facilitados por plataformas digitales?», *Revista de Estudios Europeos*, núm. 70, 2017, pp. 197 y ss.

5. LA ACTIVIDAD DE CONTROL DE LAS ADMINISTRACIONES PÚBLICAS EN EL ÁMBITO DIGITAL

Para terminar, no puedo dejar de referirme a las posibilidades que las TIC ofrecen a las administraciones públicas para el cumplimiento de su misión de control y supervisión de las actividades turísticas. Ya me he referido más arriba al hecho de que el desarrollo de las TIC por parte de las empresas y operadores en el mercado turístico, unido a la amplia liberalización que en los últimos diez años ha sufrido el sector, han contribuido a que la actividad administrativa de control sea cada más difícil para las administraciones competentes. Así, la sustitución sistemática de autorizaciones previas por sistemas de control posterior (declaraciones responsables y comunicaciones previas), han colocado a las administraciones en una difícil tesitura (47).

Sin embargo, el impulso decidido al desarrollo de la Administración electrónica desde las Leyes 39 y 40 de 2015, ambas de 1 de octubre (de Procedimiento Administrativo Común de las Administraciones Públicas, y de Régimen Jurídico del Sector Público, respectivamente), y la posibilidad de utilizar, previa habilitación legal, nuevos sistemas de control más allá de los tradicionales, pueden servir de ayuda para el cumplimiento de esta misión de supervisión del mercado turístico.

En este sentido, las administraciones, mediante el uso de tecnologías como la del *big data*, *blockchain* o *cloud computing*, pueden mejorar sensiblemente su eficacia a la hora de comprobar el cumplimiento de los requisitos por parte de los operadores en el sector turístico. No obstante, también se deben tener en cuenta los riesgos generados a los ciudadanos en sus derechos fundamentales, esencialmente el de protección de sus datos personales (48).

En esta línea, Bauzá Martorell propone que «habrá que admitir […] la opción que asiste a la Administración turística de interceptar los datos de usuarios y prestadores de servicios turísticos que circulan en las redes sociales, siendo este un medio idóneo para desplegar la actividad inspectora y consiguientemente la potestad sancionadora […] Siendo así que la realidad del sector turístico deriva hacia el mundo digital, la intervención administrativa no puede quedarse anclada en las visitas de inspección y el requerimiento de documentación, porque en ese caso no alcanza la plenitud de la relación jurídico-administrativa. El análisis de las redes se con-

(47) Corral Sastre, A., *La liberalización del sector turístico ¿Hacia un modelo de turismo sostenible?*, Reus, 2017.

(48) Valero Torrijos, J., «El big data en las Administraciones Públicas: el difícil equilibrio entre eficacia de la actividad administrativa y garantía de los derechos de los Ciudadanos», en AA. VV., *Big data. Retos y oportunidades. Actas del IX Congreso Internacional Internet, Derecho y Política.* Universitat Oberta de Catalunya. Barcelona, 25 y 26 de junio de 2013. Pp. 127 a 137.

vierte en imprescindible para asegurar el cumplimiento de la normativa turística y el análisis de macro datos desde luego permite realizar comprobaciones masivas y automatizadas de ese cumplimiento o incumplimiento (fraude) (49). Desde luego que habrá que reconocer a las administraciones competentes esta posibilidad, teniendo en cuenta, en cualquier caso, el RGPD al que me he referido más arriba y, en concreto, con pleno respeto al artículo 6 que se refiere a los supuestos en que puede considerarse lícito un tratamiento de datos personales (50).

6. CONCLUSIÓN

Visto todo lo anterior se puede concluir que el turismo ha aprovechado especialmente el uso de las TIC para mejorar los rendimientos económicos, algo que es legítimo pero que también tiene un lado negativo. Y es que, la proliferación de su uso ha permitido incrementar de manera muy importante el número de turistas que nos visitan, sobre todo en algunos destinos, lo que genera situaciones de estrés ambiental y social que pueden desembocar en un desarrollo turístico insostenible a medio y largo plazo.

El uso de estas TIC, por consiguiente, no debe centrase exclusivamente en el incremento de la oferta y la demanda, sino en un aumento de la calidad de los servicios, lo que redundará en un desarrollo económico sostenible del sector. El concepto de turismo inteligente o destino turístico inteligente implica, lógicamente, el uso de estas tecnologías, pero con una visión más amplia que el mero incremento de los beneficios económicos: mejorar la calidad de vida de los turistas y residentes, respetar la capacidad de carga de los destinos, reduciendo el estrés ambiental y social, disminuir la contaminación y hacer más eficiente el consumo energético y la movilidad, entre otros.

En este sentido, el desarrollo y la innovación tecnológica pueden coadyuvar a alcanzar un modelo de desarrollo turístico sostenible si se utilizan adecuadamente, no solo desde una perspectiva económica. En definitiva, hay que encontrar el «camino correcto del desarrollo» (51) turístico.

---

(49) Bauzá Martorell, F. J., «Big data y open data en la administración turística: acceso y reutilización de la información», *op. cit.*, p. 26.

(50) Las administraciones públicas pueden tratar datos lícitamente, según el artículo 6.1.e del RGPD cuando el «tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento».

(51) Schumacher, E. F., *Lo pequeño es hermoso*, Orbis, 1983, p. 64.

CAPÍTULO 46

SECTOR ENERGÉTICO Y AGENDA DIGITAL: REGULACIÓN Y EVOLUCIÓN TECNOLÓGICA

Vicente López-Ibor Mayor
Doctor en Derecho
Presidente de Estudio Jurídico Internacional
Ex Consejero de la Comisión Nacional de Energía

Emilio Alba Linero
Doctor en Física
Director Técnico de Quantum Business Analytics

I. PLANTEAMIENTO DE LA CUESTIÓN

Aproximarse a la agenda digital y su regulación, desde la perspectiva del sector energético, es un reto intelectual apasionante. Por varias razones. La primera, porque lo digital tiene un efecto radial de apreciación que alcanza distintas facetas. En el orden general constituye un elemento definidor de cambios trascendentales, muchos de ellos de carácter disruptivo, que observamos en nuestro sistema económico productivo. Cambios que muestran una nueva forma de producir, suministrar u ofrecer productos o servicios al mercado. Pero, también, nos invitan a reflexionar sobre la naturaleza y características de nuestras organizaciones, empresas y entidades de cualquier tipo, donde se debe reorganizar o reacomodar la dinámica productiva al hecho digital, tanto por sus potencialidades como por sus efectos. En el orden económico general, la dimensión digital in-

corpora una nueva forma de avanzar aceleradamente en la terciarización de la economía, desbordando los marcos conceptuales que anticipara Daniel Bell en su análisis sobre la sociedad postindustrial, pero tomando como referencia sus presupuestos evolutivos y la fortaleza económica de los vectores de cambio en las sociedades postindustriales. Un atributo indiscutido del desarrollo digital en su impacto en la economía, comercio e innovación social, es la aceleración que provoca sobre las realidades en las que actúa, tanto desde la oferta como en la demanda del sistema económico. Hemos podido observar hasta qué punto esta evolución acelerada del cambio ha tenido lugar en las tres últimas décadas. Así, no podemos obviar la revolución tecnológica, crecientemente acelerada, que está teniendo lugar desde que Vinton y Kahn escribieran su seminal trabajo sobre la nueva infraestructura de Internet (1) y que arroja datos verdaderamente espectaculares en horizontes temporales muy cortos.

Baste señalar, a título de ejemplo, que ya el número de teléfonos móviles ha superado al número de personas en el mundo, cuando, sin embargo, alrededor de 1.100 millones de personas carecen aún de acceso a la energía suministrada por la red. O que la mayor parte del tráfico actual de Internet es originado por la interconexión de objetos y no de las personas.

