LA REGULACIÓN DE LA FIRMA ELECTRÓNICA: MODIFICACIONES INTRODUCIDAS POR EL BORRADOR DE ANTEPROYECTO DE LEY EN RELACIÓN AL REAL DECRETO-LEY 14/1999

MARTA MORENO DELGADO
DAVID SAN MARTÍN SEGURA

SUMARIO

1. INTRODUCCIÓN

La contratación electrónica requiere inexorablemente garantías en relación con ciertos aspectos básicos de la seguridad jurídica, como la identificación de las partes, la privacidad de las comunicaciones, la seguridad e integridad de los mensajes y el no repudio del contrato por cualquiera de las partes. En el tráfico jurídico tradicional estas garantías provienen de la presencia física de las partes, la firma manuscrita, la intervención de fedatarios públicos, etc. Sin embargo, en un proceso de contratación en el que las partes no tienen por qué conocerse, ni llegar a verse físicamente, esas

garantías deben proceder de la implementación de nuevos mecanismos electrónicos y de su regulación legal. En ello precisamente consiste la firma electrónica.

La primera regulación en España fue introducida por el Real Decreto-ley 14/1999 de 17 de septiembre[1]. Su aprobación suscitó controversias doctrinales y políticas, debido a que su tramitación se produjo antes de aprobarse la Directiva 1999/93/CE sobre firma electrónica[2], a la cual debían acomodarse las legislaciones de todos los Estados miembros. El Gobierno español dio lugar así a una peculiar trasposición *ex ante*, aunque prometió la inmediata tramitación de la norma como Proyecto de Ley. No obstante, esta iniciativa decayó al expirar el mandato de las Cámaras en marzo de 2000, y no ha sido hasta diciembre de 2001 cuando se ha elaborado el borrador del anteproyecto de Ley de firma electrónica[3]. Los objetivos de esta nueva norma son principalmente corregir las deficiencias que presentaba el Real Decreto-ley de 1999, adaptarse al marco legislativo de la Directiva comunitaria e introducir novedosos instrumentos, entre los que el DNI electrónico es el más relevante.

Como puso de manifiesto parte de la doctrina, la norma debería haberse regulado desde un principio como Ley ordinaria, evitando las discrepancias con la Directiva y los defectos producidos por la ausencia de debate parlamentario[4].

Este artículo no pretende realizar un estudio exhaustivo sobre la firma electrónica. Se ha tratado de localizar los aspectos esenciales de su regulación, centrando la atención en las modificaciones y novedades recogidas en el borrador del anteproyecto de 2001 con respecto al Real Decreto-Ley de 1999. Se pretende evaluar si la nueva regulación subsana las deficiencias que presenta la actual normativa, y si las novedades que introduce son adecuadas para incrementar la confianza de los usuarios en este reciente instrumento.

Previamente se esbozarán los conceptos y fundamentos técnicos de la firma electrónica, siquiera sea de forma esquemática.

2. DEFINICIÓN Y FUNCIONES DE FIRMA ELECTRÓNICA. ASPECTOS TÉCNICOS

La firma electrónica trata de resolver las incertidumbres que se dan en la contratación electrónica, mediante un sistema que aporte garantías de seguridad a los usuarios.

El problema podría plantearse en los siguientes términos: dos sujetos –A y B-, quieren celebrar un contrato, utilizando para ello un medio electrónico, Internet. Dado que las partes no van a verse físicamente durante todo el proceso de contratación, éste sólo puede producirse a través de un mensaje en forma electrónica que A envíe a B, y en el que se contengan los términos del contrato. La ausencia de presencia física de los

[1] B.O.E. nº 224, de 18 de septiembre de 1999. Convalidado en el Congreso en sesión del 21 de octubre de 1999.

[2] Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999 (DOCE 19 enero 2000).

[3] El borrador puede ser consultado en la web del Ministerio de Ciencia y Tecnología: www.setsi.mcyt.es/novedad/firma271201.html

[4] Entre otros, MARTÍNEZ NADAL, A., *La ley de firma electrónica*, Civitas, Madrid, 2000.

contratantes y el uso de Internet como medio de emisión del mensaje produce algunas dificultades y peligros para las partes:

- En primer lugar, cómo cerciorarse de que los sujetos son quienes dicen ser. Es decir, cómo sabe B que el mensaje ha sido realmente enviado por A, cómo sabe A que quien lo ha recibido ha sido B, y no una persona suplantándole. Este riesgo procede de que en Internet las relaciones jurídicas son esporádicas y se producen sin necesidad de contactos previos.

- Existen otros problemas: cómo asegurar que el mensaje no ha sido leído por un tercero mientras fue enviado (lo que se denomina *confidencialidad*) y que no fue alterado por ese tercero (*integridad*). Estas incertidumbres se deben a que Internet es una red abierta, y en la que un mensaje recorre complejos itinerarios hasta llegar a su destino. Además, se plantea cómo garantizar a B que el emisor del mensaje no va a negar después haber sido el autor del mensaje, quedando así desvinculado del contrato (lo que suele llamarse *no repudio de origen*).

Identidad, atribución, confidencialidad, integridad y *no repudio* son las funciones que deberían lograrse para obtener plena seguridad jurídica. Ése es el objetivo con el que se crea la firma electrónica.

Ahora bien, no todos los sistemas de firma electrónica cumplen plenamente las funciones mencionadas. Existen distintas tecnologías de firma que determinarán la eficacia jurídica de los documentos sobre los que se aplican. En la actualidad, el sistema más difundido y que cumple todas las funciones indicadas es la criptografía asimétrica, basada en una infraestructura de clave pública (*ICP* o, en Inglés, *PKI*). Su funcionamiento puede describirse de la siguiente manera.

A es el emisor y signatario del mensaje, y B es el receptor. A dispone del par de claves, pública y privada, y B dispone únicamente de la clave pública (que corresponde a la clave privada de A). Así pues, A aplica su clave privada sobre el mensaje y lo envía, con lo que el mensaje queda cifrado. Cuando B lo recibe, aplica la clave pública sobre el mensaje cifrado, haciéndolo legible de nuevo. Al aplicar esa clave, además, se pondrá de manifiesto si el mensaje ha sido alterado en lo más mínimo durante la transmisión. Si la clave pública que aplica B sobre el mensaje no se corresponde con la clave privada con la que A lo firmó, el mensaje no se abrirá. De esta forma, se sabe indubitadamente que A fue quien firmó el mensaje (así no puede negar su autoría) y que el mismo no fue leído ni alterado durante la transmisión[5].

