

# **DOCUMENTOS Y FIRMA ELECTRÓNICOS.**

Francisco Hernández Guerrero  
Fiscal

WWW.FISCALIA.ORG

1.1.a) La recepción normativa del documento electrónico como objeto del tráfico jurídico.....	3
1.1.b) El documento electrónico como objeto de protección penal	9
1.1.b.1) Introducción: los documentos de la Era Digital.....	9
1.1.b.2) La protección penal del documento electrónico.....	11
El artículo 26 del Código Penal.....	11
La protección del documento electrónico en la Parte Especial del CP.....	18
1.1.c.) El documento electrónico como medio probatorio.....	22
1.1.c.1) La distinción entre fuentes y medios de prueba.....	23
1.1.c.2) El concepto de documento .....	25
Concepto doctrinal de documento .....	25
Concepto jurisprudencial de documento .....	26
Concepto legal de documento. Hacia el concepto propio de documento electrónico.....	28
1.1.c.3) Caracteres del documento como medio probatorio ....	34
1.1.d) Los documentos electrónicos en la LEC 2000 .....	42
1.1.d.1) El iter legislativo del artículo .....	43
1.1.d.2) Los medios e instrumentos del art. 299.2 LEC.....	45
1.1.d.3) La recepción y equiparación de los documentos electrónicos <i>strictu sensu</i> o cualificados, con los documentos tradicionales.....	49
1.1.e) Los documentos electrónicos en el proceso penal .....	52
1.1.e.1) Su consideración como objeto del delito y como medios probatorios. ....	52
1.1.e.2) Pruebas documentales y pruebas documentadas.....	54
1.1.e.3) La reproducción de diligencias sumariales por aplicación del art. 730 LECr.....	57
1.1.e.4) La apreciación de oficio de los libros, documentos, papeles y demás piezas de convicción.....	60

1.1.e.5) Valoración de los documentos electrónicos en el proceso penal .....	62
<b>1.2.) La firma electrónica .....</b>	<b>65</b>
1.2.a) Introducción .....	65
1.2.b) Concepto y características.....	67
1.2.c) Regulación .....	71
1.2.c.1) En Derecho Comparado .....	71
USA.....	71
Italia .....	72
Alemania .....	74
Otras experiencias .....	75
1.2.c.2) En Derecho comunitario .....	75
Fines y principios de la Directiva 1999/93/CE, de 13 de diciembre .....	76
Régimen legal de la firma electrónica.....	79
Los proveedores de servicios de certificación.....	83
Los productos de firma electrónica .....	86
1.2.c.3) En el Derecho interno .....	88
Disposiciones sectoriales.....	89
La regulación de la firma electrónica en el RD Ley 14/1999, de 17 de septiembre .....	95
1.2.d) Conclusión .....	115

*1.1.a) La recepción normativa del documento electrónico como objeto del tráfico jurídico*

Siempre se ha atribuido al Derecho, como defecto, un habitual desfase con relación a la realidad social que ha de regular. A pesar de los instrumentos legales previstos

para afrontar tal hecho<sup>1</sup>, por otra parte consustancial al procedimiento legislativo de las sociedades democráticas, lo cierto es que es más que probable que cualquier disposición normativa llegue siempre tarde a la realidad.

El Derecho Procesal Español ha vivido esta situación hasta la aprobación de la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil, en la que ha quedado reflejada, a través de una serie de preceptos a los que haremos alusión a lo largo de este capítulo, al documento electrónico, aun con ciertas reticencias y sin que quede absolutamente claro el cauce de su admisibilidad.

A nivel de tráfico jurídico y de la actuación de las Administraciones Públicas el documento en su nuevo formato digital había sido objeto de reconocimiento legal en disposiciones de naturaleza administrativa y mercantil. Es tradicional la cita del art. 49.1 de la Ley 16/1995, del Patrimonio Histórico Español, que define al documento como «toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos».

En el ámbito mercantil cabe citar la Ley 24/1988, de 28 de julio, del Mercado de Valores, que permitió -en su art. 5- la sustitución de los títulos valores representados en papel por anotaciones o registros electrónicos en cuenta, negociables mediante el Sistema de Interconexión Bursátil previsto en el art. 49<sup>2</sup>.

La más cercana Ley 7/1988, de 13 de abril, de Condiciones Generales de Contratación, alude a la contratación electrónica y al modo de acreditarse el

---

<sup>1</sup> Nos referimos a la obligación establecida en el art. 3.1. C.C. de interpretar las normas según «la realidad social del tiempo en que han de ser aplicadas»

<sup>2</sup> Esta regulación fue objeto de complementación mediante el Acuerdo de la Comisión Nacional del Mercado de Valores de 11 de marzo de 1998, que estableció la implantación del sistema de cifrado CIFRADO/CNMV, asentado en los mismos principios que el art. 45.5 LRJPAC y el RTEIT.

conocimiento de las condiciones generales de contratación que afectan a la operación concreta.

A nivel administrativo el reconocimiento del documento electrónico fue realizado a través de la Ley 30/1992, de 26 de Noviembre, de Régimen Jurídico de la Administración del Estado y del Procedimiento Administrativo Común. Su art. 45.1 apuesta por la implantación de medios electrónicos, informáticos y telemáticos en su seno para el desarrollo de su actividad, en tanto que el reconocimiento de la validez y eficacia de los documentos emitidos por dichos medios es realizado por el apartado 5º, condicionándolo a la garantía de su autenticidad, integridad, conservación, recepción en su caso por el interesado y el cumplimiento de los demás requisitos impuestos por la legislación vigente. Este precepto fue objeto de desarrollo por el Real Decreto 263/1996, de 16 de febrero, de regulación del empleo de técnicas electrónicas, informáticas y telemáticas por la Administración del Estado (RTEIT), que añadió nuevos requisitos a los documentos electrónicos administrativos<sup>3</sup>.

El RTEIT tiene un claro precedente en la legislación de la Seguridad Social. Más cercana a la realidad del empresariado, la Seguridad Social hubo de regular, sobre la cobertura normativa proporcionada por el art. 45 LRJPAC, el empleo de los medios informáticos en sus relaciones con los empresarios que debían remitirle mensualmente ingentes formularios para comprobación y pago de las obligaciones sociales a su cargo. Así, la Orden de 8 de abril de 1992, en su art. 73 –que desarrollaba el RD 1517/1991, de 11 de octubre, Reglamento General de Recaudación de los Recursos del Sistema de la Seguridad Social- permitía ya la posibilidad de remisión de datos de la relación nominal de trabajadores en soporte magnético. Los datos de afiliación, altas y bajas, así como cotizaciones podían ser remitidos mediante estas técnicas en virtud de RD 2317/1993, de 29 de diciembre, la

---

<sup>3</sup> Como pone de relieve Díaz Fraile, los de aprobación y difusión pública de las aplicaciones y programas informáticos (art. 5), garantías sobre la identidad y el ejercicio de la competencia por el órgano correspondiente (art. 2.2), o el empleo de códigos y sistemas de producción de documentos garantizados contra su uso por personas no autorizadas (art. 6.1). DIAZ FRAILE, Juan María, *Estudio de la regulación de la firma electrónica en la Directiva Europea de 13 de mayo de 1998*, Diario La Ley nº 4677-4678, 23-24 noviembre 1998.

Orden de 18 de enero de 1993 y la de 17 de enero de 1994. Ante la falta de una regulación general del empleo de estos medios por la Administración de la Seguridad Social se dictó la Orden del Ministerio de Trabajo y Seguridad Social de 3 de abril de 1995, que reguló el uso de los medios electrónicos, informáticos y telemáticos en relación con la inscripción de empresas, a filiación, altas y bajas de trabajadores, cotización y recaudación<sup>4</sup>. Su art.2.2 declara que «Los actos administrativos realizados por la Tesorería General de la Seguridad Social que se deriven de la citada transmisión de datos, tendrán plena validez y eficacia, generando los derechos y obligaciones establecidos por la normativa en vigor en relación con dichos actos», en línea con lo establecido en el rt. 45.5 LRJPAC.

La aplicación de los medios electrónicos, informáticos y telemáticos al quehacer diario de la Administración Pública exige, como se acaba de ver, el cumplimiento de los requisitos expresados en el art. 45.5 LRJPAC más los establecidos en el RTEIT y en la legislación administrativa. Garantizar la autenticidad, integridad, confidencialidad, disponibilidad y constatación de los requisitos procedimentales (tales como la identificación del órgano actuante y del ejercicio de su competencia, fecha del acto, identificación del remitente y destinatario del acto notificado y otros) sólo es posible mediante la utilización de las técnicas criptográficas que sirven de base a las firmas electrónicas avanzadas. Sin perjuicio de lo que expondremos más adelante sobre este aspecto concreto de los documentos electrónicos, diremos ahora que en el plano normativo se han adoptado las medidas funcionales precisas para hacer posible el empleo de la firma electrónica avanzada en el ámbito administrativo.

El empleo de esta firma exige la intervención de una autoridad o entidad de certificación, que expide certificados digitales que se asocian al documento electrónico y a la firma anexa al mismo, acreditando la identidad del firmante y otras condiciones de uso de la firma <sup>5</sup>. Estas funciones han sido asumidas por el

---

<sup>4</sup> Esta Orden fue posteriormente complementada por la Resolución de la Dirección General de la Tesorería de la Seguridad Social de 23 de abril de 1995, a su vez complementada por la Resolución de 17 de enero de 1996.

<sup>5</sup> El Real Decreto-Ley 14/1999, de 17 de septiembre, de firma electrónica, define el certificado en su art.

organismo autónomo Fábrica Nacional de Moneda y Timbre – Real Casa de la Moneda <sup>6</sup>, en virtud del art. 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social (más conocida como Ley de Acompañamiento de los Presupuestos Generales del Estado) <sup>7</sup>. De este modo, sólo el documento administrativo basado en una firma electrónica avanzada podrá ser considerado como documento electrónico administrativo .

---

2.i «la certificación electrónica que vincula unos datos de verificación de firma electrónica a un signatario y confirma su identidad.». En su apartado siguiente consigna la definición del certificado reconocido: «Es el certificado que contiene la información descrita en el art. 8 y es expedido por un prestador de servicios de certificación que cumple los requisitos enumerados en el art. 12.»

Por su parte, el art. 8 citado determina el siguiente contenido para el certificado reconocido:

1. Los certificados reconocidos, definidos en el art. 2.j) de este Real Decreto-ley, tendrán el siguiente contenido:

- 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, indicando su nombre o razón social, su domicilio, su dirección de correo electrónico, su número de identificación fiscal y, en su caso, sus datos de identificación registral.
- 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. Se podrá consignar en el certificado cualquier otra circunstancia personal del titular, en caso de que sea significativa en función del fin propio del certificado y siempre que aquél dé su consentimiento.
- 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 electrónica que correspondan a los datos de creación de firma electrónica 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.»

<sup>6</sup> El organismo FNMT ha sido regulado por el RD 1114/1999, de 25 de junio, que aprueba su Estatuto y la denominación de Real Casa de la Moneda. La función de entidad certificadora de las Administraciones Públicas se halla recogida en su art. 2.1g).

Los ficheros de datos empleados para el ejercicio de las funciones encomendadas fueron publicados, de acuerdo con lo exigido por el art. 20 LOPDP, en el BOE en virtud de Orden del Ministerio de Economía y Hacienda de 26 de julio de 1999.

<sup>7</sup> Dicho precepto fue desarrollado por el RD 1290/1999, de 23 de julio, en el que se establecen las condiciones técnicas y administrativas de uso de los medios electrónicos, informáticos y telemáticos en las relaciones entre y con instituciones integradas o dependientes de las Administraciones Públicas de cualquier índole, como se desprende de su art. 2.3: « Lo dispuesto en los apartados anteriores se entenderá, asimismo, sin perjuicio del empleo y aplicación de las técnicas y medios EIT que pudieran establecerse por las diferentes Administraciones públicas y los organismos públicos, y entidades vinculadas o dependientes de ellas, con independencia de que el servicio de certificación lo prestaran estos últimos o las entidades públicas o privadas que designen»

En el ámbito fiscal, como ponen de manifiesto Maronda y Tena <sup>8</sup>, la Ley General Tributaria 230/1963 de 28 de diciembre –modificada por Ley 5/1995– hace referencia a los instrumentos informáticos como soporte de las operaciones mercantiles, al considerar los programas, archivos y soportes magnéticos de los empresarios como objeto de la actuación de los inspectores (art. 142) <sup>9</sup>.

El documento electrónico, en forma de factura electrónica, surgió a la vida legal tributaria en la Ley 37/1992 de 28 de diciembre, del Impuesto del Valor Añadido, en cuyo art. 88 se aludía a la emisión de factura o documento análogo mediante vía telemática <sup>10</sup>. También se refirió a este tipo de soportes el Real Decreto 828/1995, de 29 de mayo, sobre el Impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados, que recogía –como hecho imponible– el libramiento de documentos de giro «en cualquier soporte escrito, incluidos los informáticos, por los que se pruebe acredite o haga constar alguna cosa».

En el ámbito procesal encontramos una alusión a los medios informáticos en el art. 90 de la Ley de Procedimiento Laboral. Quizá por la necesidad del ámbito laboral de hallarse más en contacto con la realidad a la que sirve como vía de solución de conflictos, el legislador admitió como medios probatorios los medios mecánicos de reproducción de la palabra, de la imagen y del sonido, salvo que se hubieran obtenido, directa o indirectamente, mediante procedimientos que supongan violación de derechos fundamentales

Correlativamente a las reformas mercantiles antes aludida en materia de títulos valores, la Ley 10/1992, de 30 de abril, de Medidas Urgentes de Reforma Procesal, introdujo un nuevo art. 1429.7 en la Ley de Enjuiciamiento Civil (LEC), en orden a

---

<sup>8</sup> MARONDA FRUTOS, Juan Luis y TENA FRANCO, M<sup>a</sup> Isabel, «La Informática jurídica y el Derecho informático», en *Revista General del Derecho*, Marzo 1997, pág. 1746

<sup>9</sup> En consonancia con la posibilidad de que los libros de comerciantes y empresarios puedan ser llevados mediante medios informáticos, tal y como autorizaba el art. 27.3 del CCom.

<sup>10</sup> Las condiciones de uso e dichas facturas están reguladas en la Orden del Ministerio de Economía y Hacienda de 22 de marzo de 1996.



permitir el ejercicio de la acción ejecutiva sobre la base de los certificados expedidos por las entidades encargadas de los valores representados mediante anotaciones en cuenta. La referencia a certificados de los valores representados suponía el reconocimiento implícito del carácter original del soporte informático, como pone de relieve Sanchís Crespo <sup>11</sup>

En 1994, en virtud de reforma operada en la LOPJ por la L.O. 16/1994, de 8 de noviembre, se reprodujo en términos miméticos el contenido del art. 45 LRJPAC, dando cobertura legal en todo el ámbito procesal <sup>12</sup> al documento judicial electrónico.

Por último, cabe citar la modificación operada en el art. 81 de la Ley 66/1997, de 30 de diciembre –que atribuía a la FNMT las funciones de entidad certificadora para la Administración Pública- por el art. 51 de la Ley 50/1999, de 30 de diciembre, de acompañamiento de los Presupuestos Generales del Estado para 2000, por virtud del cual se autoriza al organismo autónomo citado a la realización de servicios de certificación en el ámbito de la Administración de Justicia, sin perjuicio de la posibilidad de que sean prestados por otros organismos públicos o privados. De esta manera, y al igual que sucediera en el ámbito administrativo, puede hablarse de la disponibilidad de las medidas técnicas y organizativas precisas para el empleo de las técnicas de firma digital en el ámbito judicial.

### *1.1.b) El documento electrónico como objeto de protección penal*

#### 1.1.b.1) Introducción: los documentos de la Era Digital

Todos los días escuchamos y leemos noticias referentes a la Sociedad de la Información y a la Economía Electrónica (E-Commerce, como es conocida en denominación anglosajona). La conversión anunciada en 1995 por Negroponete del

---

<sup>11</sup> SANCHÍS CRESPO, Carolina, La prueba mediante soportes informáticos, Valencia, 1999, pág. 79

<sup>12</sup> Ha de recordarse que el art. 230, uno de los objetos de la reforma, se halla incardinado en el Título III dedicado a las «Actuaciones Judiciales», con clara vocación de aplicación a todo tipo de procesos.

átomo en byte <sup>13</sup>, metáfora mediante la que se aludía a la transformación de los bienes materiales –átomos- como objeto de las transacciones entre personas, por mera información manejada por los ordenadores –bytes, o unidad mínima de almacenamiento informático- , está haciendo de la informática y de las redes de ordenadores el mundo en el que se desenvuelve –o al menos se prevé que se desenvolverá- la mayor parte del tráfico económico y jurídico.

Cada vez se habla con mayor insistencia de la Economía digital, del comercio electrónico, de las necesidades de regular el emergente iceberg de la economía basada en los nuevos servicios de la información <sup>14</sup>. La conversión de la economía tradicional en economía digital verá aparecer el fenómeno de la delincuencia económica por medios informáticos. Estafas, abuso de firma digital mediante manipulación del contenido de los certificados adjuntos a éstas –o directamente el apoderamiento de las claves de firma digital- la sustracción de información con valor comercial existente en ordenadores <sup>15</sup>, serán algunos de los delitos que pronto veremos juzgar en nuestros Tribunales penales.

El Derecho Penal requiere de la existencia de soportes para que la información sea protegida, si bien es flexible a la hora de interpretar dicho concepto. Tanto como objeto del delito como prueba del mismo es preciso detenerse en el concepto de documento, el régimen jurídico de los documentos electrónicos y la incidencia de la firma digital en su generación.

---

<sup>13</sup> NEGROPONTE, Nicholas, El Mundo Digital, Madrid, 1995

<sup>14</sup> Recientemente ha sido aprobada por la Comunidad Europea la Directiva 2000/31/CE, de Comercio Electrónico, de 8 de junio, con la finalidad de crear el marco legislativo necesario para la armonización de las legislaciones nacionales, lo que hará posible la aplicación del principio comunitario de libre circulación de mercancías entre los países de la Comunidad. La Directiva, no obstante, deja claro que no pretende la armonización de la legislación penal relacionada con el Comercio Electrónico (Considerando 8<sup>a</sup>), si bien muestra una preocupación especial por la protección de los datos personales y de la confidencialidad de las comunicaciones electrónicas, temiendo el fenómeno de la criminalización del nuevo medio emergente, considerando suficiente para su protección lo establecido en las Directivas 95/46/CE de 24 de octubre y 97/66/CE , de 15 de diciembre, relativas a la protección de los datos de carácter personal y a la protección de la intimidad en materia de telecomunicaciones, respectivamente. A tal fin el Considerando 15<sup>a</sup> declara que «[...]los Estados miembros deben prohibir cualquier forma de interceptar o vigilar esas comunicaciones por parte de cualquier persona que no sea su remitente o su destinatario salvo que esté legalmente autorizada»

<sup>15</sup> Ha sido noticia últimamente el acceso a los códigos fuente de los programas comercializados por la empresa Microsoft, mediante accesos indebidos a sus ordenadores centrales. Dada la extensión del uso de los programas de esta empresa, puede observarse la magnitud del hecho cometido. EL País Digital, 28 octubre 2000.

### 1.1.b.2) La protección penal del documento electrónico

#### El artículo 26 del Código Penal

Qué duda cabe que, con este extenso bagaje normativo, los documentos electrónicos han de ser objetos merecedores de protección penal, y que por dicha razón pueden verse sometidos a un proceso penal. El vigente Código Penal alude a los documentos electrónicos en diversas ocasiones, corroborando de este modo el aserto realizado, sin perjuicio de la posibilidad de aplicación de figuras tradicionales a los nuevos documentos.

El pórtico de protección del documento electrónico tiene su sede penal en el art. 26, dentro de las Disposiciones Generales. Dicha ubicación sistemática ha merecido el aplauso de la doctrina <sup>16</sup>, dado que permite su aplicación a figuras tradicionales delictivas en las que el documento electrónico no es objeto de referencia directa, como es el caso de los delitos de falsedades regulados en el Título XVIII del Libro II. El art.26 define al documento, a efectos penales, como «todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica». La novedad del precepto reside en su recogida legal, pues el concepto era asumido como tal por la jurisprudencia de forma pacífica <sup>17</sup>

En interpretación jurisprudencial del concepto contenido en el precepto que estudiamos es conveniente la cita literal de la STS (2ª) 1254/1998, de 22 de octubre (ponente Moner Muñoz), donde se ponen de relieve los requisitos exigidos por el Derecho Penal para la protección del documento:

---

<sup>16</sup> Por todos, SANCHÍS CRESPO, *op.cit.* pág. 82.

<sup>17</sup> Sanchís cita, como muestra de lo afirmado, las SSTs (Sala 2ª) 5 febrero 1988, 19 abril 1991, 3 febrero 1997. y 22 enero 1998. SANCHÍS CRESPO, *op. cit.* Págs. 83-84.

«CUARTO.- Al amparo de lo dispuesto en el número 2º de artículo 849 de la Ley de Enjuiciamiento Criminal, se denuncia en el quinto motivo impugnación, error en la apreciación de la prueba, basado en documentos que acreditan la equivocación del juzgador.

Con carácter previo conviene partir de la doctrina general que en orden a este vicio sentencial se ha pronunciado la jurisprudencia de esta Sala, que de manera reiterada viene delimitando el concepto de documento, requiriendo en primer término que se trate de un documento en sentido estricto, entendiendo por tal el escrito, en sentido tradicional, o aquella otra cosa que, sin serlo, pueda asimilarse al mismo, por ejemplo, un diskette, un documento de ordenador, un vídeo, una película, etc., con un criterio moderno de interacción de las nuevas realidades tecnológicas, en el sentido en que la palabra documento figura en algunos diccionarios como "cualquier cosa que sirve para ilustrar o comprobar algo" (obsérvese que se trata de una interpretación ajustada a la realidad sociológica, puesto que, al no haber sido objeto de interpretación contextual y auténtica, puede el aplicador del derecho tener en cuenta la evolución social), siempre que el llamado "documento" tenga un soporte material, que es lo que sin duda exige la norma penal. (Por todas, SS.TS. 1.114/94, de 3 de junio, 1.763/1994, de 11 de octubre y 711/1996, de 19 de octubre). En la actualidad dicha fórmula jurisprudencial tiene adecuada correspondencia en la norma contenida en el artículo 26 del nuevo Código penal, según el cual "a los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica".

Con arreglo a la nueva fórmula legal, la interpretación literal del artículo 26 del Código penal de 1995 resulta insatisfactoria, y por ello, se impone hallar otra. Así, puede concluirse que documento a efectos

penales es el resultado de combinar un soporte material y datos, hechos o narraciones; caracterizándose aquélla por las notas siguientes:

a) En primer término, el documento, al ser una materialización, debe de constar en un soporte indeleble.

Por ello, se suele considerar el documento escrito como el documento por antonomasia. Ahora bien, hoy no se ven razones que impidan conferir tal condición a documentos diversos del documento escrito: la referencia a la legislación civil (arts. 1.216 ss. CC y 596 LEC) se puede explicar históricamente (el modelo francés), pero parece insuficiente. De ahí que, siguiendo las brechas abiertas por la doctrina y la jurisprudencia, el artículo 26 cierre una polémica en el sentido más correcto.