Dos aspectos o dimensiones que definen el proceso de cambio profundo que está teniendo lugar en el sector energético en su conjunto, son: la dimensión ambiental, de una parte, y la dimensión digital, de otra. En ocasiones ambos aspectos o dimensiones convergen, o se retroalimentan, pero son variables centrales que condicionan el futuro de la estructura, organización, funcionamiento y prestación de productos y servicios en toda la cadena del sector energético.

Desde la perspectiva ambiental, baste recordar los sucesivos paquetes legislativos y medidas adoptadas en materia de energía y clima, en orden a alcanzar los objetivos comunitarios acordados por las instituciones europeas en materia de reducción de emisiones (2) y, en particular, en el momento actual, el denominado Clean Energy Package, que supone una

(1) Ver Vinton G. Cerf and Robert E. Kahn: «A protocol for packet network intercommunication». New York. IEEE, 1974.

(2) «La UE contempla unos objetivos para 2030 que incluyen un 27% de penetración de energías renovables, un 40% de reducción de emisiones con relación al año 1990, y un 30% de mejora de la eficiencia energética con respecto a las proyecciones realizadas en 2007. El objetivo de reducción de emisiones a nivel de la UE se ha asignado entre sectores ETS (objetivo del –40%) y no ETS (objetivo del –30%)».

Ver «Un mundo estratégico en materia de energía y clima para el período 2020-2030». Acuerdo de París.

El Consejo Europeo de Ministros de Energía (18-12-2017) adoptó unas orientaciones generales sobre esta materia que alcanzan, entre otros, a los siguientes elementos principales:

a) Los consumidores se beneficiarán de procedimientos de notificación simplificados para instalaciones de pequeña magnitud, y los derechos y obligaciones de los «autoconsumidores de energías renovables», así como de las comunidades de energías renovables, están claramente establecidos.

transformación de gran envergadura en la regulación del sector energético, fundamentalmente, en el eléctrico. Como ha señalado Leigh Harcher (3), la conformación de un nuevo diseño del mercado eléctrico pretende dar respuesta a la mayor participación de las fuentes de energía renovable en la generación de electricidad (objetivo de alcanzar el 50% para 2030), adaptándose a la intermitencia propia de las energías renovables, aumentando la flexibilidad del sistema y garantizando la seguridad en el suministro.

Por esta razón, el 30 de noviembre de 2016, la Comisión publicó el llamado *«Clean Energy Package for all europeans»* o «Paquete de invierno», consistente en ocho propuestas [cuatro Reglamentos (4) y el mismo número de Directivas (5)] y siete comunicaciones, todo ello con el objeto de reformar el diseño y el funcionamiento del mercado de electricidad de la Unión Europea, y facilitar, en consecuencia, la transición definitiva hacia una economía basada en «energía limpia».

Así pues, en las páginas siguientes nos proponemos analizar las cuestiones referidas, con una especial preocupación e interés por la realidad comunitaria, ya que es desde aquella fuente de producción normativa

---

b) En lo que se refiere a la calefacción y refrigeración, los Estados miembros tendrán que adoptar medidas para lograr el aumento indicativo de un punto porcentual anual en la cuota de energía renovable.

c) En el sector del transporte, el objetivo de renovables para 2030 está fijado en el 14% para cada Estado miembro, y existe un objetivo secundario del 3% para los «biocarburantes avanzados», para los cuales se permitirá el cómputo por partida doble. Este objetivo para los biocarburantes avanzados tiene un objetivo intermedio vinculante de un 1% en 2025 para aumentar la seguridad de las inversiones y garantizar la disponibilidad de carburantes a lo largo del período. Se incentiva fuertemente la electromovilidad con dos coeficientes multiplicadores, de cinco para la electricidad renovable utilizada en el transporte por carretera y de dos para el transporte ferroviario.

d) Se mantiene el límite máximo actual del 7% para los biocarburantes de primera generación, a fin de ofrecer seguridad a los inversores. Si un Estado miembro fija un límite máximo más bajo, será recompensado con la opción de reducir su objetivo general para las energías renovables en el sector del transporte.

(3) Ver Leigh Hatcher y B. M. Winters: «The EU Winter Package». Briefing Paper. Febrero 1997.

(4) Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al mercado interior de la electricidad.

Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la gobernanza de la Unión de la Energía, y por el que se modifican la Directiva 94/22/CE, la Directiva 98/70/CE, la Directiva 2009/31/CE, el Reglamento (CE) n.º 663/2009, el Reglamento (CE) n.º 715/2009, la Directiva 2009/73/CE, la Directiva 2009/119/CE del Consejo, la Directiva 2010/31/UE, la Directiva 2012/27/UE, la Directiva 2013/30/UE y la Directiva (UE) 2015/652 del Consejo y se deroga el Reglamento (UE) n.º 525/2013.

Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la preparación frente al riesgo en el sector de la electricidad y por la que se deroga la Directiva 2005/89 / CE.

Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se crea la Agencia de la Unión Europea para la Cooperación de los Reguladores de la Energía (refundición).

(5) Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva 2012/27/UE, relativa a la eficiencia energética.

Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva 2010/31/UE, relativa a la eficiencia energética de los edificios.

Propuesta de Directiva del Parlamento Europeo y del Consejo relativa al fomento del uso de energía procedente de fuentes renovables (refundición).

Propuesta de Directiva del Parlamento Europeo y del Consejo sobre normas comunes para el mercado interior de la electricidad.

desde donde se proyecta en nuestro espacio político el mayor y más importante número de normas conformadoras del sector y mercado energético en el que la agenda digital incidirá –ya lo hace de hecho– de manera creciente. Y porque, además, el derecho europeo, como es sabido, se integra en los sistemas jurídicos nacionales con la nota de prevalencia o primacía en las competencias o materias a él atribuidas, convirtiéndose así en parámetro de legalidad de las normas comunitarias desarrolladas a nivel estatal.

Por consiguiente, y en relación con lo anterior, la agenda digital energética debe tener en cuenta las variaciones propias de la transformación digital que se dan cita en todos los sectores y empresas de carácter estratégico sometidas a intensa influencia regulatoria, de una parte; y de otra, a las características propias de la cadena de valor de la estructura productiva del sector, en su conjunto, y en cada una de sus fases o actividades.

Así pues, desde la perspectiva común a todas las empresas, nos encontramos con los temas vinculados a la captación, proceso, almacenamiento y transmisión interna y externa de los datos; big data, tanto en su aplicación, como en sus aspectos regulatorios; comercio electrónico; protección de la «identidad digital», etc., que deben tenerse en cuenta no sólo en la cadena de producción sino, eventualmente, en las soluciones comerciales que se ofrezcan en gran número de empresas y sectores.

Todo ello puede tener efectos determinantes, tanto en el modelo de negocio de las compañías, como en su forma de organización y funcionamiento, en la mayor resiliencia del tratamiento interno, no sólo de información y contenidos, sino de formas y procesos; y, evidentemente, con proveedores y clientes.

