>> Jorge Dávila

La legislación sobre firma electrónica se remoza

Después de casi cinco años, el Real-Decreto-Ley sobre firma electrónica tiene que ser revisado y a través de una sucesión de anteproyectos se intentan corregir errores pasados. En estos borradores se habla ya, sin vergüenza ni tapujo, del prometido *DNI electrónico* y de las *identidades jurídicas*, pero todavía hay más cosas y algunas carencias interesantes en ellos. Remozar la normativa de firma electrónica es algo necesario, aunque quizás la carencia de una normativa clara no sea la responsable de que la firma digital generalizada siga siendo, hoy por hoy, una quimera.

El actual y mutable **Anteproyecto de Ley de Firma Electrónica** –en plazo de consulta en el CGPJ y en el Consejo de Estado es los momentos en que esto se escribe– algún día reemplazará al precipitado Real-Decreto-Ley 14/1999 de 17 de septiembre, que sacrificó su calidad por la premura de adelantarse a la Directiva europea 1999/93/CE. Tras la ratificación del Real-Decreto por el Congreso de los Diputados, se acordó la tramitación de dicho Real Decreto-Ley como Proyecto de Ley para someterlo al debate parlamentario; no obstante, esta iniciativa decayó al expirar el mandato de las Cámaras en marzo de 2000 al terminar su primera legislatura el Sr. Aznar.

Este Real Decreto-Ley fue aprobado con el objetivo declarado de fomentar la rápida incorporación de nuevas tecnologías de seguridad a las comunicaciones electrónicas de las empresas y Administraciones Públicas. Según el ejecutivo, esta indicativa normativa sería un medio eficaz para potenciar el **crecimiento y competitividad** de la economía española, a la vez que conseguiría la **confianza generalizada** en la realización de transacciones electrónicas en redes abiertas. Después de cinco años, no hay la menor traza de que tal cosa haya realmente pasado o vaya a pasar en breve.

Como las prisas no son buenas consejeras, el Ministerio de Ciencia y Tecnología, desde hace tiempo intenta enmendar su "*salida de caballo andaluz, y parada de burro manchego*", y desde hace ya bastantes meses reconoce la necesidad de elaborar un nuevo texto con el máximo de publicidad que su página Web puede proporcionar.

Alegando actualizaciones tecnológicas –que no se han producido–, y la experiencia adquirida en la prestación de servicios de certificación –del todo marginal y minoritaria–, el MCyT, junto con los ministerios de Justicia, Economía, Interior y Administraciones públicas, con la asesoría de una cohorte de 50 empresas e instituciones, se ha embarcado en la redacción de varios nuevos borradores para un anteproyecto de firma electrónico y, con ello, califican de obsoleta y finalmente inútil la norma 14/1999. Los hechos contrastables son que la utilización de la firma electrónica, avanzada o no, en España, tal y como la describe el Real Decreto-Ley, es meramente anecdótica. La difusión de la firma electrónica es muy baja y este sector de la tecnología esta claramente colonizado por los Estados Unidos.

Uno de los elementos definitorios de los borradores difundidos es que el ejecutivo adopta definitivamente un estilo neoliberal claro y, de facto, abandona la firma digital a la autorregulación del mercado, pasando el Estado a un discretísimo segundo plano.

Antes de entrar en las novedades propuestas por el nuevo anteproyecto es conveniente resaltar que reconoce que los "**datos necesarios para la creación de firmas electrónicas pueden utilizarse igualmente para proteger el secreto de las comunicaciones**", pero opta por decir que "**dicha función no se contempla en el ámbito de regulación de esta Ley**", desterrando así, fuera de este anteproyecto, el espinoso tema de la defensa activa (criptográfica) de la confidencialidad de las comunicaciones digitales como derecho individual y colectivo.