Por lo tanto, si el documento tiene que constituirse mediante una declaración humana de forma razonablemente perdurable, pues de lo contrario no podría entrar en el tráfico jurídico y su finalidad probatoria no llegaría a conseguirse, no se ve obstáculo para reservar sólo al papel la posibilidad de ser soporte físico de la corporeización de dicha declaración. Cualquier otro soporte de idéntica vocación indeleble puede ser susceptible de considerarse documento y, por tanto, ser susceptible de falsificación; así, una grabación en vídeo o cinematográfica o sonora (disco o cinta magnetofónica). Lo que sucederá es que algunos de estos soportes, en ocasiones, pueden ser poco fiables; su susceptibilidad de manipulación, sin que se advierta la misma, puede ser grande. Ahora bien, si en el caso concreto esa posibilidad no se ha podido dar, no existe obstáculo para admitir un documento así materializado. Hoy día, empero, la pretendida fiabilidad del papel ha desaparecido y todos los documentos son igualmente vulnerables, por lo que ese pretendido requisito no puede ser *conditio sine qua non* para dejar de admitir lo que es de uso común en el tráfico jurídico.

b) *Otra nota es que tenga procedencia humana. Se trata de que el contenido del documento resulte atribuible a una persona.* En principio, es indiferente si se trata de una manifestación de voluntad (un testamento, por ejemplo) o una declaración de conocimiento (un acta de una sesión del Consejo de Administración, un certificado médico...), mientras su autor sea un ser humano. Ello tendrá como consecuencia necesaria que haya que establecer un autor determinado o, cuando menos, determinable. El autor de la declaración -no de los intervinientes o afectados, pues éstos quedan incluidos o referidos en el contenido del documento- ha de ser determinable, sin más problemas que los derivados de la comprensión ordinaria, aunque sea necesario el auxilio de medios técnicos de público acceso. Queda así, de entrada, excluido el documento anónimo; es decir, el que no se puede atribuir con seguridad a nadie por no constar expresamente su autor. Sin embargo, dado que el autor es determinable y no determinado, no será anónimo el documento cuando de éste pueda derivarse cuál es el autor; pero la deducción ha de serlo por el sentido, no por mediar mecanismos diversos (prueba grafológica, huellas dactilares...) de acceso no generalizado ni generalizable. El artículo 26 alude a datos, hechos o narraciones. El dato, el hecho o la narración deben reconducirse a su procedencia humana. Lo contrario sería equiparar una narración que, evidentemente, sólo puede proceder de un ser humano, a datos o hechos que pueden ser, teóricamente al menos, porciones inermes de realidad.

c) También el contenido de la declaración debe ser comprensible de acuerdo a los usos sociales, es decir, significativa en sí misma. Así, un documento extranjero, que surta efectos en España, es documento y su falsedad punible, pues sólo es necesaria, en ocasiones, su traducción; en cambio, un escrito en clave, encriptado, no es un documento a estos efectos, pues se pretende con su confección todo lo contrario; que no signifique nada para quien no esté en posesión de la

correspondiente clave; es más; no se desea su ingreso en el tráfico jurídico. Además, se ha de actualizar la nota de la significación. Análogamente a lo que sucede con determinadas abreviaturas convencionales -claves en cuya posesión están todos- o a los documentos extranjeros -para entenderlo habrá que o estudiar esos idiomas o acudir a un traductor- habrá que colegir que son documentos todas aquellas declaraciones de voluntad o de conocimiento que se confeccionen por procedimientos electrónicos o lógicos y que para su entendimiento y/o transmisión y/o transformación son necesarios instrumentos o medios que también están a disposición de cualquiera: ordenadores, modems, faxes...

d) *También se requiere la entrada en el tráfico jurídico.* Si el documento no entra (o no está concebido para entrar: documento encriptado) o, aun entrando, le faltan características esenciales (procedencia humana, autor determinable) o no significa nada (sopa de letras) y no estaremos ante un documento en el sentido de objeto de protección jurídico-penal. Ello no impide que cualquier objeto pueda integrarse en otro documento, formando así un complejo, cuya alteración entonces sí será la de un documento.

e) Por último, *el documento válido es el documento original y no tienen tal carácter las copias ni fotocopias.* Sin embargo, esta afirmación es cada vez más relativa al aumentar el tráfico jurídico y, por tanto, el número de documentos. Así, ya de antiguo a algunos documentos no originales se les reconoce ex lege valor documental bajo ciertas condiciones; tal es el caso de, por ejemplo, la copia de una demanda - art. 525 LECrim.- o la copia autenticada por un sujeto provisto de fe pública (secretarios judiciales, notarios, corredores de comercio...) La práctica forense ha ido imponiendo la aceptación de fotocopias como documentos válidos salvo que se requiera expresamente el cotejo (art.

597 LECrim.); lo mismo sucede con las traducciones privadas de los documentos extranjeros (art. 601 LECrim.).»

La sentencia citada hace referencia a todos los requisitos exigidos desde la óptica penal para la protección del documento. Como podrá apreciarse, los caracteres del documento mantenidos en el ámbito penal coinciden en gran medida con los exigidos en el ámbito civil, dejando aparte la apertura que supone con respecto a la doctrina su asimilación a los documentos. Llama la atención que la propia jurisprudencia considera, a cuatro años vista de la entrada en vigor del precepto, que éste resulta insuficiente para definir al documento como objeto de protección penal, procediendo a su redenición de acuerdo con algunos de los caracteres clásicos asignados a los documentos *strictu sensu*. No obstante, algunos de estos requisitos no se dan en los documentos electrónicos, pudiendo ser obviado en parte por la amplia definición proporcionada legalmente. Pero, aun así, esta definición amplia de documentos no coincide con la recogida en el CP en los preceptos de la parte especial, limitando por ello el alcance operativo del precepto. Y su condición omnicomprendensiva y general a todo el articulado penal.

Así, puede hablarse de la ausencia del carácter indeleble del soporte en el que conste el documento electrónico, dado que con ello sólo serían protegibles los datos almacenados en soportes magnéticos <sup>18</sup>, en tanto que en determinados tipos penales se alude a los documentos y a los datos obrantes en redes y soportes telemáticos, que no son un objeto en sí con capacidad de almacenamiento de información, sino dispositivos de flujo de información con capacidad de transmisión.

Otro tanto sucede con la referencia a la legibilidad y la voluntad de acceso al tráfico jurídico, que excluye de la consideración de documento a los cifrados. Las técnicas de cifrado no alteran para nada las necesidades de interposición de una máquina u ordenador para su legibilidad. El hecho de que, además de los equipos y programas

---

<sup>18</sup> Puede hablarse de disquetes, discos duros, discos ópticos, CDROM, DVD, floppys, discos jazz, unidades ZIP, cintas DAT, como soportes magnéticos u ópticos de almacenamiento de información digital. SANCHÍS CRESPO, *op.cit.* nota 21 pág. 23.



precisos para la lectura de un documento electrónico se requiera otro programa o equipo y la posesión de las claves de cifrado –información a manejar por el programa- no suponen la exclusión de la posibilidad de lectura; ésta será posible sólo por las personas que se hallen autorizados para su lectura, haciéndose imposible para aquellos que intercepten o se apoderen del documento. En nada se diferencian las operaciones a realizar por el ordenador cuando lee un documento no cifrado o un documento protegido por dichos mecanismos <sup>19</sup>. Es más : la tecnología actualmente sustentadora de las firmas digitales –encriptación de clave asimétrica- fue desarrollada para hacer posible la remisión de documentos a través de redes públicas de transmisión de datos de forma segura, por lo que no cabe hablar en su uso de una vocación de aislamiento del tráfico jurídico, sino todo lo contrario. De otra forma se estaría penalizando el empleo de medios de protección de la información en las comunicaciones electrónicas, frente al uso de los documentos electrónicos sin adopción de medida de protección alguna <sup>20</sup>.

Por último, también es criticable derivar del art. 26 CP la exclusiva protección a los originales y no a las copias. Si el precepto base amplía su dicción para abarcar en su seno a los documentos electrónicos, es connatural a estos la imposibilidad de distinguir entre original y copia. Es más, como acertadamente pone de relieve BONET COMPANYY <sup>21</sup>, la fijación de datos en un soporte se realiza a partir de la información almacenada en la memoria RAM del ordenador (de naturaleza volátil en cuanto el ordenador carece de suministro eléctrico o es apagado), que recoge la introducida a través del teclado u otro dispositivo de captación de información (escáner, lectura de soporte magnético, etc); de tal modo que incluso el primer

---

<sup>19</sup> De hecho casi todos los programas de ofimática empleados en la actualidad –procesadores de texto, hojas de cálculo, gestores de base de datos, clientes de correo electrónico- permiten cifrar las información por ellos procesada como mecanismo de control, o la asignación de una contraseña de lectura y acceso.

<sup>20</sup> El aserto realizado por el juzgador choca de plano con el derecho conferido al usuario de medios de telecomunicación de empleo de cifrado en las redes y servicios de tal naturaleza establecido por el art. 52 de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones. En su apartado 1º se establece que «Cualquier tipo de información que se transmita por redes de telecomunicaciones podrá ser protegida mediante procedimientos de cifrado.»

El primer inciso del apartado siguiente establece que «El cifrado es un instrumento de seguridad de la información.» Sería absurdo reconocer a estas técnicas tal condición y finalidad y excluirlas de protección penal de ser empleadas para los fines previstos por la ley.

<sup>21</sup> BONET COMPANYY, Jesús, «El Documento electrónico en el Procedimiento Administrativo Español: ¿Hacia el Documento Público Electrónico?», en *Revista Informática y Derecho* 30-32, Mérida 1999, pág. 219

registro en el disco duro es tanta copia como las demás que pueden hacerse a partir de éste. Y sin embargo, la consideración de documento no sufre por esta grabación de la información verdaderamente escrita por el usuario.

Por ello, o bien ha de entenderse precisa una interpretación del art. 26 de acuerdo con la realidad social en que ha de ser aplicada -que no es otra que la de las telecomunicaciones informáticas, en las que las redes de datos actúan de soportes virtuales de la información que por ellas pasa- o ha de estimarse que dicho precepto queda desplazado en determinados tipos delictivos, que ahora examinaremos, en los que se maneja un concepto especializado del documento electrónico.

Lo que pone de manifiesto el cotejo de la realidad y estado de la tecnología con el precepto de 1995 es su desfase para acomodarse a las nuevas concepciones del documento electrónico como información descorporeizada por su procesamiento mediante sistemas de información.

#### La protección del documento electrónico en la Parte Especial del CP

El Derecho Penal protege expresamente a los documentos electrónicos como soporte de información relevante. Es el caso del art. 197.1, donde es citado mediante la especie del mensaje de correo electrónico<sup>22</sup>. La dicción de este inciso pone de manifiesto que el legislador se representa el mensaje de correo electrónico en su formato electrónico, dado que lo considera un tipo de soporte de información distinto a los basados en el papel –a los que también alude de forma diferenciada-; al tiempo que los engloba a todos en el concepto de documento, amparado en la dicción del art. 26.

---

<sup>22</sup> Art. 197.1: «El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales...»

Por su parte, el párrafo 2º alude al documento electrónico desde una perspectiva más tecnológica y adaptada a la realidad informática actual, cual es la telemática y las comunicaciones entre ordenadores. Así, el legislador sanciona el apoderamiento, uso o modificación en perjuicio de tercero, de datos reservados de carácter personal o familiar de otro «que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos». Como más adelante veremos, las necesidades derivadas del estado de la tecnología obligan a manejar un concepto desmaterializado del documento, a pasar –en expresión de BONET<sup>23</sup>- del «documento-objeto» al «documento-información», esto es, a la protección de la información en sí, del contenido de un soporte que ahora puede tener existencia al margen del mismo. En este precepto es la información misma –los datos personales o familiares- lo que es objeto de protección, siendo su soporte meramente virtual (informático, electrónico o telemático). La referencia al soporte telemático supone el máximo reconocimiento del proceso de desmaterialización aludido, puesto que *lo telemático* alude a la conexión mediante cables y redes físicas o lógicas establecida entre ordenadores, por donde la información fluye de uno a otro mediante unos protocolos de comunicación que regulan las señales a emitir y recibir entre los sistemas informáticos<sup>24</sup>

Como soporte de información es también citado en el art. 278, entre los delitos relativos al mercado y a los consumidores. Dicho precepto sanciona el apoderamiento de «datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo» que contengan un secreto de empresa.

La causación de daños en los documentos electrónicos es objeto de sanción, como subtipo agravado, en el art. 264.2<sup>25</sup>. De nuevo aparece en este precepto la

---

<sup>23</sup> BONET COMPANY, *op.cit.*, pág. 221

<sup>24</sup> En la actualidad la telecomunicación a través de ordenadores es realizada en gran medida, aunque no de forma exclusiva, a través de Internet, un conjunto de redes de ordenadores conectados entre sí mediante los protocolos TCP/IP establecidos por la Internet Society (ISOC), organismo norteamericano encargado del establecimiento de las normas técnicas que permiten la interconexión de los sistemas informáticos entre sí. Dichos protocolos son definidos por la Internet Engineering Task Force (<http://www.ietf.org>), siendo aceptados por la comunidad internacional debido al origen norteamericano de Internet y al peso de dicho país en el conjunto de usuarios finales de la Red.

<sup>25</sup> Art. 264.2 CP: «La misma pena se impondrá al que por cualquier medio destruya, altere, inutilice o de

referencia al documento-información, al aludirse a los datos, programas y documentos electrónicos «contenidos en redes [...] o sistemas informáticos». La información almacenada en soportes físicos es aludida mediante la cita a los soportes informáticos, de naturaleza mueble y corpóreos por ello; en tanto que la existencia como meros impulsos electrónicos –información en estado puro, desmaterializada y exenta a cualquier soporte magnético- ha de encontrarse amparada en la dicción «redes» del precepto en cuestión.

La dificultad de aplicación del art. 264.2 radica determinar su autonomía o dependencia sistemática del art. 263, que establece el límite cuantitativo del objeto dañado. Si bien es cierto que el apartado no contiene referencia alguna a límites cuantitativos –como contienen el resto de preceptos del capítulo IX, lo que permitiría hablar de la posibilidad de su aplicación a las conductas que satisficieran los elementos del tipo- lo cierto es que su ubicación sistemática hace pensar que queda sometido al límite genérico de deslinde de los delitos y faltas de daños, esto es, la cantidad de cincuenta mil pesetas. En virtud de una defectuosa técnica legislativa de constantes remisiones de unos preceptos a otros, el art. 264.1 hace referencia a «el que causare daños expresados en el artículo anterior...» concurriendo las circunstancias que posteriormente se listan; la referencia sólo puede entenderse al límite cuantitativo y a la ajenidad del objeto dañado, pues no se define lo que ha de entenderse por daños. Por otra parte, el apartado 2º inicia su dicción con una referencia a las penas señaladas en el apartado anterior; mediante esa dependencia se puede considerar también sometido a la previa remisión al art. 263. Por último, la consideración conjunta del art. 263 –considerado residual respecto del resto de modalidades comisivas incluidas en el capítulo IX<sup>26</sup>- y del art. 625, relativo este último a la falta de daños, así como la consideración de la cantidad mencionada como el límite que fija el CP para distinguir delitos y faltas contra el patrimonio, lleva a considerar preciso que el valor de la información contenida en el soporte sea

---

cualquier otro modo dañe los datos, programas o documentos ajenos contenidos en redes, soportes o sistemas informáticos».

<sup>26</sup> QUINTERO OLIVARES, Gonzalo, *Comentarios al Nuevo Código Penal*, Pamplona 1996, pág. 1201

superior a esa cantidad, lo que acarreará en muchas ocasiones serias dificultades de prueba, cuando no la imposibilidad material de aplicación <sup>27</sup>

La aplicación general del art. 26 a todo el Código Penal permite incardinar al documento electrónico entre los posibles objetos de *falsedades documentales* previstos en los arts. 390 a 400. No obstante, no todas las figuras previstas en el art. 390 serán aplicables a los documentos electrónicos por cuanto que para hablar de documentos públicos electrónicos será imprescindible emplear firmas digitales, pues de otra forma no cabría cumplir los requisitos previstos de validez y eficacia de los mismos. La tecnología en que se basan las firmas digitales impiden la manipulación del documento firmado, razón por la que sólo cabrá hablar de falsedad ideológica previa al acto de la firma digital por el funcionario competente o suplantación de identidad en el empleo de las claves de firma –por haberse apoderado del soporte en que se contengan (caso de almacenarse en tarjetas inteligentes) o de las claves de cifrado en que consisten por cualquier medio de los previstos en el art. 197.1 CP, lo que permitirá hablar de un concurso medial de delitos ex art. 77.1 CP-. En cuanto a los documentos privados, dado que en éstos puede emplearse todo tipo de firmas electrónicas –esto es, sin que estén basadas en la tecnología de clave asimétrica- , e incluso como quiera que es posible su existencia sin necesidad de que consten firmados <sup>28</sup>, es posible apreciar las conductas establecidas en los tres primeros apartados del art.390 <sup>29</sup>

Lógicamente, como quiera que la legislación actual reconoce la validez y eficacia de los documentos electrónicos emitidos tanto por la Administración como por el Poder Judicial, según lo anteriormente expuesto, es aplicable a éstos la distinción entre

---

<sup>27</sup> GUTIÉRREZ FRANCÉS, M<sup>a</sup> Luz, *Delincuencia Económica e Informática en el Nuevo Código Penal*, Cuadernos del CGPJ 1996/XI, Madrid, 1996, págs. 297-298.. Dicha concepción fue aplicada en el caso “Hispahack”, juzgado en Barcelona en 1998.

<sup>28</sup> Dada la amplitud del concepto definido por el art. 26 así como de las referencias a datos y programas que hallamos en los artículos estudiados, podemos afirmar que documentos electrónicos pueden ser para el Código Penal un programa informático o una base de datos personales o no almacenados en el disco duro o en cualquier soporte magnético u óptico de un ordenador.

<sup>29</sup> En cuanto a la falsedad ideológica, esta sólo puede ser cometido por el funcionario público en el documento público, no cabiendo su comisión por particular sobre ningún tipo de documento (arts. 392 y 395 CP).

documentos públicos y oficiales y documentos privados, con las consecuencias punitivas reflejadas en los correspondientes tipos penales.

La utilización de las técnicas de cifrado y de firma electrónica requieren el uso de mecanismos físicos y lógicos para su implementación. Con el fin de proteger los documentos –o mejor dicho, la información en ellos contenida- el art. 400 prevé como delito lo que no es sino un acto preparatorio: «la fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos específicamente destinados a la comisión de los delitos descritos en los capítulos anteriores». El gran problema de la aplicación de este precepto lo constituirá la prueba del destino específico y de la voluntad de empleo para la comisión de los delitos descritos, lo que tendrá que dilucidarse, en la mayoría de las ocasiones, a través de prueba indiciaria al constituir un elemento subjetivo.

#### *1.1.c.) El documento electrónico como medio probatorio*

La Ley de Enjuiciamiento Criminal contiene escasas normas relativas a la prueba documental. Estas no son necesarias para admitir los documentos en el nuevo formato electrónico en el proceso penal, dado que el propio Código Penal se encarga, como ya hemos tenido ocasión de comprobar, de definirlo como objeto de las conductas típicas –aunque sólo a esos efectos, como remarca SANCHÍS CRESPO<sup>30</sup>–.

La carencia de normas propias hace necesario acudir al articulado de la Ley de Enjuiciamiento Civil, de aplicación supletoria a todos los restantes procesos en cuanto en sus respectivas leyes no se halle regulado<sup>31</sup>, lo que sucede con el aspecto probatorio en la Ley Rituaria Penal.

---

<sup>30</sup> SANCHÍS CRESPO, Carolina, *El soporte informático de escritura como prueba en el proceso penal*, Estudios Jurídicos del Ministerio Fiscal VIII, Madrid, 1998, pág. 651.

<sup>31</sup> «Artículo 4. Carácter supletorio de la Ley de Enjuiciamiento Civil

En defecto de disposiciones en las Leyes que regulan los procesos penales, contencioso-administrativos, laborales y militares, serán de aplicación, a todos ellos, los preceptos de la presente Ley.»

Es preciso por ello analizar qué régimen jurídico gozarán los documentos electrónicos en el proceso penal cuando éstos no sean el objeto material del delito a investigar, sino sean empleados como prueba de otros hechos.

#### 1.1.c.1) La distinción entre fuentes y medios de prueba

Una de las vías empleadas por la Doctrina para eludir el polémico límite de la admisión de nuevos medios probatorios derivado tanto del CC (art. 1215)<sup>32</sup> como de la ALEC (art. 578)<sup>33</sup> fue la de acudir a la distinción entre fuentes y medios de prueba.

De forma unánime se había entendido que los artículos precedentes constituían un *numerus clausus* de medios probatorios. Ello cuestionaba la posibilidad de aportar al proceso objetos materiales de los que podía desprenderse material probatorio pertinentes a los efectos del proceso.

La dificultad podía orillarse mediante la distinción entre fuentes y medios de prueba. Como pone de relieve SENTIS MELENDO<sup>34</sup> la fuente es un concepto metajurídico extraprocesal, que corresponde a una realidad anterior y extraña al proceso; en tanto que el medio es un concepto jurídico y absolutamente procesal. La fuente es ajena al proceso y vive con independencia de él, al que sólo accede en caso de conflicto. Por ello carece de regulación legal. Los medios de prueba, como actos procesales, han de ser limitados legalmente por virtud de los principios de legalidad procesal y seguridad jurídica, de forma que el ciudadano sepa cómo ha de actuar y

---

<sup>32</sup> Art. 1215 CC: «Las pruebas pueden hacerse: por instrumentos, por confesión, por inspección personal del juez, por peritos, por testigos y por presunciones»

<sup>33</sup> Art. 578 ALEC: «Los medios de prueba de que se podrán hacer uso en juicio son: 1. Confesión en juicio. 2. Documentos públicos y solemnes. 3. Documentos privados y correspondencia. 4. Los libros de los comerciantes que se lleven con las formalidades prevenidas en la sección 2ª, título II, libro I del Código de Comercio. 5. Dictámenes de peritos. 6. Reconocimiento judicial. 7. Testigos.»

<sup>34</sup> SENTIS MELENDO, S, *La prueba*, Buenos Aires, 1978, págs. 151, 153 y 158, citado por Sanchís Crespo, op.cit. pág. 68.

producir sus fuentes de prueba para el caso de tener que reclamar su derecho en juicio mediante las mismas. La regulación del medio de prueba no sólo hace referencia a una fuente (declaraciones de personas, informes de peritos, determinados instrumentos documentales), sino también a los trámites precisos y a la actividad que la parte ha de desplegar para aportarlos a juicio y poder ser valorados por el juzgador. Se trata, por tanto, de una institución jurídica compleja que regula el objeto, la actividad a desarrollar y la valoración que merece con respecto al hecho a probar.

La distinción es admitida por la doctrina de forma pacífica<sup>35</sup>, encontrando también amparo de signo constitucional, a juicio de algún autor<sup>36</sup> en el art. 24.2 de la Constitución, que establece el derecho a utilizar todos los medios de prueba pertinentes. Este precepto, a juicio de Picó, viene a garantizar el principio de libertad probatoria, en virtud del cual una parte tiene derecho a la admisión de cualquier elemento probatorio, previsto o no en la ley, que sirva para acreditar los hechos controvertidos<sup>37</sup>.

De esta forma, el problema a resolver en cuanto a la admisión de medios probatorios al amparo de la ALEC era su incardinación en alguno de los medios probatorios determinados en el art. 578.