Sin embargo, la aplicación de la criptografía asimétrica sobre la totalidad del mensaje puede resultar demasiado costoso, dado el actual estado de la tecnología de transmisión por Internet. Por ello suele realizarse previamente una operación sobre el mensaje: la aplicación de una función de *hash* o resumen. “La función de *hash* es el algoritmo que transforma una secuencia de bits en otra menor, y que se aplica tanto para

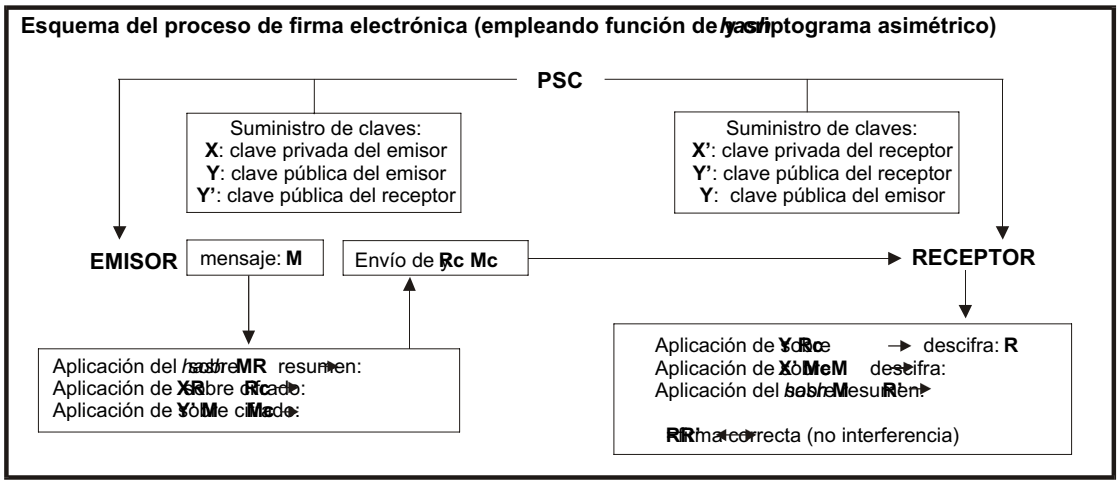
[5] Estas garantías no pueden conseguirse con la utilización de la criptografía simétrica. En ella emisor y receptor comparten una única clave, con la que el signatario cifra el mensaje, y el destinatario lo descifra. De esta forma las partes quedan indeterminadas, pues no puede especificarse de forma cierta, por ejemplo por un tercero, quién envió y quién recibió el mensaje. Lo cual puede agravarse en el caso de que las partes del contrato sean más de dos (haya por ejemplo varios destinatarios). Por lo tanto no se garantiza el *no repudio* del contrato, dado que las partes podrían negar haber firmado electrónicamente el documento. Además, la aplicación de este tipo de claves no permiten saber con certeza si el mensaje ha sido o no alterado después de su emisión.

la creación como la verificación de la firma digital"[6]. Se obtiene así un resumen, un compendio del mensaje conocido también como *huella digital*, que se caracteriza por no ser reversible y por ser único: a partir del resumen no puede obtenerse el mensaje completo inicial, y no es posible que un segundo mensaje produzca el mismo resumen o *hash*. Esto asegura la integridad del mensaje, ya que cualquier cambio en el mismo producirá un resumen diferente. El resumen cifrado del mensaje es lo que suele denominarse *strictu sensu* firma electrónica o digital.

Lo expuesto es en realidad una simplificación del proceso. A continuación se expone a modo de esquema los pasos completos que las partes deben seguir para emplear una firma electrónica basada en la criptografía asimétrica y usando una función *hash.* La obtención de confidencialidad en la transmisión exige que el protocolo sea algo más complejo que lo mencionado hasta ahora, ya que las partes manejarán dos pares de claves, una pública y una privada cada uno. El proceso es el siguiente:

1. Las partes se dirigen a un PSC (Prestador de Servicios de Certificación) para que éste les proporcione los pares de claves (una pública y una privada a cada uno).
2. El signatario:
    a) Aplicando la función de *hash*, genera un resumen del documento que desea enviar.
    b) Aplica su clave privada sobre el resumen del mensaje, consiguiendo así cifrarlo.
    c) Aplica la clave pública del destinatario sobre el mensaje original, cifrándolo.
    d) Envía conjuntamente el resumen cifrado del mensaje, y el mensaje original cifrado.
3. El destinatario (verificación):
    a) Una vez recibidos, aplica la clave pública de A sobre el resumen cifrado, consiguiendo así descifrarlo.
    b) Aplica su clave privada sobre el mensaje original cifrado, descifrándolo.
    c) Aplica la misma función de *hash* que utilizó el emisor sobre el mensaje original ya descifrado, obteniendo un resumen.
    d) Si el resumen enviado por el signatario y el obtenido por el destinatario coinciden, hay certeza de que el mensaje no ha sido alterado en la transmisión.

[6] LLANEZA GONZÁLEZ, P., "La firma electrónica", en *Iuris-actualidad y prácticas del Derecho*, nº 38, abril 2000, p. 47



El RDLey 14/1999 mantiene una posición dualista, distinguiendo entre *firma electrónica básica* y *firma electrónica avanzada* (FEA). El legislador ha basado esta diferenciación en las distintas funciones que cumple cada tipo de firma, lo cual remite a la tecnología en la que se sustentan: la firma sencilla en la criptografía simétrica y la firma avanzada en la criptografía asimétrica.

Estas definiciones se recogen en el art. 2.a y 2.b del RD-ley 14/1999 respectivamente, que se corresponden con los mismos artículos del borrador del anteproyecto de Ley de 2002, reproduciéndolos casi textualmente (cambiando únicamente la palabra "signatario" por la de "firmante").

Junto con la firma electrónica básica y la avanzada, del articulado del RDLey puede extraerse un tercer tipo de firma. Ésta deriva del art. 3.1, y es la que haya sido producida "por un dispositivo seguro de creación de firma" (definido en el art. 2.f, que remite a su vez al art. 19 –art. 24 en el borrador-) y "esté basada en un certificado reconocido" (conforme al art. 2.j, que remite a los arts. 8 y 12). Este tipo de firma despliega mayores efectos, equiparándose plenamente a la firma manuscrita y siendo admisible como prueba en juicio. Conforme al segundo párrafo del art. 3.1, se presumirá que una FEA reúne todas esas condiciones cuando el certificado reconocido en que se base haya sido expedido por un PSC acreditado y el dispositivo seguro de creación de firma se encuentre certificado conforme al art. 21.

3. ASPECTOS FUNDAMENTALES

A) El principio de neutralidad tecnológica

Este principio podría enunciarse como la exigencia de que la norma sea compatible con las diversas tecnologías existentes, pudiendo todas ellas subsumirse en la misma, sin exclusión. En la actualidad hay varias tecnologías que permiten atribuir un mensaje de datos electrónicos a su autor, y el hecho de que algunas de ellas gocen de un amplio reconocimiento internacional y, desde un punto de vista técnico sean más avanzadas, no justifica que la norma regule éstas de forma preferente. De ceñirse a una tecnología concreta, la regulación correría el riesgo de quedar obsoleta en un corto periodo de tiempo, debido al rápido desarrollo que se produce en este campo. Además,

podría darse la atipicidad de ciertas tecnologías que, aunque minoritarias, fueran empleadas por algunos usuarios.

Atendiendo al RDLey de 1999 puede concluirse que este principio no ha sido tenido en cuenta por el legislador. Si bien la norma no cita de forma expresa la tecnología que ha de ser empleada por respeto a ese principio, en el fondo, tras el concepto de FEA se esconde la firma electrónica basada en la criptografía asimétrica a partir de una ICP. Es decir, que la Directiva y el RDLey, a pesar de declararse tecnológicamente neutros[7], al regular la FEA están pensando claramente en un sistema basado en un par de claves, una pública y otra privada. Este hecho puede ser criticable, pero también de difícil solución, dado que hoy existe una tecnología de gran difusión, la firma electrónica basada en una ICP, y ésta es la única que por el momento produce un elevado grado de certeza a los efectos de atribución, identificación, privacidad, seguridad e integridad del mensaje[8].

