ESTUDIO DEL REAL DECRETO-LEY 14/1999, DEL 17 DE SEPTIEMBRE, DE FIRMA ELECTRÓNICA

Javier Cremades García
Abogado

Introducción

La firma en la teoría general del derecho

La identidad de una persona es un concepto que no se modifica a lo largo de su vida. El punto de partida de la identificación es el nacimiento, por ello el arranque de la prueba de identificación es la inscripción en el Registro Civil. Para que la persona se diga idéntica ha de mantener su continuidad jurídica, a través de los cambios de estado y de las diversas circunstancias.

Es por esta razón por la que el ordenamiento jurídico vigila la identidad de la persona, requiriendo ciertos requisitos para diversos actos, como puede ser el otorgamiento de testamento. Una de las formas más sencillas para acreditar la identidad de la persona es su firma.

A la hora de contratar es necesaria la identificación de los contratantes, existiendo en nuestro ordenamiento el principio de libertad de forma, pudiéndose perfeccionar los contratos por el mero consentimiento (1258 CCv), siendo éstos obligatorios, cualquiera que sea la forma en que se hayan celebrado, siempre y cuando concurran los requisitos necesarios para su validez (1278 CCv). Así, si la voluntad puede declararse mediante gestos o incluso por silencios, ¿cómo no se va a poder manifestar a través del ordenador?

En algunos contratos, es necesaria su documentación, pero el documento no es simplemente una cosa, sino que es una *res signata*, una cosa a la que se le han incorporado unos signos, una grafía, necesitándose en este caso la firma de la persona. Igualmente, si el documento se hace por medios electrónicos, habrá de ir en algunos casos acompañado de una firma que acredite la identidad de la persona. Así, la firma electrónica asegura la identidad de los contenidos expresados en el documento, se demuestra la autoría del documento, resultando clara la imputabilidad al autor del documento.

Un documento en soporte papel, ya sea público o privado, puede ser presentado en juicio como medio de prueba. Para comprobar la identidad del firmante, cabe que se realice la prueba caligráfica por peritos, y se conocerá así la validez de ese documento. De la misma manera, si los documentos en soporte electrónico, van firmados, ha de existir la posibilidad de que sirvan como prueba en juicio y que se pueda probar la identidad del firmante.

Nacimiento del real decreto-ley

Ha sorprendido la rapidez con la que ha surgido en España el Real decreto-ley sobre firma electrónica, teniendo en cuenta que ha aparecido en nuestro ordenamiento con anterioridad a la aprobación de la directiva comunitaria. Es consecuencia de la propuesta conjunta de los ministros de Fomento, Justicia y Energía, con el informe previo del Consejo General del Poder Judicial y de la Agencia de Protección de Datos. Queremos apuntar ahora que no se puede considerar de buena técnica legislativa que haya sido aprobado mediante real decreto-ley, que según el artículo 86 de la Constitución, solamente se podrán dictar en casos de extraordinaria y urgente necesidad. Cabría preguntarse si es realmente extraordinaria y urgente. En la exposición de motivos se afirma que debe introducirse este medio tecnológico que contribuye al desarrollo de la sociedad de la información. Otro de los motivos que apunta es el deseo de dar a los usuarios elementos de confianza en los sistemas, permitiendo su introducción y su rápida difusión. Es discutible que estos motivos se puedan considerar extraordinarios y urgentes. Sin embargo, debemos destacar que para su convalidación, no ha existido ningún tipo de debate parlamentario, lo cual denota un amplio consenso en esta materia, estando todos los grupos políticos interesados en que nuestro ordenamiento jurídico regule una materia tan novedosa.

Quizá otra razón de esta rapidez podría ser el enorme interés que ha mostrado España en este campo en los últimos años, dando gran impulso a la regulación de la firma electrónica en los foros comunitarios. Hay por tanto una especial predisposición por parte de los sectores pú-

blico y privado para que el uso de esta firma electrónica se implante rápidamente.

Algo que no puede pasar desapercibido es que el real decreto-ley versa sobre la firma electrónica y a lo largo de su desarrollo únicamente menciona la firma digital, sin referirse, por ejemplo, a la firma elaborada por tecnología analógica. Esto se debe a que la elaboración de la firma mediante tecnología digital supone un mayor grado de precisión de la misma, y en cuanto al procedimiento técnico de transmisión, al tratarse básicamente de algoritmos (compuestos de números), es más sencillo su compresión mediante técnicas digitales.

Sociedad de la información/comercio electrónico

La primera cuestión que debemos abordar es el porqué de la firma electrónica. Para ello debemos acudir a un término manido, aunque no por ello falto de actualidad, cual es la sociedad de la información. Es una realidad el hecho de que estamos globalmente relacionados, conectados, habiéndose creado unas virtuales autopistas de la información que tienen un rápido crecimiento, donde el número de usuarios de Internet en España ha aumentado en más de dos millones de personas desde 1996, alcanzando en marzo de 1999, 2.747.000, que representan el 8% de la población española, según datos publicados por la OCDE.

No hay ningún tipo de información al que actualmente no se pueda acceder por medios telemáticos, informáticos o electrónicos. Internet ha hecho posible que tengamos información sobre gran cantidad de productos de diversas empresas desde cualquier punto del mundo con un coste hasta hace pocos años impensable y en un tiempo mínimo.

Es por este motivo por el que un abultado número de empresas y de instituciones han visto en la red una posibilidad inigualable para dar salida a sus productos o servicios. Se ha creado un tipo de comercio a través de la red, el llamado comercio electrónico, que facilita sobremanera las transacciones entre particulares y las relaciones de éstos con las administraciones públicas.