A este respecto es conveniente examinar previamente los caracteres de las pruebas por documentos, así como la concurrencia de sus requisitos en los documentos

---

<sup>35</sup> MONTERO AROCA, J., *La prueba en el proceso civil*, Madrid, 1988, pág. 71. ORMAZÁBAL SÁNCHEZ, Guillermo, *La prueba documental y los medios e instrumentos idóneos para reproducir imágenes o sonidos o archivar y conocer datos*, Madrid, 2000, pág. 166. ROVANET MOSCARDÓ, Jaime, «Valor probatorio procesal del documento electrónico», en *Revista Informática y Derecho* 1, Mérida 1992. MARONDA y TENA, *op.cit.* pág. 1756-ss.

<sup>36</sup> SANCHÍS CRESPO, Carolina, *La prueba por soportes... op.cit.* pág. 70. CALVO SÁNCHEZ, M<sup>a</sup> Carmen, «Los medios técnicos, informáticos y telemáticos en el proyecto de reforma de la LOPJ», en *Revista de Actualidad Jurídica Aranzadi*, julio 1994; citada por Maronda y Tena, *op.cit.* pág. 1757.

<sup>37</sup> PICÓ i JUNOY, J., *El derecho a la prueba en el proceso civil*, Barcelona, 1996, pág. 178; citado por Sanchís, *ibid.* Pág. 70.



electrónicos. De resolverse positivamente tendríamos un enclave procesal para la admisión y régimen probatorio de dichas fuentes.<sup>38</sup>

### 1.1.c.2) El concepto de documento

#### Concepto doctrinal de documento

Con la excepción de Guasp, quien concebía los documentos como «cualquier objeto mueble que dentro del proceso puede ser utilizado como prueba» la mayoría de la doctrina identificaba documento con instrumento basado en el papel o en alguno de sus derivados, en el que mediante escrito se incorporaba o plasmaba una manifestación del pensamiento humano<sup>39</sup>. En este sentido para CORTÉS DOMÍNGUEZ es «solo y exclusivamente la representación de un pensamiento escrito en papel, pues el requisito de la escritura en papel se deduce, de forma bastante clara, de la mera lectura de las normas que regulan la prueba por documentos en la Ley de Enjuiciamiento Civil»<sup>40</sup>

No obstante, y de forma paralela a la evolución del concepto estudiado operada por la jurisprudencia, otro sector doctrinal abogó por una concepción más centrada en el carácter representativo del documento – recuérdese que, para Carnelutti, el documento no era sólo una cosa, sino una cosa representativa, como nos recuerda Sanchís<sup>41</sup>-. Así, Serra considera el documento como «todo objeto material

---

<sup>38</sup> Cuestión distinta, y no exenta de dificultad, es la de determinar si la equiparación con las pruebas documentales trae consigo la aplicación de las normas de valoración legal establecidas en el CC para los documentos públicos y privados. De ello nos ocuparemos a la hora de hablar de la valoración de los documentos electrónicos.

<sup>39</sup> Ortiz Navacerrada lo define como «todo escrito que reproduce un pensamiento o volición humanas y se aporta al proceso con designio probatorio» ORTIZ NAVACERRADA, S, «La prueba de documentos privados en el proceso civil» en *Cuadernos de Derecho Judicial*, Madrid, 1994, pág. 98, citado por Sanchís, *op.cit.*, pág. 61.

<sup>40</sup> CORTÉS DOMÍNGUEZ, Valentín y otros, *Derecho Procesal*, tomo I, vol.I «Parte General», Valencia, 1986.

<sup>41</sup> SANCHÍS CRESPO, C, *op.cit.*, pág. 62.

representativo de un hecho con interés para el proceso, representación que puede obtenerse bien mediante el método tradicional de la escritura, bien mediante los modernos medios reproductivos [...] Lo importante no es tanto la grafía como la representación»<sup>42</sup>. Para Jimena Leiva «En términos amplios, debe entenderse por documento o instrumento cualquier objeto que contiene información, que narra, hace conocer o representa un hecho, cualquiera que sea su naturaleza, su soporte o “continente”, su proceso de elaboración o tipo de firma»<sup>43</sup>.

### Concepto jurisprudencial de documento

La necesidad de obtener certeza a través de objetos materiales cotidianos a través de los cuales se manifiesta el pensamiento y obrar humano condujo a los Tribunales a la ampliación del concepto de documento, con el fin de poder acomodar las decimonónicas regulaciones civil y procesal a las exigencias del tráfico jurídico moderno, en donde –como hemos tenido ocasión de observar- obtenía reconocimiento legal a la vez que real.

No obstante, el reconocimiento jurisprudencial de una concepción amplia de documento no fue inmediato. A juicio de algunos autores<sup>44</sup>, puede hablarse de tres etapas en la evolución jurisprudencial: a) la de negación del valor probatorio de objetos en los que no concurría la condición de documento según la concepción tradicional; b) la de aceptación del valor probatorio de los medios reproductivos, advertados o completados por otros elementos probatorios; y c) la de plena admisión, como especie de la prueba por documentos, de los medios de reproducción de la palabra, imagen o sonido.

---

<sup>42</sup> SERRA DOMÍNGUEZ, M, voz «Prueba documental», en *Nueva Enciclopedia Jurídica Seix*; citado por Sanchís, *ibid.* págs. 61-62.

<sup>43</sup> JIMENA LEIVA, Renato Javier. «Naturaleza Jurídica y valor probatorio del documento electrónico» en *Revista La Ley*, 17 de julio 1998.

<sup>44</sup> BATURONES, Elías, «La jurisprudencia ante el documento electrónico (o en soporte no escrito). Su aceptación como prueba documental» en *Tapia*, octubre-noviembre 1996, pág. 69; citado por Sanchís, *op.cit.*, pág. 57.

La STS (1ª) de 30 de noviembre de 1981 es el referente jurisprudencial de la admisión de los nuevos medios probatorios –en concreto la sentencia se refería a la admisión de unas cintas magnetofónicas-, pudiendo adscribirla a la fase intermedia estudiada, dado que admite la validez probatoria de estos instrumentos pero siempre que sea acompañado de otros medios probatorios que permitan acreditar la ausencia de manipulaciones<sup>45</sup>. En esta línea cabe citar también los pronunciamientos contenidos en las SSTS (1ª) de 30 de noviembre de 1992 –que acoge a los documentos reproductivos de imágenes, sonidos y palabras en el reconocimiento judicial, por la necesidad e acreditar su fiabilidad y ausencia de manipulaciones-, 3 de octubre y 3 de noviembre de 1997<sup>46</sup> –relativos a la impugnación de los soportes magnéticos en que podían hacerse constar documentos de giro, de acuerdo con lo autorizado por el RD 828/1995 de 29 de mayo, de desarrollo del Texto Refundido de la Ley sobre el impuesto de Transmisiones Patrimoniales y Actos Jurídicos Documentados-, entre otras muchas.

La jurisprudencia ha acogido dos criterios para proceder a la evolución de su doctrina. De una parte, el funcional, derivado de la doctrina científica, en cuya virtud lo esencial del documento es la capacidad de representar una manifestación del pensamiento, amparada en el empleo por el CC del término «instrumento» en vez del más estricto de documento<sup>47</sup>. De otra, el criterio hermenéutico de la realidad

---

<sup>45</sup> Declaraba esta sentencia que «si bien es cierto que tradicionalmente el concepto de documento se ha venido identificando con un “escrito”, o sea, como un objeto o instrumento en el que queda plasmado un hecho que se exterioriza mediante signos materiales y permanentes del lenguaje..., ello no es óbice para que existan en la actualidad otros objetos que, sin tener esa condición, puedan hacer prueba fidedigna de aquéllos y que, por analogía, puedan equipararse a los mismos»

<sup>46</sup> En esta última manifestaba el TS: «Estamos asistiendo, 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 constituyen, hoy día, una nueva forma de entender la materialidad de los títulos valores y, en especial, de los documentos mercantiles»

<sup>47</sup> El empleo del concepto funcional es más destacable en la jurisprudencia penal, debido a las necesidades de acomodar el concepto clásico a la realidad penal antes de la entrada en vigor del art. 26 CP. Así, la STS (2ª) 5 de febrero de 1988 describió los documentos como «cosas muebles aptas para la incorporación de señales expresivas de un determinado significado». En la misma línea, las STS (2ª) 19 de abril de 1991, 10 de julio de 1996, 3 de febrero de 1997 y 16 de febrero de 1998. No debe olvidarse tampoco la reseñada más arriba de 22 de octubre de 1998, donde se realiza un exhaustivo estudio de los requisitos del documento a efectos penales, con las notas críticas que merece de acuerdo con la realidad social imperante.

social en que las normas han de ser aplicadas, que lleva a la aceptación ante los Tribunales de lo que goza de consideración cotidiana –y aun legal-<sup>48</sup>.

SANCHÍS, en la obra que seguimos<sup>49</sup>, concreta el concepto jurisprudencial de documento, debiendo entenderse por tal «tanto los escritos representativos como, mediante una ampliación del concepto legal, todos aquellos objetos en los que a través de la vista, el oído o el tacto, pueda percibirse una manifestación de voluntad o revelen a simple vista la existencia de un dato de interés para el proceso»

Concepto legal de documento. Hacia el concepto propio de documento electrónico

Al estudiar la protección penal del documento hicimos referencia al primer concepto legal amplio de documento conocido en nuestro Derecho, el contenido en el art. 49.1 de la Ley del Patrimonio Histórico Español. Dicha definición acogía la tesis funcionalista de documento, en la que prima su condición de objeto representativo de la realidad constituida por el pensamiento humano. Esta concepción es también la reconocida por el art. 26 del CP que ya hemos analizado *in extenso* junto a su jurisprudencia interpretadora; si bien en la Parte Especial del mismo hallamos muestras de una concepción más amplia y actual del documento electrónico como, al menos, soporte virtual de datos.

Dentro de los autores de la doctrina se han elaborado diversas definiciones del documento electrónico.

Así, HERRERA BRAVO Y NÚÑEZ ROMERO lo definen como «una representación material, destinada e idónea para reproducir una cierta manifestación de voluntad, materializada a través de las tecnologías de la información sobre soportes

---

<sup>48</sup> Ejemplo de esta línea son las SSTS (1ª) de 23 de marzo de 1987 y 30 de noviembre de 1992 ya citada, y (4ª) 7 de diciembre de 1979, así como la STCT de 26 de noviembre de 1985.

<sup>49</sup> SANCHÍS CRESPO, *ibid.*, pág. 59

magnéticos, como un disquete, un CD-ROM, una tarjeta inteligente u otra, y que consisten en mensajes digitalizados que requieren de maquinas traductoras para ser percibidos y comprendidos por el hombre»<sup>50</sup>.

Para JIMENA LEIVA «al hablarse de documentos electrónicos se alude a casos en que el lenguaje magnético constituye la acreditación, materialización o documentación de una voluntad ya expresada en las formas tradicionales y en que la actividad de un computador o de una red solo comprueban o consignan electrónica, digital o magnéticamente un hecho, una relación jurídica o una regulación de intereses preexistentes [...] Se caracterizan porque solo pueden ser leídos o conocidos por el hombre gracias a la intervención de sistemas o dispositivos traductores que hacen comprensibles las señales digitales»<sup>51</sup>

En similar sentido, ROUANET MOSCARDÓ: «En definitiva, el documento electrónico es un soporte material al que se le ha impreso por medios electromagnéticos, un pensamiento con un determinado significado. La diferencia con el clásico documento escrito estriba en que la impresión se ha hecho un lenguaje especial, distinto del común, el “lenguaje maquina”...»<sup>52</sup>

Este autor llega a afirmar, extendiendo el concepto dado, que el documento electrónico lo será no sólo cuando se halle incorporado a un soporte electromagnético, sino también cuando se haya hecho uso de la electrónica para su elaboración, según nos advierten MARONDO Y TENA<sup>53</sup>. Una intrerpretación tan amplia del documento electrónico conduciría a considerar como tales a la gran mayoría de los documentos tradicionales impresos en papel por el mero hecho de haber sido redactados mediante una máquina o procesador de textos, cuando la diferencia entre unos y otros es evidente en cuanto a los caracteres predicables de

---

<sup>50</sup>HERRERA BRAVO, Rodolfo y NÚÑEZ ROMERO, Rodolfo. *Derecho Informático*. Santiago de Chile, 1999. Disponible en <http://www.ctv.es/USERS/mpq/estrado/estrado012.htm>.

<sup>51</sup>JIMENA LEIVA, *op. cit.*

<sup>52</sup>ROUANET, *op. cit.* pág.169.

<sup>53</sup> MARONDO y TENA, *op.cit*, pág. 1755.

cada uno de ellos. La definición así pergeñada tampoco informa sobre lo propiamente característico del documento electrónico, que es su capacidad de ser procesable por un sistema informático, y de existencia sin soporte material.

A juicio de BONET<sup>54</sup> en este concepto pesa una aproximación *tradicional* al concepto del documento electrónico, heredera y deudora de la óptica procesalista-probatoria con que es concebida, lo que no es ilógico dado que la exigencia de una determinada forma en los actos públicos está orientada precisamente a la probanza del acto al que sirve de soporte. En opinión de este autor el documento electrónico ha perdido definitivamente características del documento escrito amparado en un soporte<sup>55</sup>, como son la unidad de acto entre creación y manifestación o asunción de su contenido, el de autoría –al no constar en él ningún vestigio físico que permita vincularlo a su autor-, e incluso el propio concepto de autoría humana –dado que el documento puede ser producto de un proceso automatizado de toma de decisión-, la distinción entre originales y copia, y la inmediatez de los significantes escritos –al precisarse de la intermediación de una máquina que los interprete y convierta en signos gráficos lo que no son sino impulsos magnéticos registrados en el soporte-. Todo ello hace prudente disociar al documento del soporte en que se manifiesta.

En efecto; la protección jurídica a los instrumentos o documentos se confería porque éstos constituían la única forma posible de acreditar de modo fidedigno una declaración de voluntad. La dependencia de un soporte material –como el papel, cartón, pergamino o similar- permitía la protección del contenido de dicha manifestación a través de la protección del continente, exigiéndose tanto la intervención de determinados funcionarios públicos como la verificación de ciertos ritos y trámites procedimentales. Por el contrario, en los nuevos documentos electrónicos la protección se realiza, como señala BONET<sup>56</sup> sobre el propio contenido, mediante la aplicación de las técnicas de firma digital basadas en la

---

<sup>54</sup> BONET COMPANY, José, *op.cit.* págs. 217 y ss.

<sup>55</sup> Prueba de ello es el análisis crítico realizado sobre la STS 22 de octubre de 1998, en la que se exponían los caracteres del documento basado en un soporte material.

<sup>56</sup> BONET COMPANY, *ibid.*, pág. 221.

criptografía asimétrica<sup>57</sup>, acompañando en forma de datos anexos al propio documento así firmado<sup>58</sup>, estando dichas medidas de protección indisociablemente unidas al documento originario, de tal modo que la función de garantía que supone el soporte material deja de hacerse necesaria. Todavía será precisa su materialización de algún modo –mediante impresión, almacenamiento en un soporte magnético o incluso mediante su mera visualización en pantalla- para que pueda tomarse conocimiento de su contenido y ser aportado al proceso. Pero ello no impide para que el documento exista con todos los requisitos precisos para poder ser legible, indeleble y atribuible a persona determinada.

Toda definición que asocie el documento electrónico a los soportes materiales (magnéticos, ópticos o de cualquier clase) está abocada a enfrentarse a la necesidad de acomodarse para afrontar el imparable proceso de desmaterialización

---

<sup>57</sup> La criptografía asimétrica permite la generación de un par de claves de cifrado –conjunto de caracteres con determinadas propiedades matemáticas- vinculadas entre sí de modo que no se permite la deducción de una a partir de la otra y se asegura su razonable individualidad frente a otros pares generados por la misma tecnología.

La clave privada –o, en terminología de la legislación de firma electrónica, «datos de creación de firma»- permanece exclusivamente en manos del firmante, de tal forma que nadie la conoce (ni siquiera el propio signatario, que sólo hace uso de ella a través del soporte en que se halle almacenada); ello permite excluir el repudio de la firma generada con dicha clave. La clave pública –o «dato de verificación de la firma»- asociada desde su creación a la clave privada, por el contrario, permite descifrar los mensajes encriptados con la clave privada asociada, así como verificar que la firma ha sido generada por quien es titular de la clave privada asociada a dicha clave pública.

El par de claves permite generar una firma electrónica, que consiste en la realización de varios procesamientos sobre el documento: en primer lugar, mediante la aplicación de los algoritmos Hash o de resumen, se genera una huella o impronta del contenido del documento; dicho resumen tiene siempre la misma extensión aplicado al mismo documento, lo que permite que otro usuario compruebe la modificación del documento mediante la comparación de los resúmenes o hash del documento (basta modificar cualquier carácter del documento –o un espacio en blanco- para que el hash resultante sea distinto). La huella o hash permite, por ello, acreditar la integridad del documento durante su transmisión.

El resumen o hash es firmado por el signatario con su clave privada (lo que le vincula al documento que firma como si estampara su firma o rúbrica manual sobre el papel).

El destinatario, una vez recibido el documento y la firma digital asociada, procede a descodificar el fichero en que consiste la firma aplicando la clave pública del signatario. Así obtiene el texto del hash originariamente generado por el emisor, al tiempo que comprueba que sólo ha podido ser firmado por quien aparece como titular de la clave pública (por la relación matemática existente entre ambas claves). A continuación su programa de firma realiza un nuevo compendio del documento para obtener otro hash de éste, comparando el remitido con el ahora creado. Si ambos coinciden, habrá constatado que el documento recibido no ha sido objeto de ninguna manipulación durante el envío.

<sup>58</sup> El art. 2 define la firma electrónica como «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. En el apartado b) define la firma electrónica avanzada como «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 está vinculada únicamente al mismo y a los datos a los que se refiere*, lo que permite que sea detectable cualquier modificación ulterior de éstos.»

de los documentos. Las redes telemáticas hacen posible la transmisión de documentos a través de cables de cobre o de fibra óptica, sin que haya desplazamiento de cosas materiales<sup>59</sup> La firma digital supone, como hemos visto, la autonomía de la propia información respecto del soporte contenedor de la misma. Por ello, podemos hablar de una concepción amplia de documento, que permite la inclusión del documento electrónico, y una concepción propia del documento electrónico, en que se tiene en cuenta la posibilidad de existencia como mera información ajena a soportes materiales<sup>60</sup>. La noción comienza a aparecer en la legislación.

Fue la legislación administrativa, y concretamente la de Seguridad Social, la que avanzó en la concepción propia de documento electrónico. La Orden de 3 de abril de 1995 citada en un principio incluye una serie de Anexos, entre los cuales destaca el Anexo I, al contener un glosario de términos informáticos en los que aparece, por primera vez y anticipando el sentido del art. 3 RTEIT la definición de documento, realizada en los siguientes términos: «Unidad de información procesable de modo autónomo. Equivale a EDI o mensaje». Muy interesante es también la distinción de los soportes informáticos entre soportes magnéticos e intercambio electrónico de datos, lo que nos permite hablar de una concepción muy avanzada de documento, dado que reconoce su desmaterialización. También hace alusión a términos posteriormente tan empleados como «huella electrónica», o a las impresiones autorizadas y de contraste.

También es muy significativa la manifestación contenida en la Disposición Adicional 1ª, en cuya virtud la obligación del empresario de exponer en lugar destacado del centro de trabajo los ejemplares del documento de cotización de los trabajadores

---

<sup>59</sup> Al respecto, y a modo de ejemplo, podemos recordar la polémica propia del Derecho Penal a la hora de considerar los fluidos –agua, luz, telecomunicaciones, etc- como cosas o bienes susceptibles de apoderamiento, al hilo del análisis de los delitos de defraudación de fluidos. Véase una exposición sobre la naturaleza de los mismos en GONZÁLEZ RUS, Juan José, «Aproximación al tratamiento penal de los de los ilícitos patrimoniales relacionados con medios o procedimientos informáticos» en *Informática y Derecho* nº 12, Madrid, 1986, págs. 129-138.

<sup>60</sup> Esta noción, empero, no impide que el documento electrónico se halle incorporado a un soporte material, de naturaleza electromagnética o electro-óptica. Al contrario; ese será su estado común. No obstante el documento necesitará de una concepción más amplia que le confiera protección



«se entenderá cumplida mediante la exposición o puesta a disposición de los trabajadores de dichas relaciones nominales en su forma impresa o convencional, o a través de la presentación en pantalla de ordenador o terminal informático de los datos de sus archivos, que a tal efecto serán considerados como copia autorizada de las citadas relaciones nominales de trabajadores»<sup>61</sup>

El RTEIT define el documento, en el contexto del empleo de técnicas electrónicas, informáticas y telemáticas, como «entidad identificada y estructurada que contiene texto, gráficos, sonidos, imágenes o cualquier otra clase de información que puede ser almacenada, editada, extraída e intercambiada entre sistemas de tratamiento de la información o usuarios como una unidad diferenciada.». Sobre esta definición, y de forma más sintética, define Bonet el documento –desde la perspectiva propia a la que aludimos- como «un volumen de información, determinada, procesable o procesada y susceptible de individualización»<sup>62</sup>. No obstante, el autor matiza que sólo cabrá hablar de documento electrónico cuando se halle firmado mediante firma digital, en función de la necesidad de cumplimentar los requisitos establecidos por la ley para que pueda ser tenido por prueba ante los Tribunales, a los que a continuación nos referiremos.

Información, procesabilidad e individualización son los caracteres esenciales del nuevo documento electrónico en su aproximación más tecnológica. El soporte material sigue siendo necesario para la percepción de su contenido y para la producción de efectos probatorios, si bien puede hablarse de una autonomía frente

---

<sup>61</sup> Esa sustitución de la entrega de copia impresa por la mera visualización en pantalla se halla en la L.O. 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal, en cuyo art. 14.2, al referirse al ejercicio del derecho de acceso, permite que la información a que ha de dar lugar «podrá consistir en la mera consulta de los ficheros por medio de su visualización...». Así es mantenido en el art. 12.2.a) del RD 1332/1994, de 20 de junio, de desarrollo de la LORTAD, y en el art. 15.2 de la vigente LO 15/1999, de 15 de diciembre, de protección de datos personales.

<sup>62</sup> BONET COMPANY, J, *op.cit.*, pág. 224. El autor refiere la definición al documento electrónico administrativo.

al mismo, al menos en la relación que hasta ahora se entendía inescindible. A ello nos referimos cuando hemos hablado de desmaterialización del documento<sup>63</sup>

### 1.1.c.3) Caracteres del documento como medio probatorio

De las opiniones doctrinales y jurisprudenciales cabe concluir que los caracteres del documento como medio probatorio son los siguientes:

Constituir una cosa mueble. No se está refiriendo la condición de cosa mueble como contraposición a cosa inmueble, a la que aluden los arts. 335 a 337 CC. La doctrina hace referencia, con el empleo de dicho término, a su posibilidad de ser llevados ante el Juez como medio probatorio sin desplazamiento del mismo<sup>64</sup>

El documento ha de ser inalterable, o lo que es lo mismo, gozar de una corporeidad que impida su desaparición –como sucedería con la memoria RAM de un ordenador, donde, a pesar de grabarse temporalmente la información, posteriormente desaparece en cuanto el aparato deja de ser alimentado por energía eléctrica.. Esta es una característica asociada a la anterior. A pesar de las manifestaciones realizadas en el apartado precedente sobre la desmaterialización de los documentos electrónicos, convenimos en la necesidad de que, para su consideración como medio probatorio –que no como objeto de protección penal- el documento electrónico ha de materializarse en algún tipo de soporte perdurable –lo que no impide per se su manipulabilidad-.