Los motivos fundamentales por los que este principio no ha sido respetado son dos. Por un lado, el Real Decreto-ley centra su articulado en la regulación de la FEA, dejando sin precisar muchos aspectos de la firma electrónica básica. Éste es uno de los mayores defectos de la norma, ya que, como veremos más adelante, se reconoce ese instrumento sin detallar sus efectos jurídicos, creando inseguridad (todo lo contrario del objetivo que se propone la norma). Por otro lado, según ILLESCAS ORTIZ, el respeto al principio de neutralidad podría haberse incrementado si la calificación de una firma electrónica como avanzada y su plena producción de efectos "sólo se hubiere legalmente hecho depender del cumplimiento por parte suya de los requisitos establecidos por el art. 2.b", y no haber incluido los requisitos adicionales del art. 3.1. Éste hace depender la plena producción de efectos jurídicos de la FEA de la observancia de las condiciones recogidas en otros preceptos (art. 2.f, j y ll; art.12, 20 y 21), que acaban por vincular la FEA a la inclusión en listados administrativos de los dispositivos para su creación. Según este autor, con tal medida "la violencia de la neutralidad puede resultar excesiva"[9].

El borrador del anteproyecto no ha solucionado estos problemas. Se sigue prestando escasa atención a la firma electrónica básica, centrando toda su regulación en la FEA. La plena producción de efectos jurídicos de la FEA sigue haciéndose depender finalmente de un conjunto de acreditaciones administrativas (arts. 22 y 26 del borrador).

No obstante, en el borrador se han introducido algunas modificaciones que dotan a la norma de un talante más omnicomprensivo; el reconocimiento de la eficacia de los acuerdos *inter partes* sobre las condiciones en el empleo de la firma electrónica, independientemente de la tecnología utilizada (art. 3.3). Y la determinación del plazo de validez de los certificados haciéndolo depender de la tecnología utilizada (art. 11.a).

---

[7] La Directiva sobre firma electrónica señala en su Exposición de Motivos: "los rápidos avances tecnológicos y la dimensión mundial de Internet hacen necesario un planteamiento abierto a diferentes tecnologías y servicios de autenticación electrónica de datos".

[8] La superación de esta tecnología no se encuentra muy lejana en el tiempo, debido al desarrollo de la computación cuántica, en la que trabajan algunas universidades españolas, y que dejará inutilizable la criptografía actual. JIMÉNEZ, J., "Llega el DNI digital", *PC World España* nº174, 2001, p. 106.

[9] ILLESCAS ORTIZ, R., "La firma electrónica y el Real Decreto-ley 14/1999, de 17 de septiembre", en *Derecho de los negocios* nº109, octubre 1999, p. 11.

Estos dos detalles reflejan un mayor esfuerzo del legislador por flexibilizar la norma ante las diferentes tecnologías que existan o puedan existir en el futuro, pero a nuestro juicio estas novedades puntuales son insuficientes.

B) EQUIPARACIÓN ENTRE FIRMA ELECTRÓNICA Y FIRMA MANUSCRITA

El RDLey persigue establecer una regulación clara del uso de la firma electrónica, atribuyéndole eficacia jurídica. La firma electrónica debe tener una serie de requisitos para poder afirmar su plena equiparación; el requisito fundamental es que la firma electrónica debe ser avanzada, lo que proviene del art. 3 RDLey. Además, la firma debe estar basada en un certificado reconocido (art. 8 del RDLey y 9 del borrador del anteproyecto) y haber sido producida por un dispositivo seguro de creación de firma (art. 19 del RD-ley y 24 del borrador del anteproyecto). El apartado segundo de ese art. 3.1 establece una presunción, según la cual los requisitos anteriores se entenderán cumplidos cuando el certificado reconocido en que se base la firma haya sido expedido por un PSC acreditado y el dispositivo de creación de firma se haya acogido al sistema voluntario de acreditación (art. 21 y 6 del RDLey y 22 del borrador del anteproyecto). Este art. 3.1 no ha sido modificado en el borrador.

Es especialmente importante la validez de los documentos firmados electrónicamente a la hora de presentarlos como prueba en juicio. Según el apartado primero del art. 3, al presentarse como prueba en un proceso judicial un mensaje firmado electrónicamente, serían necesarios complejos y dificultosos informes técnicos para demostrar ante el juez la existencia de los requisitos expuestos antes; y aún así su prueba podría resultar prácticamente imposible. Es aquí donde la presunción establecida por el párrafo segundo del art. 3.1 despliega sus efectos, otorgando a ese mensaje plena validez.

Como ha manifestado la doctrina, el hecho de supeditar la validez de los documentos firmados electrónicamente como prueba al cumplimiento de unos requisitos concretos y rígidos, puede plantear obstáculos innecesarios. Más aún en un Ordenamiento procesal claramente flexible en cuanto a la admisión de los medios de prueba, como es el español tras la aprobación de la nueva Ley de Enjuiciamiento Civil[10]. Sus artículos 299.2 y 382 y siguientes admiten como prueba documentos en forma electrónica[11], sin exigir requisitos más rígidos que los previstos para cualquier otro medio de prueba.

Sin embargo, conforme a la regulación del art. 3.1 del RDLey, se estaría negando tal valor, por ejemplo, al supuesto en que dos partes conocidas y de confianza se intercambiaran las claves manualmente, y hubiesen acordado que las firmas creadas

[10] Ley 1/2000, de 7 de enero. B.O.E. nº 7 de 8 de enero; rect. B.O.E. nº 90 de 14 de abril.

[11] Art. 299.2 LEC: "También se admitirán... instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso". Además, el art. 812.1.1ª prevé el proceso monitorio para la reclamación de deudas, vencidas y exigibles, de cantidad no superior a cinco millones de pesetas, cuando la deuda se acredite "mediante documentos, cualquiera que sea su forma y clase o el soporte físico en que se encuentren, que aparezca firmado por el deudor o con su sello, impronta o marca o con cualquier otra señal, física o electrónica, proveniente del deudor".

con las mismas serían vinculantes para las partes[12]. Según los principios generales de la LEC, ese documento debería ser admitido como prueba en juicio en condiciones de igualdad respecto a los firmados con un certificado reconocido, pues su fiabilidad está fuera de toda duda. El RDLey priva de valor probatorio al documento por la falta de intervención de un PSC como tercera parte de confianza, cuando es evidente que en este caso es innecesaria. Este caso concreto ha sido previsto expresamente –quizá debido a la crítica doctrinal- en el art. 3.3 del borrador del anteproyecto, donde se otorga eficacia a las condiciones acordadas por las partes en el uso de una firma electrónica[13].

Según el art. 3.2 (tanto del RDLey como del borrador), a la firma electrónica que no reúna los requisitos del apartado anterior (firma electrónica avanzada y reconocida), no se le negarán efectos jurídicos ni será excluida como prueba en juicio, por el mero hecho de presentarse en forma electrónica. Es criticable la indeterminación con la que el precepto se refiere a los efectos de las firmas que no reúnan los requisitos del art. 3.1 a la hora de admitirse como prueba en juicio. Podemos plantearnos si dicha eficacia es o no idéntica a la recogida en el apartado primero del art. 3; si es así, lo cierto es que el inciso del apartado 2 no tiene demasiado sentido. Si ambos tipos de firma se equiparan, no es coherente que el precepto diferencie ambas. Podría pensarse que, simplemente, las firmas incluidas en el apartado 2 no gozan de la presunción de validez de la que sí disfrutan las firmas reconocidas. Pero aún con ello el alcance de sus efectos queda demasiado indeterminado.