La importancia creciente del comercio electrónico radica en su enorme facturación, con un volumen previsible para 1999 de 14.000 millones de pesetas, siendo un sector con un crecimiento exponencial. La tendencia actual es el incremento de las compras por Internet, debido a que tiene un importante abaratamiento de costes con respecto a la compra por correo y un margen mucho mayor con respecto a las compras realizadas en establecimientos tradicionales; hemos de añadir que, en este último caso, el aminoramiento del factor tiempo juega un papel determinante, ya que las transacciones se realizan con mayor rapidez, puesto que los documentos electrónicos tienen la ventaja de que se puede dis-

poner de ellos de manera casi instantánea y en cualquier cantidad, y la persona que lo recibe puede trabajar sobre él directamente. La firma electrónica permite el desarrollo de una nueva tecnología, esencial para la implantación del comercio electrónico, de una importancia creciente para las PYMES, siendo éstas las que forman el grueso del entramado empresarial español. Una de las consecuencias directas de la aparición del comercio electrónico es que se van a ver modificadas las funciones actuales de los intermediarios, así como un incremento de lo que se ha venido a llamar el «teletrabajo».

Es esta rapidez y el volumen de negocio lo que exigen que se disponga de un sistema seguro. La seguridad en la red se ha puesto repetidas veces en entredicho debido a su vulnerabilidad, habiéndose sucedido las noticias relativas a la modificación de información que aparecía en páginas web, o el envío de información falsa a través de la red. Esto ha provocado una enorme desconfianza en los usuarios, por otra parte comprensible. Una de las posibles y peores consecuencias que puede tener esta falta de confianza, puede ser la ralentización del incipiente mercado electrónico.

Los gobiernos de diferentes países, entre ellos el español, conocedores de estos peligros, con su consiguiente pérdida de competitividad, están haciendo grandes esfuerzos para evitar que se sigan produciendo este tipo de situaciones. Parte del trabajo que se está llevando a cabo por parte de los estados, es consecuencia de las repetidas denuncias de asociaciones de consumidores y usuarios. Es por este motivo, como se verá más adelante, por lo que se está creando un entramado legal en aras de la protección de los usuarios, prestando especial atención a la protección de sus datos personales y familiares.

Con la firma electrónica se consiguen evitar gran cantidad de problemas que pueden hacer perder operatividad al mercado. En primer lugar, sabemos que el mensaje tiene integridad, esto es, existe la garantía de que los datos no han sido modificados desde que son emitidos hasta que son recibidos, sin que quepa una alteración fraudulenta. En segundo lugar, se garantiza la identificación de las partes intervinientes, ya que tanto el receptor como el emisor sabrán que la otra parte es quien dice ser. Otro punto a tener en cuenta es que ninguna de las partes podrá repudiar el mensaje que envió, lo cual tiene una gran importancia en el caso en el que se produzca una reclamación judicial. Por último existe la buscada confidencialidad, ya que se crean mecanismos para que ese mensaje no sea leído por una persona distinta del receptor.

Así vemos cómo a la hora de realizar cualquier tipo de transacción se sabrá por ejemplo cuántas han sido las unidades requeridas sin que quepa en un momento posterior alegar que se solicitó una cantidad distinta ya que habrá documentos firmados.

Antecedentes

Estados Unidos

Resulta interesante saber cuáles han sido los inicios de la firma electrónica. Para ello debemos remontarnos a principios de la presente década, y más concretamente a 1991, cuando el norteamericano Phil Zimmermann sacó a la luz la primera versión del primer programa de cifrado de datos disponible con carácter gratuito. A este programa se le conoce con el nombre de PGP Pretty Good Privacy, o «intimidad bastante buena». Tardó algún tiempo en llegar a Europa debido a las restricciones a la exportación por parte del gobierno de Estados Unidos, ya que la exportación de programas de cifrado de datos se equiparaban a la exportación de armas nucleares. Desde 1991 han ido apareciendo versiones internacionales avanzadas de PGP, estando el programa en la actualidad, extendido mundialmente, lo que ha proporcionado a millones de usuarios un correo electrónico que podemos considerar de alta seguridad ya que PGP hace uso de los algoritmos criptográficos más potentes de cada momento.

Europa: OCDE y la Unión Europea

Por otra parte, a mediados de la década de los '90, en el seno de la OCDE y de la Unión Europea, se despertó un gran interés para la regulación de un campo tan importante y tan actual al mismo tiempo, como es el de la firma electrónica, aunque existen trabajos anteriores relativos a las líneas que deben seguir los estados miembros respecto a la seguridad de los sistemas de información. Los trabajos de la OCDE se han centrado especialmente en los temas de autenticación y de certificación de firma electrónica, con el fin de establecer tecnologías, mecanismos y modelos de negocio globales para todos los estados miembros.

La Unión Europea quiso evitar el más mínimo problema que pudiera poner en peligro uno de los pilares básicos del derecho comunitario cual es la libre circulación de mercancías. Asimismo, y debido a la libre circulación de personas, es frecuente que ciudadanos y residentes de la Unión Europea, tengan que tratar con autoridades de estados miembros distintas de aquél en el que residen.

El 16 de abril de 1997 la Comisión europea presentó una comunicación titulada «Iniciativa europea de comercio electrónico», en la que señalaba que la firma digital es un instrumento esencial para fomentar la seguridad y la confianza en las redes abiertas. Igualmente, presentó otra comunicación sobre «El fomento de la seguridad y la confianza en la comunicación electrónica– Hacia un marco europeo para la firma digital y el cifrado», que fue refrendada por el Consejo el 1 de diciembre de 1997, el cual encargó a la Comisión que presentara una propuesta de directiva del Parlamento Europeo y del Consejo, en el menor plazo posible.