Desde la perspectiva del sector energético, abordamos esta cuestión con carácter general, si bien entendemos que así como en la generación o producción de las tecnologías energéticas, el catálogo de riesgos o amenazas de la transformación digital se vincula en gran medida a la forma de utilizar las infraestructuras –sin perjuicio del carácter «crítico» en términos de seguridad de algunas de estas infraestructuras energéticas– y el volumen y sensibilidad de los datos que han de ser procesados para las transacciones comerciales, siendo este hecho, por tanto, común en principio a cualquier tipo de empresa energética, de cualquier tecnología o fuente primaria, que desarrolle estas actividades. Sin embargo, en la vertiente de la demanda, los fenómenos de transformación digital se acentúan con los cambios regulatorios derivados del nuevo ecosistema eléctrico, fundado en mecanismos de generación distribuida que apuntan a una modificación sustantiva del modelo tradicional de regula-

ción y funcionamiento del sistema eléctrico, en su conjunto, y que se apoyan en una amplia utilización de sistemas automatizados de carácter digital.

Los grandes avances tecnológicos de las últimas décadas llevan consigo, pues, un cambio de las formas de comunicación, interrelación, producción y trabajo que tensionan las estructuras legales y regulatorias de cualquier sociedad. El sector energético y, singularmente, el sistema eléctrico, con su importancia transversal en todos los sectores productivos y domésticos, y la necesidad tradicional de grandes inversiones en plantas de generación e infraestructura de transporte, es un ejemplo paradigmático de esta tensión entre posibilidades tecnológicas y capacidad de control. A tal efecto, deben tenerse en consideración los puntos siguientes:

a) La industria y el comercio demandan altos niveles de potencia a un bajo precio para funcionar correctamente en un entorno cada vez más competitivo. En la mayoría de los Estados desarrollados, los niveles de fiabilidad de la red están en máximos históricos, debiendo ponderarse cuidadosamente la manera de transitar hacia nuevas formas de producir e intercambiar electricidad, a fin de minimizar riesgos eventuales y reforzar posibles mecanismos de optimización técnica y económica del sistema.

b) La gran mayoría de avances tecnológicos se deben a contribuciones de los operadores comerciales, obligando al regulador a atender y comprender las posibilidades de un mercado unificado de servicios eléctricos y gasistas, y la posible obligación del uso de estándares.

c) Las nuevas posibilidades de generación descentralizada y movilidad eléctrica requieren a la red formas de funcionar para la que no fue diseñada, reclamando un nuevo esfuerzo y arquitectura del sistema eléctrico y, eventualmente, gasista.

El contraste entre las posibilidades percibidas (principalmente, por la opinión pública y las empresas innovadoras en el sector) y los límites a la capacidad de actualización de la red (por la necesidad de asegurar los niveles de servicio y coste a cada momento) genera ciertos riesgos y posibles pérdidas de oportunidades y competitividad en el caso de una estrategia conservadora de implantación. Sin embargo, la variabilidad de las fuentes renovables, y más en un entorno de generación descentralizada, pueden llevar a la red a tener que responder en segundos a condiciones muy dinámicas que presenten, en una primera instancia, eventuales riesgos en la continuidad del servicio (6).

(6) https://en.wikipedia.org/wiki/2011_Southwest_blackout

La mayoría de las estrategias para minimizar las posibilidades de error en la infraestructura pasa por el despliegue de un mayor número de elementos de medida y control de la red y un sistema de comunicación y optimización permanente, en lo que se suele llamar transformación digital de la red o digitalización, especialmente de la red eléctrica. En efecto, estos mecanismos reducen el coste y tiempo de introducción de nuevas tecnologías en la red y suponen el paso lógico en la implantación de respuestas automatizadas con un tiempo más corto y eficiente de actuación (7).

II. CIBERSEGURIDAD ENERGÉTICA: RÉGIMEN JURÍDICO Y ANÁLISIS DE RIESGOS

La digitalización de la industria plantea, como hemos apuntado anteriormente, nuevos escenarios de análisis en razón de las modificaciones o alteraciones, no pocas de carácter sustantivo, en la estructura de los sectores, sus actividades y mecanismos de organización, supervisión, control y funcionamiento. Máxime siendo el sector energético una «industria de red», con infraestructuras físicas muy relevantes, caracterizadas, en determinados casos o instalaciones, como «críticas» en materia de seguridad.

Pero si hay un punto en el que el paradigma digital muestra oportunidades y riesgos, es el control de los flujos de datos en el campo de los servicios eléctricos, que reclama un especial esfuerzo en materia de seguridad o «ciberseguridad».

En tal sentido, las instituciones europeas vienen prestando especial atención a través de su Comunicación de 2015 (8), que retoma la valoración de la estrategia de ciberseguridad de la UE, lanzada dos años antes, a los trabajos del Grupo de Expertos energéticos sobre plataformas de ciberseguridad (EECSP) (9), y que aborda detalladamente un estudio subsectorial de riesgos, amenazas y lagunas en los elementos de protección digital de las infraestructuras energéticas. Pero junto a ello, se dispone por las instituciones comunitarias un conjunto pre legislativo o estratégico así como otro normativo de amplio alcance, que abarca desde la denominada «estrategia digital del mercado único» (DSM), que cubre el análisis de las infraestructuras críticas del sector

(7) http://www3.weforum.org/docs/WEF_Future_of_Electricity_2017.pdf

(8) Ver a tal respecto la Comunicación europea denominada «Building a European Data Recovery». COM(2015) 0192 final. Y también el COM(2017) 9 final y SWD(2017) 2 final.

Ver también la Directiva (EU) 2016/1148 del Parlamento y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva SRI).

(9) Energy Expert Cyber Security Platform.

energético, junto a otras como la salud o el transporte, y apunta la relevancia de disponer de estándares técnicos que permitan la interoperabilidad del sistema, además de establecer un buen número de consideraciones y previsiones en materia de ciberseguridad, y temas relativos a IoT, big data o cloud computing.

Por otro lado, la NIS Directive (2016) (10), es un componente central en la estrategia comunitaria global para prevenir y responder a ciberataques o disrupciones del sistema. Esta Directiva obliga a los Estados miembros a establecer una Estrategia Nacional en la materia, establece requerimientos de seguridad para los operadores de servicios esenciales, como el energético, y medidas de cooperación interestatales y con las autoridades comunitarias, tanto respecto de la seguridad de redes e instalaciones, como en materia de intercambio de información. Como es sabido, se considera operadores de servicios esenciales a un buen número de entidades y figuras jurídicas del sector, así, los generadores, transportistas, distribuidores y suministradores de electricidad; en el sector petrolífero los operadores de oleoductos, generadores, instalaciones de refinería y almacenamiento; y en el sector de gas natural, las compañías de suministro, distribución, transmisión, almacenamiento y operadores de sistemas de GNL.

Tampoco podemos olvidar, con relación a la normativa sobre infraestructuras críticas, la Comunicación comunitaria de 2006, ni la Directiva de 2008 (11), que establece un procedimiento para identificar y designar las infraestructuras críticas europeas (ECI), a fin de determinar las mejores prácticas para mejorar su seguridad y protección. Así como la Directiva sobre seguridad de suministro, de 18 de enero de 2006 (12) y las subsectoriales de Gas (13), o Nuclear (14).

Iniciamos el análisis desde el ángulo regulatorio español con unos breves apuntes generales de contexto. El Consejo de Ministros aprobó la Agenda Digital para España como la estrategia del Gobierno para desarrollar la economía y la sociedad digital en nuestro país (15). Esta estrategia se configura como el conjunto de las acciones del Gobierno en materia de Telecomunicaciones y de Sociedad de la Información. La Agenda se lidera conjuntamente por el Ministerio de Energía, Turismo y Agenda Digital y por el Ministerio de Hacienda y Función Pública. Dicha estrategia pretende fijar la hoja de ruta en materia de Tecnologías de la Información y las Comunicaciones (TIC) y de Administración Electrónica para el cumpli-

(10) Directiva EU 2016/1148.
(11) Directiva 2008/114/EC.
(12) Directiva 2006/89/EC del Parlamento Europeo y del Consejo.
(13) Regulation EU) n.º 994/2010.
(14) Ver Tratado EURATOM y la Convención de protección física de materiales nucleares.
(15) Acuerdo del Consejo de Ministros de 15 de febrero de 2013.

miento de los objetivos de la Agenda Digital para Europa en 2015 y en 2020, e incorpora objetivos específicos para el desarrollo de la economía y la sociedad digital en España.