Teniendo en cuenta que el principal objetivo de esta regulación es determinar los efectos de la firma electrónica y dotar a su uso de seguridad jurídica, el artículo 3.2 conlleva una grave deficiencia. Por ello es desafortunado que el legislador haya desaprovechado la oportunidad de corregir este defecto en el borrador del anteproyecto.

C) LA PRESTACIÓN DE SERVICIOS DE CERTIFICACIÓN

Éste es el apartado donde más modificaciones ha introducido el borrador del anteproyecto de Ley.

Las transmisiones de datos a través de redes abiertas como Internet, precisan la existencia de entidades especiales que ofrezcan confianza a los demás agentes de la red. Son los PSC, autoridades de certificación o terceras partes fiables (*trusted third parties*), y mediante su intervención se garantiza fundamentalmente la identidad de los agentes y la recepción de la comunicación electrónica por el interesado. La actuación de estas entidades se considera necesaria si desea garantizarse la máxima seguridad en las transmisiones electrónicas, mediante la expedición de certificados.

c.1) El titular del certificado

El titular del certificado es quien firma electrónicamente el mensaje: el signatario. Éste es definido en el art. 2.c RDLey como la persona física que cuenta con

[12] SEGURA DE LASSALETA, R., "La seguridad de la contratación en Internet: la firma electrónica", en *Revista General de Derecho*, nº 670-671 julio-agosto 2000, pp. 9002-9011.

[13] Art. 3.3: "A efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas".

un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.

A tenor de este artículo, tras la aprobación del Real Decreto-Ley se suscitó la pregunta de si una persona jurídica puede vincularse o no por medios electrónicos. La respuesta unánime de la doctrina ha sido negativa, la cual viene confirmada por el art. 8.e que incluye entre los requisitos para la obtención de un certificado reconocido la identificación del signatario únicamente por su "nombre y apellidos", y no por ejemplo por su denominación social. También confirmado por el art. 5, relativo al empleo de la firma electrónica por las Administraciones públicas, que especifica que a efectos de cumplimiento de las obligaciones tributarias se admite la expedición de certificados a personas jurídicas.

Esta cuestión ha cambiado totalmente en el nuevo borrador del anteproyecto, no dejando lugar a dudas sobre la posibilidad de que las personas jurídicas firmen electrónicamente. Ha sido regulado en el art. 10, que se refiere expresamente a "los certificados de personas jurídicas". Según éste, las personas jurídicas podrán emplear la firma electrónica mediante una persona física que les represente con poder bastante a estos efectos. Dicha persona física será la única legitimada para el uso de los datos de creación de firma y los certificados reconocidos en nombre de la persona jurídica (art. 10.2 del borrador).

No debe llevar a engaño el art. 8.f RDLey, que ya preveía que, en los supuestos de representación, los certificados reconocidos deben contener "la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente". Éste se trata de un supuesto genérico de representación civil, distinto del poder atribuido a una persona física (un administrador, por ejemplo) para actuar en nombre de una persona jurídica, como permite el borrador del anteproyecto. Coherentemente con esto, el art. 9.e del borrador establece que la identificación del firmante deberá hacerse "por su denominación o razón social, en el caso de que aquél fuera una persona jurídica", lo cual no es posible en el supuesto de representación previsto por el RDLey.

c.2) Clases de certificados: certificados reconocidos y no reconocidos

El certificado es el instrumento a través del cual se materializa la firma electrónica, permitiendo la identificación del firmante[14].

Tanto el RDLey como el borrador del anteproyecto reconocen dos tipos de certificados: ordinarios y reconocidos. Los certificados reconocidos son aquellos que contienen la información descrita en el art. 8 RDLey (9 en el borrador) y que es expedido por un PSC que cumple los requisitos del art. 12 RDLey (15 y apartados a y c del 16 en el borrador). Los requisitos para otorgar a un certificado la calidad de reconocido no se han alterado sustancialmente en el borrador.

[14] El art. 2.i del borrador del anteproyecto ha recogido una definición más clara de certificado que la que el RDLey, al reconocer su condición de documento electrónico; "Certificado: es un documento firmado electrónicamente por el prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad".

Debemos recordar que, según el art. 3.1 de ambas regulaciones, el que la firma electrónica avanzada esté basada en un certificado reconocido es requisito *sine qua non* para la plena producción de efectos jurídicos de la misma.

c.3) Validez del certificado

El RDLey se ocupa de la vigencia de los certificados en su art. 9. El borrador del anteproyecto, acertadamente, ha dividido esta regulación entre los artículos 11 y 12, destinando el primero a la vigencia, y el segundo a la revocación y suspensión de los certificados. Analizaremos las principales novedades introducidas en el borrador del anteproyecto en cuanto a la pérdida de validez de los certificados.

i) *Período de validez.* El art. 9.1.a 2ª RDLey recoge como límite temporal para los certificados reconocidos un plazo máximo de cuatro años. El borrador en su art. 11 ha suprimido ese límite temporal, dejando totalmente la determinación del plazo de validez al PSC, de acuerdo con las características de los datos de creación de firma y a la tecnología empleada para su generación (como dijimos, esto supone una mayor adecuación de la norma a las distintas tecnologías existentes).

ii) *Revocación por parte del signatario.* El art. 12.1.a del borrador del anteproyecto ha introducido como excepción el supuesto en el que se haya empleado para la firma el DNI electrónico, supuesto en el que no operará esta causa de pérdida de vigencia. Esto lleva a pensar que el único legitimado para revocar un DNI electrónico es la Administración otorgante y no su titular, aunque la confusa regulación de este instrumento en el borrador del anteproyecto no especifica nada al respecto.

iii) *Pérdida o inutilización por daños del soporte del certificado* (art. 9.1.c RDLey). La doctrina ha criticado que se recogiera este apartado, debido a que "ésta es una circunstancia técnica que no se halla debidamente perfilada y que, por ello, resulta de difícil comprensión"[15]. Quizá por ello se ha suprimido en el borrador del Anteproyecto. Sin embargo, ahora queda abierta la duda de si, en caso de pérdida o deterioro del soporte (por ejemplo de una tarjeta inteligente o del disco duro del ordenador del usuario), el certificado ha perdido su validez y, por tanto, es necesario expedir uno nuevo, o el mismo sigue vigente, bastando con reparar los daños u otorgar al usuario otro soporte (una nueva tarjeta, por ejemplo) con los mismos datos de firma. Hubiera sido preferible que el legislador hubiese regulado este supuesto de pérdida de validez de forma más detallada en el borrador del anteproyecto de ley, en lugar de suprimirlo y aumentar así la laguna que ya existía.

iv) *Utilización indebida por un tercero* (art. 9.1.d RDLey). El art. 12.1.b del borrador ha adelantado la barrera de protección, recogiendo como causa de revocación del certificado no sólo ese uso indebido, sino también la mera puesta en peligro del secreto.