En 1998, hubo reuniones con sectores privados implicados, básicamente los relacionados con la industria de la criptografía; salió a la luz la propuesta de directiva, para establecer un marco común para la firma electrónica y se publicó la opinión favorable del Comité Económico y Social. Ha sido en 1999 cuando se ha producido la mayor parte de los trabajos preparatorios, con el informe favorable del Comité de las Regiones y con un compromiso en pro de la protección de la vida privada. Se modificó la propuesta inicial por la Comisión y se publicó una posición común aprobada por el Consejo, el 28 de junio de 1999, y publicada en el DOCE el 27 de agosto de 1999 (C243/33). El Parlamento europeo ya ha emitido una decisión favorable sobre ella, y se espera la inminente aprobación de la directiva. Los primeros países que han tomado medidas relacionadas con la firma electrónica han sido España, Italia y Alemania.

El Proyecto de Directiva sobre Firma Electrónica tiene importancia, ya que hasta el momento el mosaico legislativo de los países miembros, adolece de excesiva heterogeneidad. Es ilustrativo el ejemplo de Francia y Bélgica en los que los documentos electrónicos no se admiten como prueba, al requerirse la prueba documental cuando el valor de, por ejemplo, un contrato de compra-venta, supera un determinado límite, constituyendo la referida restricción un claro perjuicio para el uso de la firma digital.

Creación de firma

Criptología

El sistema de creación de firma se basa en la ciencia de la criptología, que utiliza un sistema de algoritmos matemáticos, en los que se basa el programa PGP. Con éstos se crea una situación segura para la emisión y recepción de mensajes, debido a que tiene un sistema que evita cualquier alteración de los mismos (integridad), y lo que se transmite es un resumen aleatorio de los mensajes (algoritmo hash), así que en el caso en el que éstos sean interceptados, no podrán ser leídos. Esto se debe a que para la firma electrónica se utilizará un sistema cifrado que transforma en secuencias de números los datos que se quieren enviar. Para transformar el texto en datos cifrados, se utilizan algoritmos criptográficos. Transformar la información contenida en el texto en datos se denomina cifrado, y el cambio de datos cifrados a texto, descifrado. Existen dos tipos de cifrado, de claves asimétricas, en contraposición con lo que se ha venido utilizando hasta el momento, que han sido las claves simétricas. La diferencia entre ambas radica en que las claves simétricas utilizan un tipo de claves idénticas para cifrar y descifrar los mensajes, que son dos claves privadas.

Esto supone que las dos partes intervinientes en un proceso de encriptación y desencriptación compartan la misma clave, lo cual plantea problemas de distribución de claves en entornos no seguros, como puede ser Internet. Un algoritmo de clave pública supone que cada una de las partes intervinientes en un proceso dispone de un par de claves: una pública y una privada. La primera está destinada a ser distribuida libremente, interesando esta distribución porque cuanto más amplia sea, menos posibilidades caben de «usurpación de la personalidad». Las claves públicas pueden ser obtenidas a través de servidores de claves o a través de la página web generada por la propia persona. En cuanto a la privada, ésta ha de ser conocida únicamente por su legítimo propietario ya que va a ser la única manera de que se consigan todos los efectos requeridos para una comunicación segura. Las claves asimétricas tienen su uso en la creación de firma electrónica y en el cifrado y descifrado de mensajes.

A pesar de que la firma electrónica garantiza la autenticidad del remitente y la integridad de los datos contenidos en el mensaje por medio de claves asimétricas, el problema básico que se plantea es que cabe la posibilidad de que se haya producido una suplantación de la identidad del remitente, en el caso de que su clave pública haya sido alterada fraudulentamente por un tercero. Una solución sería el intercambio de claves públicas a través de canales seguros, pero resulta inviable tratándose de temas relacionados con el comercio electrónico, ya que habrá muchos casos en los que no exista una relación anterior. Esta situación fomenta la desconfianza en los usuarios, realizándose menos transacciones de las debidas. Por ello se plantea la necesidad de que entre en juego un tercero independiente, una «tercera parte de confianza» en la que las partes intervinientes confíen y conozcan. Esta tercera parte son las autoridades de certificación que serán las encargadas de emitir certificados de autenticidad.

No existe un sistema general para el diseño de sistemas absolutamente seguros, ni para evaluar científicamente de forma fiable su grado de seguridad. Por ello se pueden utilizar al mismo tiempo otros métodos que den mayor seguridad. Uno de ellos es la esteganografía que significa literalmente «ocultación de datos», dificultando la detección de determinados datos, pero ha de ir acompañado del cifrado de los mismos.

Autoridades de certificación

Una autoridad de certificación puede ser tanto una persona física como jurídica, cuya principal labor se va a centrar en la expedición de certificados; aunque presumiblemente dispondrá de otro tipo de servicios, tales como la admisión de suscriptores, el depósito registral de los certificados expedidos, la relación con las autoridades encargadas del re-

gistro o la publicación y recuperación de claves. A título informativo, una de las autoridades de certificación españolas (ACE), expide certificados a un precio aproximado de 2.500 pesetas, aunque en la actualidad únicamente lo están realizando en el ámbito empresarial. El coste de certificados en los que intervenga una autoridad registral ronda las 10.000 pesetas (según datos de FESTE).

Las autoridades de certificación certifican no sólo la firma digital, sino también el servidor, software. No todos los modelos sirven para la certificación de firma digital ya que, por ejemplo, el certificado X. 509, no serviría como certificado reconocido (diapositiva 19) porque no contiene la posibilidad de establecer el límite de las transacciones que se pueden realizar con él, como exige el artículo 8 j del R.D.; aunque se está pensando en hacer una mínima modificación al modelo de certificado para que se pueda trabajar con él.

Actualmente ya disponemos en España de autoridades de certificación, entre las que cabe destacar la Fábrica Nacional de Moneda y Timbre (ahora Real Casa de la Moneda), que actuará en colaboración de Correos y Telégrafos, como se recoge en la exposición de motivos del Real decreto-ley sobre firma electrónica. La Real Casa de la Moneda ya ha empezado a firmar acuerdos de colaboración con distintas instituciones, por ejemplo, con el Colegio de Abogados de Madrid el día 17 de junio, en orden a garantizar la seguridad, confidencialidad y autentificación de las comunicaciones realizadas por los colegiados a través de Internet. Se pretende que a finales de año se puedan firmar electrónicamente las comunicaciones de los colegiados con el colegio, entre ellos, y previsiblemente la de éstos con las administraciones públicas.

