19

# TECNOLOGÍA VS. REGLAMENTACIÓN

Manel Blasco Salvat
Consultor
**SEINTEX. Grupo AZERTIA**

La presente comunicación pretende simplemente reflexionar sobre algunos aspectos del avance de la Administración Electrónica en España que, a nuestro entender, no sigue el ritmo deseable. Siendo muy amplio el abanico de escenarios o temas a tratar, nos centraremos únicamente en aspectos como la firma electrónica, la protección de datos y las normativas, y todo ello necesariamente de forma muy esquemática y resumida.

La oferta actual de servicios de las empresas de tecnologías de la información y comunicaciones (TICs), en el marco de los requisitos de la normativa actual, no evoluciona a la misma velocidad que la tecnología. Mientras ésta ofrece todas las posibilidades para poder comunicar, securizar, propagar, almacenar,... cualquier tipo de información y su tratamiento, las normativas en España, sin olvidarnos de las de la Unión Europea, no ayudan, en algunos casos, a dar el impulso necesario para el desarrollo de la Administración Electrónica o, en un sentido más amplio, la comúnmente llamada Sociedad de la Información.

En el ámbito europeo, de forma distinta como acostumbra a suceder en EE.UU., se ha regulado siempre de forma excesivamente rigurosa, a nuestro entender, cualquier iniciativa o posible nuevo servicio basado en tecnología, creando, sin desearlo, dificultades o barreras para la evolución de los mismos. Cuando en base a la regulación europea, la administración española ha intentado legislar y reglamentar "a su medida" cualquier servicio o desarrollo tecnológico, normalmente ha incrementado las exigencias. Por ejemplo, para la protección de datos en Internet existe directiva europea 95/46/CE, la española 15/1999, y otras dictadas en las propias comunidades autónomas.

Entendemos que es necesario un punto intermedio entre legislar de forma muy estricta o no hacerlo, ya que la solución ideal debería basarse en un compromiso entre las ventajas e inconvenientes de los dos extremos, considerando que cualquier normativa ha de ir siempre acompañada de inversiones, acciones complementarias e impulso por parte de los distintos actores de la Sociedad de la Información.

Tal como hemos indicado, a continuación entramos a describir de forma resumida los tres aspectos mencionados.

## FIRMA ELECTRÓNICA

La legislación española se ha caracterizado por ser muy "dinámica" en temas de firma electrónica, por la cantidad de normas que se han dictado, e incluso muy "rápida", ya que en algún caso se ha anticipado a la europea. La más reciente es de diciembre de 2003 (Ley 59/2003). Esta legislación nunca implicó a organismos públicos y privados en una misma finalidad, que debería ser la puesta en funcionamiento de mecanismos basados en firma electrónica. Sin entrar a enumerar la evolución histórica, nos encontramos en la actualidad distintas problemáticas que dificultan su aceptación e impulso:

a) Existen distintos tipos de documentos: documentos firmados a mano, documentos auténticos firmados por un funcionario público o documentos públicos (fedatarios públicos). Si los intentamos equiparar con términos como *firma electrónica* (FE), *firma electrónica avanzada* (FEA) o *firma electrónica reconocida* (FER), las analogías o paralelismos a regular entre los "tipos de documento" y "tipos de firma" da como resultado una combina-

ción excesiva de soluciones, difícil de asimilar por los potenciales usuarios en la Sociedad de la Información.

b) Al querer equiparar la FER con la firma manuscrita, el problema básico es que ésta siempre se ha caracterizado por tener un "aspecto visual", ya sea en un soporte papel o en un visor o pantalla, y en cambio la FER no puede apreciarse "sensorialmente" ni tiene sentido en soporte diferente al electrónico.

c) La FER es la que tiene, normativamente, el mismo valor que una firma manuscrita, y se define como la FEA basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. Contiene "intrínsecamente" propiedades o características del propio certificado que dan validez a la misma (que el certificado se emite como tal, para la función concreta de firmar,...). Además posee unas características "extrínsecas" otorgadas por la *Autoridad de Certificación* (AC) o por el *Prestador de Servicios de Certificación* (PSC) como por ejemplo: demostrar que los métodos de firma son fiables, conservar documentos 15 años, mantener directorios de certificados emitidos y revocados, respetar la LOPD,... Deberían revisarse los mecanismos existentes para velar por el cumplimiento de estas exigencias, a fin de que ello no dependa en exceso de comprobaciones a posteriori. Sorprende, por ejemplo, la facilidad para constituirse en PSC.