Asimismo, el Ministerio de Energía, Turismo y Agenda Digital presentó a finales de 2017 el Plan Nacional 5G, a fin de introducir ordenadamente en España esta tecnología. Una de las líneas maestras del plan es, en el ámbito de la gestión y planificación del espectro radioeléctrico, diseñar y ejecutar acciones dedicadas a la ordenación, adjudicación y puesta a disposición de bandas de frecuencias necesarias para la prestación de los servicios de comunicaciones sobre redes 5G.

La implantación de la tecnología 5G deberá facilitar la prestación de servicios que requieran gran ancho de banda en movilidad, con el fin de impulsar las aplicaciones del Internet de las Cosas, como el coche conectado, el transporte inteligente o la digitalización del entorno rural, y también en el ámbito de las ciudades «Smart» (16).

Las nuevas amenazas de seguridad en el mundo digital, exigen, por tanto, una nueva forma de respuesta y protección.

En una infraestructura tradicional, los ataques a la red toman la forma de un ataque físico a las plantas generadoras o centrales/subestaciones en la distinta cadena de producción y suministro energético. Este tipo de ataque requiere, sin embargo, de la presencia y la coordinación sobre el terreno de un equipo preparado a tal efecto, y los daños son de carácter local. Sin embargo, las nuevas capas de información y accionabilidad de una red digitalizada permiten el ataque, a escala global, de la infraestructura por equipos desde cualquier parte del mundo; y requiere una adaptación e inversión constante por parte de los gestores de la red. Las publicaciones del ICS-CERT de los EEUU mencionan periódicamente al sector eléctrico como el más afectado por ciberataques de todo el catálogo de

(16) Deben tenerse en cuenta las Recomendaciones internacionales: ITU-T Y.4201 «High-level requirements and reference framework of Smart city platform» y ITU-T Y.4200 Requirements for interoperability of Smart city platforms». Su aprobación ha sido posible a través de la participación activa de España en las reuniones de la 'Comisión de Estudio 20 de la UIT sobre Internet de las cosas (IoT) y Ciudades y Comunidades Inteligentes'. La norma UNE en que se basan las recomendaciones aprobadas trata sobre las plataformas de servicios existentes en las ciudades y su interoperabilidad. Ha sido desarrollada por el Comité Técnico de Normalización CTN 178 de UNE de la Asociación Española de Normalización.

El mayor interés de estas recomendaciones radica en requerir que las plataformas de servicios de las ciudades sean abiertas y normalizadas, con independencia de los proveedores, pudiendo interoperar con sistemas externos cumpliendo condiciones de seguridad. Esto permitirá una gran reutilización de las aplicaciones desarrolladas y de que se repliquen soluciones de éxito entre las ciudades, lo que en definitiva es mejorar las ofertas de servicios y a menor coste.

En línea con lo anterior, también se están desarrollando actualmente normas (futuras recomendaciones UIT) –sobre sistemas externos tipo estación, puerto o aeropuertos inteligentes, edificios inteligentes, sistemas rurales e Inteligencia turística–, lo que permitirá desarrollar soluciones de fuerte impacto en las ciudades y abrir nuevos modelos de negocio.

Cabe recordar que las ciudades son responsables del 70% de las emisiones de carbono en el mundo, por lo que es fundamental que las autoridades locales, regionales y gubernamentales tomen medidas de calado.

sectores industriales, como se puede ver en la figura correspondiente a los meses de julio y agosto de 2017 (17):

Table 1: Assessments by sector, July / August 2017.

Assessments by Sector	July 2017	August 2017	July/August Totals
Chemical			
Commercial Facilities	4	3	7
Communications			
Critical Manufacturing			
Dams	1		1
Defense Industrial Base			
Emergency Services			
Energy	1	9	10
Financial Services			
Food and Agriculture			
Government Facilities	3	5	8
Healthcare and Public Health			
Information Technology			
Nuclear Reactors, Materials, and Waste			
Transportation Systems		5	5
Water and Wastewater Systems	4	3	7
Monthly Totals	13	25	38 Total Assessments

Además, estructuras tan estratégicas pueden ser fruto de un ataque con motivos políticos o militares, como el ciberataque que incapacitó la red eléctrica ucraniana en 2015 (18).

La ciberseguridad estaría compuesta por un compendio de normas, puesto que no existe una sola norma que lo regule todo de manera omnicomprensiva.

Como señalamos anteriormente, en la Unión Europea la Directiva Europea 2016/1148, fue adoptada con el fin de regular las medidas destina-

(17) http://time.com/3757513/electricity-power-grid-attack-energy-security/
(18) https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack

das a garantizar un elevado nivel común de seguridad en las redes y sistemas de información de la Unión.

En su artículo 14 establece que «Los Estados miembros velarán por que los operadores de servicios esenciales tomen las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilizan en sus operaciones. Habida cuenta de la situación, dichas medidas garantizarán un nivel de seguridad de las redes y sistemas de información adecuado en relación con el riesgo planteado».

Es decir, los Estados miembros velarán para que se cumpla con las medidas proporcionadas o adecuadas al riesgo planteado. Y también para que se adopten medidas a efectos de minimizar, reducir o prevenir incidentes que afecten a la seguridad. Asimismo, también se deberá notificar sin dilación indebida a la autoridad competente o al CSIRT (siglas del término en inglés Computer Security Incident Response Teams) los incidentes que tengan efectos significativos en la continuidad de los servicios esenciales que se presten para que se puedan tomar medidas con carácter institucional o nacional al respecto, en su caso.

En el mismo sentido, el artículo 16 de la misma, subraya el deber del Estado para que los proveedores de servicios digitales determinen y adopten medidas de seguridad técnicas y organizativas, para gestionar los riesgos existentes a la seguridad de las redes y sistemas de información que se utilizan. Por ello, deben adoptar medidas con relación a la seguridad de sistemas e instalaciones, gestión de incidentes, gestión de la continuidad de las actividades, supervisión, auditorías y pruebas, y cumplimiento de normas internacionales.

Con relación a esta materia, el Council of European Energy Regulators (CEER) (19) ha subrayado que «las amenazas a la ciberseguridad son uno de los riesgos más relevantes para el futuro mercado de la energía de la UE, así como para la seguridad del suministro tanto de electricidad, como de gas natural. La creciente complejidad de las tecnologías de la información y la comunicación aplicadas al sector energético conlleva que la ciberseguridad sea un aspecto de máxima relevancia para el futuro desempeño del sector».

Entre las múltiples recomendaciones presentadas por CEER, destacar:

— La necesidad de clarificar el alcance de las certificaciones sobre ciberseguridad en el ámbito del sector energético y, en concreto, la delimitación de quién debe cumplir con las mismas. En la medida que en el sector energético participan terceras compañías aportando soluciones y

(19) «The Cybersecurity Act in the Energy Context». A CEER Response Paper on the European Commission's Cybersecurity Proposals. 8 December 2017.

servicios en determinadas áreas de la cadena de valor, se estima del todo necesario que estas empresas se vean obligadas también a cumplir con los estándares a aplicar al propio sector energético. Esta medida debe favorecer también la cooperación entre sectores para el establecimiento de las normas y criterios comunes de supervisión y control.