Asimismo, todas las cámaras de comercio dispondrán para finales del verano del 2000 de dispositivos de creación de firma. Actualmente la única cámara de comercio que emite certificados es la de Barcelona. El 31 de enero del 2000 estarán en esa situación diez cámaras más, entre ellas la de A Coruña. La segunda fase finaliza el 31 de marzo y se incorporará la Cámara de Santiago de Compostela. Los certificados que van a emitir serán de tres tipos: los de servidor con un precio de 300 euros, los de empresa para una persona que costarán 200 euros, y para una persona perteneciente a una empresa sin poderes, 100 euros.

Por último hacer mención a la primera empresa privada de certificación que es *ACE*, Agencia de Certificación Electrónica, que se considera como un procesador de certificados. ACE está participada 40% por Grupo Telefónica de España, 20% por SERMEPA, 20% CECA y 20% Sistema 4B. Otra empresa privada que es autoridad de certificación es IPS. ACE ha suscrito recientemente un acuerdo de colaboración con *FESTE*, autoridad de certificación y registro. (Fundación para el Estudio de la Seguridad de las Telecomunicaciones, constituida por el Consejo General

de Corredores de Comercio, el Consejo General del Notariado, la Universidad de Zaragoza y la empresa Intercomputer S.A.).

Normativa

La firma electrónica no puede considerarse como un salto al vacío por parte del Gobierno que ha ido aprobando a lo largo de esta década diversas normas relativas a la comunicación telemática. El nuevo decreto ley, no modifica en modo alguno las normas de contratación que se contienen en el libro IV del Código civil, no debe haber colisión entre las normas del RD y las del Código civil. Es importante destacar que la propuesta de directiva recoge asimismo que los efectos de la firma electrónica se considerarán sin perjuicio de la forma de celebración de los contratos y normas del lugar. Observamos que aunque la directiva quiere conseguir una situación homogénea para todos los estados miembros, sin modificar la teoría general de obligaciones y contratos de sus respectivos ordenamientos jurídicos.

Contratación privada

En cuanto a otras normas relativas a la contratación en el ámbito privado encontramos la Ley 7/1998 sobre condiciones generales de la contratación, existiendo un proyecto de real decreto para aprobar un reglamento de contratación electrónica con condiciones generales. El proyecto se justifica por la necesidad de desarrollar el artículo 5.3 de la citada Ley de condiciones generales, que dice: «en los casos de contratación telefónica o electrónica será necesario que conste en los términos que reglamentariamente se establezcan la aceptación de todas y cada una de las cláusulas del contrato, sin necesidad de firma convencional. En este supuesto, se enviará inmediatamente al consumidor justificación escrita de la contratación efectuada, donde constarán todos los términos de la misma». También, y al hilo de esta norma, se ha de hacer referencia a la Ley general de defensa de los consumidores y usuarios que en su artículo 13.1 recoge la necesidad de la aplicación del principio de buena fe, al igual que en la directiva sobre protección de consumidores en materia de contratos a distancia.

En relación con el uso de la criptografía existen las normas del Sistema Nacional de Compensación Electrónica y un reglamento sobre la materia de 29 de marzo de 1996.

Ámbito público

En el seno de las administraciones públicas encontramos un Acuerdo de 11 de marzo de 1998 de la Comisión Nacional del Mercado de Valo-

res para la implantación de un sistema de intercambio de información a través de línea telemática, en el que se contempla el uso de la criptografía de clave pública. Anteriormente a 1992, ya existían circulares en las que se contemplaba la posibilidad de presentación de documentos en soporte informático. En la Ley del mercado de valores se establece que será la CNMV el órgano competente para aprobar las técnicas electrónicas, informáticas y telemáticas a utilizar en sus relaciones con los administrados. En el acuerdo al que nos hemos referido, se menciona expresamente el término firma digital, con el uso de encriptación asimétrica: clave pública y clave privada.

Es importante tener presente las vías que abrió la Ley 30/92 de régimen jurídico de las administraciones públicas y del procedimiento administrativo común, con las modificaciones introducidas por la Ley 4/1999, que en su artículo 45 incorporó la posibilidad de que los ciudadanos se relacionaran con ellas a través de medios electrónicos, informáticos y telemáticos. Para el desarrollo de este artículo, se aprobó el R.D. 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración general del Estado.

En la Ley 13/1995, de 18 de mayo, de contratos de las administraciones públicas y en su normativa de desarrollo no se establece nada al respecto, aunque es viable la presentación de documentos en soporte electrónico por la posibilidad que ofrece el artículo 45 de la Ley 30/92.

Ámbito tributario

En el ámbito tributario hay normas concernientes a los impuestos de valor añadido, que en su ley y reglamento (1993, 1996), hacen referencia a la facturación telemática, afirmándose que las facturas electrónicas tienen la misma validez que las facturas emitidas en soporte papel, siempre que la información contenida en la factura emitida y recibida sea idéntica. En relación al IRPF, aunque ya se podía presentar la declaración en soporte informático, se han aprobado diversas órdenes en 1999 concernientes a la presentación telemática de documentos tributarios de modelos, como el del resumen anual de las retribuciones, pagos fraccionados... Fue a raíz de un recurso presentado ante el TS, relacionado con el ITPAJD, por el que se dictó una sentencia de 3 de noviembre de 1997 en la que se afirmaba que «si se dan todas las circunstancias necesarias para acreditar la autenticidad de los ficheros electrónicos o del contenido de los discos en los ordenadores o procesadores y se garantiza, con las pruebas periciales en su caso necesarias la veracidad de lo documentado y la autoría de la firma electrónica utilizada, el documento mercantil con función de giro, debe gozar de plena virtualidad jurídica operativa».

