La regulación jurídica de la firma electrónica; sus posibilidades en el ámbito de las Administraciones Públicas (1)

SUMARIO: 1. EL PUNTO DE PARTIDA: EL ARTICULO 45 DE LA LEY 30/1992 (LPC).—2. EL DESARROLLO LEGISLATIVO DEL ARTICULO 45 DE LA LEY 30/1992: EL REAL DECRETO 263/1996, POR EL QUE SE REGULA LA UTILIZACION DE TECNICAS ELECTRONICAS, INFORMATICAS Y TELEMATICAS POR LA ADMINISTRACION GENERAL DEL ESTADO.—3. LOS DESARROLLOS SECTORIALES POSTERIORES AL REAL DECRETO 263/1996, EN PARTICULAR EL SISTEMA ADOPTADO POR LA COMISION NACIONAL DEL MERCADO DE VALORES.—4. LA REGULACION ESPECIFICA DE LA FIRMA ELECTRONICA: EL ADELANTADO REAL DECRETO-LEY 14/1999 Y LA DIRECTIVA 1999/93/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 13 DE DICIEMBRE DE 1999, POR LA QUE SE ESTABLECE UN MARCO COMUNITARIO PARA LA FIRMA ELECTRONICA: 4.1. LA REGULACIÓN ESPAÑOLA: LA APROBACIÓN MEDIANTE DECRETO-LEY. 4.2. OBJETO DEL REAL DECRETO-LEY 14/1999. Los CONCEPTOS LEGALES EN MATERIA DE FIRMA ELECTRÓNICA. 4.3. LOS CERTIFICADOS, EL DNI DIGITAL. 4.4. EL PROBLEMA DE LA ACREDITACIÓN DEL TIEMPO: EL SELLO TEMPORAL.—5. LAS AUTORIDADES CERTIFICANTES EN EL DERECHO ESPAÑOL: EL ARTICULO 81 DE LA LEY DE ACOMPAÑAMIENTO 66/1997 Y EL REAL DECRETO 1290/1999, DE DESARROLLO DE LA LPC EN MATERIA DE FIRMA ELECTRONICA.—6. ALGUNAS MENCIONES JURISPRUDENCIALES EN MATERIA DE FIRMA ELECTRONICA.—BIBLIOGRAFIA.

La utilización de las nuevas tecnologías en el ámbito de la Administración, y la relación de ésta con los administrados y ciudadanos es un requisito

(1) El presente artículo constituye el contenido de la conferencia presentada en el «Curso sobre cuestiones actuales del Derecho, la Administración y la Política», celebrado en Albacete los días 26 y 27 de marzo de 2001.

perseguido por la ley y la Constitución, y que ha sido desarrollado de forma parcial en los últimos años a medida que las técnicas informáticas y digitales han evolucionado. En la presente intervención vamos a analizar la reciente regulación (española y comunitaria) en materia de firma electrónica, y las posibilidades que este concepto abre en el campo de la relación de los ciudadanos con sus Administraciones.

1. EL PUNTO DE PARTIDA: EL ARTICULO 45 DE LA LEY 30/1992 (LPC) (2)

Cualquier referencia al uso de las nuevas tecnologías por parte de la Administración ha de comenzar con la referencia legal contenida en el artículo 45 de la Ley 30/1992, de Régimen Jurídico de las Administraciones

(2) A nivel constitucional, el artículo 18.4 de la Constitución dispone 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».* Se trata de un artículo que tan solo incidentalmente afecta a la materia de nuestro estudio, y el cual sorprende doblemente: en primer lugar, por la relativa prontitud de la Constitución a la hora de regular una materia como el uso de la informática; en segundo lugar, la referencia que se hace la misma: no se «regulará», sino que se «limitará». Dicho límite, pues, hay que buscarlo en los derechos al honor y a la intimidad personal, pero no en otros ámbitos donde la informática puede proporcionar una relación más fluida entre los ciudadanos y la Administración, por ejemplo. Por ello, el desarrollo legislativo que de este artículo se ha hecho se encuentra hoy en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (que sustituye a la anterior Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal). La Ley únicamente se ocupa de los ficheros de datos personales, ya sean éstos de titularidad pública o privada (nos referimos a las diferentes empresas de venta por correo y venta de datos de potenciales consumidores). La conexión de esta Ley Orgánica con la LPC estaría en el artículo 38.3 de la misma, que establece que todos los registros generales, así como todos los registros que las Administraciones establezcan para la recepción de escritos y comunicaciones, deberán instalarse en soporte informático. Se exceptúan expresamente del ámbito de aplicación de la LO de Protección de Datos algunos ficheros de determinadas Administraciones *ratione materiae,* como son los ficheros sometidos a la protección de materias clasificadas, los ficheros establecidos para la investigación del terrorismo y otras formas graves de delincuencia organizada; y se rigen por sus disposiciones específicas los ficheros establecidos en la legislación electoral, los que sirvan a fines meramente estadísticos, los que contengan informes sobre el personal de las FFAA, los ficheros derivados del Registro Civil y el Registro Central de Penados y Rebeldes, y los ficheros gráficos procedentes de videocámaras obtenidos por las Fuerzas de Seguridad.

De igual manera, el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración, dispone que «la utilización de estas técnicas por parte de la Administración se ajustará a la legislación en materia de honor e intimidad personal y familiar. Por su parte, el Real Decreto 1290/1999, de 23 de julio, por el que se Desarrolla el artículo 81 de la Ley 66/1997, de 30 de diciembre, en materia de prestación de servicios de seguridad en las

Públicas y del Procedimiento Administrativo Común (en adelante, LPC). Se trata, como afirma ORTEGA ALVAREZ (3), de un artículo que no sólo propone, sino que también prescribe la utilización de nuevas técnicas y medios electrónicos, informáticos y telemáticos. Este artículo consagra e impulsa la apertura decidida de la LPC hacia la mayor tecnificación y modernización de la actuación administrativa, propugnando a este respecto la utilización de aplicaciones y medios electrónicos, informáticos y telemáticos, tanto por parte de las Administraciones Públicas, en el desarrollo de su actividad y en el ejercicio de sus competencias, como por parte de los ciudadanos, en sus relaciones con dichas Administraciones Públicas. El legislador dirige en este artículo un mandato general a todas las Administraciones Públicas para el *«empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos para el desarrollo de su actividad y el ejercicio de sus competencias»* (art. 45.1 LPC). La aplicación de estos medios supone, como afirma MARTÍNEZ NADAL (4) la transformación de los tradicionales documentos realizados en soporte papel en procesos digitales en los que la palabra impresa es sustituida por un código binario (5), con la lógica consecuencia de que el documento tradicional en soporte papel es reemplazado por sus equivalentes electrónicos.

---

comunicaciones de las Administraciones Públicas a través de técnicas y medios electrónicos, informáticos y telemáticos, añade también una referencia de sometimiento *«a la norma que resulte de la incorporación al ordenamiento jurídico español de la Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos»*. Por último, el artículo 15 del Real Decreto-ley 14/1999, sobre firma electrónica, dispone en el artículo 15.1 que «El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y el que se realice en el Registro de Prestadores de Servicios de Certificación, al que se refiere este Real Decreto-ley, se sujetan a lo dispuesto en la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal, y en las disposiciones dictadas en su desarrollo».

(3) ORTEGA ALVAREZ, LUIS IGNACIO, «Nuevas Tecnologías y Procedimiento Administrativo», en *Revista Jurídica de Castilla-La Mancha*, núm. 18: Comentarios a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, agosto de 1993, pág. 212.

(4) MARTÍNEZ NADAL, APOL.LÓNIA, *Comercio Electrónico, firma digital y autoridades de certificación*, Ed. Civitas-UIB-Govern Balear, 2.ª edición, 2000, pág. 28.

(5) Los ordenadores no trabajan con un código decimal o un alfabeto, sino con un código binario, compuesto por unos y ceros, que indica a su vez que por un determinado punto pasa o no electricidad. La agrupación de estos unos y ceros da lugar a secuencias en las que se contiene la información. Por lo tanto, a diferencia del lenguaje humano, el «lenguaje máquina» no usa las letras del alfabeto, sino sólo los números 0 y 1. Cuando *hablamos* con un ordenador estamos convirtiendo nuestras letras, cifras y símbolos habituales en secuencias de ceros y unos, es decir, en una señal eléctrica (GRIERA FISA, MERCÉ y otros, *Conecta el micro*, núm. 1: Fem informática, Ed. Fundació Caixa de Pensions, 1.ª edición, 1985, págs. 37-38).

Paralelamente, se ofrece también al ciudadano la facultad de relacionarse con las diferentes administraciones a través de las mismas técnicas y medios electrónicos, informáticos o telemáticos, pero condicionando esta posibilidad a que ello sea compatible con los medios técnicos que dispongan las Administraciones (por tanto, en función del desarrollo tecnológico) y, sobre todo, con que se respeten las garantías y requisitos establecidos en cada procedimiento (art. 45.2), requisito este último que entendemos aplicable igualmente al desarrollo de la tecnología informática, en la medida en que haga posible, por ejemplo, tener constancia fidedigna de los datos del interesado, conocer que éste ha recibido efectivamente la notificación, etc. Estos requisitos se pueden resumir en dos:

Primero, que los procedimientos que se tramiten en soporte informático permitan garantizar la identificación del administrado, lo cual no es más que el correlato *informático* del deber que el administrado tiene de identificarse *ex artículo* 70.1 LPC, y que el ejercicio de la competencia se realice por el órgano que tiene atribuido dicho ejercicio (art. 45.3 LPC, correlato a su vez del principio de competencia contenido en el art. 53.1 LPC).

Un segundo requisito, de carácter técnico, sería que los diferentes programas informáticos y telemáticos a través de los cuales se ejerzan potestades públicas, sean aprobados por el órgano competente para el ejercicio de las mismas, difundiendo además públicamente sus características (art. 45.4 LPC).

El artículo 45 se cierra con la equiparación del documento tradicional al documento en soporte informático, siempre que pueda garantizarse su *«autenticidad, integridad y conservación, y en su caso, la recepción por el interesado»,* así como el cumplimiento de cualquier garantía exigida por Ley. Y en la medida en que la firma electrónica cumpla estos requisitos, estas condiciones van a ser el referente que habrá de cumplirse en cualquier regulación o posterior desarrollo que se haga de este artículo.

2. EL DESARROLLO LEGISLATIVO DEL ARTICULO 45 DE LA LEY 30/1992: EL REAL DECRETO 263/1996, POR EL QUE SE REGULA LA UTILIZACION DE TECNICAS ELECTRONICAS, INFORMATICAS Y TELEMATICAS POR LA ADMINISTRACION GENERAL DEL ESTADO

El primer desarrollo parcial del artículo 45 LPC lo encontramos en el Real Decreto 263/1996, de 16 de febrero. Este Real Decreto delimita las garantías, requisitos y supuestos de utilización de las aplicaciones y medios electrónicos, informáticos y telemáticos, y considera como órgano competente para aprobar los programas y aplicaciones a aquél que, en cada caso, tenga atribuida la competencia para resolver cada procedimiento administrativo.

El Real Decreto adopta la sistemática del artículo 45, y realiza una distinción entre cuatro supuestos:

a) Tramitación de procedimientos administrativos en soporte informático.
b) Programas y aplicaciones utilizados para el ejercicio de potestades administrativas. Los programas y aplicaciones con los que las Administraciones ejerzan potestades con efectos *ad extra* serán objeto de aprobación y difusión pública (6).
c) Relaciones entre la Administración y el ciudadano.
d) Emisión de documentos y copias.

Los fines últimos de este Real Decreto son establecer las garantías de la utilización de soportes, medios y aplicaciones con carácter general. El segundo objetivo es dar validez y eficacia, equiparando los documentos *automatizados* a aquellos que constan en soporte de papel. Precisamente, una de las obsesiones de este Real Decreto es garantizar la identificación y el ejercicio de la competencia por parte del órgano administrativo; corresponde a los ciudadanos el derecho a obtener información que permita la identificación de los medios y aplicaciones utilizadas, así como del órgano que ejerce la competencia. Ello no es más que el correlato al deber legal que consta en el artículo 35.*b)* de la Ley 39/92 de identificar a las autoridades y funcionarios.

Como norma técnica que es, este Reglamento contiene en su artículo 30 una primera serie de definiciones, muy elementales, de términos que son ajenos al jurista, pero que habrán de añadirse a los que posteriormente veamos al hablar de firma electrónica:

a) Soporte: objeto sobre el cual o en el cual es posible grabar o recuperar datos.
b) Medio: cualquier mecanismo, instalación, equipo o sistema de tratamiento de información que permite, utilizando técnicas electrónicas, informáticas o telemáticas, producir, almacenar o transmitir documentos.
c) Aplicación: programa o conjunto de programas.
d) Documento: entidad identificada y estructurada que contiene texto, gráficos, sonidos, imágenes o cualquier otra clase de información que pueda ser almacenada, editada, extraída e intercambiada entre sistemas de tratamiento de la información o usuarios como una unidad diferenciada.