No es preciso que éste sea individualizado (un disquete, y otro tipo de soporte electromagnético en el que sólo conste el documento en cuestión). Soporte material

---

<sup>63</sup> Expresión abonada por la propia dicción de la ley, que distingue entre documento y su soporte (*vid.* Art. 45.5 LRJPAC, art. 230.2 LOPJ, art. 812.2 LEC).

<sup>64</sup> Los desplazamientos del Juzgador sólo están previstos para el reconocimiento judicial regulado en el art. 353 y ss LEC. Su objeto lo serán lugares, objetos o personas siempre que lo que haya de reconocerse pueda ser percibido directamente por los sentidos; no otro sentido cabe darle a lo que puede ser objeto de «grabación mediante el empleo de medios de grabación de imagen, sonido u otros instrumentos semejantes para dejar constancia de lo que sea objeto de reconocimiento...» a los que se alude en el art. 359 LEC.

es el disco duro de un ordenador, del que puede ser individualizado en cualquier momento mediante operaciones informáticas de selección –piénsese en el registro de una base de datos, o en un conjunto de datos con individualidad propia incluidos en otra unidad (como un expediente administrativo o judicial informatizado)-. Esa perceptibilidad será precisa para poder tomar conocimiento de su contenido –por más que no lo sea para su existencia como mera información- y para poder acreditar tanto su integridad como su autoría.

El documento ha de recoger una manifestación del pensamiento o de la voluntad del hombre. No obstante, conviene advertir que el empleo actual de los sistemas de tratamiento de información puede presentarnos ante documentos elaborados de forma automatizada por los ordenadores que, a pesar de ser desencadenados de forma mecánica sin la intervención humana inmediata, se deben a su voluntad e intención. Piénsese en el empleo de códigos de programación, o de las denominadas *macros* en los ordenadores, que permiten programar la emisión de determinados documentos en respuesta de una información previamente especificada por su contenido concreto o por sus características <sup>65</sup>. La máquina no sustituye la voluntad del hombre, sino que simplifica la labor que éste realizaría por sí mismo agrupando un conjunto de operaciones en función de unos *inputs* previamente definidos por éste. La máquina no hace nada que previamente no haya programado el usuario, razón por la que, de forma mediata, la declaración o documento emitido es totalmente imputable a su designio<sup>66</sup>.

El documento ha de ser representativo de la realidad. Si su finalidad es recoger una manifestación del pensamiento humano –una declaración, una manifestación de voluntad obligatoria, un pensamiento- debe exigírsele dicha relación con la realidad.

---

<sup>65</sup> En un ejemplo sencillo, podemos aludir a las denominadas “reglas” de los clientes de correo electrónico, que permiten desde el almacenamiento en una carpeta de mensajes especificada o el reenvío de un mensaje a otro destinatario, hasta la contestación con un mensaje a modo de acuse de recibo, previamente elaborado por el usuario. Estas operaciones son realizadas de forma automática por el programa con base a los criterios especificados por el usuario.

<sup>66</sup> No obstante, y por las consecuencias jurídicas asociadas a su elaboración, el proceso de firma digital de documentos no es realizado por los programas conocido de forma automática de la máquina. Esta y los programas de firma digital exigen siempre la previa confirmación de la operación de firma, sin perjuicio de la posibilidad de poder ser firmados “en lote” diversos documentos de una sola vez.

Ello implica distinguirlo de las plasmaciones de la realidad, consistentes en fotografías, películas, cintas de audio o video, etc. En ellas es la propia realidad la que queda plasmada en el soporte, sin que sea precisa más que una actividad de percepción sensorial para aprehenderlas por el conocimiento. En cambio, los documentos incluyen representaciones de la realidad, bien mediante la palabra o mediante gráficos o imágenes que requieren una interpretación de su contenido simbólico. No basta en ellos la mera percepción, sino que es necesario un proceso de comprensión de su significado.

Estimamos que la referencia efectuada en el art. 333 LEC a la extracción de copia de documentos que no sean escritos no impide mantener esta concepción de la representatividad del documento como medio probatorio, por cuanto dicho artículo se refiere a documentos «que no incorporen predominantemente textos escritos». La presencia del adverbio «predominantemente» refiere que el escrito ha de existir, por más que en términos de contenido no constituya la mayoría del contenido del documento. El mismo carácter representativo cabrá predicar de los dibujos, croquis, planos y mapas que requieren no sólo su percepción sino también su comprensión y cotejo con la realidad representada <sup>67</sup>.

El documento ha de ser legible, como consecuencia de la naturaleza representativa de su contenido. Nada impide que la legibilidad requiera la posesión de conocimientos del idioma empleado –lo que hará precisa la previa traducción de su contenido al lenguaje comprendido por el destinatario- o la aplicación de máquinas para interpretar los signos en que se halle elaborado. La tradicional exigencia de escritura es, por tanto, sustituida por la expresión más amplia de legibilidad, entendida como susceptibilidad de ser leído –y tan leído puede ser una palabra manuscrita como los signos en pantalla que representan, en formato electrónico, esas mismas palabras<sup>68</sup>.

---

<sup>67</sup> La sede natural de los medios que permiten grabar la imagen y sonido se halla en el art. 382 LEC, al que posteriormente aludiremos.

<sup>68</sup> Sanchís Crespo habla en estos casos de representación del contenido mediante códigos inmediatos –directamente perceptibles por los sentidos- o mediatos –que requieren el concurso de una máquina-. SANCHÍS

En cuanto al uso de encriptación, al que ya nos referimos con anterioridad, baste decir que no impide la legibilidad del documento –mediante la posesión de la autorización correspondiente manifestada en las claves privadas que permiten el descifrado- por más que se requiera de la interposición de la misma máquina que ha de leer el documento y efectuar unas operaciones adicionales de conversión de caracteres aparentemente ininteligibles en otros legibles, ordenados en virtud e un patrón existente aunque oculto.

Por último, el documento como medio probatorio ha de ser fiable en un doble sentido: ha de permitir su atribución a una persona determinada o determinable –lo que convierte al escrito o mensaje anónimo en documento-, o lo que es lo mismo, ha de poder acreditarse su autenticidad; y ha de permitir la determinación de su integridad. El empleo de las firmas sirve a los fines de acreditar la fiabilidad subjetiva del documento, pudiendo ser perfectamente sustituida, en el caso de los documentos electrónicos, por las firmas digitales en virtud de las cuales se asocia a una persona (a través de su clave privada) con un documento, pudiendo determinarse ambas condiciones mediante un sencillo procedimiento informático.

Como vemos, gran parte de los requisitos exigidos se refieren al soporte en que el documento se materializa a la vida procesal, refiriéndose a éste los caracteres del origen humano del contenido, la representatividad del mismo y la legibilidad. Con la aplicación de los mecanismos de firma digital el requisito de la fiabilidad es posible asociarlo directamente a la información y no al soporte que le sirve de base material. Por ello podemos afirmar que los documentos electrónicos firmados digitalmente pueden constituir, en igualdad de condiciones cuando no en mejor situación, documentos en el sentido exigido por la legislación procesal.

---

CRESPO, *op.cit.* págs. 49-50.

Recuérdese lo manifestado en la STS (2ª) 22 de octubre de 1998: « También el contenido de la declaración debe ser comprensible de acuerdo a los usos sociales, es decir, significativa en sí misma»

La desmaterialización del soporte, más importante desde el punto de vista de la protección penal, no es obstáculo para la consideración que se propone, por cuanto alude a un estado en que los documentos se hallan transitoriamente, durante los procesos de transmisión –donde, no obstante, son objeto de protección jurídica frente a posibles destrucciones o interceptaciones-. Aun exigiendo ferreamente la constatación del presupuesto de la corporeidad en dicha fase, cabría aludir a su existencia dentro del soporte de transmisión (el cable de fibra óptica o de cobre a través de lo que se produce la transmisión), a modo de flujo de señales, que ciertamente goza de corporeidad si bien no de la condición de aprehensibilidad.

Qué duda cabe de la existencia de diferencias entre los documentos electrónicos y los tradicionales<sup>69</sup>. Empero, la concurrencia de los requisitos establecidos permite hablar de la posibilidad de equiparar, a efectos probatorios, los documentos electrónicos a los tradicionales siempre y cuando vayan signados digitalmente con una firma electrónica avanzada. Por otra parte, el reconocimiento por la ley de los documentos electrónicos administrativos y judiciales, siempre que se cumplan los requisitos prescritos por la legislación de desarrollo aplicable a cada caso a éstos, permitirá apreciar también la condición de públicos (en sus modalidades administrativo y judicial, en función de la Administración de la que procedan) a los emitidos mediante técnicas electrónicas, informáticas o telemáticas, al concurrir en ellos los requisitos formales, subjetivos y competenciales previstos por la LEC para hablar de los mismos<sup>70</sup>. Así lo entendemos, en conjunto con la

---

<sup>69</sup> Podemos citar algunas:

- Por el soporte. Generalmente son los magnéticos citados anteriormente, (disquetes, CD-ROM, videográficos)

- Por la escritura: están escritos en “lenguaje máquina” o codificado.

- Por la firma: no llevan la firma biométrica o trazado gráfico con el cual se suscribe un documento clásico para darle autoría y virtualidad, sino firma “electrónica”.

- En el documento clásico, si va firmado por la misma persona, la firma es idéntica en todos. En los electrónicos, si una persona firma varios, se generan tantas firmas como documentos haya suscrito.

- Por la lectura: en el tradicional es suficiente la intermediación entre el hombre y el documento para conocer su contenido. En el electrónico es necesaria una máquina, generalmente un ordenador, que haga de intermediario y “lea” el documento. No es perceptible directamente.

- Por la ausencia de diferencia entre original y copia.

<sup>70</sup> Establece el art. 317 LEC: «Clases de documentos públicos. A efectos de prueba en el proceso, se consideran documentos públicos:

doctrina más reciente<sup>71</sup>. Los documentos electrónicos no avalados por una firma electrónica avanzada, por el contrario, no gozarían de la posición procesal privilegiada de los anteriores, siendo preciso su adveración o complemento con otros medios probatorios (reconocimiento judicial o prueba pericial).

## Valoración de los documentos como medios probatorios

La posibilidad de aplicación del concepto de prueba por documentos a los documentos electrónicos avalados por firmas electrónicas avanzadas traería, como inexcusable consecuencia, la aplicación de las normas probatorias establecidas por la Ley<sup>72</sup>

---

1.o Las resoluciones y diligencias de actuaciones judiciales de toda especie y los testimonios que de las mismas expidan los Secretarios Judiciales.

2.o Los autorizados por notario con arreglo a derecho.

3.o Los intervenidos por Corredores de Comercio Colegiados y las certificaciones de las operaciones en que hubiesen intervenido, expedidas por ellos con referencia al Libro Registro que deben llevar conforme a derecho.

4.o Las certificaciones que expidan los Registradores de la Propiedad y Mercantiles de los asientos registrales.

5.o Los expedidos por funcionarios públicos legalmente facultados para dar fe en lo que se refiere al ejercicio de sus funciones.

6.o Los que, con referencia a archivos y registros de órganos del Estado, de las Administraciones públicas o de otras entidades de Derecho público, sean expedidos por funcionarios facultados para dar fe de disposiciones y actuaciones de aquellos órganos, Administraciones o entidades.»

<sup>71</sup> SERRA DOMÍNGUEZ, M, *Comentarios al Código Civil y a las Compilaciones Forales*, Tomo XVI, vol. 2º, Madrid, 1991. OLIVER LALANA, A.Daniel, «La Equiparación de los efectos probatorios de los documentos electrónicos y escritos ante la futura regulación de la firma electrónica» en Revista La Ley-Actualidad nº 4804, 26 de mayo de 1999. ORMAZÁBAL SÁNCHEZ, Guillermo, *op.cit.* págs. 204-205.

<sup>72</sup> Dichas normas se hallan contenidas en los arts. 319 y 326, respectivamente dedicados a los documentos públicos y privados:

«Artículo 319. Fuerza probatoria de los documentos públicos.

1. Con los requisitos y en los casos de los artículos siguientes, los documentos públicos comprendidos en los números 1.o a 6.o del artículo 317 harán prueba plena del hecho, acto o estado de cosas que documenten, de la fecha en que se produce esa documentación y de la identidad de los fedatarios y demás personas que, en su caso, intervengan en ella.

2. La fuerza probatoria de los documentos administrativos no comprendidos en los números 5.o y 6.o del artículo 317 a los que las leyes otorguen el carácter de públicos, será la que establezcan las leyes que les reconozca tal carácter. En defecto de disposición expresa en tales leyes, los hechos, actos o estados de cosas que consten en los referidos documentos se tendrán por ciertos, a los efectos de la sentencia que se dicte, salvo que otros medios de prueba desvirtúen la certeza de lo documentado.

Hasta el momento, con la ALEC aun vigente, la situación generada por la interpretación jurisprudencial del concepto de documento ha permitido la inclusión de otros distintos a los recogidos en papel con letra o grafía escrita en el elenco de los medios probatorios establecidos por los arts. 12145 CC y 578 CC, bien a través de los documentos, bien a través de la prueba de reconocimiento judicial.

Pero la admisión en juicio por la vía documental se ha producido por aplicación de la analogía, amparada en una interpretación acorde con la realidad social y con el criterio teleológico que puede hallarse en los documentos establecidos por la ALEC., y limitada a la posibilidad de ser considerados como fuente de certeza judicial sobre los hechos debatidos. Hemos comprobado que ello también es consecuencia del derecho fundamental al empleo de los medios pertinentes de prueba, recogido en la panoplia de facultades en que consiste el derecho al proceso debido y de defensa (art. 24.2 CE). Pero en modo alguno la analogía ha significado que los documentos electrónicos se *tengan* por documentos procesales, lo que ha quedado patente en la denegación de la aplicabilidad de la fuerza probatoria privilegiada aparejada a los mismos<sup>73</sup>

Así es reflejado por SANCHÍS CRESPO y MARONDA Y TENA, quienes recogen ejemplos jurisprudenciales de esa ausencia de identidad a efectos probatorios<sup>74</sup>

---

3. En materia de usura, los tribunales resolverán en cada caso formando libremente su convicción sin vinculación a lo establecido en el apartado primero de este artículo.

Artículo 326. Fuerza probatoria de los documentos privados.1. Los documentos privados harán prueba plena en el proceso, en los términos del artículo 319, cuando su autenticidad no sea impugnada por la parte a quien perjudiquen.

2. Cuando se impugne la autenticidad de un documento privado, el que lo haya presentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto. Si del cotejo o del otro medio de prueba se desprendiere la autenticidad del documento, se procederá conforme a lo previsto en el apartado tercero del artículo 320. Cuando no se pudiese deducir su autenticidad o no se hubiere propuesto prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica.»

<sup>73</sup> Prevista en los arts. 1225 a 1230 CC.

<sup>74</sup> La STS (1ª) 25 de febrero de 1986 estima que el documento auténtico, tanto tradicional como informático, posee una fuerza probatoria supeditada a que no quede contradicha por otro medio probatorio, de lo que se deduce que tiene el mismo valor que cualquier otro medio de prueba. Por su parte, Sanchís cita la STCT de 26 de noviembre de 1985, en la que se admite el valor documental de cintas de video y su valoración «como una más de esa naturaleza por el juzgador».



Los expedientes seguidos por la jurisprudencia para conseguir tal resultado han sido, como resalta SANCHÍS<sup>75</sup> la negación tácita de aplicación de los criterios valorativos propios de los documentos y el acogimiento a la valoración conjunta de la prueba –criterio de valoración de la prueba en el proceso penal-, en virtud de la cual elude pronunciarse sobre el valor probatorio otorgado a cada medio probatorio admitido y practicado, compensando la fuerza probatoria de unos y otros.

Esta autora considera que, con este obrar, se vulnera la Recomendación R (81) 20, del Consejo de Ministros del Consejo de Europa, de 11 de diciembre de 1981, relativa a la armonización de las legislaciones en materia de admisibilidad de reproducciones de documentos y registros informáticos. En virtud de la misma el organismo internacional recomienda a todos los Estados miembros conferir la presunción de validez de los documentos o registros informáticos y electrónicos siempre que sean una reproducción y registro fiel y completo de los documentos o registros originales y de su contenido. Ello no obstante, se admitirá prueba en contrario sobre su exactitud.

Nuestra opinión es que no conviene identificar toda fuente de prueba documental con los documentos como medios probatorios. En tal sentido, sólo cabe predicar la condición de documentos probatorios de los documentos electrónicos a los que quepa atribuir los caracteres anteriormente señalados, sin perjuicio de que por carencia de vía legal adecuada sean acogidos todas las fuentes probatorias documentales a través del cauce de la prueba documental. La fuerza probatoria de dichas fuentes no podrá ser otra que la libre apreciación de las mismas, al no ser *strictu sensu* documentos. De ahí que no pueda hablarse de un incumplimiento de la Resolución mencionada, pues en puridad de conceptos no podemos hablar de documentos electrónicos equiparables a medios de prueba documentales sino cuando sean amparados en firmas electrónicas avanzadas<sup>76</sup>

---

<sup>75</sup> SANCHÍS CRESPO, *op.cit.* págs. 125-126.

<sup>76</sup> Esa es la postura que parece sostener, aunque de forma confusa, la LEC 2000.

La valoración que merecen los documentos electrónicos con arreglo a la LEC 2000 será objeto de estudio en el apartado siguiente.

#### *1.1.d) Los documentos electrónicos en la LEC 2000*

La apertura del proceso civil a las fuentes de prueba. Del numerus clausus al numerus apertus

Los problemas y disensiones doctrinales advertidos con anterioridad al amparo de la ALEC han desaparecido en la nueva Ley Rituaria. En efecto, el art. 299 establece, en tres párrafos relacionados entre sí, el nuevo elenco de medios probatorios admisibles en Derecho<sup>77</sup>:

##### «Artículo 299. Medios de prueba.

1. Los medios de prueba de que se podrá hacer uso en juicio son:

1º Interrogatorio de las partes.

2º Documentos públicos.

3º Documentos privados.

4º Dictamen de peritos.

5º Reconocimiento judicial.

6º Interrogatorio de testigos.

2. También se admitirán, conforme a lo dispuesto en esta Ley, los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que

---

<sup>77</sup> Obviamente, la determinación del elenco citado se ve acompañada de la correlativa derogación de los preceptos que regulan esta materia en el CC, realizada por la Disposición Derogatoria Única, 2.2º. No obstante, la derogación se circunscribe a los arts. 1214, 1215, 1226 y 1231 a 1253. Quedan por ello subsistentes las referencias a los documentos públicos y privados –salvo la obligación de confesión sobre la autenticidad del documento del firmante y sus causahabientes, en consonancia con la exclusión de la prueba de confesión del proceso civil-, y la regulación de los restantes medios probatorios.

permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso.

3. Cuando por cualquier otro medio no expresamente previsto en los apartados anteriores de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias.»

Ciertamente, como manifiesta el Legislador en la Exposición de Motivos de la LEC<sup>78</sup> la regulación de la prueba es una de las grandes novedades de la nueva ley. En ella se instaura una apertura a la realidad de cuanto puede ser conducente para fundar un juicio de certeza sobre las alegaciones fácticas, apertura que se declara incompatible con la existencia de un número determinado y cerrado de medios probatorios. Se aprecia de este modo una recepción del derecho constitucional a la prueba tal y como ha sido expuesto más arriba, sin limitación alguna.

No se establece ni siquiera la aplicación analógica de las normas de otros medios probatorios para la presentación y realización ante el tribunal de la prueba propuesta, si bien al ser ésta una norma prevista en el CC (art. 4.1) y no ser la norma procesal una de las incluidas en el límite previsto en el apartado 2º del mismo precepto, nada impide la aplicación de las normas sobre aportación, orden y realización previstos para los restantes medios, o la combinación de éstas.

La incorporación de nuevos medios probatorios. En especial, los instrumentos que permiten archivar, conocer y reproducir datos, palabras o cifras

#### 1.1.d.1) El iter legislativo del artículo

---

<sup>78</sup> Empleamos la versión publicada como suplemento por el BIMJ el 15 de Enero de 2000.

La Exposición de Motivos de la LEC 2000 alude a estos medios como un ejemplo de la apertura a la realidad de las fuentes probatorias, que sin duda es recogido con individualidad por su reconocimiento legal y cotidiano en el tráfico jurídico y económico.

El reconocimiento de estos nuevos medios probatorios no estuvo en la mente inicial del legislador. Si comparamos el texto del Anteproyecto de LEC<sup>79</sup> con el finalmente aprobado podemos observar cómo las novedades en cuanto a medios probatorios se ceñía a la admisión de los medios de reproducción de la palabra, el sonido y la imagen (art. 351.2), no entendiéndose porqué eran excluidos del listado de medios probatorios admisibles en juicio<sup>80</sup>.

Por otra parte, si bien se recogía en el apartado 3º una previsión parecida a la redacción actual del art. 299.3<sup>81</sup> *-numerus apertus* de medios probatorios-, la referencia exclusiva a los medios del artículo anterior limitaba su alcance, al establecer como elemento de comparación a los medios audiovisuales. Parece que el propósito pudo ser admitir por una vía indirecta los nuevos medios informáticos con valor probatorio más que establecer un *numerus apertus* probatorio; de hecho, una novedad de tal magnitud en relación con la ley precedente hubiera sido puesta de manifiesto en la Exposición de Motivos, a la que no se alude en absoluto<sup>82</sup>. Esta interpretación puede ampararse también en la parca referencia a los medios electrónicos, informáticos y telemáticos –a pesar de estar ya vigente la reforma de la LOPJ operada por la LO 16/1994, que admitía su empleo en todo tipo de procesos-, a los que únicamente se cita como «medios técnicos» al referirse el art. 159 a la remisión de comunicaciones procesales.

---

<sup>79</sup> Publicado en suplemento del BIMJ, diciembre 1997.

<sup>80</sup> Quizá el propósito fuera resaltar su condición de novedad en cuanto a regulación probatoria frente a los clásicos medios citados en el apartado precedente.

<sup>81</sup> Art. 351.3 Anteproyecto LEC 2000: «Cuando por cualquier otro medio no expresamente previsto en el apartado anterior de este artículo pudiera obtenerse certeza sobre hechos relevantes, el tribunal, a instancia de parte, lo admitirá como prueba, adoptando las medidas que en cada caso resulten necesarias.»

<sup>82</sup> Pág. 13.

El Anteproyecto suscitó un rechazo unánime en la doctrina y en los informes del CGPJ, como pone de relieve SANCHÍS CRESPO<sup>83</sup>, que consideró que la concepción del legislador «se aproxima a un planteamiento doctrinal clásico, que puede estimarse superado por la realidad normativa y social»; razón por la que instaba a revisar el texto «para acomodar esta concepción a una época en la que la transcripción en papel de pensamientos, ideas, informes, registros, contratos, etc... está siendo progresivamente sustituida por la generalización de las herramientas informáticas, el soporte electrónico y los medios audiovisuales».

El planteamiento de partida fue corregido en el Proyecto aprobado por el Consejo de Ministros en su sesión de 30 de octubre de 1998<sup>84</sup>, adoptando la redacción que hoy conocemos<sup>85</sup>, e introduciendo las correspondientes reformas en el articulado relativas al empleo de medios informáticos por la Administración de Justicia y por los particulares.