— Se debe asegurar que la nueva legislación mantiene vigente las normativas en materia de ciberseguridad a nivel nacional y europeo que existían hasta el momento. La normativa europea tiene que contemplar los estándares de seguridad introducidos por alguno de los países miembros como mínimos.

— La relevancia de establecer cuál será el rol de los órganos reguladores de la energía en el ámbito de la ciberseguridad. Y también determinar qué relación debe existir entre estos reguladores y la agencia o agencias de ciberseguridad que se establezcan. En cualquier caso, el papel de los reguladores energéticos debe ser activo en la definición de los estándares.

— La implementación de nuevas medidas debe permitir periodos transitorios especialmente en el caso del sector energético, en que existe una gran cantidad de activos críticos y las inversiones para la adaptación pueden ser de importante magnitud.

Igualmente relevante en este campo normativo es la Ley de Protección de Infraestructuras Críticas, aprobada en España en 2011 y cuyo objetivo es Catalogar el conjunto de infraestructuras que prestan servicios esenciales diseñando un plan que contenga medidas de prevención y protección contra posibles amenazas.

Con relación a la ciberseguridad a nivel técnico y organizativo, hay que tener en cuenta también lo establecido por el Reglamento Europeo de Protección de Datos 2016/679, así como la existencia de otro tipo de protocolos o reglas internacionales, en especial las relacionadas con las transferencias internacionales de datos, como el Privacy Shield.

Estas tan sólo son algunas de las normas que tienen por objeto proteger el ciberespacio, pero debemos destacar, de nuevo, el Informe del Grupo de Expertos de la Comisión Europea sobre los riesgos de ciberseguridad en la red eléctrica (20), donde *se* identifican pormenorizada y sectorialmente riesgos potenciales de especial gravedad, e intencionalidad criminal:

— Ataques a puntos de fallo de la red: El objetivo de este tipo de ataque es acceder a los sistemas críticos de balanceado de la red y apagarlos directamente o mediante la simulación de algún tipo de sobrecar-

(20) https://ec.europa.eu/digital-single-market/en/news/cybersecurity-smart-grids

ga, inutilizándolos por un tiempo limitado o destruyéndolos. La defensa ante este tipo de ataque se facilita por la identificación y el relativamente reducido número de dichas infraestructuras críticas.

— Manipulación del mercado mediante falseo de información de oferta/demanda: Este riesgo se vería acentuado en un tipo de red en el que los usuarios prosumidores (generadores y consumidores a la vez) pueden intercambiar libremente servicios eléctricos. En este escenario, el gestor de la red sería equivalente al gestor de un mercado de servicios, en los que puede haber una inyección de órdenes con fines maliciosos o especulativos. Además de los riesgos económicos que puede suponer para el usuario minorista (y para lo que existen controles de acceso en los mercados financieros), esta manipulación puede comprometer los sistemas físicos, estimulando o erosionando la capacidad de generación y de transporte de la red distribuida.

— Ataques a los puntos de conectividad de la red: En una tipología de red en la que el usuario puede habilitar el funcionamiento de un punto de carga (por ejemplo, una electrolinera), este tipo de ataque busca deshabilitar programáticamente los puntos de carga y provocar el apagado de los dispositivos que estén conectados a ellos.

— Ataques a la privacidad de la información: En un mercado abierto de intercambio de servicios eléctricos (y con la teórica incorporación de la movilidad eléctrica al catálogo de demanda), existe el riesgo de acceso a la información de servicios consumidos con el fin de extraer información privada. Este escenario incrementa su complejidad, además, en el caso de que los registros de intercambio de servicios se validen mediante un sistema de cadena de bloques (blockchain), donde el único punto de entrada a la identidad de un usuario es la existencia de un pseudónimo de blockchain; es decir, la naturaleza pública de este registro puede permitir la identificación en un solo acto de los servicios consumidos por un usuario.

Todos estos puntos presentan retos a la propia existencia de la red, a la electrificación de la economía y la movilidad y a las capacidades técnicas de las instituciones de gestión y regulación. Asimismo, suponen una oportunidad para los actores del mercado en base a su capacidad para anticipar y solucionar problemas de seguridad de la red. Un estudio de la Agencia Europea para la Seguridad de la Información y la Red (ENISA) establece campos de trabajo en una serie de puntos para mejorar la capacidad de la red de evitar y mitigar fallos y ataques:

— Gobernanza y regulación del riesgo: Las instituciones deben controlar y dirigir la estrategia de privacidad y seguridad de la red, con especial hincapié en los componentes individuales que forman parte de la mis-

ma. Esta agencia debe monitorizar también la eficacia de la cadena de suministro energético para eliminar cuellos de botella y puntos superfluos que puedan ser fuentes de vulnerabilidad del sistema.

— Control de terceras partes: Los proveedores de servicios eléctricos deben ser responsables de las terceras partes con las que se asocian o subcontratan para mantener el nivel de seguridad exigido.

— Monitorizar el ciclo de vida de componentes y protocolos: Los proveedores deben estudiar e informar claramente de los requisitos y necesidades de diseño, mantenimiento y despliegue de los componentes de la red inteligente.

— Entrenamiento y formación del personal relevante: Los empleados deben ser formados en las posibilidades de fallos y las maneras de evitarlo, además de establecer, en la medida de los posible, certificaciones de confianza para evitar las posibilidades de fuga de información o sabotaje.

— Conocimiento de respuesta a incidentes: El personal y los sistemas deben conocer la respuesta necesaria ante fallos y ataques a la seguridad de la red, incluyendo el establecimiento de simulacros periódicos de problemas de esta índole.

— Auditoría y trazabilidad: Los reguladores deben asegurar que todos los actores del sistema dejan traza de las decisiones y rutinas de funcionamiento para aclarar y mejorar los procesos rápidamente en caso de fallo o descubrimiento de una vulnerabilidad.

— Continuidad de operaciones: Los actores de la red deben mejorar la redundancia de los sistemas para garantizar la prestación de servicios mínimos en caso de fallo de la red principal.

— Seguridad física: Los puntos vulnerables deben ser vigilados físicamente y visitados únicamente por personal autorizado.

— Establecimiento de sistemas de seguridad de la información: La información relevante acerca del sistema y los usuarios debe ser accedida programática y lógicamente solo por los usuarios con el nivel de permiso correcto.

En consecuencia, la ciberseguridad presenta un reto la hora de garantizar la estabilidad del sistema y dificultades en la interoperabilidad, la compatibilidad entre sistemas y las capacidades de absorción de la innovación digital en la red. Es responsabilidad del regulador trabajar y asegurar las medidas necesarias para superar estos retos, y una oportunidad para los actores y operadores comerciales de liderar la creación de valor en un nuevo paradigma de intercambio de servicios energéticos. Además, como venimos señalando, el reto de la transición energética incide de forma sobresaliente en estos aspectos. Debe recordarse que las redes gasistas y eléctricas deberán muy probablemente extenderse, modernizarse en buena medida, y automatizarse en

un período de tiempo muy corto. Y no sólo eso, sino que coexistirán, en el ámbito eléctrico, redes centralizadas y otras descentralizadas, sin perjuicio de la necesaria coordinación o cooperación entre sistemas o, cuando menos, ámbitos tecnológicos y económicos de regulación en materia de seguridad, operación y servicios, especialmente en media y baja tensión.

III. ¿DE LA ELECTRIFICACIÓN DE LA ECONOMÍA A LA TERCIARIZACIÓN DE LA ELECTRICIDAD?

La transformación de las redes presenta relevantes retos para los operadores en la planificación y operación de la red del futuro.