PRESTADORES

El último borrador conocido de este anteproyecto establece nuevos mínimos para la prestación de servicios de certificación, como son la **identificación de los titulares** de los certificados y la composición de éstos. En particular, el borrador indica que los prestadores de servicios de certificación podrán limitar su responsabilidad, "**estableciendo mecanismos de coordinación con los Registros Públicos mediante conexiones telemáticas, a los efectos de verificar los datos que figuran en los certificados en el momento de la expedición de éstos**" ¿Quiere eso decir que por el hecho de erigirme como "potencial" emisor de certificados digitales, uno puede tener acceso inmediato a todas las bases de datos y registros públicos que identifiquen completa y verazmente a todos y cada uno de los ciudadanos? Esperemos que no sea así ya que, en ese caso, las autoridades de certificación terminarán siendo el nicho óptimo para todos los *spammers*[1] y adoradores del telemarketing.

Otro de los elementos definitorios de los borradores difundidos es que el ejecutivo adopta definitivamente un estilo neoliberal claro y, de facto, abandona la firma digital a la autorregulación del mercado, pasando el Estado a un discretísimo segundo plano. Con este giro copernicano se ve la eficacia de los grupos de presión y empresas del sector de la seguridad sobre el actual MCyT.

DNI ELECTRÓNICO Y PERSONAS JURÍDICAS

En cuestiones más técnicas podemos resaltar como una de las novedades, que se hace referencia explícita al DNI electrónico, que define la firma electrónica de personas jurídicas, y que precisa los mínimos –¡realmente mínimos!–, a satisfacer para poder prestar ser-

[1] Véase como "generadores de SPAM"; es decir, de correo-e no deseado o solicitado por su destinatario.

vicios de certificación, así como las responsabilidades que con ello se asumen.

En este escenario, el prometido DNI electrónico asumiría todas las funciones electrónicas de identificación de sus titulares y de generación de firmas digitales válidas ante todas las Administraciones Públicas dejando fuera, como ya hemos dicho, la posibilidad de usarlo para el cifrado (confidencialidad) de transmisiones o datos.

En cuanto a la emisión de certificados digitales de identidad para personas jurídicas, los últimos borradores no encuentran más solución que entregar la identidad jurídica a las identidades físicas de sus administradores y apoderados. La custodia de la clave privada de firma y del certificado reconocido de las personas jurídicas corresponderá a "**una sola persona física**", cuyo nombre y apellidos figurarán en el certificado de la persona jurídica.

La inclusión de este nuevo tipo de certificados pretende ser respuesta a una demanda clásica de los servicios de certificación; no obstante, la solución propuesta parece más diseñada para las pymes que para grandes corporaciones; ya que en las mini-pymes es fácil encontrar "un solo jefe" que representa a toda la entidad jurídica. Técnicamente hay soluciones más creativas que el recurso a un modelo autocrático, pero no deben haber llamado la atención de los promotores de este anteproyecto.

El artículo 5 sobre "Firma electrónica en las Administraciones Públicas" reconoce el uso de la firma electrónica dentro de las Administraciones Públicas y sus entes públicos, y en las relaciones de cualquiera de ellos con los ciudadanos. En cada caso, la normativa sobre firma electrónica estaría acompañada por otras normas adicionales, necesarias para salvaguardar las garantías de cada procedimiento administrativo. Entre esas condiciones adicionales es significativo que se mencione sólo como posibilidad la necesidad de un fechado electrónico fehaciente (*time stamping*) de los documentos electrónicos que sean parte de un expediente administrativo.

En el artículo 10, sobre la "**Suspensión de certificados**" el anteproyecto introduce el nada claro concepto de "suspensión" como algo que quita validez al certificado, pero que no es una revocación hasta que termina pasando un cierto tiempo. Introducir este matiz de invalidez dentro del ciclo de vida de un certificado sólo tendría sentido si el certificado pudiese dejar de estar suspendido y pasar de nuevo a estar activo, pero no es éste el caso del último anteproyecto del MCyT disponible en la red.