En la Ley 66/1997 de 30 de diciembre de acompañamiento a los pre-

supuestos de 1998 se habilita a la Real Casa de la Moneda para que preste servicios de certificación.

En el ámbito de la Seguridad Social existe una Orden de 3 de abril de 1995 sobre uso de medios electrónicos en la Seguridad Social y normativa de desarrollo del Sistema RED, estuvo en vigor hasta la Resolución de 17 de enero de 1996.

Normativa básica a raíz del Real decreto-ley

En España contamos con diversos textos legislativos importantes para la firma electrónica. Además del Real decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica, encontramos una referencia expresa en la disposición adicional 1ª de la Ley 16/1999 que desarrolla los artículos 6 y 22 del Real decreto-ley. También contamos con el Reglamento 994/99 de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal en desarrollo del artículo 18.4 de la Constitución Española en el que se afirma que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»; con este reglamento se pretende que haya un uso global seguro y confiable de la informática, dando una serie de medidas de seguridad técnicas y organizativas, tratamiento de datos, e intimidad personal y familiar. Y por último, la Ley orgánica 5/92 de 29 de octubre de regulación del tratamiento automatizado de datos.

Real decreto-ley

Continuando con el estudio del Real decreto-ley 14/1999 de 17 de septiembre, sobre firma electrónica. Entró en vigor el 19 de septiembre siendo convalidado el 21 de octubre. En su exposición de motivos se afirma que con él se persigue que haya confianza en los sistemas por parte de los usuarios para que se produzca un rápido desarrollo del comercio y la información. Teniendo en cuenta el principio de legalidad vigente en nuestro sistema jurídico, se echaba en falta una regulación concreta sobre la firma electrónica.

El Real decreto-ley 14/1999 requerirá buen número de normas reglamentarias de desarrollo, como se dispone en su disposición final segunda que habilita al Gobierno para el desarrollo del Real decreto. Se desarrollará también mediante ley, pues será necesario establecer la tasa para consulta del Registro de prestadores de servicios de certificación, según establece el artículo 7 del R.D.; por último hace referencia a la actualización de la cuota por el reconocimiento de acreditaciones y certificaciones del artículo 23 mediante real decreto.

Una de las finalidades básicas del real decreto-ley es impulsar su uso de una manera generalizada: no sólo en el seno de las administraciones públicas, sino principalmente en las relaciones entre los particulares. Con respecto a las administraciones públicas, como se ha dicho anteriormente, existen ya diversas normas que dan alguna validez al empleo de la firma electrónica en el ámbito de la Administración tributaria, la Dirección General de Aduanas y la Tesorería de la Seguridad Social, y en otras administraciones.

Efectos jurídicos

Los efectos jurídicos de la firma electrónica tienen una gran importancia en el conjunto del real decreto-ley, como así se desprende de la exposición de motivos y del articulado. Básicamente se persigue equiparar el valor de la firma electrónica y la firma manuscrita, siempre y cuando se den unas condiciones de seguridad.

Llegados a este punto es necesario diferenciar entre la firma electrónica y la *firma electrónica avanzada*. La primera se refiere al conjunto de datos en formato electrónico, anejos o asociados a otros datos utilizados como medio para identificar formalmente a su autor. La firma electrónica avanzada permite la identificación del signatario creada por medios mantenidos bajo su control, siendo posible detectar cualquier modificación posterior. Así únicamente será admitida como prueba en juicio la que sea firma electrónica avanzada.

Existe pues una *presunción legal iuris tantum* (admite prueba en contrario), favorable a la validez de la firma electrónica cuando el prestador está acreditado y el dispositivo de creación de firma empleado está certificado oficialmente. En el caso en el que no sea avanzada, o siéndolo no está basada en un certificado reconocido, sin dispositivo seguro de creación de firma, no se rechazará de plano su admisión como prueba en juicio, pero carecerán de la eficacia atribuida a la firma manuscrita.

La firma digital plantea una serie de problemas, que no pueden surgir respecto a la firma manuscrita, cuales son que en un documento firmado digitalmente no es posible distinguir entre el original y la copia, y que la firma manuscrita es única, mientras que es posible disponer de varios pares de claves. El efecto legal que se quiere conseguir está íntimamente vinculado con la confianza que se tenga en la Agencia de Certificación.

En el artículo 1 *in fine*, se hace una referencia expresa a que los servicios que prestan los prestadores de servicios, no sustituyen, no modifican en modo alguno las funciones que tienen atribuidas las personas facultadas para dar fe de las mismas o para su elevación a públicos. El

documento firmado electrónicamente no tendrá valor de documento público, ya que si se necesita en algún documento su elevación a público, sería necesario que el notario verificara la identidad de los contratantes y su capacidad de obrar, no siendo esto posible mediante la técnica de firma digital.

Grupos cerrados de usuarios

Mención aparte merece los efectos legales de las firmas digitales en entornos cerrados de usuarios. Éstas se utilizan para intercambio de datos en el seno de una misma empresa, una empresa con sus filiales o entre compañías entre las que hay una inconmensurable confianza. Suelen usar para el cifrado de sus mensajes claves simétricas, y ya hemos mencionado anteriormente su falta de seguridad. Por otra parte, las claves simétricas suelen ser modificadas con cierta asiduidad, por lo que se pueden dar por válidas unas cuando ya no lo son, u operar con unas claves creyendo que son válidas. Por ello tienen una importante dificultad probatoria. La solución estriba en la consideración de las cláusulas contractuales de los contratos que se hayan suscrito, aplicando los principios probatorios tradicionales.

Sobre la utilización de la firma en los grupos cerrados de usuarios, en la primera propuesta de directiva se afirma que «la presente directiva no debe regular la firma electrónica utilizada por grupos cerrados, por ejemplo, cuando ya existen relaciones contractuales. En estos contextos debe prevalecer la libertad contractual».