v) *Publicación de la revocación o extinción del certificado*. Estas incidencias deben ser publicadas por el PSC en un registro que la propia entidad deberá crear a tales efectos (art. 11.e del RDLey y 15.1.e del borrador). El nuevo art. 13 del borrador del anteproyecto advierte la responsabilidad del PSC por el retraso en esa publicación. La

[15] MARTÍNEZ NADAL, *op. cit.*, p. 108.

revocación surte efectos frente a terceros de buena fe desde la publicación en dicho registro.

vi) *Revocación de oficio*. El borrador del anteproyecto establece en su art. 12.4 una nueva obligación para el PSC, consistente en la revocación de oficio del certificado cuando tenga conocimiento de las circunstancias previstas en los apartados 1 y 2 del mismo artículo[16]. Puede darse un nuevo supuesto de responsabilidad del PSC, si no lleva a cabo esta revocación de oficio. En el RDLey no se especifica esta obligación de revocar de oficio el certificado; según la regulación vigente, parece que la revocación siempre tendrá que ser a instancia del usuario, o de la autoridad judicial o administrativa competente.

vii) *Irretroactividad de la suspensión del* certificado. El art. 13.4 del borrador declara novedosamente este principio de forma expresa.

viii) Otra novedad es la determinación del plazo durante el que debe estar publicado en el Registro la revocación: hasta la fecha en que hubiera finalizado su periodo de validez.

c.4) Obligaciones de los PSC

Sólo se hará referencia a las novedades más importantes recogidas en el borrador del anteproyecto.

i) Con el fin de aportar más seguridad y confianza para los usuarios, se establece la prohibición de que los PSC almacenen o copien los datos de creación de firma de las personas a la que hayan prestado sus servicios. Esta prohibición se contenía ya en el art. 11.c RDLey, pero el borrador (art. 15.1.c) ha suprimido la mención "salvo que éste lo solicite", cerrando toda posibilidad de que el PSC almacene o copie dichos datos, aún en el caso de petición por el usuario.

ii) Se han introducido cambios en lo relativo a la responsabilidad de los PSC, de los cuales se tratará después.

iii) El borrador recoge un artículo nuevo, el 16, especificando más detalladamente las comprobaciones previas que el PSC debe hacer antes de la emisión de un certificado reconocido. Estas comprobaciones van dirigidas a constatar la identidad del usuario, la exactitud del contenido del certificado, su titularidad, la complementariedad de los datos de creación y verificación de firma, etc. Debe valorarse positivamente la concreción de estas obligaciones previas por el PSC, para garantizar la exactitud del certificado y evitar fraudes.

iv) El art. 17 del borrador introduce la nueva exigencia de que el solicitante de un certificado reconocido deba personarse físicamente ante las personas encargadas de

[16] Esas circunstancias son: solicitud de revocación formulada por el firmante; puesta en peligro de los datos de firma, o uso indebido de los mismos por un tercero; resolución judicial o administrativa que lo ordene; fallecimiento del firmante o extinción de la personalidad jurídica del titular del certificado; incapacidad; terminación de la representación o disolución de la persona jurídica representada; cese en su actividad del PSC; y descubrimiento de inexactitudes graves en los datos aportados por el firmante para la obtención del certificado, o modificación de las circunstancias verificadas para la obtención del mismo.

verificar su identidad. Esta obligación constaba ya en la versión inicial del borrador no oficial de la propuesta de Directiva sobre firma electrónica, y sin embargo, fue suprimida en la versión oficial de la propuesta presentada por la Comisión, y por ello finalmente no fue introducida en el RDLey español. MARTÍNEZ NADAL ha señalado que la comprobación de identidad del solicitante es un elemento esencial, y que la no personación física "priva al certificado de su función básica y esencial de distribución segura de claves públicas y otros elementos de verificación de firmas electrónicas"[17].

Reconociendo que el medio de la personación física del usuario para la comprobación de su identidad, es el que mayores garantías de seguridad ofrece respecto a la no suplantación de la personalidad, sin embargo esto puede suponer una excesiva rigidez en un instrumento que pretende aportar flexibilidad en la contratación telemática, como es la firma electrónica. Debe buscarse el equilibrio entre los dos fines esenciales que trata de conseguir la firma electrónica, la agilidad en la contratación y la seguridad jurídica en su uso, y quizá el medio de la personación física suponga una traba demasiado pesada, desde el punto de vista de la comodidad de los usuarios. En cualquier caso, este problema podría subsanarse parcialmente si las empresas de prestación de servicios de certificación dispusieran en el futuro de una red de sucursales descentralizadas, cercanas al usuario.

D) DISTRIBUCIÓN DE RESPONSABILIDADES

El RDLey 14/1999, además de un régimen general de sanciones para los PSC en caso de incumplimiento de sus obligaciones, recoge un régimen de responsabilidad civil por los daños y perjuicios que causen a sus usuarios o a los terceros que contraten con ellos, cuando actúen con negligencia. Las normas principales que se recogen en el RDLey sobre la responsabilidad de los PSC son dos: el art. 12.g y el art. 14. El primero de ellos establece cuantías mínimas en recursos disponibles por dichos operadores de cara a afrontar su responsabilidad por daños y perjuicios, tanto en términos absolutos (mil millones de pesetas, 6.010.121,04 euros) como relativos (el cuatro por cien de los importes de las transacciones objeto de certificación). Algún autor ha criticado lo excesivo de estas cifras, en especial la segunda de ellas[18]. Pero esta exigencia no es general para todos los PSC, sino sólo para aquellos que expidan certificados reconocidos.

En cambio, todos están sujetos a las pautas del art. 14. Este artículo establece un régimen de responsabilidad severo respecto a los PSC, contractual y extracontractual, por culpa o negligencia –pero no objetiva-, con inversión de la carga de la prueba, al establecer que deberá ser el PSC quien demuestre que actuó con la debida diligencia. Se trata de un régimen de responsabilidad próximo al previsto en la Ley de Servicios de la Sociedad de la Información y de Comercio electrónico, inspirado en el principio de actuación diligente del prestador de servicios[19].

---

[17] MARTÍNEZ NADAL, A., "Comentarios sobre la regulación de la firma electrónica", en *Partida Doble* nº 106, diciembre 1999, p. 19.

[18] ILLESCAS ORTIZ, *op. cit.*, p. 13.

[19] Esta norma (más conocida como LSSI o simplemente como "Ley de comercio electrónico") está aún en fase de tramitación, encontrándose actualmente pendiente de aprobación por el Senado. Los artículos 12 a 16 del Proyecto de Ley detallan el régimen de responsabilidad de los Prestadores de Servicios de la Sociedad de la Información, que gira en torno al principio de diligencia de éstos en su actua-

El borrador del anteproyecto de ley ha introducido algunas modificaciones importantes en este régimen de responsabilidad. En primer lugar, se ha suprimido la cuantía relativa respecto a los recursos disponibles por el PSC, exigiéndose sólo la absoluta de 6.000.000 de euros. En segundo lugar, se ha establecido la obligatoriedad de que la garantía de la responsabilidad de los PSC frente a terceros se haga mediante la contratación de un afianzamiento mercantil prestado por una entidad de crédito o de un seguro de responsabilidad civil (art. 15.1.j). El art. 12.g RDLey sólo indica la contratación de un afianzamiento mercantil o un seguro como una posibilidad para el PSC, pero no como una obligación.