En el artículo 13 es donde se centran las obligaciones a cumplir por los prestadores de servicios de certificación, y de las cuales habría que resaltar el apartado (c). En este apartado el prestador de servicios de certificación acepta "**no almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios**"; dicho de otro modo, tienen que demostrar "**que no pueden hacerse con una copia de la clave privada de firma**" de ninguno de sus clientes. Cuando no es el titular el que genera en privado su clave de firma, es imposible demostrar que no se haya podido copiar; esto debería descartar soluciones como, por ejemplo, que el Ministerio del Interior sea el que generase las claves de firma de los DNIs electrónicos. Para evitar querer decir esto, en el punto (h) de ese mismo artículo se acepta la "generación delegada" de las identidades de firma, pero se pide "**garantizar su confidencialidad durante el proceso de generación y su entrega, por un procedimiento seguro, al firmante**". La aceptación de esta **generación delegada de las identidades de firma** debilitará, en el futuro, la eficacia jurídica de las firmas que con ellas se generen.

En este mismo artículo se pretenden incluir algunas cautelas sobre la salvaguarda histórica de certificados para la posible verificación de firmas durante no menos de quince años, pero la solución propuesta no trata correctamente el problema de la **verificación de firmas históricas**[2] por lo que la componenda propuesta no es eficaz ni correcta.

Lo que para mi está muy claro desde 1999 es que tener una normativa adecuada sobre firma digital no es lo que activará las relaciones administrativas o comerciales en redes abiertas.

El artículo 14 sobre las condiciones de emisión de certificados, enumera correctamente requisitos mínimos que se deben exigir a la emisión de un certificado de identidad, pero además abre la interesante posibilidad de emitir nuevos **certificados con pseudónimos**.

Para evitar que puedan zafarse de sus responsabilidades los "enmascarados" detrás de un pseudónimo, los emisores de estos certificados habrán de hacer constar este hecho en los certificados y, además, guardar celosamente la relación de esos alias con los nombres reales de los ciudadanos. Partes de esta relación se entregarán a las autoridades judiciales cuando así lo requieran éstas.

DISPOSITIVOS DE CREACIÓN DE FIRMA

En el artículo 20 se hace una descripción más precisa y bastante correcta de las características que deben tener los dispositivos seguros de creación de firma; sin embargo, la verificación de firmas queda relegada al artículo 21. En este caso, el anteproyecto no sabe cómo resolver el problema de que el firmante esté realmente firmando los que ve en pantalla. La razón de ello es que los dispositivos en los que se está pensando (tarjetas inteligentes y llaves USB) no tienen pantalla y tan sólo "firman" un valor *hash* calculado por alguna aplicación que está fuera del perímetro de seguridad del dispositivo de seguridad. La solución de este problema requiere artefactos más grandes y más caros, aunque al precio que están los teléfonos móviles pronto pueden llegar a generalizarse en el mundo de la electrónica de consumo.

Podemos decir que, a pesar de todo, es de agradecer que se corrijan errores anteriores y que la normativa sobre Firma Electrónica se actualice; aunque, visto el éxito de iniciativas anteriores, no es de esperar un éxito excesivo en esta ocasión. Lo que para mi está muy claro desde 1999 es que tener una normativa adecuada sobre firma digital **no es** lo que activará las relaciones administrativas o comerciales en redes abiertas. Mal que bien, hemos tenido una norma y no se le puede echar la culpa, ni siquiera parcialmente, a que este sector no haya funcionado.

Quizás haya que buscar las causas en otros sitios: neoliberalismos electorales, empresas del sector, una administración en estado cianótico, una pobre formación técnica generalizada, la carencia de I+D+I suficiente y de calidad, la cultura del "pelotazo" y del "aparentar", la "resistencia pasiva" de estructuras y arcanos, etc., para llegar a entender por qué la firma electrónica generalizada es todavía hoy una quimera, un animal mitológico de la era del caído NASDAQ Rey. ■

Jorge Dávila Muro
Director
Laboratorio de Criptografía
LSSI - Facultad de Informática - UPM
jdavila@fi.upm.es

[2] Es decir, verificar firmas digitales después de haber expirado el certificado que da autenticidad a la firma.