La firma electrónica en el seno de las administraciones públicas

El real decreto hace una referencia expresa al uso de la firma electrónica en el seno de las administraciones públicas. En primer lugar establece la posibilidad de que se establezcan condiciones adicionales (un ejemplo de ellas, pudiera ser disponer de un servicio de consignación de fecha y hora), en las relaciones entre distintas administraciones o dentro de una misma y en las relaciones con los particulares. Tenemos que tener presente que el artículo 45 de la Ley 30/92 LRJAP y PAC establece la posibilidad de que la relación administrado-administración sea a través de medios telemáticos. El Comité de Legislación de FESTE, propuso que los atributos del certificado constaran en documento público. El real decreto recoge la exigencia de que rijan los principios de objetividad, proporcionalidad y no discriminación en todas las actuaciones llevadas a cabo por las administraciones públicas.

Los usos para los que se prevé la firma electrónica son, entre otros, la expedición de diferentes carnets, como el de identidad o el de conducir;

certificados de nacimiento y los de penales; y el cumplimiento de numerosos trámites administrativos.

El R.D.-ley contempla la posibilidad de que haya un sometimiento a un régimen específico en algunos temas, por ejemplo, los relativos a información clasificada, seguridad pública o defensa, y temas relacionados con obligaciones tributarias, en este caso tendente a garantizar el cumplimiento de las mismas, pudiendo ser el signatario tanto una persona jurídica como física. Las funciones de certificación corresponderán a los órganos que dispone la LGT y la Ley 21/1992.

Los servicios de certificación serán prestados en régimen de libre competencia, por ello se ha establecido la obligación de que haya separación de cuentas en el caso de las administraciones públicas.

Acreditación

La acreditación de la actividad de entidades certificadoras que se sometan voluntariamente a ese trámite, corresponderá a las administraciones públicas.

La acreditación de las entidades de certificación corresponde a una «entidad de evaluación» (organismo independiente creado por el gobierno mediante R.D). Para llevar a cabo su labor, deberá hacerlo conforme a las referencias que se publiquen en el BOE. Algo curioso es que en el R.D-ley, como se han adelantado a la directiva, se refiere a que los productos de firma electrónica han de cumplir las normas técnicas que se publiquen en el DOCE, normas que servirán de criterios de evaluación a la entidad anteriormente citada; pero que en el caso de no se publiquen en el DOCE, serán publicadas en el BOE. La entidad de evaluación tendrá en cuenta informes técnicos, y el cumplimiento de los requisitos reglamentarios que se necesitan para ser acreditados.

En todo lo relativo a la acreditación, se ha establecido en la D.A.1ª del R.D-Ley 16/99 (por el que se adoptan medidas para combatir la inflación y facilitar un mayor grado de competencia en las telecomunicaciones), que se habilita al ministro de Fomento para que mediante órdenes ministeriales desarrolle normas relativas a la acreditación. El que sea mediante O.M. supone una mayor agilidad en su tramitación y aprobación.

Se presta especial atención a la acreditación porque a los clientes de ese prestador de servicios de certificación les da mayor seguridad jurídica y confianza; y, en cuanto al prestador, se le abre la posibilidad de expedir certificados reconocidos, aceptados en el ámbito comunitario. Por el hecho de estar acreditados les serán establecidos una serie de derechos y obligaciones específicos por el órgano de evaluación.

Por el hecho del reconocimiento de la acreditación y por certificar una serie de dispositivos técnicos se establece una tasa, cuyo hecho imponible es el propio reconocimiento, siendo el prestador de servicios el sujeto pasivo. La cuota es de 47.500 pesetas por cada acto del órgano de evaluación, siendo actualizada dicha cantidad por real decreto. El devengo de dicha tasa se producirá en el momento de la solicitud, dejando la liquidación de la misma a desarrollo reglamentario.

Protección de datos

En el R.D. aparecen varias menciones relativas a la protección de datos. Esto se debe a que se considera primordial proteger a los usuarios de posibles vulneraciones de su intimidad personal y familiar. Hay varios artículos en los que se quiere dar protección a los datos, como en los artículos 8,11 y 15. En ellos se aprecia la necesidad de contar con consentimiento expreso para pedir otros datos que se contengan en el certificado, pudiéndose requerir la identidad del signatario en el caso en el que hay dado un seudónimo. Es importante la prohibición relativa al almacenaje y copia de los datos para la creación de firma, cuyo incumplimiento se sanciona en la Ley 5/92 sobre protección de datos. Los datos que ha de solicitar el prestador de servicios al usuario han de ser los estrictamente necesarios. Las entidades de evaluación también se han de ajustar a lo contenido en la Ley 5/92, cuando hagan comprobaciones de datos.

Los datos de los usuarios, dentro de las entidades de certificación, sólo podrán ser consultados por las personas que estén autorizadas al efecto. El signatario, o una persona autorizada por éste, han de tener la posibilidad de poder anotar o modificar sus datos, así como detectar los posibles cambios técnicos que puedan afectar a la seguridad de sus datos personales y de sus mensajes. Se hace una referencia expresa a la situación de un posible cese de actividad de un prestador de servicios. Para pasar los datos pertenecientes a certificados por él expedidos, a otro prestador de servicios de certificación, será imprescindible que cuente con el consentimiento expreso de la persona a favor de la cual se ha expedido el certificado.

Teniendo en cuenta que ha de prevalecer en todo momento, lo contenido en la Ley 5/92 de regulación del tratamiento automatizado de los datos de carácter personal, se establecen una serie de excepciones en virtud de las cuales los prestadores de servicios deben facilitar la identidad de los signatarios. En primer lugar, siempre que así lo soliciten los órganos judiciales en el ejercicio de sus funciones; el artículo 11.2 letra d) de la Ley 5/92 relativo a la cesión de datos, afirma que no se exige consentimiento del afectado «cuando la cesión que deba efectuarse tenga por destinatario el Defensor del Pueblo, el Ministerio Fiscal o los jueces o tri-

bunales, en el ejercicio de las funciones que tienen atribuidas». En segundo lugar, según disponga la legislación relativa a temas tributarios, de defensa de la competencia, y seguridad nacional.