Como novedad, el borrador ha introducido en el art. 20.2 un nuevo supuesto de responsabilidad. Éste trae causa del art. 7 de la Directiva sobre firma electrónica, en el se otorga validez a los certificados reconocidos expedidos por un PSC establecido en un Estado extracomunitario, si éste, cuando reúne ciertos requisitos, es avalado por un PSC establecido en un Estado miembro.

El art. 20.2 del borrador prevé la responsabilidad del PSC establecido en España y que haya avalado a otro PSC establecido dentro del Espacio Económico Europeo, por el incumplimiento por parte de este último de sus obligaciones[20].

La incorporación de la posibilidad de que las personas jurídicas puedan ser titulares de un certificado de firma electrónica ha determinado la inclusión de un nuevo supuesto de responsabilidad en art. 10.3. Éste se refiere a la responsabilidad de los miembros de la persona jurídica en el uso del certificado, estableciendo un régimen dual:

- La persona autorizada para utilizar los datos de firma responderá por el uso negligente de los mismos (cuando infrinja las obligaciones del art. 21.1. letras c, e y f).

- Los administradores y representantes legales serán responsables por la inexactitud de los datos del certificado y la omisión de solicitud de revocación o suspensión en caso de quebrantamiento de la confidencialidad (es decir, las obligaciones de los arts. 21.1, letras a, b y e).

Como vimos antes, entre las obligaciones de los PSC se recoge la de establecer un sistema que permita publicar, de forma segura e inmediata, la revocación de los certificados (art. 12.c RDLey). Teniendo en cuenta que la principal causa de revocación tiene su origen en una puesta en peligro de la clave privada (pérdida, extravío, etc.), lo que exige la finalización anticipada del periodo de validez del certificado, ese sistema de publicidad tiene el objetivo de dar a conocer a terceros usuarios que el certificado ha

---

ción. Por ejemplo, según su art. 15, los Prestadores de Servicios de alojamiento o almacenamiento de datos serán responsables por la información alojada a petición de los usuarios excepto que: a) no tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o b) si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos. En definitiva, recae sobre el Prestador de Servicios la carga de demostrar su desconocimiento sobre la ilicitud de los datos o su diligencia en la retirada de los mismos.

[20] Concretamente, el PSC español responderá en caso de que el PSC avalado incumpla las obligaciones previstas en los apartados b a e del art. 16 del borrador del anteproyecto: comprobar la exactitud de la información contenida en el certificado; incorporación en éste de todos los datos exigidos; la titularidad del certificado y, la complementariedad de los datos de creación y verificación de firma.

sido revocado y que no deben por tanto confiar en el mismo. La regla para los PSC en general se contiene en el art. 11.e RDLey, y se limita a exigir un registro en el que figurarán las circunstancias que afecten a la suspensión o pérdida de vigencia de los efectos de un certificado. La responsabilidad para el PSC surgirá en el supuesto de retraso en la publicación de este hecho, por los eventuales perjuicios que de ello se deriven. Este supuesto de responsabilidad no se recoge de forma expresa en el art. 14 del RDLey, sino que se deduce del supuesto genérico del apartado 1 de ese artículo. Sin embargo, el borrador del anteproyecto lo ha recogido de forma expresa en el art. 13.3[21].

MARTÍNEZ NADAL ha advertido cómo, sin embargo, el legislador español y el comunitario han obviado otros supuestos de responsabilidad derivados de la revocación, como la responsabilidad por posibles utilizaciones ilegítimas de la clave de firma desde el momento de la pérdida de la misma hasta la publicación de la revocación del certificado correspondiente. A falta de criterio legal expreso, como ocurre en el caso de pérdida de tarjetas de crédito, acabará asumiendo esta responsabilidad el titular del certificado y la clave de firma correspondiente. Pero en ambos casos sería deseable la existencia de límites a tal responsabilidad, especialmente rigurosa, pues puede llegar a ser objetiva, independientemente de la diligencia o negligencia del titular en la custodia de la clave[22]. El legislador no ha subsanado esta deficiencia en el borrador del anteproyecto.

Otro hecho criticable es el establecimiento de un régimen de responsabilidad distinto para los PSC que emitan certificados reconocidos y el resto de autoridades de certificación. En nuestra opinión, el que los documentos firmados con arreglo a los certificados emitidos por los primeros tengan una mayor eficacia, no justifica que los usuarios de los mismos gocen además de una especial protección. Una cosa son los efectos del certificado, y otra distinta la protección de los usuarios de ese servicio por ejemplo en caso de revocación del certificado, que debería ser similar en todos los casos.

En cuanto a la protección específica de los consumidores, el art. 14.4 del RDLey resulta algo confuso, al indicar: "lo dispuesto en este artículo se entiende sin perjuicio de lo establecido en la legislación sobre protección de los consumidores y usuarios". Esta cláusula de inmodificabilidad introduce la duda de si ésta opera, respecto de consumidores y usuarios, sólo en lo que se refiere al régimen de la responsabilidad de los PSC, quedando inaplicada esa legislación protectora en el resto de los ámbitos al utilizar la firma electrónica. Esta especificación se recoge en el art. 20.4 del borrador del anteproyecto.

Aunque desde luego ésa no es la finalidad de la norma, sino que parece ser un mero recordatorio, no tiene demasiado sentido incluirla sólo en lo que al régimen de responsabilidad se refiere. Para asegurar un adecuado nivel de protección a los usuarios, la Ley 26/1984, de 19 de julio, para la defensa de los consumidores y usuarios debe entenderse plenamente aplicable en todos los ámbitos del uso de la firma electrónica, cuando quien la utilice pueda ser considerado usuario a los efectos del art. 1 de dicha

[21] Art. 13.3: "El prestador de servicios responderá de los perjuicios que se causen al firmante o a terceros de buena fe, por la falta de publicación en el Registro de certificados de la revocación o suspensión del certificado o por el retraso en su publicación".

[22] MARTÍNEZ NADAL, A., "Comentarios sobre la regulación....", *op. cit.*, p. 29.

Ley[23]. Además, cuando los perjuicios causados al usuario deriven de un defecto en cualquiera de los elementos necesarios para la utilización de la firma electrónica, será aplicable el régimen de responsabilidad por productos defectuosos de los arts. 28 y siguientes de la Ley 26/1984, y la Ley 22/1994 de responsabilidad civil por los daños causados por productos defectuosos[24].

Pero, lógicamente, el PSC no responderá siempre que se produzca un perjuicio para el usuario, sino que existen ciertas conductas de éste que pueden exonerarle de toda responsabilidad. Así, el PSC no responderá de los daños y perjuicios causados por el uso de un certificado que exceda los límites indicados en el mismo; ni por el mal uso que pueda hacerse de una clave de firma extraviada o sustraída, cuya custodia corresponde en exclusiva al titular; tampoco en caso de que éste pierda, por ejemplo, la tarjeta con su firma electrónica y/o revele el PIN, casos en los cuales el usuario deberá correr con las consecuencias. ILLESCAS ORTIZ ha opinado, en relación al RDLey, que no hubiera estado de más que el texto legal incluyera alguna norma expresa reguladora de la conducta del signatario electrónico[25].

Esto ha sido solucionado en el nuevo art. 21 del borrador de Anteproyecto, donde se recogen una serie de deberes del firmante, cuyo incumplimiento exonera al PSC de toda responsabilidad[26].