A futuro, las redes energéticas tendrán que integrar flujos bidireccionales de millones de puntos de conexión, gestionar una intermitencia renovable muy superior a la actual y estar dotada de una infraestructura digital y de telecomunicaciones que permita una mayor monitorización, control y automatización de la red.

Todo ello debe tenerse en cuenta también en el contexto del desarrollo de las denominadas «smart cities», donde el despliegue de nuevas infraestructuras energéticas, la sensórica, los sistemas de eficiencia energética y movilidad, cobrarán nuevo protagonismo y operatividad.

El conjunto de soluciones que canalizan esta conjunción urbana de generación descentralizada y servicios de movilidad basados en datos, suele englobarse en el concepto de Smart Grid. Una Smart Energy Grid o Smart Grid (red de suministro inteligente) es una red energética que, usando los avances en sensores, comunicación y computación, permite la interacción bidireccional entre el consumidor final (particular o industrial) y las compañías eléctricas, todo ello encaminado a ajustar la producción al consumo de energía, mejorar la distribución, reducir el gasto energético y disminuir las emisiones producidas en la producción, distribución y consumo de energía.

El desarrollo de las Smart Grids requiere importantes inversiones en las redes eléctricas y en la instalación, como viene haciéndose en este último año, de equipos de consumo y contadores inteligentes (Smart Metering) en los domicilios de los consumidores.

También en este campo, las Empresas de servicios energéticos proporcionan servicios de mejora de la eficiencia energética en las instalaciones o locales de un usuario, afrontando un determinado riesgo económico por desarrollarlo. En la práctica, según se señala en el Libro Blanco de las Ciudades Inteligentes, los contratos de servicios energéticos están orientados a la renovación y sustitución de las instalaciones energéticas (alumbrado, calefacción, etc.) por otras más eficientes,

consiguiéndose una disminución de emisiones en CO_2 de más del 10%. Dicha renovación, lejos de suponer un gasto extra para las corporaciones, supone un ahorro relevante en costes energéticos. Todos los costes y riesgos implicados son asumidos por la ESE, por lo que, además, liberan recursos de gestión para el cliente, en contraposición al modelo tradicional.

Otro aspecto que debe subrayarse en conexión con esta temática, es el de la edificación sostenible, que es aquella que asegura la calidad ambiental y la eficiencia energética de un edificio durante todo su ciclo de vida, desde su fase de diseño y su construcción hasta su fase de mantenimiento y derribo. Para ello, se deben seguir una serie de criterios, algunos de ellos aplicables a cualquier otro ámbito de una Smart City: integración de energías renovables (colectores solares), integración de servicios eficientes (limitadores de caudal, sistemas de alumbrado con sensores de presencia, etc.), adecuación a las condiciones del entorno: adaptación a las condiciones climáticas (sistemas de aislamiento, ventilación, etc.), orientación, impacto paisajístico, selección de materiales y métodos constructivos sostenibles, mantenimiento del edificio, y deconstrucción y valorización de residuos.

En este contexto, debe tenerse muy especialmente en cuenta el Cuarto Paquete Legislativo de reforma del sector energético en el marco del mercado interior y la lucha contra el cambio climático, ya mencionado. La normativa a la que aludimos tiene gran significación en la transformación regulatoria del sector, y aunque las menciones a la digitalización y su estructura productiva son muy escasas, implícitamente no pocas de las figuras y planteamientos que formula deben descansar en su desarrollo, y en la implementación efectiva de la mayor digitalización de la demanda eléctrica.

Uno de los aspectos principales de esta reforma energética, además de los ya citados de tratar de contribuir de manera eficaz a la descarbonización de la economía, es su interrelación con otros sectores industriales y comerciales. Hablamos de interrelación, e incluso interpenetración sectorial, ya que determinados aspectos regulatorios, e incluso materiales, en el desarrollo de esta reforma normativa, sólo tendrán lugar si concurren en la misma diversos sectores. Tal es el caso de la movilidad eléctrica en su relación con la distribución, infraestructuras y suministro eléctrico; los aspectos digitales y de la sociedad de la información en su vinculación tanto con infraestructuras energéticas, como con unidades y sistemas de almacenamiento, entre otros. O el caso, ya citado, de la edificación, que guarda, asimismo, relaciones de conexión con los

nuevos sistemas de calefacción y refrigeración, de transporte, y con la esfera digital.

Entre las nuevas figuras que plantea la reforma, como son las comunidades energéticas o los autoconsumidores o los agregadores, y determinados aspectos del nuevo diseño del mercado, la presencia, progresivamente intensiva, de los aspectos digitales es muy notable. Evidentemente, si abordamos temas más concretos, como los denominados «contadores digitales», por sí mismos o con relación a otros equipamientos y servicios que provee el sector, de nuevo el ámbito digital se convierte necesariamente en protagonista.

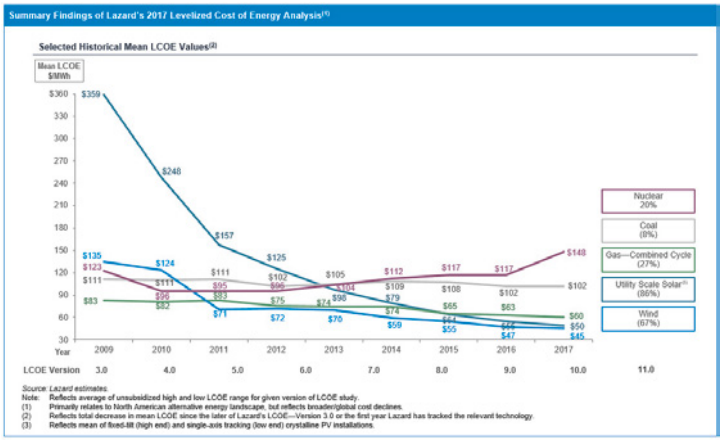
Nuria Encinar ha subrayado con propiedad la existencia de «un consumidor eléctrico digital», definiéndolo como el consumidor capacitado que interactúa en las plataformas web de las compañías eléctricas para todos los aspectos inherentes a la contratación del suministro, o cualesquiera otras relaciones con los productores de electricidad, para su consumo propio, utilizando una amplia variedad de dispositivos tecnológicos, como los teléfonos móviles, relojes inteligentes, tabletas, u ordenadores portátiles. Este consumidor accederá en tiempo real a la información necesaria para conocer la electricidad consumida, a las lecturas reales y a las que son más económicas, almacenará una cantidad notable de información que le permitirá aumentar el ejercicio de su derecho de elección, proceder a comparativas de ofertas y, en lo deseable, comprender de una manera más precisa los términos de facturación y suministro de estos servicios. Apunta también Encinar que se denominaría «relación comercial digital de electricidad» a todas las que se producen en el entorno del sector eléctrico, los consumidores, los dispositivos técnicos y los agentes que operan en el mismo para ofrecer las necesidades de aquellos en relación con el producto electricidad. Naturalmente, todos estos temas tienen una estrecha vinculación con los aspectos derivados de la protección de datos, la propiedad o titularidad de los mismos, su tratamiento, proceso y, en primer término, el consentimiento para su uso, acceso y almacenamiento, lo que en la doctrina jurisprudencial alemana, ya en los años ochenta, se denominaba «el principio de autodeterminación informativa» (21).

Los nuevos modelos de negocio deberán estar más ligados al carácter digital del servicio eléctrico: enlazar los ingresos con la creación de valor motivada por el consumo energético y el coste de operar y equilibrar una

(21) Ver Nuria Encinar: «Derecho de Comercio Eléctrico». Thomson Reuters. 2018.