d) La ley indica que a la firma electrónica, aunque que no sea FER, "no se le negarán efectos legales". Una FE, que por algún motivo intrínseco o extrínseco no es FER, no puede equipararse a la firma manuscrita, sin embargo, sí puede ser admitida procesalmente en una prueba judicial. ¿Debe ser un juez quien decida la validez de ésta FE?.

e) La FEA está vinculada únicamente al firmante, permitiendo su identificación. La ley no especifica quién debe realizar la identificación, pudiendo ser ésta realizada por un organismo público o privado. ¿No sería lógico que la "identificación" la realizara un funcionario u organismo público en vez de una entidad privada, sobretodo cuando la FEA tiene un efecto legal?.

f) La vigente Ley de firma electrónica 59/2003 regula las prestaciones y obligaciones de las personas jurídicas, aunque no son éstas normalmente las que firman, ya que lo hacen siempre personas físicas (en el acto de firmar el bolígrafo lo maneja una persona, no una empresa).

g) Existen algunos PSC que publican de forma retribuida el acceso a sus *Listas de Certificados Revocados* (RCL), penalizando la propagación de uso de los mismos.

h) Mucha gente duda de la "validez" de una firma electrónica, desconociendo seguramente la enorme seguridad que proporciona frente a la firma manuscrita.

i) Aunque se realicen muchas peticiones de certificados reconocidos (tarjetas criptográficas) a las AC, existen, sin embargo, muy pocos ordenadores personales con lectores de tarjetas criptográficas. Es necesario promocionar la distribución de los mismos, implicando a sectores de equipamiento de hardware, a fin de que un lector de tarjeta criptográfica sea tan común como empiezan a serlo ya los distintos lectores de tipos de tarjetas de fotos digitales (CompactFlash o SmartMedia), propagados por las empresas interesadas para impulsar el propio mercado de consumo.

j) Es necesaria una convergencia de necesidades adecuadamente normalizada para la implantación de los certificados reconocidos a nivel interestatal, diferenciando la Unión

Europea de los otros países del mundo, ya que la validez de una FER fuera del estado español no está convenientemente reconocida. Deben armonizarse todas las legislaciones para poder dar validez al certificado reconocido en otros países. Se está intentando regularizar el DNI electrónico, pero ¿existirá un pasaporte electrónico?

Como contrapunto existen buenas implementaciones en algunos campos como los Notarios y/o Registros, que permiten realizar la inscripción de una empresa en 48 horas, realizar visados de profesionales colegiados como Arquitectos, Ingenieros,... todas ellas "corporativas", casi nunca de relación entre organismos, ya sean públicos o privados.

## PROTECCIÓN DE DATOS

Cada país europeo tiene su propia regulación destinada a la protección de datos personales. A continuación expondremos algunos aspectos para mostrar los puntos débiles de la normativa actual:

a) Existen resoluciones judiciales que no consideran como "transferencia" de datos ciertas informaciones obtenidas en Internet, basándose en el principio de que son accedidas *desde cualquier lugar, están virtualmente en todas partes y, por tanto, no existe consecuentemente "movimiento de datos"*.
b) La información accesible desde las redes públicas, por ejemplo Internet, es muy difícil de registrar a nivel de propiedad intelectual, sobretodo entre diferentes países, ya que el hecho de visualizar una página de contenidos, significa por sí mismo una transferencia de un lugar a otro (concepto contrario al del punto anterior).
c) Todo organismo público o privado debe declarar a las Agencias de Protección de Datos (estatal o comunidad autónoma), las estructuras de información que contengan datos personales. Sin embargo, no tiene mucha utilidad, a nuestro modo de ver, conocer sólo la estructura de un modelo de datos, ya que lo importante es el posible movimiento de los datos personales entre dos partes, aunque sea en un registro formal, puesto que de esta manera se podría estudiar la "ubicación" o "propagación" de los mismos.
d) Con la regulación actual, podría interpretarse que una empresa no debería trabajar con los datos de los clientes sin su permiso expreso, regulado en el *documento de seguridad* de la empresa, situación difícil de asumir en muchos casos.
e) Sería más lógico realizar contratos entre organismos que registrar en las Agencias de Protección de Datos las estructuras de información de los mismos.
f) En una relación entre dos partes, por ejemplo una compra-venta, no puede atribuirse a ninguna de ellas la titularidad "exclusiva" de la información generada en la transacción.
g) La transferencia de datos personales entre países no está resuelta de forma simple y global, creándose "paraísos" de fraude de propiedad de la información.
h) Existe un nuevo peligro para las personas que envían correos electrónicos, cuya cuenta de correo está identificada con su nombre. Se están implementando procesos en los servidores de correo para conocer o relacionar lo que buscamos o enviamos y así llegar a "cierto conocimiento" de las personas. Si consideramos éste conocimiento como datos "personales". ¿No estaríamos en un caso de imposibilidad de protegerlos?.