(6) Correlativamente, el artículo 5 de este Real Decreto dispone que no será necesaria dicha aprobación cuando el uso de potestades sea meramente instrumental, esto es, con efectos *ad intra.*

Tanto los soportes, los medios como las aplicaciones pueden utilizarse en cualquier actuación administrativa, particularmente en la tramitación de procedimientos administrativos. Como requisito para posibilitar esta utilización, las técnicas deben asegurar la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información. En concreto, las medidas de seguridad deben garantizar:

a) La restricción de su utilización sólo a personas autorizadas.
b) La prevención de alteraciones o pérdidas de datos e informaciones.
c) La protección de los procesos informáticos frente a manipulaciones no autorizadas.

Es en el artículo 6 donde encontramos el primer avance de lo que luego supone la regulación de la firma electrónica. En este artículo se dispone que los documentos de los particulares que hayan sido emitidos por procedimientos electrónicos, informáticos y telemáticos serán válidos siempre que quede acreditada su integridad, conservación y la identidad del autor, así como la autenticidad de su voluntad, mediante la constancia de códigos u otros sistemas de identificación. Por otra parte (art. 7), la transmisión o recepción de comunicaciones entre la Administración y cualquier persona física o jurídica (o viceversa) podrá realizarse a través de soportes, medios y aplicaciones informáticos, electrónicos y telemáticos, siempre que cumplan los siguientes requisitos:

a) Garantía de disponibilidad y acceso a los mismos.
b) Compatibilidad entre los usados por el emisor y el destinatario.
c) Medidas de seguridad que eviten la interceptación y alteración de las comunicaciones.

Por otra parte, las comunicaciones y notificaciones (aunque no se especifica, pensamos que el Decreto se está refiriendo a las expedidas por la Administración) serán válidos, siempre que:

a) Exista constancia de la transmisión y recepción de sus fechas y del contenido íntegro de las comunicaciones. La referencia a las fechas es clave, dada la importancia y efectos que el cómputo de plazos tiene en Derecho Administrativo (7). Asimismo la expresión «conte-

(7) El propio Real Decreto así lo reconoce en el artículo 7.4: Las fechas de transmisión y recepción son las válidas a efectos de cómputo de plazos y términos. Para ello se anotarán en los registros generales o auxiliares a que hace referencia el artículo 38 de la LPC, artículo que —recordemos— impone a la Administración la instalación en soporte informático de los registros generales, y de todos los registros que las Administraciones establezcan para la recepción de escritos y comunicaciones de los particulares.

nido íntegro» recuerda la mención que hace el artículo 58 de la LPC al «texto íntegro» de la resolución en materia de notificaciones, y creemos que es en la efectividad de las notificaciones informáticas de lo que está hablando el legislador cuando menciona el contenido íntegro de las mismas.

b) Se identifique fidedignamente al remitente y al destinatario de la comunicación (art. 59.1 LPC). En el caso de tratarse de un particular, pensamos que dicha identificación fidedigna puede muy bien ser proporcionada por la firma electrónica.

Otro Real Decreto, el 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro, admite en su artículo 3 como medio de presentación de solicitudes, escritos y comunicaciones por los administrados, las presentadas por medios informáticos, electrónicos o telemáticos, remitiendo la regulación de estos al Real Decreto 263/1996.

3. LOS DESARROLLOS SECTORIALES POSTERIORES AL REAL DECRETO 263/1996, EN PARTICULAR EL SISTEMA ADOPTADO POR LA COMISION NACIONAL DEL MERCADO DE VALORES

Establecido ya el uso de las nuevas tecnologías por parte de la Administración, faltaba un elemento que permitiera tener la certeza de la autenticidad de la identidad del interesado. Pero hasta la aprobación del sistema de firma electrónica, aparecen en el Derecho español determinadas experiencias de regulación del uso de medios informáticos de marcado carácter parcial y sectorial. Este es el caso de la Comisión Nacional del Mercado de Valores, que por Acuerdo de 11 de marzo de 1998 estableció un «Sistema de Intercambio de Información» (8) a través de línea telemática, con el fin de conseguir la necesaria celeridad en las relaciones jurídicas de la Comisión sin merma de la seguridad jurídica. Dicho sistema está basado en los principios de autenticidad, confidencialidad, integridad, conservación, acuse de recibo y disponibilidad (norma 1.ª del Acuerdo). Podemos considerar este acuerdo la primera regulación, bien que sectorial, de la firma electrónica en el Derecho español (9).

(8) *BOE* de 27 de marzo de 1998. Concretamente se trata del Sistema CIFRA-DOC/CNMV, cuyas características técnicas se describen en el Anexo I del Acuerdo.

(9) Ello no quiere decir que sea el primer supuesto de utilización de soportes informáticos por parte de los particulares en su relación con la Administración. También en

La regulación de la CNMV trae causa directa del Real Decreto 263/1996, con el fin de adecuar todos los procedimientos de envío de soportes informáticos existentes hasta entonces (10). Para ello se aprueban una serie de aplicaciones electrónicas, informáticas y telemáticas descritas en los anexos, que configuran un sistema de intercambio de información, para su utilización gradual por los interesados. Concretamente, el sistema de firma electrónica aprobado en el anexo I cumple con los siguientes requisitos:

1. Autenticidad: Identificar suficientemente al emisor y al receptor del documento y dar certeza de las fechas y horas de envío y recepción. En la tramitación de procedimientos administrativos, la aplicación garantizará la identificación y competencia de la Comisión Nacional del Mercado de Valores. La información y documentación transmitida a través de este sistema tendrá plena validez y eficacia. De esta manera, las fechas de transmisión y

---

el año 1996 aparece una referencia directa a la firma electrónica, pero de manera muy incidental y en una ley autonómica. Se trata de la Ley catalana 19/1996, de Presupuestos de la Generalitat de Cataluña para 1997, en cuya Disposición Adicional 8.ª-1 se *«autoriza al Departamento de Economía y Finanzas para que pueda establecer la utilización de un sistema de intercambio electrónico de documentos con los proveedores de la Generalidad. Este sistema permitirá la sustitución de documentos impresos en papel por documentos grabados en soporte electrónico y la sustitución de los sistemas de autorización y control instrumentados mediante sellos y diligencias por autorizaciones y controles establecidos por las mismas aplicaciones informáticas, así como, en sustitución de los controles, validaciones de acceso restringido o firma electrónica»*. La misma disposición, con el mismo tenor literal, vuelve a aparecer en la Disp. Dic. 8.ª de la Ley catalana 20/1998, de Presupuestos de la Generalitat de Cataluña para 1999.

(10) Ello, a su vez, es consecuencia directa de la previsión legal contenida en el artículo 49 de la Ley 24/1988, de 28 de julio, del Mercado de Valores, según el cual, *«Las Bolsas de Valores establecerán un Sistema de Interconexión Bursátil de ámbito estatal, integrado a través de una red informática, en el que se negociarán aquellos valores que acuerde la Comisión Nacional del Mercado de Valores, de entre los que estén previamente admitidos a negociación en, al menos, dos Bolsas de Valores, a solicitud de la entidad emisora y previo informe favorable de la Sociedad de Bolsas a que se refiere el artículo siguiente, conforme a lo que se establezca reglamentariamente»*. Tradicionalmente, ha sido en el ámbito de la Comisión Nacional del Mercado de Valores donde el uso de soportes informáticos ha sido exhaustivo, incluso con anterioridad a la aprobación de la LPC. De esta manera, la presentación de documentos en soporte informático aparece en la Circular 3/1990, de 23 de mayo, que establece que la presentación de los estados reservados y públicos de las sociedades y agencias deberá hacerse en soporte informático, de acuerdo con los requerimientos técnicos establecidos en cada momento; la Circular 7/1990, de 27 de diciembre, permite que los estados financieros reservados de las Instituciones de Inversión Colectiva puedan presentarse en soporte informático; y la Circular 5/1992, de 28 de octubre, establece también la presentación en dicho soporte de los estados financieros reservados de las Sociedades gestoras de las Insituciones de Inversión Colectiva y las Sociedades Gestoras de Cartera. Como consecuencia de la aplicación de estas circulares, el envío de información a la Comisión mediante soportes informáticos por parte de las entidades supervisadas pasó a ser la regla general, recibiéndose por esta última un promedio de 1.000 disquetes al mes.

recepción acreditadas en las comunicaciones realizadas a través de este sistema, serán válidas a efecto de cómputo de plazos y términos, a cuyos efectos se anotarán en un registro auxiliar, de acuerdo con el artículo 38.3 de la LPC.

2. Confidencialidad: Asegurar que ningún usuario distinto de emisor y receptor tiene acceso al documento.

3. Integridad: Garantiza que cualquier alteración del contenido del documento durante la transmisión será detectada por el receptor.

4. Conservación: Archiva adecuadamente los documentos en la Comisión Nacional del Mercado de Valores e impide su pérdida o manipulación.

5. Acuse de recibo: Impide rechazar el envío y da certeza al remitente de que la recepción ha tenido lugar.

6. Disponibilidad: Asegura que el documento sea accesible a los usuarios autorizados.

Pero es en el Anexo I del Acuerdo, a la hora de describir las características del sistema, donde nos encontramos la primera definición del concepto de firma electrónica: Se trata de un sistema basado en un cifrado de la información remitida, al que se le complementa con una firma electrónica (que es la que proporciona la autenticidad) y un adecuado procedimiento de intercambio de mensajes y acuses de recibo en el que, tanto el emisor como el receptor combinan dos claves, una de ellas pública y la otra reservada (11).

La segunda alusión sectorial a la firma electrónica la encontramos en la Orden de 12 de abril de 1999, del Ministerio de Industria y Energía, por la que se dictan instrucciones técnicas complementarias al Reglamento de Puntos de Medida de Consumos y Tránsitos (12), cuando habla en el punto séptimo de las características de los concentradores de medidas secundarios (13). La Orden dispone que en el caso de optar por un procedimiento *«software»*, se empleará, preferentemente, el método denominado de «firma electrónica». Como la regulación general sobre la firma electrónica no había sido aún aprobada, la Orden precisa también qué debe entenderse por firma

(11) La clave pública es el elemento que debe ser puesto al alcance de cualquier persona que lo requiera, y que está relacionado por procedimientos matemáticos con la clave privada; su custodia corresponde a la Autoridad de Certificación en su directorio. Por su parte, la clave privada es el elemento secreto que queda custodiado por la persona certificada con garantías de seguridad.

(12) Se está refiriendo al Real Decreto 2018/1997, de 26 de diciembre, relativo a consumos y tránsito de energía eléctrica.

(13) Para quienes somos profanos en la materia, un concentrador secundario garantiza la integridad de la información enviada por comunicaciones cuando la información que se puede obtener por lectura local del registrador se corresponde, byte a byte, con la recibida en el concentrador principal, a excepción de las modificaciones que introduzcan los protocolos específicos del canal de comunicaciones.

electrónica, con lo que de nuevo tenemos una definición: Este método establece una correspondencia entre un fichero de datos y una firma electrónica, generada en el extremo origen mediante algoritmo, que se adjunta con el anterior, conformando así el fichero mensaje. Cualquier modificación sobre el fichero de datos o sobre la firma electrónica, realizada en un punto intermedio de la cadena de comunicación, es detectada en el extremo destino, al deshacerse la correspondencia entre ambas partes del fichero mensaje.