#### 1.1.d.2) Los medios e instrumentos del art. 299.2 LEC

El nuevo medio probatorio reconocido en el precepto citado engloba en su seno a los conocidos medios audiovisuales y a los medios informáticos. Ambos son objeto de una regulación básica en los arts. 382 y 383 los primeros, y 384 los medios informáticos. Decimos «básica» porque, como pone de relieve ORMAZÁBAL<sup>86</sup>, el legislador ha previsto la regulación mínima sobre la base de la analogía que estos medios mantienen con las pruebas documentales, a que se hace referencia en la propia Exposición de Motivos, debiendo remitirse el aplicador a los preceptos relativos a este tipo de prueba para hallar su completo estatuto<sup>87</sup>. Y ello como

---

<sup>83</sup> SANCHÍS CRESPO, Carolina, «El soporte informático de escritura como prueba en el proceso penal» en *Estudios Jurídicos del Ministerio Fiscal VIII*, Madrid, 1998, pág. 653.

<sup>84</sup> Publicado en BIMJ como suplemento al núm. 1832 el 1 de noviembre de 1998.

<sup>85</sup> Pueden compararse las págs. 2803-2806 del Proyecto y las 49-52 de la Ley.

<sup>86</sup> ORMAZÁBAL SÁNCHEZ, Guillermo, *Los prueba documental y los medios...op.cit.* págs. 170 y 176.

<sup>87</sup> Así, encontramos referencias a estos medios en el art. 265.2, relativo al momento de aportación al

medida de cautela ante la variedad de medios probatorios que pueden acogerse a su abrigo, imposibles de una previa y detallada regulación procesal que, más que facilitar su realización, dificultaría su régimen probatorio por virtud del inexorable avance tecnológico al que se verán sin duda sometidos.

Dado el carácter no representativo, sino plasmativo, de los medios citados en el primer inciso del art. 299.2 –luego desarrollado en el art. 382-, que los excluye de la consideración de documento de acuerdo con lo mantenido hasta el momento<sup>88</sup>, nos centraremos en los medios regulados en el art. 384 LEC.

No obstante, con ORMAZÁBAL<sup>89</sup>, debe matizarse que también mediante soportes informáticos pueden recogerse palabras, imágenes o sonidos. Serán incluidos, como medios de reproducción, cuando las palabras, imágenes o sonidos sean contemplados desde su perspectiva plasmativa de la realidad, y no en su dimensión representativa o simbólica; pues en tales casos los medios informáticos sólo aportan su capacidad de almacenamiento como un soporte magnético más, y no permiten –por su mero empleo- atribuir condición documental a lo que no es sino objeto de reconocimiento judicial o de este nuevo medio.

En cuanto se refiere a la regulación de los medios informáticos, cabe sintetizarla en los siguientes aspectos:

- a) La proposición de los instrumentos deberá realizar al tiempo de interponer la demanda, acompañándola en su presentación ante el Juzgado, de acuerdo con lo dispuesto en el art. 269.2 LEC.
- b) La aportación se realizará ante el Secretario del Juzgado, sin perjuicio de que, al tiempo de dictarse sentencia, deban ser examinados

---

proceso; 289.2 y 3, sobre forma de practicarse la prueba; y 300, relativo al orden de práctica

<sup>88</sup> Y que también es propósito del legislador, que precisamente introduce esta modalidad probatoria para evitar forzar el concepto tradicional de prueba documental para incluir en él lo que se aporte al proceso con fines de fijación de la certeza de los hechos, que no sea subsumible en los restantes medios de prueba (E.M., pág. 51)

<sup>89</sup> ORMAZÁBAL, *ibid.* pág. 182

directamente por el tribunal (art. 289.3). La prueba no es preciso que sea realizada en la vista oral, tal y como se desprende del apartado 1º del citado artículo, donde se prevé la reproducción de las cifras y datos «en su caso»

- c) A diferencia de lo previsto en el art. 382.1, en el caso de aportarse instrumentos que permiten conocer datos y cifras no se recoge en la ley la obligación de aportar copias de los mismos. Parece que esta ausencia no es sino un error del precepto, dado que en el mismo se alude a necesidad de que sean reproducidos mediante los medios aportados a instancia de parte o de oficio con el fin de que las partes «con idéntico conocimiento que el tribunal» alegue y proponga lo que a su derecho convenga. Si, de una parte la alegación de pruebas en que se funde la pretensión ha de hacerse en el momento inicial con vistas a que la demandada tenga conocimiento, desde el primer momento, de los términos de la litis<sup>90</sup>; si la reproducción tiene por objeto que las partes puedan proponer y alegar «con idéntico conocimiento que el tribunal»; y si, por último, de acuerdo con el art. 279 «las pretensiones de las partes se deducirán en vista de las copias de los escritos, de los documentos y de las resoluciones del tribunal, que cada litigante habrá de conservar en su poder», documentos de los que sólo podrá tener copia, pues nunca se entregarán los autos originales (apartado 2º), no queda otro remedio que considerar que en estos supuestos habrá de proporcionarse una copia del instrumento aportado a fin de preservar el derecho de defensa del contrario.
- d) Los instrumentos podrán ser acompañados de los dictámenes y medios de prueba instrumentales oportunos para advenir, o para impugnar, la autenticidad y exactitud de los aportados. Parece que en estos casos se producirá la realización de la prueba ante el tribunal, de conformidad con la posibilidad prevista en el art. 289.1, dado que ante éste tendrá que practicarse la prueba complementaria si consiste en informes periciales o testificales.

---

<sup>90</sup> Exposición de Motivos, pág. 49.

- e) También habrán de aportarse los instrumentos o medios de reproducción (máquinas o programas) en caso de que el tribunal no goce de ellos. Ello afectará a la legibilidad del instrumento, dado que, por los avances de la técnica, los datos o cifras pueden haber sido registrados mediante programas ya en desuso o de difícil empleo.
- f) La prueba será valorada de acuerdo con las reglas de la sana crítica. Se someten al principio valorativo general, alejándose de este modo de las normas probatorias aplicables a los documentos (arts. 319 y 326), a pesar de su similitud ontológica en algunos casos. La norma es cautelosa con el empleo de estos medios, todavía no frecuentes en nuestros foros, sometidos a un proceso vertiginoso de evolución tecnológica que hace tambalear hoy lo que fue un bastión inexpugnable hace días. No obstante, como pone de relieve ORMAZÁBAL<sup>91</sup> si ciertos procedimientos de autenticación adquieren predicamento en la comunidad científica y técnica, difícilmente dejarán los órganos judiciales de darles crédito y de tener por probados los hechos así acreditados.
- g) La documentación de la prueba se hará de la forma más adecuada a la naturaleza del instrumento (art. 384.3.inciso II). Parece adecuado la aplicación a este supuesto de lo dispuesto en el art. 383 para los medios de reproducción de la palabra y del sonido o imagen, levantándose acta por el Secretario donde se hará constar todo lo preciso para la identificación de los medios probatorios empleados, así como de las justificaciones y dictámenes aportados y de las pruebas practicadas.
- h) Este contenido tendrá que ser complementado con lo que establecen los arts. 146.2 y 147, sobre documentación de las actuaciones judiciales, sobre todo en caso de que hayan de celebrarse en vista oral –como se deduce del art. 289.1 si hay que practicar prueba complementaria-.

---

<sup>91</sup> ORMAZÁBAL SÁNCHEZ, Guillermo, « La prueba mediante documento digitalmente firmado» en *Actualidad Civil* n° 8, *marginal XI*, Madrid, 1999, pág. 231.



- i) Por último, el art. 384 hace referencia a la custodia de los medios por el Tribunal

1.1.d.3) La recepción y equiparación de los documentos electrónicos *strictu sensu* o cualificados, con los documentos tradicionales

Si bajo la vigencia de la ALEC el problema con que se encontraban los documentos electrónicos era si podían ser admitidos al proceso como medios probatorios por alguno de los cauces previstos en el art. 578, la nueva LEC plantea el problema opuesto, a saber, a través de qué medio probatorio tendrá cabida el documento electrónico.

Ya hemos señalado anteriormente que los documentos electrónicos amparados en una firma electrónica avanzada –la que permite asociar un documento a una persona mediante su clave privada o dato de creación de la firma- gozan de todos los caracteres exigidos por la doctrina para ser considerados documentos a efectos probatorios, como pruebas documentales.

La aparición de un nuevo medio probatorio específicamente constituido para no forzar el concepto tradicional de prueba documental –según reza la Exposición de Motivos en su apartado X- parece dar al traste con la equiparación hasta ahora intentada con los documentos públicos y privados. Así se desprende también para ORMAZÁBAL<sup>92</sup>, quien únicamente considera aplicables *analógicamente* las normas de valoración de los documentos a los instrumentos consistentes en documentos electrónicos firmados digitalmente. El recurso a la analogía supone la negación de base de otra condición para estos instrumentos que la de medio probatorio ex art. 384.

---

<sup>92</sup> ORMAZÁBAL SÁNCHEZ, Guillermo, *La prueba documental...op.cit.* págs. 202-ss.

SANCHÍS CRESPO también parece aceptar, aunque de forma crítica, la subsunción de los documentos electrónicos en la categoría de «instrumentos que permiten archivar, conocer o reproducir datos, cifras...», echando en falta un cierto valor en el legislador para aceptar los logros proporcionados por la tecnología y la ciencia hoy día<sup>93</sup>.

Nuestra opinión difiere de la de estos autores. De la propia dicción de la LEC parecen desprenderse argumentos para predicar la asimilación del documento electrónico cualificado por el empleo de firma digital en las categorías de documentos públicos o privados:

La LEC incluyó, tras la tramitación parlamentaria del Proyecto legislativo de 1998, un inciso en el art. 327 relativo a los Libros de comerciantes, incluidos entre los documentos privados, que complementaba lo recogido en el correlativo art. 328 del Proyecto. El precepto aprobado establece « Cuando hayan de utilizarse como medio de prueba los libros de los comerciantes se estará a lo dispuesto en las leyes mercantiles. De manera motivada, y con carácter excepcional, el tribunal podrá reclamar que se presenten ante él los libros *o su soporte informático*, [las cursivas son nuestras] siempre que se especifiquen los asientos que deben ser examinados.». La presentación de los documentos, aun en formato electrónico, no impedirá que sea considerado como documento privado. De haber querido eludir dicha equiparación con los documentos privados tradicionales hubiera bastado la referencia a los medios del art. 384.1, que también pueden consistir en «cifras y operaciones matemáticas llevadas a cabo con fines contables...»<sup>94</sup>

---

<sup>93</sup> SANCHÍS CRESPO, *La prueba por soportes...op.cit.* pág. 164.

<sup>94</sup> La legislación registral permite la presentación telemática de las cuentas anuales ante los Registros Mercantiles, así como la legalización de los mismos en los Registros Mercantiles mediante igual procedimiento de presentación, siempre que se hallen firmados con firma electrónica avanzada, en los términos previstos por el RD-Ley 14/1999 de 17 de septiembre, de firma electrónica. Así lo autorizan las Instrucciones de la DGRN de 26 de mayo, 12 de noviembre y 31 de diciembre de 1999. Véase un estudio pormenorizado de las mismas en ALAMILLO DOMINGO, Ignacio, «La firma electrónica y los Registros» en Revista Electrónica de Derecho Informático, <http://www.redi.org>

El art. 812.1 permite presentar, para acudir al proceso monitorio, «documentos, cualquier que sea su forma y clase o el soporte físico en que se encuentren, que aparezcan firmados por el deudor o con su sello, impronta o marca o con cualquier otra señal, física o electrónica, proveniente del deudor» [las cursivas son nuestras]. Supone el máximo y más explícito exponente del reconocimiento de los documentos electrónicos, pues sólo en los mismos cabe hablar de huellas o marcas electrónicas. Por esta vía tendrán expedita el acceso al proceso todas aquellas reclamaciones derivadas del comercio electrónico, siempre que no excedan de 5.000.000 pts. y no se oponga expresamente el deudor, en cuyo caso se sustanciará de acuerdo con las reglas del procedimiento que corresponda según la cuantía (art. 818.1).

Por último, los conceptos de documento público sostenidos por la LEC. En la Exposición de Motivos se hace referencia al fundamento de la fuerza probatoria de los mismos, así como el papel que corresponde en su definición a las normas reguladoras de éstos<sup>95</sup>. Estas normas, que no son otras que los arts. 45.5 LRJPAC y 230.2 LOPJ, permiten la existencia, con plena validez y eficacia de documento original, a los elaborados con medios electrónicos, informáticos y telemáticos, siempre que cumplan los requisitos de autenticidad, integridad, conservación y los establecidos por las respectivas normas. Como hemos estudiado en extenso, estos requisitos se ven cumplimentados mediante la utilización de la firma electrónica avanzada por el titular del órgano, tal y como reconoce la Resolución de la DGRN de 26 de mayo de 2000; por lo que carecerá de sentido reconocer procesalmente el valor integrador –para la determinación de los medios probatorios documentales- de las normas de origen administrativas o judiciales para después negarles tal condición por el hecho de constar en soporte electrónico.

---

<sup>95</sup> Exposición de Motivos, XI, pág. 50: «Los documentos públicos, desde el punto de vista procesal civil, han sido siempre y deben seguir siendo aquéllos a los que cabe y conviene atribuir una clara y determinada fuerza a la hora del referido juicio fáctico. Documentos privados, en cambio, son los que, en sí mismos, no gozan de esa fuerza fundamentadora de la certeza procesal y, por ello, salvo que su autenticidad sea reconocida por los sujetos a quienes puedan perjudicar, quedan sujetos a la valoración libre o conforme a las reglas de la sana crítica. La específica fuerza probatoria de los documentos públicos deriva de la confianza depositada en la intervención de distintos fedatarios legalmente autorizados o habilitados. La ley procesal ha de hacerse eco, a sus específicos efectos y con lenguaje inteligible, de tal intervención, pero no es la sede normativa en que se han de establecer los requisitos, el ámbito competencial y otros factores de la dación de fe»

Estos argumentos legales, unidos al hecho de que los documentos electrónicos cualificados por el empleo de la firma electrónica avanzada satisfacen los requisitos exigidos doctrinal y jurisprudencialmente a los documentos como prueba, nos hacen sostener que se producirá la incorporación al proceso de éstos a través de los artículos relativos a los documentos públicos y privados, en tanto que todos los documentos electrónicos no firmados con firma electrónica avanzada deberán hacerlo a través del art. 384, debiendo en su caso ser objeto de las correspondientes pruebas complementarias que aseguren su exactitud y autenticidad.

No obstante, cabe decir que no bastará con que el documento se halle firmado con una firma electrónica avanzada, sino que ésta deberá revestir los caracteres indicados en el art. 3.1.I del RD-Ley 14/1999; esto es, que el certificado reconocido en que se base sea emitido por un prestador de servicios de certificación acreditado y que el dispositivo de creación de la firma se halle acreditado mediante la homologación pertinente efectuada de acuerdo con las normas técnicas publicadas en el DOCE o en el BOE, de conformidad con el procedimiento previsto a tal fin en el RD-Ley.

#### *1.1.e) Los documentos electrónicos en el proceso penal*

##### 1.1.e.1) Su consideración como objeto del delito y como medios probatorios.

Hemos podido comprobar que el documento electrónico no es una realidad ajena a nuestro Derecho. Sin perjuicio de las complicaciones derivadas de la falta de preceptos de naturaleza procesal que permitieran hablar del reconocimiento explícito de éstos como medios probatorios, la jurisprudencia allanó el terreno haciendo de la cuestión un problema de naturaleza meramente académica.

El artículo 26 CP despejó, desde el punto de vista penal, las dudas acerca de la capacidad de los nuevos soportes informáticos para llenar las necesidades de tipicidad penal de los preceptos de la Parte Especial, acogiendo en el seno de su

regulación un concepto más amplio que el derivado de la aplicación supletoria del CC por virtud de su art. 4.3<sup>96</sup>. Los documentos electrónicos en que concurren los requisitos establecidos en la jurisprudencia –STS 22 de octubre de 1998, analizada al principio del capítulo, con las matizaciones realizadas al mismo- serán aportados al proceso como piezas de convicción, sin deber exigírsele más requisitos para su admisión..

No obstante, como quiera que la LECr no dispone de normas propias sobre los medios probatorios documentales –aparte de las que reseñaremos a continuación-, habrá de acudir a la regulación examinada de la LEC en virtud del art. 4 de ésta, que determina su aplicación supletoria a los procesos penales en todo lo no dispuesto por aquella. Habrá que exigirle, por ello, a todo documento electrónico o soporte informático aportado distinto del objeto del delito los mismos requisitos que la naturaleza del medio probatorio en que se constituya exija. De este modo, y en coherencia con lo mantenido hasta el momento, los documentos electrónicos públicos o privados cualificados por su firma digital serán tenidos por prueba documental; los soportes de grabación de imagen, sonido o palabras –aun de naturaleza informática, siempre que su uso lo sea para recoger plasmaciones de la realidad- por los medios previstos en el art. 382; y los soportes y documentos electrónicos que no puedan equipararse a pruebas documentales –documentos de ordenador, bases de datos, programas, etc- tendrán su cabida a través del medio regulado en el art. 384 LEC.

La aparición de la LEC supone, por ello, una reordenación de los medios probatorios, en virtud de la cual cada uno de ellos queda regido por su propio procedimiento probatorio. En tal sentido, las referencias a los videos, cintas magnetofónicas y soportes informáticos realizadas por los Tribunales en sus

---

<sup>96</sup> «Conforme a la fórmula legal, lo que caracteriza al documento no es el soporte, que puede ser cualquier cosa, ...«*todo soporte*», dice la regla. Por lo tanto deben darse por zanjadas las polémicas entre los que creían que solamente tenía carácter de documento lo que como tal fuera admitido por el derecho procesal, y los que sostenían que la condición documental depende de otros factores, y no sólo de su aceptación por las leyes de procedimiento» (QUINTERO OLIVARES, Gonzalo, *Comentarios al Nuevo Código Penal*, Pamplona, 1996, págs. 294-295)

decisiones orientadas a la prueba documental han de entenderse ahora canalizadas hacia los medios regulados ex novo por los arts. 299.2 y 3, y 382 a 384 LEC.<sup>97</sup>

Habremos eso sí, que examinar los específicos y escasos preceptos que la LECr dedica a la prueba documental, para excluir de ese modo la aplicación de las normas concurrentes de la LEC.

#### 1.1.e.2) Pruebas documentales y pruebas documentadas

Una diferencia derivada del art. 741 LECr es la de pruebas documentales y pruebas documentadas.

El art. 741 establece que «El Tribunal, apreciando, según su conciencia las pruebas practicadas en juicio, las razones expuestas por la acusación y la defensa y lo manifestado por los mismos procesados, dictará sentencia dentro del término fijado por la ley»

La Exposición de Motivos de la LEC hace referencia a esta distinción en su apartado XI cuando expresa que «No habrá de forzarse la noción de prueba documental para incluir en ella lo que se aporte al proceso con fines de fijación de la certeza de los hechos que no sea subsumible en las nociones de los restantes medios de prueba. Podrán confeccionarse y aportarse dictámenes e informes escritos, con sólo apariencia de documentos, pero de índole pericial o testifical ...».

La existencia de las pruebas documentadas es consecuencia de la necesidad de documentación de las actuaciones judiciales, tal y como previene el art. 229.1

---

<sup>97</sup> De hecho, con la regulación supletoria de la LEC relativa a este tipo de medios probatorios tiene cobertura lo que no era sino consecuencia de la práctica señalada jurisprudencialmente, a saber, la necesidad de practicar o complementar dichos documentos con dictámenes periciales y declaraciones testificales que acrediten su exactitud e integridad (STS 2ª 353/1996, de 3 de abril), de acuerdo con lo previsto en el art. 382.2 LEC.

LOPJ<sup>98</sup>. El delito, como hecho histórico, requiere una intervención inmediata para poder recoger cuantos vestigios sirvan al esclarecimiento de los hechos. De ahí que la LECr articule normas para la intervención inmediata de la Policía Judicial, como auxiliares del Juez, encaminada a la captación de cuantos elementos de prueba puedan servir al esclarecimiento de los hechos, haciéndose especial hincapié en la celeridad con que han de realizarse estas diligencias (art. 786 LECr). La distancia temporal que puede producirse entre el momento del acopio de los vestigios y el del enjuiciamiento; la perdurabilidad temporal de algunos de ellos, unido a la necesidad de realización de contrapruebas por aplicación del derecho constitucional de defensa (que incluye, no olvidemos, el de uso de los medios de prueba pertinentes), exige la documentación de todas las actuaciones de investigación, a las que no cabrá dar más valor que el de material preparatorio de lo que posteriormente constituirá la prueba en sí.

La consecuencia que se desprende del precepto, unánimemente aceptada por Doctrina y jurisprudencia, es la exclusión del carácter de prueba de lo practicado con anterioridad al juicio oral. Dicho material sólo podrá ser considerado preparatorio de la vista oral<sup>99</sup>. Como señala SANCHÍS CRESPO<sup>100</sup>, «los actos de investigación se orientan a descubrir datos, a proporcionar los elementos necesarios para que puedan hacerse las afirmaciones posteriores de hechos. A su lado, los actos de prueba son netamente distintos, ya que son actividades procesales por las que se

---

<sup>98</sup> Art. 229.1 LOPJ: «Las actuaciones judiciales serán predominantemente orales, sobre todo en materia criminal, sin perjuicio de su documentación».

La inspección ocular del lugar del delito constará por escrito: art. 332. La del cuerpo del delito se documentará de forma detallada por el instructor: art. 335, 337, 340; a la que se añadirán los análisis e informes periciales precisos: arts. 343, 355, 359. Las diligencias de reconocimiento del delincuente se harán constar igualmente de forma escrita: art. 369. Las declaraciones del imputado serán documentadas, conforme se desprende de los arts. 393, 396, 397, 401 a 404. Las declaraciones testificales durante el sumario se harán constar por escrito, como se desprende de los arts. 428, 437, 443 a 445 y 714. En relación a los careos, art. 453. Respecto de la pericial, art. 478.

Con respecto a los nuevos medios de reproducción previstos en el art. 299.2 LEC, a falta de regulación paralela en la LECr, se estará a lo dispuesto en los arts. 146.2, 147 y 383.

<sup>99</sup> Claramente se refiere a este papel del sumario el art. 299, cuando establece que «Constituyen el sumario las actuaciones encaminadas a preparar el juicio y practicadas para averiguar y hacer constar la perpetración de los delitos con todas las circunstancias que puedan influir en su calificación, y la culpabilidad de los delincuentes...»

<sup>100</sup> SANCHÍS CRESPO, Carolina, «El soporte informático de escritura...» *op. cit.* pág. 645.

tiende a alcanzar el convencimiento psicológico del juzgador sobre la existencia o inexistencia de afirmaciones de hechos que han sido aportados al proceso».

El criterio de distinción es aplicado legalmente por la legislación del procedimiento del Tribunal de Jurado<sup>101</sup>, en cuyo art. 34.1, al regular los testimonios que han de acompañar al auto de apertura de juicio oral, se incluyen «b) La documentación de las diligencias no reproducibles y que hayan de ser ratificadas en el juicio oral.». Dichos testimonios no incluyen, obviamente, los efectos, instrumentos del delito ocupados y demás piezas de convicción, a los que dedica el apartado siguiente.. El legislador, en la Exposición de Motivos de la LO 5/1995, manifestó su deseo de erradicar la costumbre de sobrevaloración de las diligencias documentadas, para lo que vetó radicalmente la aportación de las mismas<sup>102</sup>.