Certificados digitales

Los certificados digitales han de cumplir una serie de requisitos para que sean considerados como tales. El primero de ellos es que el certificado ha de ser reconocido por un prestador de servicios acreditado, y en segundo lugar, la firma digital ha de ser creada con un dispositivo seguro de creación de firmas (1º los datos para la generación de la firma puedan producirse sólo una vez y que se asegure *razonablemente* (hay algunas indeterminaciones) su secreto; 2º los datos no puedan ser derivados de los de verificación de firma y que la firma no pueda ser falsificada por medios tecnológicos; 3º los datos puedan ser protegidos por el signatario de su utilización por terceros), que esté avalado por una entidad de evaluación acreditada. Es importante destacar que la falta de los requisitos antedichos no implica *per se* que se nieguen los efectos jurídicos a la firma, ni que se imposibilite su presentación en juicio como prueba.

Certificados reconocidos

Para que un certificado reconocido pueda desplegar enteramente sus efectos, ha de constar: a) que ha sido expedido como tal, debiendo poseer un código identificativo único; b) cuál es su periodo de validez; y c) si existe algún tipo de limitación en cuanto a su uso y máximo valor de las transacciones que con él se pueden realizar. En otro orden de cosas, ha de contener la identificación del prestador de servicios que lo ha expedido, así como la identificación del signatario o de su representante en su caso. Asimismo, aparecerá la firma electrónica avanzada del prestador y los datos relativos a la verificación de la firma.

Los certificados reconocidos tienen una vigencia máxima de cuatro años. No tiene, a priori, una razón concluyente para que se haya establecido este plazo. Una posibilidad es que se prevé que en el plazo de cuatro años surjan nuevas tecnologías que lleguen a poder interferir en los mensajes o incluso descifrar las claves. Por poner un ejemplo, diremos que la validez de los certificados expedidos por FESTE se hacen en su mayoría por un año.

Los certificados, pueden perder su vigencia con anterioridad si es revocado por el signatario, su representante o un tercero autorizado, o si sobreviene la muerte o incapacidad del signatario o de su representado. Los certificados perderán también su vigencia si son utilizados indebi-

damente por un tercero, si contienen inexactitudes importantes de los datos en él contenidos, o si se pierde o inutiliza el soporte del certificado. Si el prestador de servicios cesa en su actividad, los certificados por él expedidos perderán su vigencia salvo que sean traspasados a otro prestador de servicios. Las autoridades judiciales o administrativas podrán establecer su pérdida de vigencia mediante resolución.

Antes de la entrada en vigor de la ley ya se expedían certificados. Por ello, el R.D en su disposición transitoria única, afirma que los certificados que se hayan expedido antes de la entrada en vigor conservarán su validez siempre y cuando ya hubieran desplegado algún tipo de efectos.

La vigencia de los certificados podrá quedar en suspenso temporalmente por el prestador si así se lo ordena el signatario o una autoridad judicial o administrativa. Siempre que se produzca alguna de las causas de pérdida de vigencia de un certificado, el prestador desde que tenga conocimiento de ellas, tiene la obligación de publicar dicha falta de vigencia en su registro particular. La falta de publicación o su retraso conlleva para el prestador de servicios una serie de responsabilidades.

Una de las finalidades de la propuesta de directiva es establecer un marco común para el uso de la firma electrónica en todos los estados miembros. Por ello, el R.D., en relación con la propuesta de directiva, ha establecido una serie de condiciones alternativas para el reconocimiento de certificados que provengan de terceros países, debiendo cumplir alguna de las que a continuación se describen: el prestador de servicios que haya expedido el certificado ha de haber sido acreditado mediante alguno de los sistemas voluntarios de cualquiera de los estados miembros; el certificado, debiendo cumplir unos requisitos, ha de estar garantizado por alguno de los prestadores de servicios de cualquier estado miembro; cabe la posibilidad de que la Unión Europea firme un acuerdo de reconocimiento con terceros países o con organizaciones internacionales.

Prestadores de servicios

Para los prestadores de servicios se crea un registro, siendo necesario solicitar su inscripción antes de que dé comienzo su actividad. En los términos en los que está redactado el real decreto, parece que lo que se exige es que los prestadores de servicios formulen la solicitud, no siendo necesario esperar la finalización del trámite de la inscripción –o en el caso en el que ya existieran, continuar– para llevar a cabo la inscripción certificadora. Para los prestadores de servicios que hubieran iniciado su actividad con anterioridad a la entrada en el R.D., disponen de un plazo de un año para adaptarse al mismo.

Este registro será dependiente del Ministerio de Justicia, se ha decidido que dependa del Ministerio de Justicia porque se pretende fortalecer la idea de que la firma electrónica tenga valor en juicio. El hecho de que exista un registro público en el que aparezca una relación de todos los inscritos, ofrece una mayor seguridad a los usuarios. En el registro aparecerán los datos y el alcance de la actividad de los prestadores, y sus datos serán dados de baja de oficio cuando se tenga conocimiento del cese de su actividad. Los datos contenidos en el registro podrán ser consultados por cualquier persona debiendo pagarse una tasa cuya cuantía aún no está establecida. En la actualidad aún no se ha creado.

El R.D. da una gran importancia a la actividad de los prestadores de servicios, por esta razón ha establecido para ellos una serie de obligaciones, responsabilidades, y un régimen de control.