4. LA REGULACION ESPECIFICA DE LA FIRMA ELECTRONICA: EL ADELANTADO REAL DECRETO-LEY 14/1999 Y LA DIRECTIVA 1999/93/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 13 DE DICIEMBRE DE 1999, POR LA QUE SE ESTABLECE UN MARCO COMUNITARIO PARA LA FIRMA ELECTRONICA

La promulgación del Decreto-ley 14/1999 supone la consagración legal de la regulación específica de la firma electrónica. No resulta nuevo que es en el ámbito del comercio electrónico donde la firma electrónica va a encontrar un amplio desarrollo, sin embargo este aspecto de la firma electrónica no es el que nos interesa (14), sino su utilización en el ámbito de las Administra-

(14) La regulación establecida por el Decreto-ley y la Directiva europea en materia de firma electrónica es una regulación general, no sólo de los usos administrativos de la misma. De hecho, el ámbito de aplicación de la firma electrónica habrá de conocer una enorme incidencia práctica en el campo del comercio electrónico. Todos los aspectos relacionados con los problemas legales del comercio electrónico corresponden al Derecho Mercantil. En este sentido, vid. los trabajos de MARTÍNEZ NADAL, APOL.LÒNIA, *La Ley de Firma Electrónica,* Ed. Civitas, 1.ª edición, 2000, 311 págs. MARTÍNEZ NADAL, APOL.LÓNIA, *Comercio Electrónico, firma digital y autoridades de certificación,* Ed. Civitas-UIB-Govern Balear, 2.ª edición, 2000, 305 págs. En particular, sobre contratación y comercio electrónico, vid. DEVOTO, MAURICIO y LYNCH, HORACIO M., *Banca, comercio, moneda electrónica y firma digital,* pág. 4. Artículo electrónico en la Red (www.it-cenit.org.ar/Publicac/BancaMD/Bancoml), aunque originalmente publicado en la Revista Jurídica *La Ley,* de Buenos Aires. DÍAZ FRAILE, JUAN MARÍA, «Comentarios a la Directiva y al Proyecto de Ley español de Comercio Electrónico de 2000», en *Revista Crítica de Derecho Inmobiliario,* núm. 663, enero-febrero de 2001, págs. 81 a 122. DOMÍNGUEZ LUELMO, ANDRÉS, «Contratación electrónica y protección de los consumidores: Régimen jurídico», en *Revista Crítica de Derecho Inmobiliario,* núm. 660; julio-agosto de 2000, págs. 2327 a 2389. MATEO DE ROS, RAFAEL, y CENDOYA MÉNDEZ DE VIGO, JUAN MANUEL (coordinadores): *Derecho de Internet: contratación electrónica y firma digital,* Ed. Aranzadi, año 2000, 1094 págs y un CD-ROM. GARCÍA MÁS, FRANCISCO JAVIER, «La contratación electrónica: la firma y el documento electrónico», en *Revista Crítica de Derecho Inmobiliario,* núm. 652, mayo-junio de 1999, págs. 765 a 796.

ciones Públicas en sus relaciones con los ciudadanos o, dicho de otra manera, en el ámbito del artículo 45 de la Ley 30/1992 (15).

Con todo, no nos es posible avanzar en la comprensión jurídica del Decreto-ley sobre firma electrónica sin antes dar unas nociones sobre qué es un sistema de firma electrónica. Lo primero que hay que señalar es que al igual que sucede con la firma manuscrita, la firma electrónica permite tener la certeza absoluta de que la persona que envía un documento electrónico es quien dice ser. Así, por ejemplo, se podría equiparar el requisito de incorporar una firma electrónica a un documento presentado a la Administración, por ejemplo, por correo electrónico, a la firma manuscrita en cualquier otra solicitud o instancia. En este sentido se entiende plenamente el contenido del artículo 70.1.*d)* de la LPC, cuando dice que uno de los requisitos que deberá contener la solicitud del interesado será la firma del mismo *«o la acreditación de la autenticidad de su voluntad expresada por cualquier medio»;* creemos que la firma electrónica cumple perfectamente con esta exigencia legal. Actualmente el *World Wide Web* (o simplemente, el «Web») y el correo electrónico tienen un importantísimo papel en materia de difusión de información de las Administraciones Públicas (piénsese, por ejemplo, en las diferentes páginas «Web» de las distintas Administraciones Públicas), pero también como medio de realización de actuaciones del particular ante las Administraciones de forma prácticamente interactiva y *on-line,* en el caso del «Web», o por medios de almacenamiento y reenvío de un mensaje a través de determinados agentes de transferencia de mensajes (caso del correo electrónico). Como señala MARTÍNEZ NADAL, el WWW y el correo electrónico son dos aplicaciones de Internet que, dada su configuración como red abierta, ofrece el problema de la seguridad (16).

Los riesgos más importantes del uso de sistemas electrónicos informáticos y telemáticos pueden ser resumidos en cuatro:

a) Que el autor del mensaje haya sido suplantado (por ello, lo primero es garantizar la identidad).

b) Que el mensaje sea alterado (integridad del mensaje).

---

(15) Las posibilidades en este sentido son enormes, desde la más sencilla presentación de documentos hasta el cumplimiento de obligaciones fiscales vía línea informática, posibilidad de conocer el estado de tramitación de un expediente o los resultados de una oposición, cumplimentación de trámites administrativos sin que sea necesario el desplazamiento físico del administrado o, a nivel policial, presentación de deuncias a través de correo electrónico.

(16) El origen de Internet estriba en el intercambio de información militar (Milnet). En la actualidad, la seguridad en la red ha devenido una de las prioridades, lo que ha dado lugar a la aparición de distintas soluciones tecnológicas (MARTÍNEZ NADAL, APOL.LÓNIA, *Comercio Electrónico, firma digital y autoridades...,* ob. cit., pág. 30).

c) Que el emisor del mensaje niegue haberlo transmitido o el destinatario recibido (no rechazo), al igual que ocurre con las notificaciones escritas.

d) Que el contenido del mensaje sea leído por una persona no autorizada (confidencialidad).

Las firmas electrónicas y los correspondientes certificados son tecnologías seguras que contribuyen a resolver estos problemas creados de la utilización de medios informáticos, al permitir la confirmación inequívoca de la identidad del remitente y la integridad del mensaje. Las firmas manuscritas desaparecen y son reemplazadas por una variedad de métodos que son incluidos en el concepto amplio de firma electrónica. De esta manera, una firma electrónica sería cualquier método o símbolo basado en medios electrónicos utilizados para autenticar un documento, que además cumple algunas, todas y en ocasiones más funciones que la firma manuscrita (17). Sin embargo, debemos huir del concepto literal de firma; así, por ejemplo, no es válido a efectos de autentificar, una firma manuscrita que el particular escanea e incluye en un documento electrónico. Y no puede ser válido porque falta la seguridad a la hora de saber quién firma el documento (cualquiera puede escanear nuestra firma) (18). En un concepto amplio de firma electrónica habría que incluir estos supuestos, pero como vemos no ofrecen seguridad. Por ello se acude al concepto de firma digital, que es una variedad específica de firma electrónica. El sistema de firma digital se basa en la criptografía de claves asimétricas (19). Las claves se utilizan para cifrar (encriptar) el contenido del documento y para firmarlo electrónicamente: se cifran o firman

(17) Como precisa MARTÍNEZ NADAL, partiendo de un texto de Naciones Unidas sobre el Derecho Mercantil Internacional, las funciones tradicionales de una firma son: identificar a una persona, proporcionar certidumbre en cuanto a su participación personal en el acto de una firma, y vincular a esa persona con el contenido del documento (MARTÍNEZ NADAL, APOL.LÒNIA, *Comercio Electrónico, firma digital y autoridades...,* ob. cit., pág. 39, en nota).

(18) Este supuesto se plantea también en los actos administrativos realizados por escrito cuando se utiliza un sello de tinta para firmar un acto determinado; la utilización del sello no ofrece una total garantía de que el acto haya sido firmado por el titular concreto de la competencia.

(19) La criptografía es una rama de las matemáticas. Las claves asimétricas aparecieron en 1976, y fueron inventadas en la Universidad de Standford, en Estados Unidos. Se trata de unos criptosistemas basados en el uso de un par de claves asociadas: una clave privada, conocida por su titular, que debe mantenerla en secreto (normalmente, en una tarjeta inteligente); y una clave pública, relacionada matemáticamente con la privada, y que puede ser accesible para cualquiera. Aunque las claves estén relacionadas matemáticamente, el diseño y ejecución de un criptosistema asimétrico hace imposible que las personas que conozcan la clave pública puedan derivar de ella la clave privada. Esto es a lo que se llama inderivabilidad de las claves, que se encuentra establecida en el Ane-

utilizando una de las claves y se descifran con la clave complementaria, relacionándose ambas claves por una fórmula compleja (un algoritmo matemático) de forma que del conocimiento de la clave pública no se pueda deducir el de la clave privada. La firma electrónica consiste, pues, en cifrar un resumen del contenido del documento, extraído mediante un algoritmo que asegura la unicidad del resumen con la clave privada del firmante que incluye la fecha y hora. Cualquier variación en el contenido del documento supondría un cambio en el resumen, es decir, en la firma que se obtendría al aplicar de nuevo el algoritmo.

La firma electrónica garantiza así, a cualquiera que reciba el documento y que sea capaz de descifrarlo con la clave pública del firmante, la identidad del emisor y que el contenido del documento no ha sido alterado durante la transmisión, así como la fecha y hora en que ha tenido lugar su firma. Si, posteriormente, el conjunto formado por el documento y la firma electrónica se cifra con la clave pública del destinatario, quedará garantizado que sólo este último tendrá acceso al contenido del documento transmitido, aplicando previamente para descifrarlo su clave privada.

Para que el sistema de firma electrónica sea operativo antes de iniciar la transmisión de cualquier documento, el emisor y el receptor deben intercambiarse sus claves públicas. Para ello, la Administración (en este caso, la Comisión Nacional del Mercado de Valores) lleva a cabo una gestión centralizada de las claves públicas que permite acreditar la correspondencia entre la clave pública y el usuario autorizado.

A la hora de enviar, el emisor realiza los siguientes pasos:

a) El emisor firma electrónicamente el documento a enviar utilizando su clave privada.

b) El emisor cifra el documento y la firma con la clave pública del receptor.

c) Finalmente, el emisor envía el documento y la firma por el medio telemático establecido.

---

xo III de la Directiva y en el artículo 19 del Decreto-ley español. Este sistema ha suplantado al más primitivo basado en la criptografía simétrica o criptografía tradicional, en el que ambas partes compartían una clave común que era utilizada para cifrar (encriptar) y descifrar el mensaje, y que debía ser secreta para evitar el acceso autorizado a datos confidenciales; el principal problema que planteaba este sistema era conseguir que ambas partes conocieran la misma clave sin que ningún tercero se enterase (MARTÍNEZ NADAL, APOL.LÓNIA, *Comercio Electrónico, firma digital y autoridades...*, ob. cit., págs. 44-45 y 55-56. Vid. también DEVOTO, MAURICIO y LYNCH, HORACIO M., *Banca, comercio, moneda electrónica y firma digital,* pág. 4. Artículo electrónico en la Red (www.it-cenit.org.ar/Publicac/BancaMD/Bancoml), aunque originalmente publicado en la Revista Jurídica *La Ley,* de Buenos Aires).

Para realizar las operaciones de recepción y acuse de recibo, el receptor:

a) Descifra el documento con su clave privada y obtiene el documento original y la firma del emisor.
b) Descifra de nuevo el documento con la clave pública del emisor y comprueba que el contenido no ha sido alterado, así como la identidad del emisor y la fecha y hora en que se firmó.

El receptor firma electrónicamente el documento utilizando su clave privada. El receptor envía al emisor esta firma electrónica por el medio telemático establecido como acuse de recibo. Así, por ejemplo, en el envío de una instancia a la administración mediante el uso de la firma electrónica, el administrado cifraría la solicitud con una clave privada que sólo él conoce, y sería descifrado por la Administración utilizando la clave pública del administrado que la Administración conoce. De esta manera, el documento que le es presentado a la Administración sólo se puede descifrar con la clave pública del administrado si fue cifrado con la clave privada; asimismo, no es posible averiguar cuál es esa clave privada (20). Con ello, la Administración que recibe el documento sabe que éste fue cifrado o firmado por el concreto administrado que posee dicha clave privada. Resulta necesario tener la seguridad de que la clave pública pertenece efectivamente a la Administración; ésta es la tarea de las autoridades de certificación, a las que ya nos referiremos en el apartado siguiente (21). De esta manera la firma digital consigue, iguales e incluso superiores efectos que la tradicional firma manuscrita, pues da integridad, autenticidad y evita el problema del rechazo o negación. Por ello las diferentes legislaciones existentes en el Derecho comparado han equiparado los efectos de la firma manuscrita y la digital (22).

(20) Esta precisión tiene su sentido, ya que la clave privada deriva de la clave pública, pero el sistema está hecho de tal manera que no es posible averiguar una partiendo de la otra. A esta característica se le denomina inderivabilidad.

(21) El sistema requiere de una infraestructura grande y compleja, pero esencial, de tal manera que las autoridades certificantes operen bajo estrictas normas predeterminadas. La determinación de la referida estructura está relacionada con la política de intervención legislativa que se adopte con referencia a la validez del documento electrónico. Todas las cuestiones relativas a la naturaleza, efectos y plazo de validez de los certificados y la responsabilidad de las autoridades de certificación ha sido objeto de regulación por parte del Derecho público.