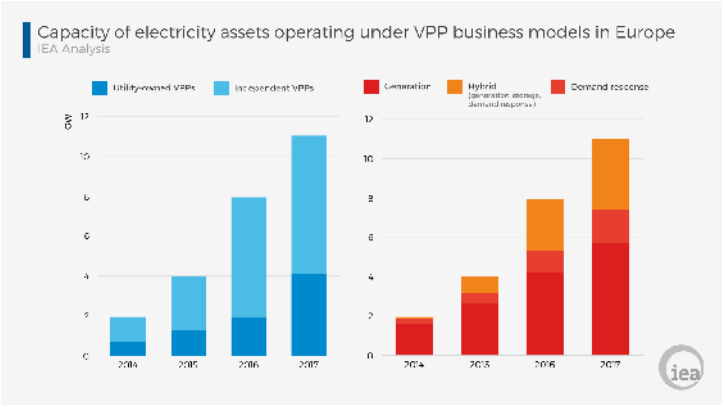
red más difícil de gestionar y operar (22). En particular, es razonable suponer que las nuevas vías de negocio ligadas a las comercializadoras eléctricas vendrán de servicios de valor añadido más allá del perímetro habitual del suministro energético, como la perfilización de usuarios, la consultoría de eficiencia energética a nivel doméstico e industrial y la integración a nivel de usuario de servicios de movilidad eléctrica. Un ejemplo relevante lo constituirá el diseño de plantas virtuales (VPP), un modelo de generación-consumo basado en comunidades descentralizadas y nuevos servicios digitales (23).

(22)



Esta transformación ya se está advirtiendo en el campo de la industria: en 2017 los ingresos agregados de las 20 mayores compañías eléctricas de Europa eran un 35% menores que en 2012, y la tendencia no muestra signos de revertir.

(23)



Como ejemplos de estos servicios auxiliares de optimización, la IEA estima que un sistema de *demanda inteligente* (es decir, que proporcione el mismo servicio al usuario, pero con un perfil de demanda más ajustado a la capacidad de oferta puntual) puede equivaler a una inyección de 185 GW (o la capacidad de generación combinada de Australia e Italia); esto equivale a una inversión en infraestructura por encima de los 200 mil millones de dólares.

La digitalización de un sector económico implica cambios bruscos en la organización y esencia de la actividad productiva, que resumimos a grandes rasgos en los siguientes puntos:

— Se prevén inversiones en redes eléctricas. Sólo en España, entre 30 y 34 mil millones de euros hasta 2030 (24).

— Disminución de las barreras de entrada: Los costes de prestación de la actividad por primera vez, o los costes de introducir un nuevo bien o servicio en el mercado, se reducen en tanto la forma de prestar la actividad se modifique mediante la programación de software, en vez del montaje tradicional de una cadena de distribución o manufactura. Estos cambios afectan incluso a servicios que necesitan de una inversión de capital inicial (tal como coche o alojamiento), puesto que dicha inversión se traslada a los actores del mercado que ya hayan realizado dicha inversión por estos u otros motivos (lo que se suele agrupar bajo el paraguas «economía colaborativa»). El coste de entrada cambia, por tanto, al conocimiento y despliegue de un sistema tecnológico, cuyos costes también están en continuo descenso. Es importante mencionar aquí la disminución de las barreras de entrada de tipo geográfico, siendo la digitalización la palanca más notable de expansión a nuevos mercados de una empresa que ha demostrado un funcionamiento eficiente en un nivel local.

— Cambios en la forma de demanda y compromiso del consumidor: El punto anterior implica que la mayoría de productos y servicios compiten en un mercado global con abundancia de capacidad instalada. En este sentido, el consumidor digital demanda un nivel cada vez mejor de servicio y precio y, ante todo, disminuye su capacidad de invertir tiempo en acomodarse a las peculiaridades de una oferta en concreto. Este marco explica la inversión cada vez mayor por parte de las empresas *experiencia de usuario* (UX), marketing viral o tendencias como la gamificación de los nuevos servicios.

— Erosión de las economías de escala: El rendimiento decreciente de las inversiones de capital en cadenas de suministro clásicas, junto con la

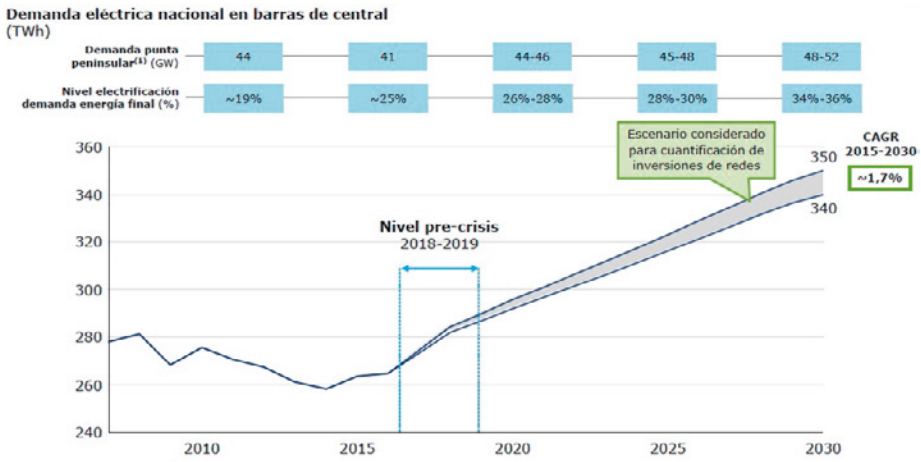
(24) Ver informe Monitor-Deloitte «Hacia la descarbonización de la economía: la contribución de las redes eléctricas a la transición energética». 2018.

disminución de costes de comunicación y computación, implica que la innovación deja de ser un elemento propio de grandes organizaciones para realizarse también en operadores pequeños con capacidad para crear y servir un nuevo nicho de negocio. Este cambio de paradigma implica que las economías de escala tradicionales (de competencia dentro de un mercado) perderían importancia frente a la economía de gama (o competencia hacia un nuevo mercado).

Así pues, ¿cómo pueden responder los actores principales del mercado energético ante estos retos? En primer lugar, hay una gran oportunidad en la mejora de *la experiencia de usuario:* Existe una tendencia a adaptar la oferta de cualquier producto al idioma más cercano a las necesidades de usuario, eliminando la tradicional oferta y facturación por *energía y limitación de potencia* y facturando por elementos comprensibles, como cargas de dispositivos, uso de electrodomésticos o selección de climatización. Asimismo, los sistemas de tarificación horaria (variable o fija) se deben paquetizar en formas de cobro más comprensibles y transparentes para el usuario, al estilo de las tarifas personalizadas de otros bienes de flujo.

En segundo lugar, el mercado debe satisfacer una creciente *autonomía de usuario*: Un servicio exitoso debe permitir al cliente la toma de decisiones conscientes e instantáneas. Estas decisiones pueden ser incrementales como la forma de consumo y la elección de sistema de tarificación, hasta disruptivas tal y como la fracción de energía que quiero consumir de la red frente a mi producción propia, o la capacidad de consumir servicios eléctricos de varios proveedores de manera simultánea, sean estos otros particulares o grandes comercializadoras.

Según el INE, más del 66% de la actividad económica de nuestro país está dedicada al sector terciario. Sector de servicios que observa en la actualidad, además, una nueva transformación de carácter excepcional por el surgimiento de la denominada economía de plataformas en la que se establecen, de forma generalmente muy eficiente, intercambios de bienes y servicios, con modelos innovadores y de bajo coste, apoyados en las tecnologías de información, acceso a Internet, y comunicaciones. La revolución digital supone un reto para esta estructura sectorial al promover un cambio radical o disruptivo del modelo energético tanto productivo (descentralizado, desintermediado) como de consumo (incluyendo la electrificación del sector del transporte). Un análisis de Deloitte estima que, junto con un ligero aumento de la demanda eléctrica total, el porcentaje de la demanda energética total cubierta por el sector eléctrico va prácticamente a doblarse en los próximos años [ver Figura].