Obligaciones

Una diferencia básica que hace el R.D. en el establecimiento de obligaciones para los prestadores de servicios es distinguir si expiden meros certificados o certificados reconocidos. Para todo tipo de prestadores, deberán comprobar la identidad de los solicitantes por los medios admitidos en derecho, no pudiendo almacenar ningún tipo de datos, debiendo poner a disposición del signatario los dispositivos de creación y de verificación de firma, informándole previamente de las condiciones del certificado. Como ya se ha comentado, deberán solicitar su inscripción en el registro de prestadores de servicios, y mantener un registro de los certificados que hayan emitido con las circunstancias relativas a la validez de los mismos. Los datos podrán consultarse si así lo autoriza el signatario. Si cesan en su actividad deberán comunicarlo a sus signatarios con dos meses de antelación.

Los prestadores de servicios reconocidos junto con las anteriores obligaciones, tendrán las siguientes: en el aspecto económico se establecen unas cantidades que se pueden considerar altas, intentando que, aunque se presten en régimen de libre competencia, los que accedan puedan responder plenamente de sus posibles infracciones, sin que haya resquicios de inseguridad para los posibles signatarios. La cantidad será equivalente al 4% de la suma del límite del valor de las transacciones de todos los certificados expedidos, y en el caso en el que no haya limitación se establece la cantidad de 1.000 millones de pesetas, cantidad modificable por real decreto, que podrá ser garantizada mediante aval.

Otro tipo de obligaciones son las que se refieren a garantías técnicas, y otras de información a los posibles signatarios. Una obligación a tener en cuenta es que ha de conservar la información durante al menos 15 años. Este periodo se ha establecido con vistas a reforzar la posible presentación de los documentos firmados digitalmente como prueba en juicio.

Responsabilidad

Para determinar la responsabilidad de los prestadores habrá que estar a la legislación sobre consumidores y usuarios. Los prestadores responderán de los daños y perjuicios que se deriven de todo incumplimiento de las obligaciones establecidas para ellos o por negligencia. Se estará tanto a la culpa contractual como extracontractual. En el caso en el que haya un uso indebido de un certificado, responderán si en el certificado no concretaron la existencia de un límite de uso y de valor. Es importante saber que los prestadores responden personal e ilimitadamente con todos sus bienes presentes y futuros. En cualquier tipo de proceso será a ellos a quien les corresponda la carga de la prueba, debido a que se les presume con suficientes y mayores medios técnicos que a los posibles signatarios.

Infracciones y sanciones

Control de la actividad

El control de la actividad que lleven a cabo los prestadores tanto de los certificados reconocidos como de los no reconocidos, corresponderá a la Secretaría General de Comunicaciones, adscrita al Ministerio de Fomento. Sus funcionarios serán considerados como autoridad pública. Los prestadores tienen la obligación de proporcionar la documentación sobre ellos mismos que sea solicitada por la SGC. Ésta tiene autoridad para dar órdenes de obligado cumplimiento para los prestadores.

La potestad para imponer sanciones a los prestadores de servicios, corresponde a la SGC; sin embargo el Ministerio de Justicia y otros órganos competentes tendrán la posibilidad de incoar un procedimiento tras una presentación motivada a la SGC. Cabe la posibilidad de que se adopten una serie de medidas cautelares en el caso de la comisión de posibles infracciones graves y muy graves. La Ley establece dos tipos concretos de medidas cautelares, aunque establece que no son *numerus clausus*: el cese temporal de la actividad y la suspensión de la vigencia de los certificados expedidos por el presunto infractor.

Infracciones

Al igual que las obligaciones para prestadores de certificados reconocidos y meros certificados no son las mismas, las infracciones que puedan cometer ambos se modulan de diferente manera. Si los prestadores de certificados reconocidos incumplen alguna de las obligaciones que ha de cumplir todo prestador se considerará infracción muy grave, en contraposición de la situación de los prestadores de meros certificados, que en el caso en el que causen daño se considerarán infracción grave, y en caso contrario, leve. Pa-

ra los prestadores de certificados reconocidos se exceptúan como muy graves las relativas al almacenamiento de datos, la falta de solicitud en el registro, y otros incumplimientos que se recojan en el R.D.

La clasificación de las infracciones que puedan cometer los prestadores de certificados reconocidos respecto a obligaciones específicas, dependerá del daño que causen. Así, si causan daño, se considerarán muy graves, y si no lo causan graves. Se exceptúa de esta clasificación los requisitos de fecha y hora, la demostración de la fiabilidad de sus servicios y la falta de información a los usuarios que se considerarán en todo caso graves. La falta de algún requisito en los certificados se considera infracción leve.

La falta de cumplimiento de las resoluciones de la SGC será falta grave. En el caso en el que el incumplimiento sea grave y reiterado se tornará en infracción muy grave. El resistirse por parte de los prestadores a la actuación inspectora de la SGC se considera infracción muy grave, y la falta de colaboración infracción leve.

El no comunicar el cese de su actividad o el que se haya iniciado contra ellos un procedimiento de suspensión de pagos o quiebra, será infracción muy grave.

Mención aparte merece las infracciones que se puedan cometer en relación con el artículo 11.c) relativo a la copia y al almacenaje de datos. El R.D. no establece ningún tipo de infracción, lo cual a priori puede resultar sorprendente sabiendo que el R.D. pretende una total protección de los datos personales. La respuesta está en que se deja esta clasificación a la Ley orgánica 5/92 de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), debiendo acudir a ella para conocer las infracciones y sanciones. Pudiera ser encuadrable, como infracción grave, si se realiza una creación de ficheros privados con finalidades distintas de las que constituyen el objeto legítimo de la empresa o si se recogen datos sin el consentimiento expreso de los afectados. Las infracciones graves llevan aparejada multa de cincuenta millones una pesetas, a cien millones de pesetas, prescribiendo a los dos años.

Sanciones

Las sanciones, la actualización de las cuantías, y los criterios de graduación de las multas que establece el real decreto, son las mismas que las establecidas en el artículo 82 de la LGT, salvo para las infracciones leves que el tope se establece en dos millones.