(22) No es este el lugar para analizar el Derecho comparado en materia de firma digital. El primer lugar que procedió a regular la firma digital fue el Estadio de Utah, en Estados Unidos *(Utah Digital Signature Act),* que entró en vigor el 1 de mayo de 1995, y que ha servido de modelo a otras regulaciones estadounidenses: Arizona, Georgia, Hawai, Oregón, Washington, Illinois, California, Florida, etc. Unicamente diremos, siguiendo a DEVOTO y LYNCH, que caben las siguientes posturas legislativas:

4.1. LA REGULACIÓN ESPAÑOLA: LA APROBACIÓN MEDIANTE DECRETO-LEY

Lo primero que llama la atención de la regulación de la firma electrónica en el Derecho español es la forma jurídica que el legislador español ha utilizado para regularla: el Decreto-ley. El legislador trata de autojustificar la *«extraordinaria y urgente necesidad»* a la hora de dictar un Decreto-ley en el deseo de dar a los usuarios de los nuevos servicios, elementos de confianza

---

Una postura amplia en que el legislador establece la validez del documento electrónico, sin hacer referencia a su soporte material ni al tipo de lenguaje utilizado (regulaciones de los Estados de California y Florida).

Una postura restringida, en que el legislador se preocupa no sólo de establecer la validez jurídica del documento electrónico, sino también de reglamentar su uso, a la vez que determina detalladamente la infraestructura técnica y operacional que se utilizará para el uso del mismo (regulaciones de los Estados de Utah y Georgia).

Una postura detallista, en que el legislador revisa todo el ordenamiento jurídico para derogar, modificar o añadir normas que hagan compatibles el sistema con el documento electrónico (caso de la ley federal alemana).

Como sistemas mixtos se pueden citar el Reglamento italiano y la Ley chilena sobre documentos electrónicos, que se limitan a enumerar unos principios, remitiendo a un posterior desarrollo reglamentario (DEVOTO, MAURICIO y LYNCH, HORACIO M., *Banca, comercio, moneda electrónica y firma digital...,* ob. cit., pág. 5).

A nivel europeo, la primera regulación sobre firma electrónica tiene lugar en Italia, a través de la Ley de 15 de marzo de 1997, núm. 59, por la que se delega al gobierno la atribución de funciones y deberes a las regiones y entes locales para la reforma de la Administración Pública y para la simplificación administrativa. Esta norma delega a una normativa posterior los aspectos técnicos y legales concretos para dicha modernización. Así surge el Reglamento que contiene las modalidades de aplicación del artículo 15.2 de la Ley de 15 de marzo de 1997, núm. 59, en formación, archivo y transmisión de documentos con instrumentos informáticos y telemáticos. El artículo 2 del Reglamento italiano establece que los documentos informáticos serán válidos y eficaces a todos los efectos legales si son acordes con las exigencias del reglamento; en concreto, el artículo 10.2 equipara la firma digital sobre un documento informático a la firma escrita en soporte papel, y el artículo 8 establece que cualquiera que pretenda utilizar la criptografía asimétrica con los efectos del artículo 2 debe conseguir un par de claves adecuado y hacer pública una de ellas a través del procedimiento de certificación efectuado por un certificador.

En Alemania, la Ley reguladora de la firma digital y las autoridades de certificación fue aprobada por el Bundestag el 13 de junio de 1997. La finalidad de esta Ley es proporcionar las condiciones para crear una infraestructura segura para el uso en Alemania de las firmas digitales, aunque el cumplimiento de la ley es voluntario.

En Portugal, el Decreto-ley número 290-D/99, de 2 de agosto, tiene como objetivo regular la validez, eficacia y valor probatorio de los documentos electrónicos y la firma digital.

Por último, en Francia no existe ley que regule directamente las firmas digitales, pero sí el uso de la criptografía (Ley núm. 96-650, de 26 de julio de 1996), aunque existe una normativa en preparación específicamente para la firma electrónica, al igual que sucede en Reino Unido, Dinamarca, Finlandia y Bélgica (MARTÍNEZ NADAL, APOL.LÓNIA, *Comercio Electrónico, firma digital y autoridades de certificación...,* ob. cit., págs. 52 y 93 a 95).

y por la existencia de un sector empresarial que podría prestar un servicio de certificación de la firma electrónica con suficiente calidad, tal y como confiesa la Exposición de Motivos. Sin embargo, surgen dudas más que razonables acerca de la prisa del legislador, sobre todo cuando se encontraba en fase de elaboración un proyecto de directiva a nivel europeo del que la normativa española hubiera tenido que hacer una trasposición. En efecto, la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, llegó al DOCE el 19 de enero de 2000, esto es, tan sólo cuatro meses después de que el Gobierno español adoptase este Decreto-ley. Se trata de un caso paradigmático de regulación nacional *ex ante,* que desde luego no es lo habitual cuando existe una legislación comunitaria (23). La promulgación de la normativa española, además de puentear la intervención del Parlamento, ha conseguido una regulación que discrepa en algunos puntos de lo que después ha establecido la Directiva y que tendrá por tanto que ser reformada para efectuar la correcta trasposición de la misma. Todos estos elementos hacen, con mucho, sospechosa la demora y la urgencia del Ejecutivo español en la adopción de este Decreto-ley, que más parece motivada por presiones empresariales que por una necesidad legislativa concreta (24). Con todo, este Decreto-ley fue convalidado sin mayor problema a través de la Resolución del Congreso de los Diputados, de 21 de octubre de 1999. Sin embargo, unos días antes, el Gobierno volvía nuevamente a sorprendernos con un Real Decreto-ley 16/1999, de 15 de octubre (nada menos que sobre medidas para combatir la inflación), en cuya Disposición Adicional primera *«Se faculta al Ministerio de Fomento para que reglamentariamente desarrolle lo previsto en (...) los artículos 6 y 22 del Real Decreto-ley 14/1999, de 17 de septiembre (...)»,* es

(23) La regulación española, con todo, no es independiente de la comunitaria. Como la propia Exposición de Motivos del Decreto-ley confiesa, se parte del Proyecto de Directiva del Parlamento Europeo y del Consejo, por la que se establece un marco común para la firma electrónica, cuya tramitación se encontraba ya muy avanzada. Sin embargo, como advierte MARTÍNEZ NADAL, no es menos cierto que por no haber sido definitivamente aprobado, el texto comunitario era susceptible de pequeñas variaciones y discrepancias, como efectivamente sucedió (MARTÍNEZ NADAL, APOL.LÓNIA, *La Ley de Firma Electrónica,* Ed. Civitas, 1.ª edición, 2000, pág. 26).

(24) MARTÍNEZ NADAL añade otra crítica a estos argumentos. La urgencia no se justificaba desde el momento en que, como hemos visto, ya estaban aprobadas diversas normas sectoriales que regulaban la firma electrónica de forma parcial, y con las que era posible inferir una regulación mínima en materia de firma electrónica (MARTÍNEZ NADAL, APOL.LÓNIA, *La Ley de firma electrónica,* Ed. Civitas, 1.ª edición, 2000, pág. 23. De la misma autora, vid. «Comentarios de urgencia al urgentemente aprobado Real Decreto-ley 14/1999, de 17 de septiembre», en Revista *La Ley,* núm. 4.939 y 4.949, 1 y 2 de diciembre de 1999, págs. 1 a 5 en ambos números). En todo caso, no era conveniente regular a nivel nacional sin conocer antes la versión promulgada de la directiva comunitaria.

decir, que además de reconocer la incompleta regulación hecha en su día por el Decreto-ley 14/1999, se habilita a Fomento para que a través de una Orden Ministerial desarrolle todo lo relativo a servicios de certificación y dispositivos de verificación de firma (25).

Por su parte, la elaboración de la Directiva Comunitaria 199/93/CE fue menos azarosa. El proceso se abre el 16 de abril de 1997 con la *Comunicación de las Comunidades Europeas al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones sobre la iniciativa europea de comercio electrónico* (26); y en el mismo año, el 8 de octubre de 1997, con una *Comunicación de la Comisión de las Comunidades Europeas al Consejo, al Parlamento y al Comité Económico y Social y al Comité de las Regiones garantizando la seguridad y confianza en las comunicaciones electrónicas: Hacia un marco europeo para las firmas digitales y la encriptación* (27). Tras estas comunicaciones, la Conferencia Europea Ministerial de Bonn (6 y 8 de junio de 1997) manifestó la necesidad de un marco legal y técnico común para las firmas digitales. El 1 de diciembre del mismo año, el Consejo invitó a la Comisión a que presentara una propuesta de Directiva del Parlamento Europeo y del Consejo en materia de firma digital. La Comisión presentó ya en 1998 un borrador de propuesta de directiva sobre un marco común para las firmas electrónicas que, finalmente, fue aprobado como Directiva el 13 de diciembre de 1999.

4.2. OBJETO DEL REAL DECRETO-LEY 14/1999. LOS CONCEPTOS LEGALES EN MATERIA DE FIRMA ELECTRÓNICA

El Decreto-ley se dicta por el Gobierno central al amparo de las competencias exclusivas del Estado de los artículos 148.1.8.ª, 18.ª y 21.ª de la

(25) En el ejercicio de esta habilitación, el Ministerio de Fomento ha dictado ya la Orden de 21 de febrero de 2000, que contiene el reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.

(26) [COM (97) 157 final]. La finalidad de esta Comunicación es fomentar el crecimiento del comercio electrónico en Europa. Básicamente se trata de proporcionar un acceso amplio y asequible a la infraestructura, los productos y los servicios necesarios para el comercio electrónico mediante tecnologías y servicios seguros y fáciles de usar. Y, en segundo lugar, implantar tecnologías seguras (como firmas digitales, certificados digitales) y un marco jurídico e institucional que sirva de apoyo a estas tecnologías.

(27) [COM (97) 503]. El principal objetivo de esta comunicación es desarrollar una política europea en la materia, estableciendo un marco común para las firmas digitales que, al crear un marco que genere confianza en las mismas, asegure el funcionamiento del mercado interno. Las medidas deberían aplicarse a más tardar en el año 2000 y ser lo suficientemente flexibles como para admitir desarrollos tecnológicos.

Constitución en materia de legislación civil, de bases del Régimen Jurídico de las Administraciones Públicas y de telecomunicaciones (28). Según la Exposición de Motivos, el objetivo del Decreto-ley es *«establecer una regulación clara del uso de ésta* (la firma electrónica), *atribuyéndole eficacia jurídica y previendo el régimen aplicable a los prestadores de servicios de certificación».* Este objetivo se reitera en el artículo 1: se regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación (29). El artículo 1 del Decreto-ley coincide básicamente con el artículo 1 de la Directiva (titulado «ámbito de aplicación»). Ambos instrumentos normativos únicamente regulan las firmas electrónicas como un elemento que, junto con el sistema de certificados, permite solucionar los problemas de autoría, integridad y no rechazo de origen.

Como en otras normas, también en el Decreto-ley se contienen una serie de definiciones, de las cuales la que más nos interesa es la propia definición de firma electrónica [art. *2.a)]: «Es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge».* Este concepto coincide básicamente con el establecido en el artículo 2.1 de la Directiva: *«los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación».* Se trata de un concepto amplio de firma que, sin embargo, resulta insuficiente, pues carece de un elemento exigido por el artículo 45 de la LPC: la seguridad. Por ello, el legislador afina más y define,

(28) Disposición Final 1.ª del Decreto-ley 14/1999.

(29) En este artículo se precisa que el Decreto-ley no afecta a la tradicional Teoría civil del contrato, en lo que se refiere a las normas relativas a celebración, formalización, validez y eficacia de los contratos. Tampoco supone la sustitución de las funciones que corresponden a los fedatarios públicos (notarios y corredores de comercio) en cuanto a personas que dan fe o elevan los documentos a públicos. De hecho dos recientes regulaciones han establecido la posibilidad de presentar las cuentas anuales en los Registros Mercantiles a través de procedimientos telemáticos, así como de legalizar los libros de los Registros Mercantiles a través de procedimientos telemáticos (Instrucciones de la Dirección General de los Registros y del Notariado de 30 y 31 de diciembre de 1999, respectivamente). En ambos casos se remite a la regulación vigente en materia de firma electrónica avanzada y a la preceptiva intervención de la entidad prestadora de servicios de certificación, aunque la Instrucción de 30 de diciembre es más explícita y alude expresamente al Real Decreto-ley 14/1999 y a la Resolución de la Dirección General de los Registros y del Notariado de 12 de noviembre de 1999).

La precisión es una novedad del Decreto-ley español (no se incluye en la Directiva), y viene a establecer una salvaguarda de la actividad de los fedatarios públicos a los que en ningún caso va a poder sustituir un prestador autorizado de servicios de certificación, cuya función es distinta y, además, no está revestida de los atributos propios de aquéllos. Por ello, como afirma MARTÍNEZ NADAL, esta precisión resultaba innecesaria (MARTÍNEZ NADAL, APOL.LÓNIA, *La Ley de Firma Electrónica,* Ed. Civitas, 1.ª edición, 2000, pág. 32).

quizá de forma tautológica, la *«firma electrónica avanzada»* [art. 2.*b)*]: *«Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que esté vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación ulterior de éstos»*. Se trata de una firma que reúne unos requisitos que añaden calidad a la simple firma electrónica, haciéndola más segura (30). Se trata, como vemos, de una subespecie de firma electrónica (31) (32), por lo que quizá hubiera sido más conveniente hablar de firma digital (33). De hecho, los efectos jurídicos de los que habla el artículo 3 del Decreto-ley (y 5.1 de la Directiva) hablan únicamente de la firma

(30) Los requisitos son similares y equiparables a los que se contienen en el artículo 2.2 de la Directiva, aunque esta última los enuncia de una forma un poco más clara: *«firma electrónica avanzada: la firma electrónica que cumple los requisitos siguientes:*

a) estar vinculada al firmante de manera única;

b) permitir la identificación del firmante;

c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control;

d) estar vinculada a los datos a que se refiere, de modo que cualquier cambio ulterior de los mismos sea detectable».