Este aumento se debe a varios factores, el principal de los cuales es el aumento de las soluciones de movilidad eléctrica (principalmente transporte privado y de mercancías por carretera), pero también una mayor demanda fruto del crecimiento económico y una disminución de los costes de generación y distribución.

El cambio de escenario se produce, sin embargo, cuando intentamos analizar el impacto de la digitalización en este aumento de demanda, a través de los cambios en el comportamiento del usuario descritos anteriormente. Es de prever un aumento de las empresas dedicadas a las ofertas de servicios eléctricos, como la domótica, la optimización de costes o la posibilidad de utilizar la capacidad de generación propia como moneda de respaldo. Entre otros varios, dos fenómenos se vislumbran en este terreno, con muy importantes efectos económicos, jurídicos y regulatorios. El impacto del Internet de las Cosas (IoT) en el sector, directa o indirectamente. Y las nuevas infraestructuras de cadenas de bloques o «blockchain».

Como nos recuerda Moisés Barrio Andrés, dentro del IoT es cada vez más numeroso un tipo de objetos que pertenecen a la categoría de los denominados «contadores inteligentes», es decir, dispositivos electrónicos de medición de energía (gas y electricidad), calefacción, climatización, agua u otras magnitudes, y que van a permitir, en una dimensión mucho mayor que la de los contadores analógicos tradicionales, la generación, transmisión y análisis de datos sobre los usuarios y sus patrones de consumo. A través de estos sistemas, los operadores de

redes, los proveedores y otros actores podrán recopilar información detallada sobre el consumo de energía y las pautas de utilización, así como adoptar decisiones relativas a consumidores individuales sobre la base de perfiles de uso (25).

Un paradigma descentralizado, con multitud de productores y almacenadores y diferentes necesidades de consumo propio, transformaría esta estructura básica. El registro por cadena de bloques o *blockchain* cumple exactamente esa función: permite la comprobación de todos los intercambios de manera a la vez infalsificable y distribuida. Además, permite simultanear el registro de transacciones con una cuenta virtual o *monedero electrónico*, que puede dar cuenta del estado actual de la batería propia o la moneda convertible que puede ofrecerse a cambio de un determinado catálogo de productos o servicios.

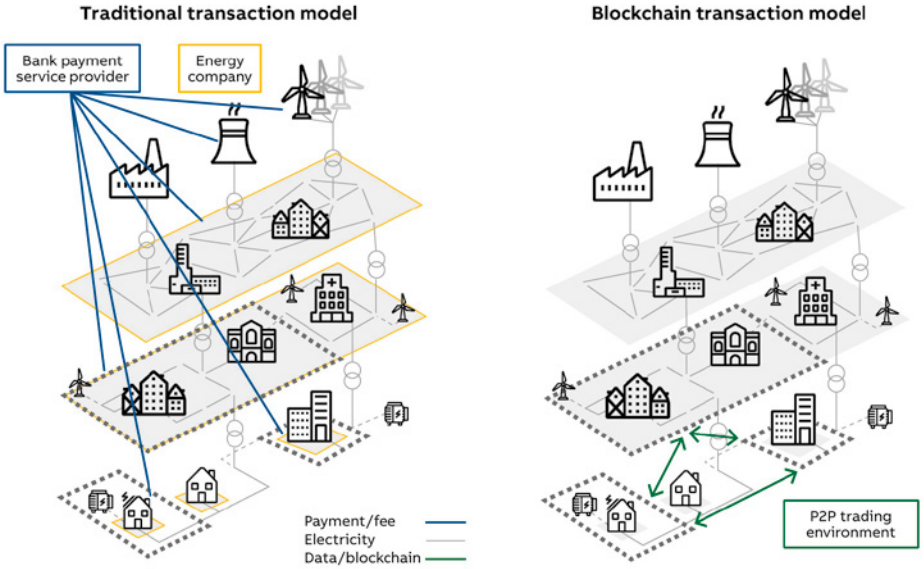


Figura: Ilustración del paradigma descentralizado de intercambio de servicios registrado mediante blockchain. *Izquierda*: Modelo tradicional en los que grandes generadores, consumidores, industrias y hogares con capacidad de generación intercambian servicios cotizados en una moneda común, centralizados en los proveedores de servicios bancarios. *Derecha*: Modelo descentralizado, en los que transacciones entre particulares se acreditan en un registro común no modificable; y las condiciones de intercambio (los «precios») son fijadas individualmente por cada uno de los actores [Fuente: Energy Market Intelligence]

(25) Ver «Internet de las Cosas». Moisés Barrio Andrés. Editorial Reus. Madrid 2018.

Desde un punto de vista puramente energético, y por tanto más fundamental, el registro por cadena de bloques se enfrenta a un problema mayor: el alto consumo energético necesario para su funcionamiento en sus formas establecidas actualmente. En particular, Bitcoin consume mundialmente más de 50 TWh anualmente (26), mientras que otras alternativas menos conocidas como Ethereum ya se acercan a los 5 TWh por año (27).

En conclusión, el paradigma descentralizado permitiría a los actores individuales (y, de forma especialmente innovadora, a los hogares) manejar sus preferencias de consumo de forma mucho más personalizada, a la vez que contribuyen a la oferta de servicios en función de sus capacidades de inversión en infraestructura de almacenamiento y generación. Estas reformas tienen el potencial de mejorar el poder adquisitivo energético de manera global, además de fomentar la movilidad eléctrica y nuevos servicios que hoy inician su camino de viabilidad, como el almacenamiento en formas no convencionales. Un gran desafío tecnológico, pues, con no pocos retos regulatorios, económicos y sociales.

(26) https://digiconomist.net/bitcoin-energy-consumption

(27) Nuevas implementaciones de sistemas de cadenas de bloques, como HyperLedger [https://www.hyperledger.org/], pueden contribuir a la implantación de este registro.

SUMARIO

Páginas

I
LA PERSONA EN EL MUNDO DIGITAL

Páginas

Páginas

Páginas

Páginas

Páginas

Páginas

Páginas

Páginas

Páginas

Páginas

VI
SEGURIDAD Y CIBERDEFENSA

CAPÍTULO 26. Seguridad pública en el mundo digital.

CAPÍTULO 27. El derecho a la ciberseguridad.

CAPÍTULO 28. De la ciberdefensa a las armas autónomas letales.

VII
TRABAJO Y MERCADO LABORAL EN UN MUNDO DIGITAL

CAPÍTULO 29. El futuro del trabajo y el empleo en la era de la digitalización y la robótica.

Páginas

Páginas

Páginas

IX

CREATIVIDAD, ACCESO A LA CULTURA Y DEPORTE EN UN MUNDO DIGITAL

Páginas

Páginas

X

JUSTICIA Y TUTELA DE LOS DERECHOS EN UN MUNDO DIGITAL: EL PAPEL DE LA TECNOLOGÍA EN LA REGULACIÓN, LA SUPERVISIÓN Y LA RESOLUCIÓN DE CONFLICTOS

CAPÍTULO 38. Ciberjusticia, métodos alternativos de resolución de controversias y tecnología.

CAPÍTULO 39. Autonomía privada y autotutela: oportunidades y riesgos de los *smart contracts*.

Páginas

Páginas

Páginas