No obstante, y como pone de relieve la doctrina<sup>103</sup>, el valor del sumario no queda totalmente excluido, pues tendrá presencia mediata a través de los testimonios que las partes podrán solicitar en cualquier momento, de acuerdo con el art. 34.3 LOTJ. Estos podrán ser empleados como elementos de contraste, como ya autorizaba el art. 714 LECr., en el interrogatorio de acusados, testigos y peritos, cuando aprecien contradicciones en sus declaraciones sumariales y las realizadas en la vista oral. Dichas manifestaciones sumariales no podrán ser leídas, si bien su contenido, mediante los testimonios citados, acompañarán al acta (art. 46.5); acta de la que, por otra parte, será entregada copia a cada jurado, por lo que no podrá negarse de

---

<sup>101</sup> L.O. 5/1995, de 22 de mayo, del Tribunal de Jurado.

<sup>102</sup> En el Apartado III.1 de la Exposición de Motivos de la LO 5/1995 se encuentra la primera referencia directa al tema: «Se quejaba Alonso Martínez de la costumbre, tan arraigada de nuestro Jueces y Tribunales, de dar escaso o ningún valor a las pruebas del plenario, buscando principal o casi exclusivamente la verdad en las diligencias sumariales practicadas a espaldas del acusado. La presente Ley concibe que el juicio oral ante el Tribunal del Jurado, debe culminar la erradicación de esa malformación procesal mediante la práctica ante él de toda la prueba.». La alusión es complementada, de forma más clara y directa, con lo expuesto en el apartado III.3: «De otra, la exclusión de la presencia, incluso física, del sumario en el juicio oral evita indeseables confusiones de fuentes cognoscitivas atendibles, contribuyendo así a orientar sobre el alcance y la finalidad de la práctica probatoria a realizar en el debate. La oralidad, intermediación y publicidad en la prueba que ha de derogar la presunción de inocencia lleva en la Ley a incidir en una de las cuestiones que más polémica ha suscitado, cual es la del valor probatorio dado a las diligencias sumariales o previas al juicio y que se veta en el texto del mismo.»

<sup>103</sup> AAVV: *Ley de Enjuiciamiento Criminal y Ley del Jurado*, Madrid, Colex 1996, pág. 652.



la forma pretendida el valor de las diligencias de investigación a través de este tortuoso vericuetto procedimental.

Por otra parte, como pone de manifiesto la Circular 4/1995 de la Fiscalía General del Estado «sobre el Proceso ante el Tribunal del Jurado: Las actuaciones en el Juzgado de Instrucción», el examen de las diligencias sumariales también se hará preciso para la adopción de otras decisiones durante el juicio oral, como la libertad o prisión, el control de la eventual conformidad (art. 50), la declaración de pertinencia o no de las pruebas (art.37.d); y resolución sobre muchas previas cuestiones previstas en el art. 36. «EL Magistrado-Presidente, llamado por la Ley a decidir sobre esos puntos, no podrá hacerlo en la mayoría de las ocasiones sino poder examinar las actuaciones realizadas durante la fase de investigación. El sentido común impone permitir al Magistrado-Presidente reclamar al Instructor testimonios distintos de los específicamente previstos en el art. 34.1, sin perjuicio de los que las partes puedan presentar (art. 34.1) al evacuar cualquier petición.»

La naturaleza documentada de muchas de las pericias que será preciso aportar junto con los medios informáticos que se propongan como pruebas hará preciso tener en consideración los preceptos reseñados. Los soportes magnéticos, programas y demás objetos relacionados con la comisión de los hechos, no obstante, no se verán afectados por esta regla de aportación indirecta, al exigir la LOTJ su remisión directa al Tribunal junto con los testimonios precedentes (art.34.3).

#### 1.1.e.3) La reproducción de diligencias sumariales por aplicación del art. 730

##### LECr

Lo que se acaba de exponer encuentra una excepción en el art. 730 LECr., en cuya virtud “Podrán también leerse a instancia de cualquiera de las partes las diligencias practicadas en el sumario, que, por causas independiente de la voluntad de aquellas, no puedan ser reproducidas en el juicio oral»

Este precepto, como excepción al régimen de inmediación, concentración, publicidad y contradicción propio del proceso penal y a lo expresamente determinado en el art. 741 LECr sobre lo que constituye la base probatorio en que se ha de basar el Tribunal para dictar sentencia, debe ser interpretado restrictivamente. Las diligencias sumariales pueden ser practicadas sin la presencia del inculpado y de su defensa si se ha decretado secreto sumarial (art. 302.2 LECr). La valoración por esta vía de material probatorio puede conculcar las garantías esenciales del derecho al proceso debido (art. 24.2 CE).

Deben ser puestos de manifiesto los siguientes extremos en orden a la comprensión de su estricto sentido:

Las diligencias que pueden ser objeto de lectura son únicamente las practicadas por el Instructor, excluyéndose los actos de investigación policial (STS 24 de febrero de 1997).

La imposibilidad de reproducción en juicio ha de ser sobrevenida y ajena a la voluntad de la parte proponente. De haberse podido prever, ésta debería acudir a la petición de prueba anticipada al tiempo de formular su escrito de conclusiones provisionales; lo que se aplica tanto a las pruebas periciales como testificales<sup>104</sup>

Las pruebas periciales consistentes en informes técnicos basados en conocimientos muy especializados podrán ser considerados directamente por el Tribunal, en atención a su condición de muy difícil o imposible reproducción, por la vía de los arts. 726 y 730 LECr, si cuentan con constancia documental en autos que permita su valoración y contradicción en juicio, sin que en tal supuesto sea absolutamente imprescindible la presencia en dicho acto de quienes lo emitieron para su interrogatorio personal (STC 127/1990, de 5 de julio). No obstante, parece razonable que, pudiendo preverse en estos casos –pericias sobre delitos informáticos o

---

<sup>104</sup> El art. 657.3 LECr establece que «Podrán pedir además las partes que se practiquen desde luego aquellas diligencias de prueba que por cualquier causa fuere de temer que no se puedan practicar en el juicio oral, o que pudieren motivar su suspensión»

relacionados con los nuevos medios informáticos- la razonable imposibilidad de reproducción en juicio, sean desarrolladas como pruebas anticipadas las pericias que tengan por objeto acreditar los hechos cometidos con base en el art. 657.3.<sup>105</sup>

Será precisa pedir su expresa lectura, sin que baste la fórmula del foro de «por reproducida». La finalidad de tal petición es traer al plenario el material o contenido del acto sumarial, permitiendo así su conocimiento por las partes y por el Tribunal y la posibilidad de contraargumentar y alegar lo que convenga (STS 628/1995, de 4 de mayo).

El Ministerio Fiscal deberá identificar por el número de folio o localización en autos las diligencias sumariales de que pretenda valerse como pruebas documentadas reproducibles y solicitar su expresa reproducción en los supuestos del art. 730 , sin que pueda ampararse en la fórmula rituarial antedicha<sup>106</sup>

El precepto jugará una especial importancia en los fenómenos de criminalidad informática o en los que se hallen envueltos documentos electrónicos. Las pericias serán precisas no sólo para acreditar el hecho cometido (análisis de ficheros registro de conexiones telemáticas, del contenido de soportes magnéticos ...) sino también para la adveración de los documentos presentados (por ejemplo, para acreditar la condición de seguros de los dispositivos de creación de una firma electrónica avanzada, que permitirá tener al documento electrónico por prueba documental).

---

<sup>105</sup> A pesar de lo expuesto, la realidad cotidiana, la constatación de la cualificación técnica de algunas oficinas y organismos oficiales permiten conferir a los informes por ellos emitidos un valor de prueba pericial o cuasipericial exenta de ratificación personal, siempre que por la otra parte no sea propuesta pericia de contradicción. Así, SSTC 127/1990, de 5 de julio, 24/1991, de 11 de febrero y 11 de marzo de 1991. El Tribunal Supremo, en STS 14 de marzo de 1994, basa la validez de estos informes no sólo en la cualificación técnica pública de los organismos oficiales –nunca de los privados-, sino también «en la actitud pasiva de la parte a quien perjudican dichos dictámenes o informes y no insta su contradicción, bien proponiendo su ratificación en juicio, o bien articulando prueba en contrario»

<sup>106</sup> Instrucción de la FGE de 27 de febrero de 1989, «A propósito de la Sentencia del Tribunal Europeo de Derechos Humanos de 6 de diciembre de 1988» (caso Barerá, Messegué y Jabardó).

#### 1.1.e.4) La apreciación de oficio de los libros, documentos, papeles y demás piezas de convicción

La Legislación penal y procesal se refiere a los efectos e instrumentos del delito de forma diferenciada a las restantes pruebas. El art 127 CP se refiere a aquellos para establecer su comiso, salvo pertenencia a tercero de buena fe no responsable del delito que los haya adquirido legalmente. La jurisprudencia ha entendido por efectos del delito todos los bienes o cosas que se encuentran, mediata o inmediatamente, en poder del delincuente como consecuencia de la infracción, aunque sea el objeto de la acción típica (STS 1304/1994, de 21 de junio). Los documentos electrónicos sobre los que recaiga la acción delictiva o que hayan servido para su comisión (programas a los que se refieren los arts 270.3 y 400), o que acrediten su comisión y le sean intervenidos accederán al proceso en tal calidad, quedando sometidos al régimen de aportación de oficio<sup>107</sup>

La LECr distingue la condición de piezas de convicción o efectos del delito de la prueba documental, si bien todos ellos podrán ser libremente apreciados por el juzgador<sup>108</sup> (art. 726 LECr)., en cuya virtud «El Tribunal examinará por sí mismo los libros, documentos, papeles y demás piezas de convicción que puedan contribuir al esclarecimiento de los hechos o a la más segura investigación de la verdad».

Así, las partes tienen la obligación de manifestar en sus escritos de conclusiones provisionales las pruebas de que intenten valerse (art. 656.1 LECr). Se constituye

---

<sup>107</sup> El art. 334 LECr ordena al Instructor «recoger en los primeros momentos las armas, instrumentos o efectos de cualquier clase que pudieran tener relación con el delito y que se hallen en el lugar en que éste se cometió, o en sus proximidades, o en poder del reo, o en otra parte conocida.».

Para ello podrá ordenar la entrada y registro de cualquier domicilio, público o privado, en busca de efectos o instrumentos del delito, o libros, papeles u otros objetos que puedan servir para su descubrimiento y comprobación (art. 546 LECr).

A tal fin, la Policía Judicial podrá secuestrar los efectos citados hasta tanto llegue la Autoridad Judicial, siempre que exista peligro de que no haciéndolo pudieran desaparecer algunas pruebas de los hechos ocurridos (art. 785.1.a) LECr).

<sup>108</sup> La misma facultad es concedida a los miembros del Jurado por el art. 46.2: «Los jurados verán por sí los libros, documentos, papeles y demás piezas de convicción a que se refiere el artículo 726 de la Ley de Enjuiciamiento Criminal».

por ello en el momento preclusivo para su aportación, sin que les sea admisible la aportación posterior de nuevos medios probatorios. En el caso del procedimiento abreviado, las partes no obstante podrán proponer prueba en el mismo acto de la vista oral, siempre que pudiera practicarse en el acto (art. 793.2), debiendo abrirse un turno de intervenciones sobre su admisión o no, resolviéndose por el juzgador en ese mismo acto. En este supuesto no cabe hablar de preclusión probatoria, aunque ha de advertirse que puede esconder una práctica destinada a mermar los derechos de contradicción, al poder sorprender al contrario con nuevos elementos probatorios de los que no se tenía conocimiento, y que –como en el caso de los delitos informáticos o en los que se hallen implicados documentos o piezas de convicción de tal naturaleza- no puedan ser objeto de la adecuada ponderación en ese breve acto.

Las piezas de convicción y efectos del delito, por su parte, son remitidos de oficio por el Instructor al órgano de enjuiciamiento (art. 622.1 LECr); son colocadas en el local del Tribunal (art. 688.1) y son apreciadas libremente por el Tribunal (art. 726).

En relación con la aparente obligación de presencia física de las piezas ante el órgano de enjuiciamiento que parece imponer el art. 688.1, la jurisprudencia ha tenido ocasión de matizar que no constituye un vicio *in procedendo* (por todas, STS 18 de septiembre de 1990). No obstante, será motivo de casación por denegación de prueba si concurren los siguientes requisitos, sintetizados por RODRÍGUEZ FERNÁNDEZ<sup>109</sup>:

- a) Que las piezas de convicción estén incorporadas a la causa
- b) Que exista una petición de parte en su escrito de conclusiones provisionales para completar otras pruebas personales
- c) Denuncia en el plenario de la parte proponente, haciendo constar la protesta procedente así como los argumentos que justifican la

---

<sup>109</sup> RODRÍGUEZ FERNÁNDEZ, Ricardo, *Ley de Enjuiciamiento Criminal*, Granada, 1998, pág. 476

necesidad de la presencia de la pieza (para posibilitar el juicio de pertinencia del medio propuesto)

- d) Necesidad de la prueba, en el sentido de que, si hubiera sido presentada ante el Tribunal, el fallo pudiera haber sido distinto, careciendo de efectos impugnativos cuando por las restantes pruebas practicadas sobre los mismos hechos quedaran acreditados los extremos de que se trate (STS 21 de marzo de 1994).

Como puede apreciarse, si bien la aportación al proceso no requiere del impulso de la parte, su consideración como medio probatorio sí que precisará de la expresa petición, cual otra documental más, en los escritos de conclusiones. Con ello se consigue un tratamiento análogo al de la prueba documental, de la que sólo se diferencia por la relación con el objeto material del delito.

#### 1.1.e.5) Valoración de los documentos electrónicos en el proceso penal

A diferencia de lo que ocurre en el proceso civil, donde los medios probatorios documentales gozan de una posición probatoria privilegiada en relación a los restantes medios, en el proceso penal rige el principio de apreciación en conciencia de las pruebas practicadas, de acuerdo con el art. 741 LECr inciso 1º. Como reza la STS (2ª) de 3 de octubre de 1997, «En materia de valoración de pruebas, ha de partirse del indiscutible principio de que dicha función es competencia propia y exclusiva del juzgador, según viene establecido normativa y jurisprudencialmente»

El significado del precepto analizado puede estructurarse en los siguientes aspectos<sup>110</sup>:

---

<sup>110</sup> Seguimos la reseña jurisprudencial contenida en el comentario al art. 741 LECr efectuados en AAVV, *Ley de Enjuiciamiento Criminal*, Pamplona, 1999, pág. 683-ss.

- a) La estimación «en conciencia» no supone actuación o razonamiento arbitrario, fuera de toda lógica, en donde se dé pie a lo meramente impalpable o inaprehensible<sup>111</sup>, sino una apreciación lógica de la prueba no exenta de pautas y directrices de rango objetivo<sup>112</sup>. Ello permitiría valorar, con relación a una firma electrónica, los criterios y presunciones establecidos a favor de las firmas electrónicas avanzadas cualificadas en el art. 3.1.2 de la RD-Ley 14/1999 sobre firma electrónica. O apreciar el grado técnico y seguridad ofrecida por un método de firma alternativo, amparado en el empleo de pruebas periciales de corroboración.
- b) La ley no confiere ninguna prioridad probatoria a ningún medio, a diferencia de lo que sucede en la LEC. Por ello, la distinción allí elaborada entre documentos electrónicos con firma electrónica avanzada cualificada o sin ella, a los efectos de conferirles valor probatorio privilegiado, carece de interés penal, siendo todos valorados en igualdad de condiciones; algo a lo que, como ya se dijo, venía siendo aplicado por los Tribunales que admitían su validez como medios de prueba.
- c) El artículo exige que la apreciación probatoria recaiga sobre las pruebas practicadas en juicio. Implica tácitamente que éstas han de haber sido desarrolladas con pleno cumplimiento de las garantías previstas para cada una de ellas en la Ley Rituaria<sup>113</sup>
- d) La valoración se predica del conjunto de medios probatorios, razón por la que no puede alegarse la presunción de inocencia para debatir cada episodio, vicisitud, hecho o elemento debatido en el proceso penal o parcialmente integrante de la resolución judicial que le ponga término.<sup>114</sup>

---

<sup>111</sup> STS 12 de julio de 1990.

<sup>112</sup> STS 10 de abril de 1997.

<sup>113</sup> STS 12 de julio de 1990.

<sup>114</sup> STC 44/1989, de 20 de febrero.

- e) Al admitirse la valoración en conciencia del material probatorio, el juicio realizado está exento de control casacional o por vía de apelación, salvo los supuestos previstos en el art. 849.2 LECr.

En este último aspecto conviene que retomemos la diferencia entre pruebas documentales y pruebas documentadas. La LECr admite la interposición de recurso de casación «Cuando haya existido error en la apreciación de la prueba, basado en documentos que obren en autos, que demuestren la equivocación del juzgador sin resultar contradichos por otros elementos probatorios» (art. 849.2). De la doctrina jurisprudencial cabe establecer dos criterios para diferenciar el concepto de documento manejado en este artículo, en relación al art. 26 CP o la amplitud probatoria auspiciada por el principio de libertad probatoria:

Los documentos casacionales deen haberse producido fuera del proceso, lo que excluye cualquier acto de documentación de pruebas o de diligencias sumariales, como las ya examinadas<sup>115</sup>

Los documentos que se refiere el art. 849.2 son los estrictamente considerados por las normas procesales, esto es, «un instrumento formal con valor probatorio preconstituido o producido fuera de la causa y aportado a ella y que haga fe no sólo del acto a que se refiere, fecha, intervinientes y fedatario o certificante, sino también certeza de su contenido. Tales como los enumerados en los arts. 1216 a 1230 CC – on las limitaciones y valor probatorio que señala para cada uno d eellos- y las certificaciones expedidas por los funcionarios públicos que están autorizados para ello, en lo que se refiere al ejercicio de sus funciones y en cuanto al conocimiento de su competencia objetiva»<sup>116</sup>

Al exigir la interpretación exegética el sometimiento a los criterios diferenciadores entre documento y demás medios probatorios análogos, excluyendo expresamente

---

<sup>115</sup> Por todas, STS 20 de octubre de 1997.

<sup>116</sup> STS 28 de abril de 1989.



el sentido ampliatorio del concepto actual de documento, vuelve a cobrar vigencia, a efectos casacionales, entre documentos electrónicos amparados en firma digital y los restantes, puesto que –como no dejamos de manifestar- éstos serán equiparables a aquellos en virtud de sus mecanismos de protección tanto de su contenido como de su autor.

## **1.2.) La firma electrónica**

### **1.2.a) Introducción**

Al hablar del documento electrónico se hizo referencia a dos aspectos que van casi inseparables: la firma electrónica y la criptografía. Es tiempo de dedicarnos por extenso a su análisis.

La firma electrónica y la criptografía solucionan dos problemas esenciales en el documento electrónico que le aquejan: la confidencialidad y la autenticidad. Como veremos, los esfuerzos técnicos y legislativos –tanto a nivel nacional como supranacional– pivotan sobre esos dos puntos de manera casi esencial. La mayoría de los documentos en que se incorpora un pensamiento o una declaración de voluntad requieren que vayan suscritos o asumidos por su autor, y ello se lleva a cabo mediante la firma, entendiendo por tal un «trazado gráfico, conteniendo 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»<sup>117</sup>

MENDIVIL, en similares términos, manifiesta que «El problema de la autenticidad en un documento tradicional se soluciona mediante la firma autógrafa. Mediante ella, un individuo, o varios, manifiestan su voluntad de reconocer el contenido de un documento, y en su caso, a cumplir con los compromisos que el documento

---

<sup>117</sup> COUTURE, citado por ROUANET MOSCARDO en «Valor Probatorio Procesal del Documento Electrónico», *op. cit.* pag. 170.

establezca para con el individuo»<sup>118</sup>. Ambos problemas, el de la confidencialidad y el de la autenticidad, «se resuelven mediante la tecnología llamada «Criptografía». La criptografía es una rama de las matemáticas, que al aplicarse a mensajes digitales, proporcionan las herramientas idóneas para solucionar los problemas antes mencionados. Al problema de la confidencialidad se le relaciona comúnmente con técnicas denominadas de “encriptación” y el problema de la autenticidad mediante técnicas denominadas de «firma digital», aunque ambos en realidad se reducen a procedimientos criptográficos de encriptación y des- encriptación»<sup>119</sup>

Y trasladado al campo de la contratación cobra especial relieve. Históricamente estuvo vinculada a la palabra como medio de expresión de la voluntad, «a través de la cual se producía la manifestación del consentimiento. Posteriormente se dió paso al papel como soporte de la documentación contractual (contratos, facturas, documentos de giro, etc). Esta constancia documental en soporte papel ha llegado a tener no solo eficacia meramente probatoria, sino que en muchos casos ha sido elemento constitutivo de la perfección de determinados contratos -ad solemnitatem-»

120

Si tenemos en cuenta la certeza que demanda el tráfico jurídico mercantil en las transacciones económicas, y sobre todo en la llamada «contratación electrónica», a través de la telemática y de las redes como Internet, se desprende fácilmente la importancia de la firma en estos documentos y el apresuramiento de los Gobiernos para establecer los cauces legales.

Así, se forma lo que podríamos denominar un trípode casi inseparable: documento electrónico-firma digital-criptografía.

---

<sup>118</sup> MENDIVIL, Ignacio, *El ABC de los Documentos Electrónicos*. Disponible en <http://www.seguridata.com/labcintro.htm>

<sup>119</sup> MENDIVIL, *op. cit.* pag. 2

120 DIAZ FRAILE, Juan Maria, «Estudio de la Regulación de la Firma Electronica en la Directiva Europea de 13 de mayo de 1998» (I), en *Revista “La Ley”*. Año XIX Núm.. 4677, pag. 2

### 1.2.b) Concepto y características

ORMAZÁBAL describe la firma electrónica como «ciertos procedimientos mediante los que alguien encripta un mensaje informático utilizando una clave privada que sólo él conoce, lo envía a su receptor a través de la red y da a conocer a éste una clave pública mediante la cual dicho receptor desencripta el mensaje y puede constatar que aquél sólo pudo ser encriptado por quien poseía dicha clave privada. De este modo el receptor puede comprobar la identidad del emisor y la autenticidad del mensaje. En este sistema resulta esencial la intervención de una tercer persona de confianza (en el caso alemán las denominadas «entidades de certificación», sometidas a aprobación e inspección administrativa), que certifican que la clave pública corresponde a quien afirma ser su titular»<sup>121</sup>

Se basa, pues, en lo que se denomina «criptografía de claves asimétricas», como veremos mas adelante, que permite el descifrado con una clave de lo que lo ha sido previamente con la clave ligada matemáticamente a ella.

DÍAZ FRAILE establece unos requisitos, que si bien van referidos al ámbito de la contratación, son extensivos a todo documento:

- a) Asegurar que aquel con quien se contrato es realmente quien dice ser (*autenticación*)
- b) que el mensaje no ha sido modificado o alterado en su contenido (*integridad*)
- c) Que nadie, no autorizado, lo lee o accede al mismo. (*Confidencialidad*)
- d) que no podrá ser rechazado, una vez aceptado, salvo pacto de retractación o desistimiento (*no repudiación*)<sup>122</sup>

---

<sup>121</sup> Citado por DIAZ FRAILE, op. cit. pag 3

<sup>122</sup> DIAZ FRAILE, op. cit. pag 4

Hay que destacar que a diferencia de la firma autógrafa, si dos documentos son diferentes, entonces la firma digital es diferente. En otras palabras, la firma digital cambia de documento a documento, si un sujeto firma dos documentos diferentes producirá dos documentos firmados diferentes. Mientras la autógrafa es la misma, con idénticos o similares trazos, la digital es distinta en cada documento, ya que va asociada al documento y se forma con una combinación del documento en si.