(31) Como señala MARTÍNEZ NADAL, tras el concepto de «firma electrónica avanzada» se esconde la firma digital basada en la criptografía asimétrica. Sin embargo, razones de neutralidad tecnológica impiden regular expresamente este tipo de firma basada en una concreta tecnología, pero está claro que la «firma electrónica avanzada» es hoy la firma digital. Por ello, tras la neutralidad tecnológica del concepto, se esconde la realidad material de la firma digital. Y más concretamente, una firma digital basada en la PKI, aunque el objetivo de la Directiva de ser «tecnológicamente neutral» no le permiten ser tan explícita, en un intento de pervivir a los frenéticos cambios de la tecnología (MARTÍNEZ NADAL, APOL.LÒNIA, *La Ley de Firma Electrónica,* Ed. Civitas, 1.ª edición, 2000, ob. cit., pág. 45, en nota. También, de la misma autora, *Comercio Electrónico, firma digital y autoridades de certificación...,* ob. cit., pág. 42).

(32) MARTÍNEZ NADAL cita una clasificación de firmas electrónicas realizada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL) en orden decreciente en función de su mayor seguridad: firmas electrónicas, firmas digitales, firmas digitales verificadas por referencia a un certificado emitido por una autoridad con licencia a la que la autora balear añade las firmas digitales verificadas por referencia a un certificado emitido por una autoridad de certificación especialmente cualificada e incluso, finalmente, las firmas digitales autenticadas ante notario (MARTÍNEZ NADAL, APOL.LÓNIA, *Comercio Electrónico, firma digital y autoridades de certificación...,* ob. cit., pág. 68).

(33) Así, por citar un ejemplo, habla indistintamente de firma electrónica o digital el artículo 35.6 de la Orden del Ministerio de Justicia, de 19 de julio de 1999, por la que se aprueba la Ordenanza del Registro de Bienes Muebles, cuando establece que *«La identificación de los créditos cedidos, de su fecha y de la persona de los deudores no necesitará constar en el modelo oficial presentado a inscripción; a estos efectos bastará que tales circunstancias consten en soporte magnético, cuyo contenido certifique el Banco de España o que se remitan por éste directamente de forma telemática a través de correo electrónico o similar. Para ello, previamente, aquél deberá aportar los datos identificativos de la firma digital o electrónica que permitan identificar al remitente».*

electrónica avanzada, y la equiparan a la firma manuscrita respecto de los datos consignados en documentos de soporte papel, siendo esta firma digital admisible como prueba en juicio (34). Para el resto de firmas electrónicas que no reúnan estos requisitos (que no sean «avanzadas») el Decreto-ley dispone que no se les negará valor jurídico ni serán excluidas como prueba en juicio, pero el legislador tampoco concreta qué consecuencias tendrá una firma que no sea avanzada (35). Volvamos al caso de la firma manuscrita escaneada; opinamos, en principio, que podrá surtir efecto mientras el particular no la niegue, de la misma manera que sucede hasta ahora con la firma manuscrita, ya que esta firma electrónica no ofrece la necesaria seguridad, aparte de su nula aportación respecto de la integridad del mensaje. Por ello, *de lege ferenda*, MARTÍNEZ NADAL entiende que hubiera sido más conveniente adoptar una posición técnica abierta para no desalentar el recurso a otras técnicas futuras y seguras, pero excluyendo técnicas actuales inseguras, y centrándose también en la regulación de la firma digital. Precisamente el artículo 12 de la Directiva contiene previsiones para incorporar posibles modificaciones a la vista de los avances tecnológicos:

«Artículo 12: Revisión

1. La Comisión procederá al examen de la aplicación de la presente Directiva y presentará el oportuno informe al Parlamento Europeo y al Consejo, a más tardar el 19 de julio de 2003.

2. Dicho examen permitirá, entre otras cosas, determinar si conviene modificar el ámbito de aplicación de la presente Directiva en vista de la evolución tecnológica y comercial y del contexto jurídico. El informe incluirá, en particular, una valoración de los aspectos de armonización, basada en la experiencia adquirida. El informe irá acompañado, en su caso, de propuestas legislativas».

El resto del artículo 2 del Decreto-ley [apartados *d)* a *l),* y apartados 3) a 13)] de la Directiva, definen los elementos necesarios para la creación y

(34) El Decreto-ley establece en este sentido una remisión a las normas procesales, la cual hay que entender hoy referida a la Ley de Enjuiciamiento Civil 1/2000, artículos 299 y siguientes. El artículo 299.2 de la nueva LEC es muy elocuente al respecto, cuando dispone que se admitirán como prueba, entre otros, los instrumentos que permitan archivar y conocer palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, que resulten relevantes para el proceso. Esta posibilidad se desarrolla en los artículos 382 a 384 de la nueva LEC.

(35) El Decreto-ley español sigue en este aspecto los pasos de la Directiva, y adopta una postura dualista a la hora de definir la firma electrónica. Sin embargo, como advierte MARTÍNEZ NADAL, este dualismo es irrelevante por cuanto a esta dualidad corresponde una mayor o menor calidad en las firmas, lo cual resulta trascendente para el reconocimiento de los efectos legales de las mismas.

verificación de una firma electrónica, e introducen también una serie de definiciones jurídicas de conceptos eminentemente técnicos en los que no nos detendremos.

4.3. LOS CERTIFICADOS, EL DNI DIGITAL

Para que el sistema de firma electrónica funcione es necesario contar con un certificado reconocido. A diferencia de lo que ocurre con las firmas manuales, que tienen una asociación intrínseca con una persona física determinada, al estar hecha del puño y letra del firmante, un juego de claves usado para crear una firma digital no tiene una asociación intrínseca con nadie: un bit informático es exactamente igual a otro bit (36), y el par de claves (la pública y la privada) no son más que un par de números, no asociados a persona alguna (37). Por ello son necesarios otros instrumentos como las terceras partes de confianza (las autoridades de certificación) y los certificados. En el apartado siguiente veremos cómo la FNMT era la encargada de garantizar las comunicaciones de las Administraciones Públicas realizadas por medios electrónicos, informáticos y telemáticos (38). Sin embargo, ello no supone que a la FNMT se le haya otorgado el monopolio para ser autoridad de certificación a los efectos previstos en la firma electrónica. En este campo rige el principio de libre competencia, y la prestación de servicios de certificación no está sometida a autorización previa, sin que quepa es-

(36) Ye hemos dicho que un ordenador trata la información codificada en forma binaria, que podemos representar por los números 0 y 1, a los que se denomina bits. El bit es la unidad elemental de información y toma uno de esos valores (AGUAGO MUÑOZ, RICARDO y otros: *Basic Básico. Curso de programación,* Ed. Computer School, Madrid, 1989, pág. 23).

(37) MARTÍNEZ NADAL, APOL.LÓNIA, Comercio Electrónico, firma digital y autoridades de certificación..., *ob. cit.*, pág. 63.

(38) En este sentido, el artículo 5 del Decreto-ley se limita a señalar que se podrá supeditar el uso de la firma electrónica en el seno de las Administraciones y en las relaciones que mantengan los particulares, a las condiciones adicionales que se consideren necesarias, para salvaguardar las garantías de cada procedimiento. Estas condiciones adicionales que se establezcan podrán incluir la prestación de un servicio de consignación de fecha y hora, respecto de los documentos electrónicos integrados en un expediente administrativo. El citado servicio consistirá en la acreditación por el prestador de servicios de certificación, o por un tercero, de la fecha y hora en que un documento electrónico es enviado por el signatario o recibido por el destinatario.

Podemos citar un primer ejemplo de desarrollo legislativo de esta posibilidad. Se trata del Real Decreto 1891/1999, de 10 de diciembre, por el que se modifica el Reglamento General de la Gestión Financiera de la Seguridad Social aprobado por Real Decreto 1391/1995, de 4 de agosto. Este Decreto prevé (Disp. Adic. 5.ª) que las actuaciones relativas al pago de las obligaciones de la Seguridad Social podrán ser realizados por técnicas y medios electrónicos, informáticos y telemáticos, en los términos establecidos en el artículo 5 del Real Decreto-ley 14/1999, en relación con el artículo 45 de la LPC.

tablecer restricciones a los servicios de certificación procedentes de los Estados de la Unión Europea (39). Por razón de la materia podrá someterse a un régimen específico la utilización de la firma electrónica en las comunicaciones que afecten a información clasificada, a la seguridad pública o a la defensa (40).

Podemos definir los certificados como registros electrónicos que atestiguan que una clave pública pertenece a un determinado individuo o entidad (41). Ello permite la verificación de que una clave pública dada pertenece fehacientemente a una determinada persona. Un certificado por sí solo no es más que una certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad. La principal función del certificado es unir un par de claves con la firma de un determinado suscriptor, asociar la identidad de una persona determinada a una clave pública concreta (e indirectamente, a una clave privada); de esta manera, el certificado viene a ser una especie de «documento de identidad digital», que funciona como un identificador único dentro de la red, y que permite a su poseedor ser identificado como tal dentro de la misma; además de evitar que alguien utilice una clave falsa haciéndose pasar por otro (42). Que además el certificado sea

---

Por otra parte, los documentos en los que se formalicen o se notifiquen a los interesados y que sean producidos o reproducidos, incluida la firma, por medios electrónicos, informáticos o telemáticos, gozarán de la validez y eficacia de los documentos originales siempre que en ellos figure la impresión mecánica del número secuencial del documento, incluidos los dígitos de verificación y la clave de identificación del centro o unidad emisor y del titular del órgano del que emana el acto o documento de que se rate.

(39) Esta última precisión es totalmente redundante por cuanto sabemos que la de prestación de servicios entre los diferentes Estados de la Unión es una libertad reconocida en los artículos 3.1.*b)* y 23 y sigs. del Tratado de la Comunidad Europea. Por ello, el artículo 10 del Decreto-ley regula únicamente el valor de los certificados emitidos por prestadores de servicios establecidos en un Estado no miembro, que serán equivalentes a los expedidos en España cuando el prestador reúna los requisitos establecidos en la normativa comunitaria (remisión, pues, a la Directiva); que el certificado esté garantizado por un prestador de servicios de la Unión Europea y que el certificado o el prestador estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países.

(40) Este supuesto no es más que la limitación, trasladada al campo de la firma electrónica, de la limitación contenida en el artículo 105 de la Constitución que a su vez ha sido desarrollada en el artículo 37.5 de la LPC respecto al acceso de los ciudadanos a archivos y documentos respecto de la defensa nacional o la seguridad del Estado. En materia de secretos oficiales sigue en vigor la preconstitucional Ley 9/1968, de 5 de abril, modificada por las Leyes 48/1978 y 11/1995.

(41) En parecidos términos se expresa el artículo 2.9 de la Directiva. El certificado es la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de ésta.

(42) En su forma más simple, contienen una clave pública y un nombre, la fecha de vencimiento de la clave, el nombre de la autoridad certificante, el número de serie del

«reconocido» supone su expedición por un prestador de servicios de certificación y que contiene una serie de informaciones (43).

El artículo 2.*f)* del Decreto-ley (y 2.6 de la Directiva) disponen que el dispositivo de creación de una firma electrónica debe ser «seguro». El dispositivo es simplemente un programa o un aparato informático que sirve para aplicar los datos de creación de la firma; el dispositivo es además «seguro» cuando cumple los siguientes requisitos establecidos en el artículo 19 del Decreto-ley (y Anexo III de la Directiva):

1.° Que garantice que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure, razonablemente, su secreto.

2.° Que exista seguridad razonable de que dichos datos no puedan ser derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología existente en cada momento.

3.° Que los datos de creación de firma puedan ser protegidos fiablemente por el signatario contra la utilización por otros.

4.° Que el dispositivo utilizado no altere los datos o el documento que deba firmarse ni impida que éste se muestre al signatario antes del proceso de firma.