4. EL D.N.I. ELECTRÓNICO , LA PRINCIPAL NOVEDAD DEL BORRADOR DEL ANTEPROYECTO DE LEY

El DNI electrónico es uno de los elementos que integran el Plan Info XXI, propuesto por el Gobierno con el objetivo de extender y popularizar el uso de las nuevas tecnologías en la Administración y entre los ciudadanos[27]. Según el Plan Info XXI, este nuevo DNI tendrá una doble finalidad: la función identificativa tradicional del DNI –ahora en las transacciones telemáticas-, y la capacidad de poder firmar electrónicamente con él. Para cumplir estas dos funciones el DNI contará con dos certificados digitales. Este instrumento permitirá efectuar una firma electrónica basada

[23] Concretamente, debe tenerse en cuenta el art. 25 de la Ley 26/1984, que establece que "el consumidor y el usuario tienen derecho a ser indemnizados por los daños y perjuicios demostrados que el consumo de bienes o la utilización de productos o servicios les irroguen salvo que aquellos daños y perjuicios estén causados por su culpa exclusiva o por la de las personas de las que deba responder civilmente".

[24] La firma electrónica puede entenderse incluida en el concepto legal de producto recogido en el art. 2 de la Ley 22/1994.

[25] "Un grado de diligencia habría debido ser establecido en relación con la posesión, la custodia, el empleo y el funcionamiento de tal equipo material e inmaterial", lo que hubiera ayudado a fijar criterios de responsabilidad, no sólo del PSC, en caso de controversia. ILLESCAS ORTIZ, *op. cit.*, p. 13.

[26] Según el art. 21 del borrador del Anteproyecto de Ley, son deberes inherentes a la condición de firmante: proporcionar al PSC información veraz, completa y exacta de los datos que deben constar en el certificado; comunicar al PSC cualquier modificación de las circunstancias reflejadas en el certificado; conservar con la máxima diligencia sus datos de creación de firma; solicitar la suspensión o revocación del certificado en caso de duda del mantenimiento de la confidencialidad sobre sus datos de creación de firma; abstenerse de utilizar sus datos de creación de firma desde que el certificado caduque o el PSC le notifique su revocación o suspensión (conforme al art. 12.4); respetar los límites que figuren en el certificado.

[27] El Plan puede consultarse en www.infoxxi.es . Dicha web incluye una presentación detallada del proyecto de DNI electrónico, en www.infoxxi.es/dni.htm (*click* en información adicional).

en una infraestructura de clave pública, y los certificados digitales empleados serán de los denominados "reconocidos". En conclusión, se trata de una FEA que gozará en cuanto a sus efectos jurídicos de la presunción del art. 3.1.2ª RDLey 14/1999. El proyecto está siendo desarrollado por la Dirección General de la Policía en colaboración con la Fábrica Nacional de Moneda y Timbre, y el Gobierno se ha propuesto su implantación en cuatro fases.

El borrador del anteproyecto de Ley de firma electrónica ha recogido el primer intento de regulación del DNI electrónico, en sus artículos 2.m, 6, 7 y Disposición final 2ª.

El art. 2.m recoge una definición amplia de este instrumento, que hace referencia a sus dos funciones: identificación y firma electrónica[28]. El art. 6 regula más detalladamente las funciones que desempeñará el DNI electrónico. Cabe destacar su apartado 3, donde se determina su utilidad para acreditar la identidad del ciudadano en un procedimiento administrativo[29]. Y el art. 7 se ocupa de los requisitos y características de los DNI electrónicos. La Disposición final 2ª habilita al Gobierno para adaptar la regulación reglamentaria del DNI a las previsiones contenidas en el borrador, y para dictar las demás disposiciones reglamentarias necesarias para aplicación y desarrollo del DNI electrónico.

Observando la regulación del borrador y los objetivos previstos para el DNI electrónico por el Plan Info XXI, en nuestra opinión existen algunas dudas en cuanto a la futura aplicación de este documento.

En cuanto a su ámbito de aplicación, el Plan Info XXI y el propio Ministerio de Ciencia y Tecnología, afirman la posibilidad de emplear el DNI electrónico en todo tipo de transacciones telemáticas (tanto entre ciudadanos y las Administraciones Públicas como entre particulares)[30]. No obstante, el borrador del anteproyecto regula únicamente de forma expresa su uso ante las Administraciones Públicas, quedando indeterminado su posible utilización entre particulares. Sería conveniente que las futuras redacciones del articulado, recogiesen una regulación detallada sobre la utilización del documento en todos los ámbitos.

Respecto a este uso *inter privatos*, el art. 6.4 del borrador garantiza que "la emisión de Documentos Nacionales de Identidad electrónicos por el Estado no impedirá la prestación de otros servicios de certificación a los ciudadanos". Sin embargo, si lo que se pretende es la generalización del DNI electrónico, los ciudadanos ya dispondrán de un certificado emitido por un PSC público, y por tanto, el papel de los PSC privados quedará muy reducido. La Exposición de motivos del borrador especifica que los certificados contenidos en los DNI electrónicos podrán utilizarse de manera complementaria con otros certificados, citando expresamente los certificados de atributos y los certificados de personas jurídicas. Cabe pensar que, si todos los ciudadanos llegáramos a dispo-

[28] Art. 2.m: "Documento Nacional de Identidad electrónico: Documento Nacional de Identidad, emitido por el Estado, que incorpora facilidades para la identificación y verificación electrónica de la identidad personal, así como para la creación y verificación de firmas electrónicas."

[29] La Ley 30/1992 de Régimen Jurídico y Procedimiento Administrativo Común ya preveía en su art. 45 la posibilidad de incorporar medios técnicos en los procedimientos administrativos.

[30] Según este Ministerio, "El DNI electrónico es una tarjeta equivalente al DNI actual, al que se añadirán facilidades de firma electrónica, y que podrá ser utilizada en las relaciones con cualquier Administración Pública y con los particulares y empresas". www.setsi.mcyt.es/novedad/firma271201.html

ner de un DNI electrónico, ése sería el ámbito al que quedaría reducida la actividad de los PSC privados: certificados complementarios (que incorporasen funciones adicionales) y certificados de personas jurídicas (ya que éstas no podrán ser titulares de un DNI electrónico). Esto contradice el propio espíritu de la norma, que en su art. 4.1 establece el principio libre competencia en la prestación de servicios de certificación. No obstante, no se especifica si el DNI electrónico será obligatorio para todos los ciudadanos, como para que su uso se generalice en un futuro cercano.

También se plantean algunas incertidumbres desde el punto de vista de la protección de los datos de carácter personal.

Por un lado, la implantación del DNI electrónico supone la creación de un ingente archivo donde se centralicen los datos exigidos para ese documento, pertenecientes a todos los ciudadanos que lo suscriban[31]. Aunque ese sistema informático deberá reunir las garantías exigidas por el art. 9 de la Ley Orgánica 15/1999 de protección de datos de carácter personal, es preocupante su hipotética vulnerabilidad frente a posibles intromisiones de *hackers*, dada la importancia y amplitud de los datos que en él se almacenarían.