i) Las modalidades del control del "correo basura" entre los distintos países de la Unión Europea es muy distinta. Mientras en países como Italia y Alemania se exige un consentimiento explícito para recibir correo, en Grecia existe una lista de "no enviar" y en España se considera la aceptación de forma implícita. Actualmente, el incumplimiento de las normativas del "correo basura" únicamente es sancionado en algunos países.

En resumen, en el ámbito de la protección de datos debería cambiarse el enfoque de controlar los "tipos" de datos por el de controlar la "finalidad" de los mismos.

## NORMATIVAS

Se está regulando continuamente la comunicación telemática de muchos trámites administrativos o judiciales. Pensamos que dichas reglamentaciones no son lo suficientemente "completas" para protocolarizar comunicaciones totalmente electrónicas entre las partes, ya que la mayoría de las veces dicha comunicación es un proceso paralelo, en el que se requiere o se obliga a enviar igualmente la comunicación en soporte papel (correo, fax,...).

Por ejemplo el RD 209/2003 (registros telemáticos) no especifica la obligatoriedad de su utilización en ciertos colectivos o transacciones específicas, dejando indefinido el organismo o ente que arbitre dichas comunicaciones. Los documentos que deben publicarse para un simple registro telemático (boletines, calendarios, definir trámites,…) hace desistir a cualquier organismo que desea impulsar algún servicio de éste tipo.

Actualmente, casi todos los servicios de tramitación on-line requieren de pasos o acciones en soporte papel y/o presencia posterior para conformar el trámite realizado.

No debemos olvidar la cantidad de legislación existente en todos los ámbitos tecnológicos, a la que se sumarán próximamente artículos de la nueva constitución europea, por ejemplo referentes a la protección de datos. Estos cambios pueden provocar una inestabilidad en los procesos, servicios o soluciones ya existentes.

## CONCLUSIONES

Para cada casuística concreta las leyes españolas no deberían ser más exigentes que las europeas, siendo deseable una unificación normativa, menos rigurosa y que armonice las necesidades de todos los actores implicados. Esta "suavización de requisitos" no implica necesariamente bajar el grado de requerimiento de las normativas, aunque puedan ser necesarias inversiones públicas en cada escenario para conseguir el mismo efecto.

Muchas de las soluciones que actualmente están funcionando en la Administración Electrónica, no alcanzan el cumplimiento total de la normativa actual, ya que seguramente si se vieran obligadas a ello nunca se hubieran puesto en funcionamiento.

Para cada normativa a implementar, los organismos privados están "esperando" que las administraciones públicas "inicien" sus inversiones en servicios de la Administración Electrónica, necesitando además de la colaboración de las empresas privadas para el impulso final en la Sociedad de la Información.

La confianza en la red y sus servicios, y en consecuencia en la Administración Electrónica, sólo se conseguirá implicando tanto a organismos públicos como privados trabajando siempre

en una misma dirección y suavizando las exigencias legales de cualquier servicio o técnica a aplicar. La tecnología ya está a nuestra disposición, pero no su correcta implementación o difusión, ni tampoco las inversiones necesarias para su impulso. Por ejemplo, que el ciudadano no peticione certificados reconocidos, puede estar provocado por los pocos servicios existentes, y no existen más servicios por falta de demanda de los mismos. Todos los organismos, especialmente las administraciones públicas, debe aunar esfuerzos para cerrar este círculo de necesidades.