---

certificado y la firma digital del que otorga el certificado. Los certificados se inscriben en un registro, considerado como una base de datos a la que el público puede acceder directamente en línea *(on-line)* para conocer acerca de la validez de los mismos. Los usuarios o firmantes son aquellas personas que detentan la clave privada que corresponde a la clave pública identificada en el certificado. Por lo tanto, la principal función del certificado es identificar el par de claves con el usuario o firmante, de forma tal que quien pretende verificar una firma digital con la clave pública que surge de un certificado tenga la seguridad que la correspondiente clave privada es detentada por el firmante.

(43) Dicho contenido es el que se enumera en el artículo 8 del Decreto-ley:

a) La indicación de que se expiden como tales.

b) El código identificativo único del certificado.

c) La identificación del prestador de servicios de certificación que expide el certificado.

d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

e) La identificación del signatario, por su nombre y apellidos o a través de un seudónimo que conste como tal de manera inequívoca.

f) En los supuestos de representación, la indicación del documento que acredite las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente.

g) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del signatario.

h) El comienzo y el fin del período de validez del certificado.

i) Los límites de uso del certificado, si se prevén.

j) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

4.4. EL PROBLEMA DE LA ACREDITACIÓN DEL TIEMPO: EL SELLO TEMPORAL

Otro problema que se plantea en el sistema de firma electrónica es el de la acreditación del momento exacto en el que el documento ha sido presentado, lo cual tiene una importancia enorme, dado el sistema de plazos al uso en las diferentes Administraciones Públicas. La firma electrónica no proporciona por sí sola prueba alguna del momento temporal en el que el documento ha sido presentado; por ello al sistema de firma hay que completarlo con una marca temporal: combinando la firma digital con un sello temporal digital puede llegar a probarse que el documento fue presentado en un momento determinado. El sellado de un documento incluye todos los datos contenidos en el mismo, de forma que resulte imposible alterar ni uno solo de ellos, ni tampoco incluir una fecha u hora diferente a la que el documento fue presentado (44). El legislador español y comunitario han abordado estos problemas [art. 12 del Decreto-ley y Anexo II.*c)* de la Directiva], y ello se ha traducido en la exigencia de que los proveedores o prestadores de servicios que expidan certificados reconocidos garanticen el que pueda determinarse con precisión la fecha y hora en la que se expidió o revocó un certificado (45).

5. LAS AUTORIDADES CERTIFICANTES EN EL DERECHO ESPAÑOL: EL ARTICULO 81 DE LA LEY DE ACOMPAÑAMIENTO 66/1997 Y EL REAL DECRETO 1290/1999, DE DESARROLLO DE LA LPC EN MATERIA DE FIRMA ELECTRONICA

Un sistema basado en la criptografía necesita de una tercera parte de confianza (46), que debe actuar para asegurar el vínculo entre la clave pública

(44) El propio plazo de vida de los certificados digitales plantea nuevos problemas respecto a la eficacia temporal de los mismos una vez que éstos caducan; sin embargo, este no es el problema objeto de nuestro estudio. Sobre este aspecto, vid. MARTÍNEZ NADAL, APOL.LÓNIA, *Comercio Electrónico, firma digital y autoridades...*, ob. cit., págs. 77 y sigs.

(45) En todo caso, como afirma MARTÍNEZ NADAL, el valor probatorio del sello temporal dependerá de que sea proporcionado por un sistema seguro y de confianza. La autora cita varios sistemas técnicos actuales, que enunciaremos sólo a título enumerativo: *a)* Sistema de envío y simple sellado por la tercera parte de confianza; *b)* Sistema que consiste en añadir la hora y fecha al mensaje para su posterior firma por la tercera parte de confianza, y *c)* Sistema de vinculación de documentos para evitar manipulaciones del sello temporal MARTÍNEZ NADAL, APOL.LÓNIA, *Comercio Electrónico, firma digital y autoridades...*, ob. cit., págs. 78 y 79).

(46) Una tercera parte de confianza *(Trusted tird party, o TTP)* consiste en una o varias autoridades de certificación cuya misión es la de emitir certificados que, a la vez, sirven para distribuir la clave pública y asociar de forma segura la identidad de una

y el titular de la clave privada, además de desarrollar otras funciones igualmente importantes (por ejemplo, autenticar fechas y horas de determinadas acciones o publicar las claves que ya no son de confianza). La Autoridad Certificante (o Autoridad de Certificación) es una entidad dedicada a la emisión de certificados que contienen información sobre algún hecho o circunstancia del sujeto del certificado. Esta entidad puede emitir distintos tipos de certificados. Así, un certificado de identificación simplemente identifica y conecta un nombre a una clave pública. Los certificados de autorización proveen otro tipo de información correspondiente al usuario. Otros certificados colocan a la Autoridad Certificante en el rol de notario, pudiendo ser utilizados para la atestación de la validez de un determinado hecho o que un hecho efectivamente ha ocurrido. Otros certificados permiten determinar el día y hora en que un documento fue digitalmente firmado *(Digital time-stamp certificates).*

El interesado en operar con una firma digital, tras crear el par de claves, deberá presentarse ante la Autoridad certificante a efectos de registrar su clave pública, acreditando su identidad y cualquier circunstancia que le sea requerida para obtener el certificado que le permita «firmar» el documento de que se trate.

En el Derecho español, la Ley de Acompañamiento de los Presupuestos de 1998 (Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social), contiene en su artículo 81 una habilitación a la Fábrica Nacional de Moneda y Timbre (en adelante, FNMT) para actuar como autoridad de certificación en materia de firma electrónica *(«Prestación de servicios de seguridad por la Fábrica Nacional de Moneda y Timbre para las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos»).* La Ley de Acompañamiento faculta a la FNMT para la prestación de los servicios técnicos y administrativos necesarios para garantizar la seguridad, validez y eficacia de la emisión y recepción de comunicaciones y documentos a través de técnicas y medios electrónicos, informáticos y telemáticos en las relaciones que se produzcan entre:

---

persona concreta a una clave pública determinada. A la tercera parte de confianza se la denomina también autoridad de certificación, entidad de certificación, proveedor (o prestador) de servicios de certificación o simplemente certificador (MARTÍNEZ NADAL, APOL.LÓNIA, *Comercio Electrónico, firma digital y autoridades de certificación...,* ob. cit., pág. 65). Como la misma autora señala, la terminología para referirse a las terceras partes de confianza es muy variada, y denota la opción del legislador sobre la naturaleza de las mismas. Así, «Autoridad», parece atribuirles naturaleza pública, mientras que la expresión «prestador de servicios» parece querer excluir cualquier connotación de carácter público y darles una naturaleza estrictamente comercial; la categoría intermedia sería la de «prestador» de servicios de certificación, que es la que utiliza el Decreto-ley español. *Ibidem,* pág. 128.

a) Los órganos de la Administración General del Estado entre sí o con los organismos públicos vinculados o dependientes de aquélla, así como las de estos organismos entre sí.

b) Las personas físicas y jurídicas con la Administración General del Estado y los organismos públicos vinculados o dependientes de ella.

El artículo 81.2 habilita a la FNMT, en colaboración con la entidad pública empresarial Correos y Telégrafos y de acuerdo con las disponibilidades presupuestarias, para procurar la máxima extensión de la prestación de los servicios señalados para facilitar a los ciudadanos las relaciones a través de técnicas y medios electrónicos, informáticos y telemáticos con la Administración General del Estado y, en su caso, con las restantes Administraciones. Para dicha extensión de los servicios, se tendrán especialmente en consideración los órganos e instrumentos previstos en el artículo 38.4 de la LPC. Lo que se pretende, pues, es que la FNMT actúe como entidad certificadora de las Administraciones Públicas, emitiendo certificados que permitan comunicaciones electrónicas seguras dentro de la Administración, y entre ésta y los administrados, esto es, una autoridad de certificación a nivel estatal que actúe no sólo para la Administración del Estado, sino también para el resto de administraciones, autonómicas, municipales e instrumentales (47). El fin último no es otro que dar la mayor difusión a los servicios que garanticen la seguridad, validez y eficacia de las comunicaciones y documentos para facilitar a los ciudadanos las relaciones a través de estas técnicas y medios electrónicos, informáticos y telemáticos.

Este artículo 81 ha sido recientemente modificado a través de otra Ley de Acompañamiento, concretamente la Ley de 29 de diciembre de 1999, añadiendo dos nuevos apartados al artículo 81 de la Ley 66/1997. En el primero de ellos, relativo al ámbito judicial, se faculta a la FNMT, con la colaboración de Correos, a prestar los servicios técnicos, administrativos y de seguridad cuando los mismos fueran solicitados tanto por los órganos jurisdiccionales como por las partes intervinientes en un proceso, en relación con aquellos actos de postulación procesal que puedan practicarse a través de técnicas y

(47) Para ello, la Ley de Acompañamiento prevé expresamente una habilitación a la FNMT para prestar, en su caso, a las Comunidades Autónomas, las entidades locales y las entidades de Derecho público vinculadas o dependientes de ellas, los servicios de certificación en las relaciones que se produzcan a través de técnicas y medios electrónicos, informáticos y telemáticos entre sí, con la Administración General del Estado o con personas físicas y jurídicas; siempre que, previamente, se hayan formalizado los convenios o acuerdos procedentes. El régimen jurídico de los servicios mencionados será el previsto en los artículos 38, 45 y 46 de la LPC.

medios electrónicos, telemáticos e informáticos (48). El segundo apartado añadido contempla la posibilidad de prestar los diferentes servicios a que alude el artículo 81 por otros proveedores que no sean la FNMT o Correos en condiciones no discriminatorias (49).

La Ley de Acompañamiento mandaba dictar al Gobierno las disposiciones precisas para la regulación de la prestación de servicios técnicos de seguridad en las comunicaciones de la Administración General del Estado y sus organismos públicos a través de técnicas y medios electrónicos, informáticos y telemáticos. En cumplimiento de esta previsión se dictó el Real Decreto 1290/1999, de 23 de julio, por el que se desarrolla el artículo 81 de la Ley 66/1997 en materia de prestación de servicios de seguridad en las comunicaciones de las Administraciones Públicas a través de técnicas y medios electrónicos, informáticos y telemáticos, regulando el ejercicio de la facultad de prestación de estos servicios por la FNMT. Sin embargo, como el propio Real Decreto reconoce, no se lleva a cabo una regulación exhaustiva de los citados servicios de seguridad, en primer lugar por la existencia de una regulación general (compuesta por la LPC y el Real Decreto 263/1996, que ya vimos anteriormente), sino por estar pendiente de aprobación en ese momento lo que después fue la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica, que analizaremos más tarde, y en la cual se regulan los

(48) La disposición se condiciona a los procedimientos previstos en la Ley Orgánica del Poder Judicial 1/1985, y sus normas de desarrollo. Pero el precepto hay que conectarlo con la aprobación, finalmente, de la nueva Ley 1/2000 de Enjuiciamiento Civil, y las posibilidades que la misma abre en materia de notificaciones o, por ejemplo, de presentación de documentos como poderes y libros de los comerciantes, que originan un buen volumen de papel y fotocopias en los Juzgados.

(49) En el caso español, uno de estos proveedores están siendo en la actualidad las Cámaras de Comercio, que han creado un servicio de certificación digital denominado Camerfirma, dirigido principalmente a empresas y cuyo reconocimiento es internacional, al estar el proyecto Camerfirma coordinado por las Cámaras de Comercio europeas e impulsado a nivel estatal por las Cámaras de Comercio, Industria y Navegación que actúan como red de autoridades locales de registro, representadas por el Consejo Superior de Cámaras de España, quien actúa como Autoridad de Certificación y como interlocutor a nivel internacional. Las Cámaras de Comercio resultan idóneas para desempeñar esta función por varias razones: En primer lugar, porque tienen entre sus objetivos la representación y defensa del comercio, tanto nacional como internacional, incluso del comercio generado por medios telemáticos. En segundo lugar, las Cámaras han ejercido históricamente el papel de tercera parte de confianza, es decir, de certificadoras. Porque las Cámaras son entidades neutrales, sin intereses económicos directos en las transacciones que realizan. Finalmente la existencia de las Cámaras en todo el mundo hace que su conocimiento y reconocimiento sea internacional (página web de Camerfirma: www.camerfirma.com).

La otra autoridad de certificación reconocida es la Agencia de Certificación Electrónica, con capital mayoritario de Telefónica.

servicios de autenticación electrónica de datos que presta la FNMT. Por ello, la primera crítica que se le puede hacer a este Real Decreto es su adelantada publicación, en más de siete meses a la Directiva comunitaria, con el riesgo de desconexión y descoordinación que ello supone, adelanto que el legislador español vuelve a cometer con la promulgación, esta vez tan sólo tres meses antes de la llegada de la Directiva con el Real Decreto-ley 14/1999, desconectado a su vez del Real Decreto 1290/1999.