Por otro lado, esa centralización de datos supondría poner en manos del PSC público encargado de gestionar la firma a través de DNI electrónico más datos de los estrictamente necesarios para desempeñar su función. Como hemos dicho, el DNI electrónico unifica dos funciones, una de identificación y otra de firma electrónica. Los datos necesarios para cada una de estas funciones son diferentes: para expedir un certificado reconocido basta con el nombre y apellidos de su titular (según el art. 9 del borrador), mientras que la función de identificación exige el conocimiento de los datos consignados en el DNI tradicional. Este hecho vulneraría el art. 18.2 del borrador (art. RDLey), según el cual para la emisión de certificados únicamente se requerirán los datos necesarios para la expedición y el mantenimiento de los mismos. Además, ello supone una contradicción con el art. 4.1 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, que establece que "los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido".

5. CONCLUSIÓN

Con esta nueva regulación de la firma electrónica, el legislador tiene el objetivo de solucionar las deficiencias en las que ha incurrido el RDLey de 1999, ocasionadas principalmente por su acelerada tramitación. Sin embargo, como hemos expuesto a lo largo de este artículo, únicamente ha incidido en ciertos aspectos puntuales, dando respuesta a algunas críticas planteadas por la doctrina, pero manteniendo la estructura fundamental y los principios de la norma anterior. Por ese motivo, las soluciones puntuales introducidas en el borrador son, a nuestro juicio, insuficientes para atajar los problemas que presenta el RDLey. Incluso, alguna de estas modificaciones parciales ha introducido nuevas distorsiones en la norma.

[31] El DNI electrónico deberá recoger los datos ya consignados en el DNI tradicional más los exigidos para los certificados reconocidos según el art. 9 de borrador y 8 del RDLey.

Todo esto viene provocado por una innecesaria urgencia en la aprobación de la norma todavía vigente, y de la inadecuada utilización (demasiado frecuente) de la figura del Real Decreto Ley. Éste es un instrumento legislativo previsto constitucionalmente sólo para casos de extraordinaria y urgente necesidad (art. 86.1 CE), y es evidente que en este caso no se daba ninguna de las dos circunstancias, sobre todo teniendo en cuenta la inminente aprobación de la Directiva comunitaria sobre la materia.

Por otro lado, la novedosa regulación del DNI electrónico ha provocado duras críticas por parte de algún sector de la doctrina[32]. En nuestra opinión esta regulación es ciertamente insuficiente, aunque teniendo en cuenta que el DNI electrónico es un instrumento en pleno desarrollo (aún en su segunda fase), puede considerarse que el legislador lo ha introducido como forma de sondear la opinión de los ciudadanos y la doctrina, y confiamos en que en las posteriores redacciones de la norma esa regulación sea perfeccionada[33].

BIBLIOGRAFÍA

ALAMILLO DOMINGO, I., y BARQUÍN GÓMEZ, D., "La firma electrónica y los registros", en *R.E.D.I. (Revista Electrónica de Derecho Informático)*, http://v2.vlex.com/es/asp/boletines_mail.asp

ÁLVAREZ-CIENFUEGOS SUÁREZ, J.M., *La Firma y el Comercio Electrónico en España. Comentarios a la Legislación Vigente*, Aranzadi, Pamplona, 2000.

BOLÁS ALFONSO, J., "Firma electrónica, comercio electrónico y fe pública notarial", en *Revista jurídica del notariado* nº 36, octubre-diciembre 2000, pp. 31-64.

CASTELLÁ MUÑOZ, O., "La firma electrónica", en www.emprendedoras.com

FERNÁNDEZ DOMINGO, J.I., "La contratación electrónica y el Real Decreto-Ley 14/1999 sobre firma electrónica", en *Actualidad Civil* nº 2, 2000, pp. 527-548.

GALINDO AYUDA, F., "Comentarios al borrador de anteproyecto de Ley de firma electrónica", *La Ley*, http://www.laley.net/temas/tema0605.html

GARCÍA MÁS, F.J., "La contratación electrónica: la firma y el documento electrónico", en *Revista crítica de Derecho inmobiliario* nº 652, mayo-junio 1999, pp. 765-790.

[32] GALINDO AYUDA ha llegado a sugerir que "toda regulación y referencia al DNI electrónico desaparezcan del borrador de anteproyecto de firma electrónica". "Comentarios al borrador de anteproyecto de Ley de firma electrónica", publicado en la web de la revista *La Ley*: http://www.laley.net/temas/tema0605.html

[33] El Ministerio de Ciencia y Tecnología advierte en su web que la regulación del DNI electrónico "no puede hacerse sin un debate previo sobre su encaje en el Ordenamiento jurídico, del que la consulta pública sobre esta Ley puede ser un buen exponente". www.setsi.mcyt.es/novedad/firma271201.html

HERNÁNDEZ MARTÍNEZ, J., "El futuro DNI electrónico", en http://www.iniciativasnet.com/197iniciativas.htm

ILLESCAS ORTIZ, R. "La firma electrónica y el Real Decreto Ley 14/1999, del 17 de septiembre" en *Derecho de los negocios* Nº109, octubre 1999, pp. 1-13.

JIMÉNEZ, J., "Llega el DNI digital", en *PC World España* nº 174, 2001, pp. 103-106.

LLANEZA GONZÁLEZ, P., "La firma electrónica", en *Iuris-actualidad y practicas del Derecho* nº 38 abril 2000, pp. 44-52.

MARCOS MARTÍN, J.L. y BALSELLS TRAVER, M., "La firma electrónica: génesis y regulación en Boletín Económico ICE (información comercial española)" nº 2646, 19 marzo 2000, pp. 31-36.

MARTÍNEZ NADAL, A., *La ley de firma electrónica*, Civitas, Madrid, 2000.

MARTÍNEZ NADAL, A., "Comentarios sobre la regulación de la firma electrónica", en *Partida Doble* nº106 diciembre 1999, pp. 14-33.

MATEU DE ROS, R. y CENDOYA MÉNDEZ DE VIGO, J.M. (coordinadores), *Derecho de Internet*, Aranzadi, Pamplona, 2000.

PÉREZ SUBÍAS, M., "Comercio, firma electrónica y las preocupaciones de los usuarios", en la web e la Asociación de Usuarios de Internet, http://www.aui.es/biblio/articu/Articulos/comerciofirma.htm

RODRÍGUEZ ADRADOS, A., "La firma electrónica", en *Revista de Derecho privado* nº 12, diciembre 2000, pp. 913-939.

SEGURA DE LASSALETA, R., "La seguridad de la contratación en Internet: la firma electrónica" en *Revista General de Derecho* nº 670-671, julio-agosto 2000, pp. 9002-9011.

SUÑÉ LLINÁS, E., "Documento digital y firma electrónica", en *Revista general de legislación y jurisprudencia* nº 2, marzo-abril 2000, pp. 209-242.

TUYA, M., "La regulación de la firma electrónica" http://www.baquia.com

VATTIER FUENZALIDA, C., "El régimen legal de la firma electrónica", en *Actualidad civil* nº 1, 2000, pp. 411-419.

- Otros documentos consultados en Internet:

Guía sobre el uso y eficacia de la firma electrónica publicada por el Ministerio de Justicia, http://www.mju.es/guia_f_elect.htm

Aspectos jurídicos del comercio electrónico, en "Internet Contract Soft", http://www.onnet.es

VLex España, http://v2.vlex.com/es/asp/noticias_detalle.asp?Articulo=115925

Web del Ministerio de Ciencia y Tecnología, www.setsi.mcyt.es

Plan Info XXI, www.infoxxi.es