Todo lo anterior se puede sintetizar de la siguiente manera: Si un documento firmado es autenticado con una determinado llave o clave publica, puede afirmarse que fue firmado con la correspondiente llave o clave privada.

A diferencia de la autógrafa, que es una biometría y efectivamente prueba el acto personal de la firma, la firma digital solo prueba que se utilizó la clave privada del sujeto y no necesariamente el acto personal del firmado. La consecuencia es que no es posible hacer manifestar de forma irrefutable que una persona firmó un documento. En realidad lo que hay que probar es que el sujeto es el responsable de que el documento ha sido firmado con su clave privada.

Otra diferencia importante es la validez. Mientras la autógrafa nos acompaña permanentemente, la digital es perdurable, teniendo una validez de fecha a fecha, incluso de momento a momento.

Inmediatamente surgen dos cuestiones:

- Garantías en orden a la autoría de la firma o clave.
- Si ha mediado tiempo desde que se emitió el documento, su validez.

Para establecer las garantías en orden a la autoría y pertenencia de la firma surgen las llamadas «entidades de certificación», autoridad certificadora, etc...; básicamente

son entidades, públicas o privadas, que registran y almacenan la clave pública de una persona, al tiempo que certifica que le pertenece y es suya. Una vez comprobada la pertenencia, emiten un certificado. Para ello las legislaciones rodean de requisitos a estos servicios de certificación. Así la Directiva Europea de 1999 que posteriormente analizaremos exige, entre las más destacadas:

- a) demostrar la fiabilidad necesaria para prestar servicios;
- b) utilizar un servicio de revocación rápido y seguro;
- c) comprobar debidamente la identidad y capacidad de obrar de la persona a que se expide un certificado reconocido;
- d) contar con personal con experiencia y la cualificación técnica necesaria;
- e) utilizar sistemas dignos de confianza y productos de firma electrónica que garanticen la protección toda alteración;
- f) tomar las medidas contra falsificación de certificados.

Respecto al tiempo de validez, por norma general las firmas electrónicas tienen un periodo –dado que a dicho periodo va asociada la responsabilidad de la entidad certificadora–, pudiendo revocarse anticipadamente. Tiene su importancia sobre todo en las relaciones comerciales, careciendo de validez aquellos documentos firmados con una clave expirada. Cobra relieve en aquellos supuestos en que se emitió siendo válido el certificado y se recibe el documento con una firma expirada.

Igualmente han de contar con un servicio de «revocaciones», para caso de pérdida de la clave privada o sospechas de uso no autorizado por terceras personas. Al igual que deben poseer relaciones de certificados válidos, deben contar con listas de claves revocadas.

Los certificados pueden adoptar múltiples formas. El formato más difundido está definido por la norma ITU- X.509.V.3

Son escasas las resoluciones judiciales sobre la firma electrónica, a pesar de tener vida propia en nuestro ordenamiento desde 1995. Ello indica la fiabilidad práctica que ha generado su uso, que no hace necesario el recurso a la acción legal de impugnación.. No obstante, es de destacar la STS (1ª) de 3 de noviembre de 1997 (Ref. Aranzadi 1997(8251). Con un admirable sentido de la actualidad, la sentencia que citamos expresó las siguientes características sobre la firma digital y su valor en el tráfico jurídico:

«La firma es el trazado gráfico, conteniendo 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 orografía, 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, al igual que en el caso de los documentos comunes, 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 alfa-numéricos que permitan asegurar la procedencia y veracidad de su autoría y la autenticidad de su contenido»

### 1.2.c) Regulación

Antes de iniciar el examen de la regulación comunitaria y nacional conviene realizar un breve panorama de la legislación aprobada o en estudio en otros países sobre la firma digital.

#### 1.2.c.1) En Derecho Comparado

##### USA

Como refiere CUERVO ÁLVAREZ <sup>123</sup> varias fueron las normas precedentes a la Ley de Utah de firma digital. No se referían a la firma o documentos electrónicos, sino al empleo de programas de cifrado. Desde los años setenta venía siendo empleado el denominado Data Encryption Standard (DES) para el cifrado de información sensible en la Administración americana. En 1993 comenzó el proceso de renovación y sustitución del algoritmo DES por otro, pero el procedimiento tuvo que suspenderse ante las iniciativas del Gobierno de aprovechar la revisión para imponer la política denominada «Key Escrow» (depósito de claves), en virtud de la que las agencias de inteligencia del Gobierno podrían acceder a los mensajes cifrados con el algoritmo skipjack. Una de las formas de lograr este propósito fue el intento de imponer el

---

<sup>123</sup> CUERVO ÁLVAREZ, José, «La firma digital y entidades de certificación», en *Revista Informática y Derecho* n° 30-32; Mérida 1999, págs. 244-246.

«Clipper chip», procesadores empleados para el cifrado de la información que incorporaban una «backdoor» o puerta trasera, que permitiera a las Agencias de Seguridad poder acceder a los mensajes codificados. Tras un proceso de renovación retomado en enero de 1997, en el verano de 2000 se adoptó como nuevo estándar americano de encriptación (AES, American Encryption Estándar) el algoritmo Rijndael.

Por su importancia e influencia en las legislaciones estatales norteamericanas deben citarse las Digital Signatures Guidelines, de 1 de agosto de 1996, emitidas por la American Bar Association.

El Estado de Utah fue el primero a nivel internacional en regular la firma electrónica, en la llamada “Utah Digital Signature Act” , de 27 de febrero de 1995, modificada en 1996 (Utah, Code §§ 46-3-101 to 46-3-104 a 46-3-504).

Dada su extensión, tecnicismo e innovación legislativa, ha servido de modelo a otras que se han promulgado posteriormente o que se hallan en elaboración . Trata tanto de la firma electrónica como del documento firmado digitalmente y establece la equiparación con la manuscrita cuando:

- a) esté respaldada por una autoridad de certificación reconocida
- b) concorra un elemento intencional o volitivo: voluntad de signatario de firmar digitalmente
- c) buena fe del destinatario.

La Ley Utah pretende ser complementada por la Act of Electronic Notarization, de 1997.

Italia



La legislación italiana sobre firma electrónica está basada en la Legge 15 marzo 1997 n° 59, titulada «Autorità per l'informatica nella pubblica amministrazione. Schema di regolamento concernente: "Atti, documenti e contratti in forma elettronica". Su art. 15.2 establece, al modo del art. 45.2 LRJPAC española, la validez de los documentos formados por la Administración Pública y por los ciudadanos con instrumentos informáticos y telemáticos, al igual que los contratos estipulados en la misma forma.

Por Decreto del Pte. de la República de 10 de noviembre de 1997, núm.513 se aprobó el «Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n. 59», que complementa dicha ley. Consta de 22 artículos. En el segundo establece las definiciones, en número de 15. Así por firma digital, el art. 1 establece: «per firma digitale, il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici»

Se ocupa del Registro de las claves, de las entidades de certificación, revocaciones, documento electrónico y escrito, remitiendo a la eficacia probatoria de los documentos a las normas del Código Civil. Equipara la firma digital a la manuscrita.

Dos elementos son de interés en esta regulación. Por una parte, el art. 10.IV establece que «la adición de firma digital integra y sustituye, a cualquier fin previsto por la normativa vigente, la adición de sellos, estampas, timbres, contraseñas y marcas de cualquier género». Esta regla supone la asunción correcta de la inteligencia de lo que comporta el empleo de técnicas informáticas de autenticación de documentos electrónicos. Su empleo hace innecesario requisitos formales pensados para soportes alterables o falsificables, algo que no puede predicarse de un documento electrónico, que es autónomo del soporte –pues es la propia

información la que es objeto de protección directa, no el soporte que le sirve de base material—. Similar criterio ha sido adoptados registralmente por la Resolución Circular de la DGRN española de 26 de abril de 2000 <sup>124</sup>.

El otro lo constituye el reconocimiento de los documentos públicos electrónicos, al establecer su art. 16.I que «se tiene por reconocida, en el sentido del art. 2703 CC, la firma digital cuya adición es autenticada por el notario u otro oficial público autorizado». Similar es el criterio que se desprende de la Resolución de la DGRN antes citada para el ordenamiento español, con la importante consecuencia de deber obtener el mismo tratamiento de prueba documental regulada por el art. 317.2 LEC que el resto de documentos notariales.

#### Alemania

El borrador del Proyecto de Ley de Firma digital «On the basis of § 16 of the Digital Signature Act of 22 July 1997 (Federal Law Gazette I S.1870, 1872)» de 1997, consta de 16 artículos, siguiendo las directrices de la Directiva Europea y la “Digital Act” de Utah.

El art. 2º, que se ocupa de las definiciones dispone en el apartado 1 «Una firma digital dentro del significado de esta ley es un sello creado con una clave privada de firma sobre información digital, tal sello permite, mediante el uso de la clave pública asociada rotulada por un certificado de clave de un certificador, o de una Autoridad según el art. 3, que sean verificados el propietario de la clave de firma y el carácter de no falsificado de la información»

---

<sup>124</sup> Establece el apartado V.3º : «Distinto es también el caso de los requisitos meramente formales a que queda sujeto la creación del instrumento público. [...] El hecho de que la autenticidad de la escritura pública puede ser asegurada mediante mecanismos distintos, basados en las nuevas tecnologías, hacen que el conjunto de tales requisitos formales deban ser interpretados de acuerdo con su finalidad de forma subordinada a su necesaria compatibilidad con la nueva regulación de la firma electrónica, de manera tal que, quedando garantizada la finalidad de asegurar la autenticidad del documento por otras vías, no cabe que tales formalidades se erijan en obstáculo insalvable para el empleo de la firma electrónica en el ámbito notarial. En la medida de su incompatibilidad –y a la espera de su adecuación normativa– han de entenderse derogados los correspondientes preceptos reglamentarios con relación a los documentos públicos electrónicos, como consecuencia de la entrada en vigor del Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.»

Al igual que la italiana, regula los registros, los Servicios de Certificación, requisitos que deben reunir, aunque no otorga equiparación con la firma manuscrita.

#### Otras experiencias

La más importante que debe ser mencionada es la Ley Modelo sobre Aspectos Jurídicos del Comercio Electrónico, aprobada por el Pleno de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI-UNCITRAL) el 14 de junio de 1996 (Resolución 51/162 de 16 de diciembre de 1996).

También merecen mención las Guidelines for Cryptography Policy, de 27 de marzo de 1997, de la OCDE. En ellas se establecen una serie de recomendaciones del organismo internacional para la cooperación y el desarrollo a la hora de legislar sobre firma digital y criptografía en los Estados miembros.

Por último, y como destaca CUERVO ÁLVAREZ <sup>125</sup>, en el plano técnico de la normalización hay que reseñar la Norma ISO/IEC-7498-2 (Arquitectura de Seguridad de OSI), que regula los aspectos y servicios de seguridad, integridad, confidencialidad, integridad, autenticidad, control de accesos y no repudio en sistemas informáticos.

#### 1.2.c.2) En Derecho comunitario

Tras un prolongado debate en el seno de las instituciones comunitarias el 13 de diciembre de 1999 fue aprobada la Directiva 1999/93/CE, por el que se establece el marco comunitario para la firma electrónica <sup>126</sup>.

---

<sup>125</sup> CUERVO ÁLVAREZ, José, *op.cit.* pág. 256.

<sup>126</sup> Esquemáticamente podemos resumir el iter legislativo de la siguiente manera:

## Fines y principios de la Directiva 1999/93/CE, de 13 de diciembre

Los propósitos sostenidos por la Directiva son:

- a) lograr el reconocimiento legal de las firmas electrónicas, mediante el reconocimiento de efectos jurídicos y probatorios a todas, con independencia de la tecnología en que se basen (art.1.1).
- b) A diferencia de lo mantenido en las propuesta inicial, que sostenía el criterio definido por la Digital Signature Act 1995 del Estado de Utah (EEUU), no se establecen presunciones de equiparación por la concurrencia de determinados requisitos, dado que con ello sólo lograrían reconocimiento de efectos legales las firmas electrónicas que los verificaran, siendo el propósito de la Directiva no pronunciarse por ningún sistema, dejando la puerta abierta a posibles avances tecnológicos en este campo <sup>127</sup>
- c) Propiciar la libre circulación de productos y servicios relacionados con la firma electrónica (Considerandos 5 y 7, este último relativo a la incidencia en el principio de libre circulación de personas). Para ello evita someter a autorizaciones previas la prestaciones de servicios de certificación o asociados (Considerando 10 y art. 3.1) y

---

13/06/1998	Aprobación de la Propuesta de la Comisión COM (98)297final
13/01/1999	Procedimiento de 1ª lectura en el Parlamento Europeo
29/94/1999	Proposición Enmendada de la Comisión COM(99)195final
28/06/1999	Posición Común del Consejo 28/1999
Octubre 1999	Procedimiento de 2ª lectura en el Parlamento Europeo
13/12/1999	Aprobación de la Directiva 1999/93/CE
2001	Fecha límite de transposición de la Directiva
2003	Fecha de la primera revisión de la Directiva

Fuente: servidor web DGXV, <http://www.europa.eu.int/en/comm/dg15.html>

<sup>127</sup> A pesar de lo cual las definiciones que contiene sobre datos de creación y verificación de firma sí supone la aceptación íntegra de la tecnología hoy día preponderante en esta materia, cual es la de cifrado asimétrico.

elimina los obstáculos a la libre circulación de estos productos mediante el establecimiento de un régimen de equiparación (art. 7.1).

- d) Trata cuestiones conexas inescindibles, como lo son el tratamiento automatizado de datos derivado de estos servicios, para lo que remite a la Directiva 1995/46/CE (Considerando 24 y art. 8); y determinados aspectos del mercado global, como es el reconocimiento mutuo de certificados emitidos en países ajenos a la Unión (Considerando 23 y art. 7.2)

Hay que tener en cuenta que la legislación comunitaria sobre firma digital no se limita a lo establecido en esta Directiva. El empleo de medios criptográficos de alta seguridad obliga a considerar el Tratado de Wasenaar, así como los restantes acuerdos internacionales sobre tecnología de doble uso, debido al interés de la Defensa y Seguridad Nacional en este tipo de productos <sup>128</sup>. También ha de prestarse atención al Quinto Programa Marco sobre Investigación y Desarrollo (I+D), así como a los logros que se consigan en el ámbito de la autorregulación, por la que la Comisión apuesta decididamente <sup>129</sup>

Los principios subyacentes en la Directiva son:

- a) Neutralidad en cuanto a la tecnología y a las soluciones legales de implementación que cada país adopte.
- b) No discriminación de ninguna de las modalidades de firma electrónica, certificados, prestadores de servicios y sistemas de acreditación que se empleen.

---

<sup>128</sup> Véase más adelante cómo el legislador español, al amparo de la regulación de los ficheros de datos personales mantenidos por la FNMT en el ejercicio de sus funciones como prestador de servicios de certificación, ha hecho uso de la facultad prevista en el art. 52.2 de la LGT, conocida como «key escrow» o política de almacenamiento de claves privadas de cifrado.

<sup>129</sup> El empleo de esta técnica regulatoria, de autonomía privada, ha dado algunos buenos resultados en EEUU, donde las ABA (American Bar Association) Digital Sign Guidelines son consideradas como un estándar para el mercado de productos de certificación.

- c) Respeto a la libertad contractual y a la autonomía de las partes, no regulándose los posibles sistemas de firma establecidos entre particulares (Considerando 16 y art. 5.2) <sup>130</sup>
- d) Respeto, y por ello no armonización, de las legislaciones nacionales civiles, para lo que expresamente se excluye de su ámbito «otros aspectos relacionados con la celebración y validez de los contratos u otras obligaciones cuando existan requisitos de forma establecidos en las legislaciones nacionales o comunitaria, ni afectan a las normas y límites contenidos en las legislaciones nacionales y comunitarias que rigen el uso de documentos» (art.1.2.) <sup>131</sup>

Las posibilidades de firmas electrónicas, en función de su tecnología y del tipo de certificado que las acompañe, son las siguientes:

- a) Firmas electrónicas. No son discriminadas, prohibiéndose negarles efectos jurídicos y su admisibilidad como prueba en juicio (art. 5.2)
- b) Firmas electrónicas basadas en certificados reconocidos. Se aplica el principio anterior.
- c) Firmas electrónicas basadas en certificados no reconocidos. Se aplica el principio anterior.
- d) Firmas electrónicas avanzadas. Se aplica el principio anterior.
- e) Firmas electrónicas avanzadas basadas en certificados no reconocidos. Se aplica el principio anterior.
- f) Firmas electrónicas avanzadas que cumplen los requisitos establecidos en los Anexos I a III. Son objeto de equiparación

---

<sup>130</sup> El Considerando 16 manifiesta que «no se debe privar a las firmas electrónicas utilizadas en estos sistemas de eficacia jurídica ni de su carácter de prueba en los procedimientos judiciales»

<sup>131</sup> A diferencia de lo que sí hace la DSA Utah 1995, al establecer los requisitos para la validez de las firmas electrónicas y de los documentos electrónicos con ellos firmados.

a las firmas manuscritas en relación a los documentos a los que se incorporen

- g) Firmas en el Sector Público. Sin pronunciarse sobre el tipo de firma a emplear, la Directiva permite la imposición de condiciones suplementarias de validez por las legislaciones nacionales, siempre que con ello no se discrimine a los nacionales de otros Estados de la Comunidad.

### Régimen legal de la firma electrónica en la Directiva

El contenido de la Directiva se ocupa de precisar el marco mínimo de regulación nacional de las firmas electrónicas –fundamentalmente, su valor jurídico-, de los productos de firma electrónica, y de los proveedores de servicios de certificación.

La firma electrónica es definida en el art. 2.1 como «los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizado como medio de autenticación». Como puede apreciarse, la admisión de la firma electrónica supone *de facto* la admisión de los documentos electrónicos, dado que no puede existir sin ellos <sup>132</sup>.

La forma de la firma también merece algún comentario.

En primer lugar, ésta constituye un conjunto de datos en forma electrónica que, o bien forman parte del mismo documento signado («anejos a otros datos electrónicos») o bien están enlazados a ellos por un procedimiento informático (enlace entre el fichero en que está el documento firmado y el que recoge los datos de la firma).

---

<sup>132</sup> No obstante, la Directiva es muy cuidadosa en no penetrar en terrenos relativos a la forma de los contratos, de la prueba y su valoración judicial, ni de la admisión en determinados sectores normativos nacionales de los documentos y de las firmas electrónicas (véanse especialmente los Considerando 17 y 21, así como el art. 1.2).

En segundo término, dichos datos pueden revestir cualquier modalidad, no necesariamente han de basarse en la técnica criptográfica simétrica (con empleo de una misma clave para cifrar o descifrar) o asimétrica (una clave sirve para firmar y otra para verificar la firma). Lo único que se nos dice es que sirve como medio de autenticación, es decir, de identificación de sus autor. El empleo de una firma electrónica podía ser simplemente la huella digital o cualquier otro dato biométrico humano digitalizado. La falta de asociación al documento de dichos datos de creación de firma impide garantizar mediante este mecanismo la integridad del documento. La integridad no es un resultado conseguido con la firma electrónica simple u ordinaria; para ello es preciso una firma electrónica avanzada.

La Directiva también define la firma electrónica avanzada, modalidad cualificada de la anterior, en el art.2.2 como «la firma electrónica que cumple los requisitos siguientes:

- 1) estar vinculada al firmante de manera única
- 2) permitir la identificación del firmante
- 3) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control
- 4) estar vinculado a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable.»

La firma definida de forma descriptiva logra dos propósitos: la identificación de su autor, y la integridad del documento firmado. El primero de los propósitos exige, a su vez, dos condiciones: a) que los datos estén vinculados al mismo de forma única; y b) que el firmante los pueda tener bajo su exclusivo control. Puesto que la técnica de firma y la tecnología criptográficamente que le sirve de base ya han sido explicadas –y con ello cómo la firma se asocia al documento y garantiza su integridad- nos ocuparemos de describir las consecuencias derivadas de los requisitos de identificación del usuario firmante según la definición comunitaria.



El sistema de identificación se basa en la sustitución de un dato biométrico de una persona (su firma, producto de sus características físicas y psicológicas, las que permiten asociarla a una persona en concreto con exclusión de otras) por un conjunto de datos. A semejanza de lo que sucede en la vida real, en el que las firmas manuscritas son únicas como las huellas digitales, las firmas electrónicas – generadas mediante programas o «dispositivos de creación de firmas»<sup>133</sup> han de ser igualmente únicas, lo que se consigue mediante la exigencia a los programas o dispositivos de creación de firmas de que la generación de los datos de creación y verificación de firmas sean únicos y razonablemente secretos (Anexo III.1.a) ). Este es un requisito tecnológico de la firma, que controla la parte ajena a las posibilidades de control del usuario<sup>134</sup>. Pero, para garantizar que *jurídicamente* y no sólo *informáticamente* la firma sea única, se exige también que dicha clave esté bajo el exclusivo control del firmante, de modo que nadie pueda sustraérsela. A este objetivo se refiere el Considerando 18 cuando manifiesta que «El almacenamiento y la copia de los datos de creación de forma pueden poner en peligro la validez jurídica de la firma electrónica». Cualquier práctica de almacenamiento de claves, por más que pueda constituirse en un servicio añadido a prestar por las empresas del sector, puede cuestionar la validez y el no repudio del documento firmado con dichas claves<sup>135</sup>

---

<sup>133</sup> La Directiva los define como «programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma» (art. 2.5).

<sup>134</sup> El firmante no tiene que realizar nada para generar su clave de firma. En algunos programas, como el popular PGP (Pretty Good Privacy), se le pide que genere aleatoriamente una cadena de caracteres (mediante pulsaciones libres del teclado). Lo único que ha de hacer es proteger el acceso al mismo mediante una password o palabra clave o contraseña para poder hacer uso de él.

<sup>135</sup> Uno de los requisitos exigidos al proveedor de servicio que expide certificados reconocidos es, precisamente, el de «no almacenar ni copiar los datos de creación de firma de la persona a la que el proveedor de servicios de certificación ha prestado servicios de gestión de claves».

Como solución legal al problema de la pérdida de las claves privadas o datos de creación de firma se prevé la figura de la «guía de usuarios» al que se refiere el Considerando 9, más conocida como servicios de directorio. Los directorios de certificados incluyen atributos y contenido complementario de los certificados emitidos, y son mantenidos por las propias empresas certificadoras. En ellos se pueden hacer constar los períodos de validez de los certificados, las incidencias que les afectan y los límites de uso. Si bien no son citados expresamente por la Directiva, su existencia se deduce del art. 6.2, donde se habla de la responsabilidad del prestador de servicios de certificación «por no haber registrado la revocación del certificado», lo que supone la existencia de algún servicio de acceso público donde pueda consultarse tal eventualidad. Como figura intermedia de la revocación puede hablarse de la suspensión del certificado, que implica la carencia temporal de efectos de un certificado, sin necesidad de volver a generarse posteriormente el mismo. Con servicios así no se hace preciso el almacenamiento de las claves o datos de creación de firma.