El Real Decreto 1290/1999, de 23 de julio, desarrolla el artículo 81 de la Ley de Acompañamiento 66/1997 en materia de prestación de servicios de seguridad en las comunicaciones de las Administraciones Públicas a través de técnicas y medios electrónicos, informáticos y telemáticos, regulando el ejercicio de la facultad de prestación por parte de la FNMT de los servicios de seguridad, técnicos y administrativos necesarios para garantizar la seguridad, la validez y la eficacia de las comunicaciones de la Administración General del Estado y sus organismos públicos (50). El ejercicio de la facultad atribuida a la FNMT, en colaboración con Correos, comprende el garantizar la validez y eficacia de los actos y documentos de los actos y documentos emitidos y recibidos por:

(50) En el Anexo del Real Decreto se establece el listado concreto de servicios, cuya implantación se prevé realizar en varias fases (aunque no se indica cuándo comienza cada una de ellas). Así, los servicios que la FNMT ofrecerá en una primera fase son:

— Generación de claves.
— Emisión de certificados de clave pública.
— Revocación de certificados de clave pública.
— Archivo de certificados de clave pública.
— Registro de eventos significativos.
— Registro de usuarios.
— Publicación de políticas y normas.
— Publicación de certificados de clave pública.
— Publicación de listas de revocación.
— Servicio de directorio.
— Servicios de recuperación de claves de soporte de confidencialidad.
— Expedición del título de usuario.
— Información administrativa de los servicios.

En una segunda fase de implantación, la FNMT podrá prestar también los siguientes servicios técnicos y administrativos:

— Constancia de fecha y hora (fechado digital) en transacciones electrónicas, informáticas y telemáticas, realizadas por la FNMT de forma automática y a petición de los participantes en la transacción.

— Verificación y reconocimiento de la autenticidad de los usuarios, realizada por la FNMT de forma automática y a petición de los destinatarios.

En una tercera fase más avanzada de la implantación, la FNMT podrá prestar servicios técnicos y administrativos que faciliten a los usuarios que lo requieran la implantación de servicios que incluyan las siguientes funciones de seguridad:

— Certificación de contenido de las transacciones EIT.

— Confirmación de envío, entrega y recepción de los mensajes intercambiados entre dos partes.

a) Los órganos de la Administración General del Estado en sus relaciones recíprocas o con los organismos públicos vinculados o dependientes de aquélla, así como las de estos organismos entre sí.

b) Las personas físicas y jurídicas, en sus relaciones con la Administración General del Estado y los organismos públicos vinculados o dependientes de la misma.

c) Las Comunidades Autónomas, entidades locales, las entidades de derecho público dependientes o vinculadas a las mismas, cuando se hubieran formalizado los correspondientes convenios o acuerdos con la FNMT (51). La suscripción de dicho convenio convierte a las Admiistraciones en «usuarios públicos» de los servicios de la FNMT (52).

d) Las entidades gestoras y servicios comunes de la Seguridad Social, así como aquellos organismos públicos que ejerzan potestades administrativas, de acuerdo con la LPC.

Los servicios técnicos y administrativos, a los que nos hemos referido en el apartado anterior, son aquellos que permiten las siguientes operaciones:

a) Acreditar la identidad del emisor y del receptor de la comunicación, así como la autenticidad de su voluntad.

b) Garantizar la integridad y conservación del contenido del documento en su emisión y recepción.

c) Acreditar la presentación o, en su caso, la recepción por el destinatario, de notificaciones, comunicaciones o documentación.

---

(51) La regulación de dichos convenios se desarrolla en el artículo 76 de este Real Decreto. Los convenios determinarán el régimen de realización de los servicios a través de medios electrónicos, informáticos o telemáticos. Para información general, el Ministerio de Administraciones Públicas mantendrá a disposición del público la relación de Administraciones a las que la FNMT preste estos servicios.

(52) Ello supone una diferencia, establecida en el artículo 9 de este Real Decreto, con los llamados «usuarios privados», que para adquirir esta condición necesitan realizar una solicitud en el Registro de usuarios creado al efecto en la FNMT y la aceptación de las condiciones de utilización de los sistemas electrónicos, informáticos y telemáticos. Cuando se cumplan estos requisitos, la FNMT expide en el plazo de un mes el correspondiente certificado electrónico (título de usuario). El plazo de un mes criticable por su amplitud, cuando lo que precisamente se trata con la aprobación de estos medios es facilitar las relaciones lo más rápidas e inmediatas posibles entre la Administración y los ciudadanos. Como corrobora el artículo 11, la FNMT dispone de un registro de usuarios en el que deberán inscribirse los usuarios privados para actuar como tales. Hasta que no se realice la inscripción, al usuario privado no se le entregará el soporte que le permita actuar como tal. Por el contrario, los usuarios públicos (las Administraciones) que hayan suscrito convenio serán inscritos de oficio.

La utilización de Correos permite que a través de sus oficinas los ciudadanos puedan presentar sus solicitudes de inscripción en el registro de usuarios, acreditar su identidad y recoger los correspondientes títulos de usuario. Correos también puede colaborar, como lo ha hecho desde siempre con la presentación de solicitudes y documentación por escrito, con la FNMT en la prestación del servicio de constatación de la fecha y hora de presentación de documentos, lo que supone que, incluso a nivel de relaciones informáticas con la Administración, el particular podrá seguir haciendo uso de las oficinas de Correos (53).

Todas las comunicaciones, notificaciones o documentos, así como sus copias, emitidos a través de estas técnicas, gozarán de la validez y eficacia prevista en el artículo 45 LPC y en los artículos 6 y 7 del Real Decreto 363/1996, de 16 de febrero. La FNMT proporciona a cada usuario un certificado electrónico (título de usuario), aunque con carácter previo comprueba la capacidad e identidad de la persona que lo solicita.

En las disposiciones adicionales del Real Decreto se establecen a título ejemplificativo algunos usos que pueden dar idea de la utilización que en la práctica cotidiana pueden tener los medios electrónicos, informáticos y telemáticos. Así, el caso de cumplimiento de obligaciones tributarias o el pago de cualquier otro derecho económico a favor de las Administraciones Públicas, tanto si el pago se efectúa directamente como a través de entidades de crédito.

Como siempre, es en el Anexo donde se contienen una serie de definiciones y requisitos del sistema; estos requisitos son triples, como a continuación veremos, técnicos, de seguridad y administrativos:

1. REQUISITOS TÉCNICOS

1.1. Generación y gestión de claves. La FNMT proporcionará a los usuarios: Dos claves complementarias de autenticidad, una pública y otra privada, que permitirán identificarse de manera fidedigna al usuario ante cualquier receptor de un mensaje.

---

(53) Recordemos que estos extremos están regulados a nivel reglamentario por el Decreto 1653/1964, de 14 de mayo, conforme a la redacción dada al mismo por la Orden de 14 de agosto de 1971 y el Decreto 2655/1985. Es en el artículo 205 donde se establece el régimen de admisión de instancias y escritos dirigidos a centros o dependencias administrativas. Algunas disposiciones de este Reglamento se han convertido en práctica administrativa habitual, e incluso han pasado a ser recogidas en la redacción de la LPC.

La confirmación de esta nueva función se encuentra hoy en el artículo 5 del Real Decreto 176/1998, de 16 de febrero, por el que se aprueba el Estatuto de la Entidad empresarial Correos y Telégrafos, el cual incluye, junto con las funciones tradicionales encomendadas a Correos, *«f) La realización de cuantas actividades y servicios relacionados con las telecomunicaciones le sean encomendados por la normativa vigente»*.

Dos claves complementarias de confidencialidad, una pública y otra privada, que servirán de soporte para prevenir la divulgación no autorizada del contenido de la transacción. Las claves, tanto de los usuarios como de la propia FNMT, serán generadas por esta última, utilizando mecanismos que garanticen su seguridad técnica y criptográfica (54). El período de vigencia de las claves de autenticidad propia de la FNMT no será superior a cinco años. Los cambios en las claves de la FNMT no implicarán modificaciones en las claves en vigor que estén utilizando los usuarios.

Las claves privadas de confidencialidad se archivarán cifradas y de forma segura. Por el contrario, las claves privadas de autenticidad no serán archivadas y por tanto no se conservarán en ningún tipo de soporte, salvo en la tarjeta u otro dispositivo externo que se entregue al usuario.

1.2. Emisión, revocación y archivo de certificados de clave pública: La FNMT podrá emitir los siguientes tipos de certificados: certificados de autenticidad y certificados de confidencialidad (55). Todos los certificados emitidos por la FNMT tendrán validez por un período no superior a tres años a partir de la fecha de emisión del certificado. Transcurrido el período establecido, el certificado caducará, pasando al archivo histórico de la entidad. En los certificados revocados constará, además del contenido propio del certificado activo, la fecha, hora y el motivo de su revocación (56).

1.3. Registro de eventos significativos: La FNMT mantendrá registro de cada actuación que realice de todos los eventos significativos relacionados con su propia actividad y la de los usuarios del sistema.

El registro de eventos no podrá ser modificado por medios no autorizados; tendrá un alto grado de disponibilidad y de fiabilidad, y guardará traza de los accesos realizados.

1.4. Servicios de Directorio. La FNMT publicará los certificados de clave pública en un directorio de acceso público, que deberá permanecer físicamente en el entorno seguro de la infraestructura técnica de la FNMT.

---

(54) La especificación técnica de este mecanismo escapa a la comprensión del jurista medio; en concreto se utilizan algoritmos de cifrado asimétrico tipo RSA, con una longitud mínima de clave de 1.024 bits.

(55) Las especificaciones técnicas respecto de los certificados escapan también a la comprensión del jurista. Así, los certificados cumplirán los requisitos definidos por la Unión Internacional de Telecomunicaciones, sector de normalización de las telecomunicaciones, en la Recomendación UIT-T X.509, versión 3, de fecha junio de 1997 o posterior.

(56) Los certificados revocados se publicarán en listas de revocación, cuyos requisitos técnicos serán los definidos por la Unión Internacional de Telecomunicaciones para formatos de listas de revocación, sector de normalización de las telecomunicaciones, en la Recomendación UIT-T X.509, versión 2, de fecha junio de 1997, o posterior.

1.5. Expedición de título de usuario: Consiste en una tarjeta inteligente o en otro soporte de seguridad equivalente (57). Dispondrá de las medidas de seguridad físicas necesarias de forma que no pueda ser manipulado externamente o alterar su comportamiento.

Dispondrá de las medidas de seguridad lógicas para que este dispositivo no pueda ser leído por medios externos, de forma no autorizada. En el caso de que el volumen de actividad lo justifique se podrá instalar una configuración informática, que contará con un entorno criptográfico y un control de acceso seguros.

2. REQUISITOS DE SEGURIDAD

2.1. Plan integral de seguridad: La FNMT dispondrá de un Plan integral de seguridad permanentemente actualizado, basado en la metodología *magerit* de análisis y gestión de riesgos de sistemas de información de las Administraciones públicas.

2.2. Productos y sistemas de las tecnologías de la información: Los niveles de seguridad de los productos y sistemas se establecerán siguiendo «Criterios de evaluación de la seguridad de los productos y sistemas de las tecnologías de la información» (ITSEC/ITSEM) o posterior. Los niveles de seguridad serán según la norma citada.

3. REQUISITOS ADMINISTRATIVOS

3.1. Publicación de políticas y normas: La FNMT publicará los procedimientos que regirán en relación con los usuarios y la utilización de sus servicios. Las políticas y normas estarán a la libre disposición en el servidor «web» de la FNMT.

3.2. Requisitos del Registro de Usuarios: Los interesados presentarán la correspondiente solicitud, según los modelos que se establezcan al efecto. La solicitud debe completarse con la comparecencia de los interesados ante los órganos y organismos de la forma que reglamentariamente se establezca. El usuario presentará la documentación que acredite su identidad, así como su capacidad legal en el caso de actuación en nombre de terceras personas físicas o jurídicas, y cualquier otra documentación que se requiera al efecto.

(57) En caso de que al particular se le entregue una tarjeta, el dispositivo físico externo en el que se encuentran las claves privadas deberá ser accesible, vía estándares de mercado tipo PC/SC, y ofrecer un interfaz normalizado de acceso a las funciones criptográficas.

6. ALGUNAS MENCIONES JURISPRUDENCIALES EN MATERIA DE FIRMA ELECTRONICA

Son todavía muy pocas las ocasiones en que la jurisprudencia ha hablado de firma electrónica, y en todas ellas el problema ha aparecido de manera incidental; no existe por el momento jurisprudencia sobre la aplicación del Decreto-ley 14/1999.

La primera sentencia con que contamos es la sentencia de la Sala de lo Contencioso del TS, Sección 2.ª, de 3 de noviembre de 1997. Se trata de una sentencia muy completa y gráfica en la materia. El supuesto de hecho fue la impugnación por parte de la Asociación Española de Banca Privada de determinados artículos del Reglamento General del Impuesto sobre Transmisiones Patrimoniales y Actos Jurídicos Documentados (Real Decreto 828/1995, de 29 de mayo). En concreto, el artículo *76.3.c).2* del Reglamento estableció un concepto amplio de documento, que incluía los documentos informáticos: *«a efectos de lo dispuesto anteriormente, se entenderá por documento cualquier soporte escrito, incluidos los informáticos, por los que se pruebe, acredite o haga constar alguna cosa»*. El recurrente pretendía eliminar, mediante la presente impugnación, la frase *«incluidos los informáticos»*. Sin embargo, el Tribunal se opone a esta interpretación literal de documento. Si bien es cierto que casi toda la jurisprudencia que, con base en los artículos 578 de la Ley de Enjuiciamiento Civil y 1.215 del Código Civil, aboga por la virtualidad jurídica del documento en soporte electrónico, principalmente, sobre la problemática de su admisión —siempre que se den todas las cautelas necesarias para cerciorarse de su autenticidad— como prueba procesal. Y se plantea la duda de si los principios que rodean el gravamen fiscal de los documentos mercantiles son asimilables a los que se dan en el proceso judicial y de si el impuesto documental que se analiza es compatible con el soporte informático.

Según la recurrente, no existe en nuestro ordenamiento jurídico precepto alguno que otorgue al tenedor de un soporte informático esa legitimación a que se ha hecho referencia, pues, en su opinión, no puede emitirse un título valor o documento mercantil sino con la firma de su emisor y tal firma y/o su constancia por escrito no puede suplirse —termina diciendo— por ningún soporte informático. Pero, como señala el Tribunal, tal punto de vista ha quedado ya obsoleto. *«Estamos asistiendo* —dice el Supremo— *en cierto modo, en algunas facetas de la vida, incluso jurídica, al ocaso de la civilización del papel, de la firma manuscrita y del monopolio de la escritura sobre la realidad documental. El documento, como objeto corporal que refleja una realidad fáctica con trascendencia jurídica, no puede identificarse, ya, en exclusiva, con el papel, como soporte, ni con la escritura, como unidad de significación. El ordenador y los ficheros que en él se almacenan consti-*

tuyen, hoy día, una nueva forma de entender la materialidad de los títulos valores y, en especial, de los documentos mercantiles.

Cierto que, en el Texto Refundido del ITPyAJD de 1993 e, incluso, en la Ley General Tributaria, no se hace referencia directa a este nuevo sistema documental. Pero ello no implica, de entrada, que la ampliación conceptual que, al respecto, se contiene en el precepto reglamentario que estamos examinando implique, sin más, una desvirtuación del principio de legalidad, ante una aparente falta de habilitación legal específica, pues no debe olvidarse que, dentro del alcance de la llamada reserva legal relativa, el Tribunal Constitucional ha declarado que aquellos elementos de las relaciones tributarias que no sean esenciales pueden quedar en manos, a efectos de su matización y complementariedad aclaratoria, de los órganos titulares de la potestad reglamentaria y de las disposiciones generales que, en consecuencia, promulguen. Al fin y al cabo, no debe olvidarse que el ordenamiento jurídico, como sistema unitario y general, y no anclado en el puro positivismo legalista, goza de la fuerza normativa —expansiva— necesaria y suficiente como para justificar el ejercicio de la potestad reglamentaria de la Administración en la materia que examinamos».

El Tribunal hace además una recopilación de toda la normativa aprobada hasta entonces en materia de documentos digitales: *«debe tenerse consecuentemente en cuenta la proliferación de normas legales (y reglamentarias) que han venido patrocinando y recogiendo el uso, con los efectos jurídicos pertinentes, del documento en soporte electrónico».* Así:

— La Ley del Patrimonio Histórico de 1985 recoge, en su artículo 49, una definición amplia y completa del documento *«toda expresión en lenguaje natural o convencional, y cualquiera otra expresión gráfica, sonora o de imagen, recogida en cualquier tipo de soporte material, incluido el informático».*
— La Ley del Mercado de Valores de 1988 regula las operaciones de Bolsa que se llevan a cabo mediante el Sistema de Interconexión Bursátil, integrado, como señala la propia Exposición de Motivos de la Ley, mediante una red informática.
— La Ley 37/1992, de 28 de diciembre, sobre el IVA, permite, en su artículo 88.2, que las facturas puedan emitirse por vía telemática; posibilidad que ha sido más detallada en la Orden Ministerial de 22 de marzo de 1996. Y el Reglamento del IVA, aprobado por el Real Decreto 1624/1992, de 19 de diciembre, recoge, en su artículo 62.3, la posibilidad de llevar libros o registros de carácter informático, siempre que se ajusten a los requisitos señalados en el citado Reglamento.
— La Orden Ministerial de 24 de julio de 1996, que desarrolla el Real Decreto de 22 de diciembre de 1995 relativo, en el ámbito fiscal, a la

declaración anual de operaciones con terceros, establece, en el apartado 2 del punto segundo, que *«será obligatoria la presentación en soporte directamente legible por ordenador de aquellas declaraciones anuales de operaciones con terceros que contengan más de cien personas o entidades relacionadas con la declaración»*.

— La Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común señala que los documentos emitidos por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas gozan de la validez y eficacia del documento original, siempre que quede garantizada su autenticidad, integridad y conservación (asimilándose, en cuanto a su validez y eficacia, las copias de originales almacenadas por los citados medios).

— La Ley Orgánica del Poder Judicial de 1985 permite, a tenor de su artículo 230, la utilización por los Juzgados y Tribunales de cualesquiera medios técnicos, electrónicos, informáticos y telemáticos para el desarrollo de su actividad y ejercicio de sus funciones, siempre que ofrezcan las adecuadas garantías de autenticidad e integridad.

— La propia Comunidad Europea ha potenciado el desarrollo de la transmisión electrónica de datos (programas *Electronic Data Interchange),* facilitando la celebración de contratos tipo entre pequeñas y medianas empresas, dándose al mensaje electrónico normalizado el mismo valor que al documento escrito y firmado.

De todo ello se desprende que la admisión del documento electrónico es una realidad en nuestro ordenamiento, *sub conditione,* sin embargo, de acreditar su autenticidad. Y es aquí donde el TS se refiere a la firma electrónica por contraposición a la manuscrita.

En el caso analizado por el Tribunal, el documento, que ha de cumplir una función de giro, debe reunir, para gozar de predicamento jurídico, los elementos determinantes de su autenticidad y de su autoría, y, en especial, la firma de quien asume su contenido y la efectividad de su clausulado. La firma es el trazado gráfico, que contiene habitualmente el nombre, los apellidos y la rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y virtualidad y obligarse con lo que en ellos se dice. Aunque la firma puede quedar reducida sólo a la rúbrica o consistir, exclusivamente, incluso, en otro trazado gráfico, o en iniciales, o en grafismos ilegibles, lo que la distingue es su habitualidad, como elemento vinculante de esa grafía o signo de su autor. Y, en general, su autografía u ologrаfia, como vehículo que une a la persona firmante con lo consignado en el documento, debe ser manuscrita o de puño y letra del suscribiente como muestra de la inmediatez y de la voluntariedad de la acción y del otorgamiento.

Pero la firma autógrafa no es la única manera de signar, pues hay otros mecanismos que, sin ser firma autógrafa, constituyen trazados gráficos, que asimismo conceden autoría y obligan. Así, las claves, los códigos, los signos y, en casos, los sellos con firmas en el sentido indicado. Y, por otra parte, la firma es un elemento muy importante del documento, pero, a veces, no esencial, en cuanto existen documentos sin firma que tienen valor probatorio (como son los asientos, registros, papeles domésticos y libros de los comerciantes). En consecuencia, aunque puede haber documentos electrónicos sin firma, el documento electrónico (y, en especial, el documento electrónico con función de giro mercantil) es firmable, en el sentido de que el requisito de la firma autógrafa o equivalente puede ser sustituido por el lado de la criptografía, por medio de cifras, signos, códigos, barras, claves u otros atributos alfanuméricos que permitan asegurar la procedencia y veracidad de su autoría y la autenticidad de su contenido.

Por lo tanto, si se dan todas las circunstancias necesarias para acreditar la autenticidad de los ficheros electrónicos o del contenido de los discos de 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 en soporte informático, con función de giro, debe gozar, como establece el artículo 76.3.*c)* del Reglamento de 1995, de plena virtualidad jurídica operativa.

De la misma fecha y sección es la sentencia del Tribunal Supremo (Sala de lo Contencioso) (Recurso 544/1995). El supuesto de hecho es el recurso contra el mismo reglamento del Impuesto de Transmisiones Patrimoniales, esta vez por parte de la CEOE. El Tribunal llega a la misma conclusión respecto de la admisión del documento electrónico y la autenticidad que proporciona la firma electrónica: *«se desprende la realidad de admisión del documento electrónico, bajo condición de que quede garantizada su autenticidad, y que esto es factible, inclusive mediante lo que podría calificarse hoy de firma electrónica —cifras, códigos, claves y similares procedimientos—, es algo universalmente admitido».*

Por último, encontramos dos sentencias, de igual fecha, 19 de octubre de 1998, de la Audiencia Provincial de Las Palmas (Sección 2.ª), dictadas en sendos sumarios sobre utilización fraudulenta de tarjetas de crédito tras un delito de robo. Se alude a la firma electrónica, pero a un concepto muy elemental de la misma (el equivalente a interpretar los datos de una banda magnética). El tribunal interpreta como una modalidad de estafa la *«manipulación informática o artificio semejante»*, porque en esta clase de estafas es en las que se asegura la operación mediante una «firma electrónica» coincidente con la clave identificativa que figura en la banda magnética de las tarjetas. Se aparta de la clase tradicional de estafas, ya que el engaño se sofistica, haciéndose de este modo con un activo patrimonial a través de una transferencia no consentida.

BIBLIOGRAFIA EN MATERIA DE FIRMA ELECTRONICA

AGUADO MUÑOZ, RICARDO y otros: *Basic Básico. Curso de programación.* Ed. Computer School, Madrid, 1989, 254 págs.

— *Derecho sobre Internet* (libro electrónico disponible en la red, en la página web del BSCH: www.derechosobreinternet.com).

DEVOTO, MAURICIO y LYNCH, HORACIO M.: *Banca, comercio, moneda electrónica y firma digital,* pág. 4. Artículo electrónico en la Red (www.it-cenit.org.ar/Publicac/BancaMD/Bancoml), aunque originalmente publicado en la Revista Jurídica *La Ley,* de Buenos Aires.

DÍAZ FRAILE, JUAN MARÍA: «Comentarios a la Directiva y al Proyecto de Ley español de comercio electrónico de 2000», en *Revista Crítica de Derecho Inmobiliario,* núm. 663, enero-febrero de 2001, págs. 81 a 122.

DOMÍNGUEZ LUELMO, ANDRÉS: «Contratación electrónica y protección de los consumidores: Régimen jurídico», en *Revista Crítica de Derecho Inmobiliario,* núm. 660, julio-agosto de 2000, págs. 2327 a 2389.

GARCÍA MÁS, FRANCISCO JAVIER: «La contratación electrónica: la firma y el documento electrónico», en *Revista Crítica de Derecho Inmobiliario,* núm. 652, mayo-junio de 1999, págs. 765 a 796.

GRIERA FISA, MERCÉ y otros: *Conecta el micro,* núm. 1: Fem informática, Ed. Fundació Caixa de Pensions, 1.ª edición, 1985, 93 págs.

MARTÍNEZ NADAL, APOL.LÓNIA: «Comentarios de urgencia al urgentemente aprobado Real Decreto-ley 14/1999, de 17 de septiembre», en Revista *La Ley,* núm. 4.939 y 4.949, 1 y 2 de diciembre de 1999, págs. 1 a 5 en ambos números.

— *Comercio Electrónico, firma digital y autoridades de certificación,* Ed. Civitas-UIB-Govern Balear, 2.ª edición, 2000, 305 págs.

— *La Ley de Firma Electrónica,* Ed. Civitas, 1.ª edición, 2000, 311 págs.

MATEO DE ROS, RAFAEL, y CENDOYA MÉNDEZ DE VIGO, JUAN MANUEL (coordinadores): *Derecho de Internet: contratación electrónica y firma digital,* Ed. Aranzadi, año 2000, 1094 págs. y un CD-ROM.

ORTEGA ALVAREZ, LUIS IGNACIO: «Nuevas Tecnologías y Procedimiento Administrativo», en *Revista Jurídica de Castilla-La Mancha,* núm. 18: Comentarios a la ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, agosto de 1993, págs. 211 a 217.

JOSÉ MARÍA ARISTÓTELES MAGÁN PERALES
Profesor Ayudante-Doctor de Derecho Administrativo
Facultad de Derecho de Albacete
Universidad de Castilla-La Mancha