Ello no obstante, no debe confundirse este servicio con el de almacenamiento de las claves de cifrado, empleadas no para firmar, sino para cifrar los contenidos. El cifrado garantiza la confidencialidad; y, aunque

Evidentemente, este proceso de sustitución de un dato biométrico como la firma manuscrita por un conjunto de datos electrónicos, por más que el programa con que sean generados garantice su unicidad física y su secreto, sólo puede proporcionarlo la intervención de una persona o entidad que certifica la asociación de esos datos a una persona en concreto. Para ello las firmas se acompañan de los denominados certificados digitales, que no son sino otro conjunto de datos electrónicos anejos a una firma o asociados lógicamente a ella que permite identificar al titular de los datos de verificación de firma (o clave pública) <sup>136</sup>. Si el certificado reúne determinada información y es proporcionado por una entidad física o jurídica que cumple unos requisitos organizativos y técnicos de los que permita deducirse la seguridad y confianza de sus servicios, el certificado adquiere la condición de certificado «reconocido» <sup>137</sup>

La existencia de un certificado, reconocido o no, asociado a una firma electrónica no es atributo exclusivo de la firma electrónica en ninguna de sus modalidades, simple o avanzada. Pueden existir sin necesidad de certificados, y cumplirán sus funciones de identificación la primera, y de identificación y de garante de la integridad de lo firmado la segunda. Pero sólo el empleo de la firma electrónica avanzada basada en un certificado reconocido puede satisfacer las necesidades de la firma manuscrita. Por ello sólo a este tipo de firmas se le proporciona un valor jurídico equivalente al de las firmas manuscritas, a través de lo que MARTÍNEZ NADAL <sup>138</sup> denomina

---

basado en la misma tecnología, emplea un par de claves privada-pública distintas de las usadas para la firma.

<sup>136</sup> La identificación del firmante se realiza con base en su clave pública o dato de verificación de firma, y por ello de forma indirecta. Es la asociación matemática inescindible entre ésta y la clave privada o dato de creación de firma –que puede y de hecho es desconocido para el propio firmante– lo que permite su identificación a través de la clave asociada.

<sup>137</sup> La Directiva define el certificado como «la certificación electrónica que vincula uso datos de verificación de firma a una persona y confirma su identidad» (art. 2.9), y al certificado reconocido como «el certificado que cumple los requisitos establecidos en el anexo I y es suministrado por un proveedor de servicios de certificación que cumple los requisitos establecidos en el anexo II».

Serán, pues, los contenidos informativos del certificado –que, por otra parte, delimitarán la responsabilidad del certificador, según el art. 6.1, 3 y 5- y las características técnicas y legales de éste las que determinen que hablemos de unos u otros certificados.

<sup>138</sup> MARTÍNEZ NADAL, Apolonia, «Aproximaciones al borrador de Propuesta de Directiva para un marco común en materia de firma electrónica y proveedores de servicios relacionados», en *Actualidad Informática Aranzadi* 29, octubre 1998.

«equivalente funcional», esto es, el establecimiento de las condiciones que ha de reunir para ser lograr esa equiparación jurídica. Y estos requisitos son los analizados relativos al tipo de firma (electrónica avanzada), al tipo de información complementaria (certificado reconocido) y al tipo de proveedor que ha de garantizar la realidad de dicha información y producto (proveedor que cumple los requisitos del Anexo II).

Como manifiesta un sector de nuestra doctrina <sup>139</sup> la Directiva puede haberse extralimitado con la inclusión del art. 5 en su ámbito de competencias, al establecer normas de valoración procesal, campo ajeno a la regulación comunitaria al ser tradicionalmente incluido en el concepto de orden público <sup>140</sup>. Sin perjuicio de dejar constancia de esta opinión, y sumándonos a los manifestado por ORMAZÁBAL <sup>141</sup>, el art.5 de la Directiva –y su trasposición normativa mediante el RDLFE- tendrán una notable influencia en el ánimo del juzgador para convencerse de la autenticidad del instrumento aportado al proceso como prueba.

#### Los proveedores de servicios de certificación

Los proveedores de servicio de certificación, definidos en el art. 2.11) de la Directiva como «la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica», son objeto de especial atención. A pesar del principio general de no discriminación y de libertad de acceso y prestación de servicios ya citados, lo cierto es que el cumplimiento de los requisitos previstos en los Anexos a la Directiva en cuanto a organización y medios materiales, proporcionará a las firmas y certificados por ellos emitidos un valor privilegiado en el mercado, al equipararse legalmente la firma digital a la firma manuscrita.

---

<sup>139</sup> OLIVER LALANA, Daniel, *op.cit.*. DÍAZ FRAILE, *op.cit.*

<sup>140</sup> El art. 8.2 CC así lo establece, cuando expresa que «Las leyes procesales españolas serán las únicas aplicables a las actuaciones que se sustancien en territorio español, sin perjuicio de las remisiones que las mismas puedan hacer a las leyes extranjeras, respecto a los actos procesales que hayan de realizarse fuera de España.»

<sup>141</sup> ORMAZÁBAL SÁNCHEZ, Guillermo, *La prueba documental y los medios... op.cit.*, pág. 228

La denominación propició una discusión doctrinal acerca de su oportunidad. Frente a la tendencia a emplear la denominación de «autoridad o entidad de certificación», el principio de no discriminación llevó a escoger la de «proveedor» por cuanto las primeras hacían alusión a la posible condición pública y legitimadora de las intervenciones por ellas realizadas, acercándolos a los fedatarios públicos –a los que expresamente se dejan al margen de la Directiva (art. 1.2)-.

Los proveedores de estos servicios, como acabamos de ver en la definición de la Directiva, no son sólo los de expedición de certificados o generación de firmas electrónicas. El Considerando 9 se refiere expresamente a «cualesquiera otros servicios o productos que utilicen firmas electrónicas o se sirvan de ellas, como los servicios de registro, los servicios de estampación de fecha y hora, los servicios de guías de usuarios, los de cálculo o asesoría relacionados con la firma electrónica». Parecía más adecuado por ello reservar la denominación de proveedores de servicio de certificación a los que, al menos, prestaran dichos servicios, y no al que presta servicios asociados que nada tienen que ver con la actividad de certificación. De hecho, los requisitos de sometimiento a un régimen de responsabilidad civil por la prestación de servicios de firma electrónica son limitados en función de dos criterios, que no tienen en cuenta este catálogo abierto de servicios: de un lado, que la prestación de servicios se realice al público (Considerando 22 y art. 6); de otro, que la actividad haya consistido en la generación o aval<sup>142</sup> de un certificado reconocido. Quiere esto decir que la emisión de otro tipo de certificados no determinará este tipo especial de responsabilidad civil, sino la genérica prevista para cualquier persona que obre en el tráfico jurídico. No obstante, este régimen de responsabilidad es previsto como mínimo por el precepto comentado, por lo que los Estados pueden ampliarlo a toda la prestación de servicios al público relacionados, con independencia de si los certificados emitidos son o no certificados; pero siempre que el prestador de servicios emita o gestione servicios de certificación y generación de firmas<sup>143</sup>.

---

<sup>142</sup> A esta actuación de avalista de certificados, que implica la intervención de otro prestador de servicios, se refiere el art. 7.1, en relación a los certificados emitidos por prestadores no instalados en la Comunidad. Dicha vía es una de las posibilidades de reconocimiento de efectos de certificados no comunitarios.

<sup>143</sup> El régimen de los proveedores siempre se asocia en la Directiva a actividades relacionadas con la generación de firmas o con los certificados que las avalan, con independencia de la naturaleza y contenidos de

Sucintamente, concretamos el régimen de los prestadores de servicio de certificación previstos en la Directiva:

- a) Posibilidad de prestación de todo tipo de servicios relacionados con la firma electrónica (Considerando 9)
- b) Principio de libertad de establecimiento, lo que supone la ausencia de necesidad de autorización previa (Considerando 10)
- c) Previsión de un régimen voluntario de acreditación del cumplimiento de los requisitos técnicos y organizativos determinados por la ley, con el fin de acrecentar la seguridad, confianza y calidad de estos servicios (Considerando 11). El régimen de adhesión a estas acreditaciones ha de ser completamente voluntario, sin perjuicio de que los que se sometan a él obtengan beneficios comerciales por el reconocimiento y mayor demanda de sus productos, auspiciada por un régimen privilegiado de prueba legal.
- d) Posibilidad de que los prestadores de estos servicios sean personas físicas o jurídicas, y en este caso, públicas o privadas (Considerando 12). Lo que determina el sometimiento a este bloque normativo es la prestación de servicios al público.
- e) Establecimiento de un régimen de supervisión administrativa (Considerando 13), sin perjuicio de que dicho régimen de supervisión pueda ser de índole privada –como sería el caso de entidades de evaluación establecidas al amparo de los sistemas de acreditación voluntarios previstos en el art. 3.2-. No obstante, la Directiva sí establece indirectamente el sometimiento a dicha supervisión para los prestadores de servicios de certificación que emitan certificados reconocidos <sup>144</sup>

---

unos y otros. Parece ilógico someter al mismo régimen de responsabilidad a quien presta servicios de auditoría, por ejemplo, relacionados con estas tecnologías, sin perjuicio del sometimiento al régimen de responsabilidad civil contractual o extracontractual previsto en el CC.

<sup>144</sup> Art. 3.3: «Los Estados miembros velarán por que se establezcan un sistema adecuado que permita la

- f) Previsión del sistema de reconocimiento de certificaciones cruzadas, o lo que es lo mismo, reconocimiento mutuo de servicios de certificación (Considerando 23, y art. 7), en el marco de relaciones de Derecho Internacional Privado.
- g) Sometimiento a un régimen específico de responsabilidad civil por la prestación al público de este tipo de servicios (Considerando 22 y art. 6), en el que responderán de la veracidad de los datos contenidos en el certificado; del control único por el firmante de su clave de creación de firma; de la asociación y correcto funcionamiento de las claves pública y privada de firma; y de los daños derivados de una mala gestión de la información sobre revocación de un certificado. Este régimen puede limitarse a determinados usos del certificado y a determinados límites de transacciones.

#### Los productos de firma electrónica

El tercer pilar sobre el que se asienta el régimen de la firma electrónica es el establecimiento de condiciones para los productos de firma electrónica.

Los productos de firma electrónica son definidos en el art. 2.12 como «el programa informático o el material informático, o sus componentes específicos, que se destinan a ser utilizados por el proveedor de servicios de certificación para la prestación de servicios de firma electrónica o que se destinan a ser utilizados para la creación o la verificación de firmas electrónicas» . Son tanto los empleados en el ámbito profesional para realizar la actividad de los proveedores de servicio como los anteriormente definidos por la Directiva como dispositivos de creación y de verificación de firmas.

---

supervisión de los proveedores de servicios de certificación establecidos en su territorio que expidan al público certificados reconocidos»

Al igual que sucedía con las firmas, los proveedores y los certificados, los productos de firma electrónica –fundamentalmente los dispositivos de creación de firmas– pueden ser simples o denominados «seguros» (art. 2.6). Estos últimos serán los que cumplan los requisitos enumerados en el Anexo III, que define los resultados a cubrir por estos medios para garantizar la unicidad y razonable secreto <sup>145</sup>de los pares de claves generados, de modo que pueda proporcionarse seguridad de la identificación que a través de ellas se realizará del firmante.

Además de los requisitos establecidos, la Directiva incluye un Anexo IV con *Recomendaciones para la verificación segura de la firma*, las que como su propia denominación indica no tendrán carácter obligatorio –y así, no son citadas en el articulado de la Directiva–.

Como conclusión del examen realizado de la Directiva hemos de indicar que la libertad de establecimiento de los prestadores de servicios de certificación, la no discriminación entre ellos, el establecimiento de certificaciones avaladas entre prestadores comunitarios y extracomunitarios, y de requisitos técnicos y organizativos a cumplir tanto por los prestadores de estos servicios como por los productos, firmas y certificados anexos, lleva a un panorama en el que no existirá una única firma por usuario, sino tantas como servicios u organismos las proporcionen o faciliten. El sistema habrá de permitir el empleo en una actividad de firmas distintas de las nacionales –y aun así, de las empleadas en la organización concreta– siempre que cumplan los requisitos técnicos establecidos por la legislación y el prestador de servicios de certificación ostente las acreditaciones pertinentes. De reconocer firmas pasaremos a reconocer certificados, y con ello prestadores de servicios. No habrá que analizar tanto las firmas en sí (basta comprobar si cumplen las normas de homologación establecidas por la Autoridad pública –art. 3.4 y 5–) sino el régimen de los prestadores de servicios que las avalan o garantizan.

---

<sup>145</sup> Esta ambigua mención permite tanto la supervivencia de dispositivos de creación de firmas que puedan resultar invulnerables a ataques «normales» por hackers o crackers, aunque no a ataques por medios específicos (como las sesiones a veces organizadas para probar la seguridad de una clave de longitud determinada, como se realizó en 1998 con las claves criptográficas de 512 bits), como a los que puedan generar claves que, si bien resultan infranqueables a medios *razonables* de ataque, no lo sean desde el punto de vista matemático, si ello comporta un empleo de tecnología *no razonable o usual*. Pero también permite poder hablar de claves válidas aunque su «ruptura» sea posible para organismos gubernamentales.

Serán las actividades de éstas las que estarán bajo el control de las partes en el acto jurídico, y será este el tema de la prueba en los procesos en los que se aporten documentos signados por tales medios.

### 1.2.c.3) En el Derecho interno

A pesar de que la regulación sobre la firma digital fuera introducida en nuestra legislación por el RD-Ley 14/1999, con anterioridad el empleo de las firmas digitales y otros mecanismos de autenticación habían sido objeto de reconocimiento y legalización por numerosas disposiciones sectoriales de carácter administrativo.

La necesidad de acomodación a la realidad del tráfico jurídico y económico, donde los intercambios electrónicos de datos (EDI) eran suficientemente conocidos y empleados con toda normalidad, unido a la atribución a los administrados del derecho a comunicarse con las Administraciones Públicas mediante técnicas electrónicas, informáticas y telemáticas en virtud del art. 45.2 LRJPAC, llevaron a las diversas Administraciones a regular –de forma singularizada– el empleo de los códigos de identificación y otros signos electrónicos a emplear en la remisión de documentación exigida por la legislación sectorial concreta.

La aprobación del RTEIT en 1996 no ha dejado, al igual que el RD-Ley 14/1999, sin efecto dichas regulaciones sectoriales, que no obstante deberán cumplir los requisitos establecidos con carácter genérico en ambas normas y en sus disposiciones de desarrollo.

Antes de estudiar el régimen instaurado por el RDLFE –por lo demás adelantado al haber analizado ya el régimen comunitario, del que diverge sólo en algunos aspectos– conviene conocer los dos ejemplos de regulación de las firmas electrónicas articulados en el seno de la Administración Pública Española, a fin de contemplar el panorama legal completo a que pueden verse sometidas las firmas digitales empleadas en el territorio nacional.



## Disposiciones sectoriales

En paralelo a las disposiciones generales contenidas en las normas estudiadas, el Derecho Español contempló, desde años antes, el empleo de firmas y sellos o marcas digitales par la autenticación de las comunicaciones telemáticas mantenidas con los administrados.

Son de especial interés, por su anticipación y precisión técnica, la normativa de la Administración de la Seguridad Social y de de la AEAT.

### ❖ La Administración de la Seguridad Social

La Tesorería General de la Seguridad Social fue pionera en España en el empleo de medios telemáticos en su relación con los administrados. El ingente y periódico volumen de datos que los empresarios debían proporcionar a la Seguridad Social, relativos al cumplimiento de los pagos de las cotizaciones de sus empleados y al estado de afiliación de los mismos, obligó a la adopción de mecanismos de automatización y tratamiento de la información. Ello exigía la necesidad de implantar medios técnicos de autenticación de los datos remitidos, para poder acreditar el cumplimiento así realizado de las obligaciones del empresario mediante los medios informáticos y telemáticos.

Tras la aprobación de la LRJPAC, fundamneto legal del empleo de estos medios por la Administración y el ciudadano, la Orden 3 de abril de 1995, del Ministerio de Trabajo y la Seguridad Social aprobó el uso de medios electrónicos,informáticos y telemáticos en relación con la inscripción de empresas, afiliación, altas y bajas de trabajadores, cotización y recaudación.

El empleo de estos métodos estaba sometido a previa autorización por la Administración, estando abierto su uso no sólo a los sujetos obligados (empresas, agrupaciones de empresas entre otros), sino también a los profesionales colegiados que en el ejercicio de su actividad profesional tuvieran que presentar o confeccionar documentación relativa a los actos a que se refiere esta norma, debiendo ostentar la representación del sujeto obligado.

En el art. 4, destinado a la regulación de las impresiones en papel de los datos remitidos telemáticamente, se exige para su autorización «la inclusión en la misma del número secuencial de documento, huella electrónica y la clave de identificación de la Tesorería General de la Seguridad Social».

En complemento de esta norma se dictó una Resolución de 23 de mayo por la Dirección General de la Tesorería General de la Seguridad Social, en la que se permitía el empleo de dos medios alternativos y excluyentes entre sí: el soporte magnético y el intercambio electrónico de datos.

Muy interesante resultaba su Anexo I, donde se definían por primera vez en el Derecho Español los conceptos relacionados con las comunicaciones telemáticas. De entre ellas cabe destacar, por su empleo generalizado en otros ámbitos, las siguientes:

- a) Documento: unidad de información procesable de modo autónomo. Equivale en términos EDI a mensaje.
- b) EDI: Palabra formada por las iniciales de Electronic Data Interchange con la que se conoce la modalidad de conexión telemática de intercambio electrónico de datos.
- c) Huella electrónica: Serie de caracteres calculada por un procedimiento algebraico por el que de cualquier documento, sea cual fuere su soporte informático y extensión, puede calcularse una serie de números y letras que define el documento original y permite determinar

cualquier modificación del mismo, sea por incorporación, eliminación, transposición o rectificación de caracteres, palabras, líneas, párrafos o páginas. Recibe su nombre del simil con la huella digital humana <sup>146</sup>.

- d) Soporte informático: Elemento, comparable al papel en la escritura, que hace llegar la información al destinatario con unas reglas que determinan su estructura, contenido, disposición de los datos y formato.

El empleo del intercambio electrónico de datos ha ido desplazando, por su seguridad y ventajas de funcionamiento, a los soportes magnéticos –con lo que se justifica la necesidad de aceptación del concepto avanzado de documento que hemos defendido, y del que se tiene en este trabajo varias definiciones– . Fruto de ello ha sido el establecimiento de la obligación –sustituyendo así la facultad conferida por la Resolución de mayo de 1995– de todos los profesionales colegiados que tramiten la documentación relativa a seguros sociales al sistema de Remisión Electrónica de Datos (RED) <sup>147</sup>.

La recepción dentro del ordenamiento jurídico de la Seguridad Social de las disposiciones relativas al uso de la firma electrónica ha sido realizada por la modificación operada en el Reglamento General de Gestión Financiera de la Seguridad Social (RD 1391/1995, de 4 de agosto) por el RD 1891/1998, de 10 de diciembre. Dicha disposición añade una disposición adicional quinta en los siguientes términos:

---

<sup>146</sup> Como puede apreciarse, la huella digital es sinónimo del «hash» o resumen del que hemos hablado al describir el proceso de firma electrónica de un documento basado en la tecnología de cifrado asimétrico.

<sup>147</sup> La incorporación de los Graduados Sociales fue contemplada en la Orden de 26 de enero de 1996, complementada por la Resolución de 15 de abril de 1998.

La disposición adicional sexta del Reglamento general de Recaudación de los Recursos del Sistema de la Seguridad Social, aprobado por RD 1637/1995, de 6 de octubre –y modificado por el RD 2302/1998, de 25 de septiembre– extendió la obligación de incorporación a los profesionales colegiados y demás personas que en el ejercicio de su actividad cumplimenten este tipo de documentación. La Resolución de 30 de marzo de 1999 ha venido a fijar los plazos y condiciones en que debe efectuarse esta incorporación por parte de dichos profesionales.

«Disposición adicional quinta. Aplicación de medios técnicos: validez y eficacia de los documentos producidos a través de los mismos.

1.Las actuaciones relativas al pago de las obligaciones de la Seguridad Social y demás actos regulados en el presente Reglamento 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, de 17 de septiembre, sobre firma electrónica, en relación con el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

2.Los documentos en los que se formalicen o se notifiquen a los interesados los actos a que se refiere este Reglamento, 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 trate.»

Con esta norma no sólo se recoge el empleo de la firma electrónica en la Administración de la Seguridad Social <sup>148</sup>, sino que se hace uso de lo autorizado por el art. 5 RDLFE, estableciendo las condiciones adicionales de validez jurídica que ya se venían empleando en esta Administración. Con todo, la autorización de la posibilidad de uso de la firma electrónico –no su uso obligatorio– puede comportar problemas probatorios sobre el carácter de sus documentos desde el punto de vista del proceso, al no ser equiparables todas las firmas con las firmas manuscritas, de conformidad con el art. 3.1 RDLFE. Ello supondrá que los documentos de la

---

<sup>148</sup> Aunque, a diferencia de lo que sí efectúa la DGRN en su Resolución de 26 de abril de 2000, en relación con las comunicaciones y documentos que reciban por vía telemática, por la que exige al emisor el empleo de firma electrónica avanzada basada en un certificado reconocido.

Seguridad Social, sin perjuicio de su reconocimiento como documentos oficiales, como medios probatorios sólo podrán ser amparados en el art. 384 LEC, siendo susceptibles de pruebas de contraste en cuanto a su fiabilidad.

#### ❖ La Administración Tributaria

La AEAT ha realizado un esfuerzo para adaptar las normas reguladoras de los distintos tributos a las posibilidades ofrecidas por la informática y la telemática. Han quedado reflejados las recepciones legislativas de las facturas electrónicas en la legislación sobre IVA.

De modo análogo al empleado por la Seguridad Social, también en la AEAT se permite la presentación telemática de declaraciones tributarias de origen empresarial mediante el empleo de firmas electrónicas manifestadas en códigos de identificación, generados mediante tecnología de cifrado simétrico (es decir, la clave de cifrado y descifrado es la misma). La Orden del Ministerio de Economía y Hacienda de 29 de junio de 1998 reguló las condiciones generales y el procedimiento para la presentación telemática de las declaraciones-liquidaciones mensuales de grandes empresas correspondientes a los códigos 111, 320 y 332 <sup>149</sup>.

Las normas citadas se basan en la identificación del administrado mediante la generación criptográfica y asignación de un Número de Referencia Completo (NRC), que posteriormente le permitirá conectarse con el servidor web seguro de la AEAT, a través del cual se realizará la presentación telemática de las declaraciones. La asignación del NRC se realizará por la AEAT o las entidades colaboradoras a la hora de efectuar los ingresos, y contendrá la información relativa a la empresa y al tipo de declaración realizada. A continuación, en conexión telemática con la AEAT, ésta generará la declaración validada con un Código electrónico que identificará los datos

---

<sup>149</sup> Posteriormente ha sido derogada por la Orden de 20 de enero de 1999, complementada por la Orden de 30 de septiembre de 1999 para la presentación de las declaraciones-liquidaciones correspondientes a los modelos 110, 130, 300 y 330.

enviados <sup>150</sup>, que debe ser impreso y conservado para validar la declaración realizada.

Auspiciados por el deseo del Gobierno de introducir a España en el rango de cabeza de los países líderes de la Sociedad de la Información, de acuerdo con las directrices marcadas por la Comunidad Europea, ha sido sin duda el Impuesto sobre la Renta de las Personas Físicas –por su especial incidencia en un mayor número de ciudadanos– el que ha visto aparecer la primera aplicación real de la firma electrónica avanzada en el campo de las relaciones Administración-ciudadano.

Sobre la base normativa de la posibilidad de presentación telemática de las declaraciones tributarias, contenida en varias disposiciones legales <sup>151</sup>, se determinó por Orden del Ministerio de Economía y Hacienda de 13 de abril de 1999 las condiciones generales y el procedimiento para la presentación telemática de declaraciones del Impuesto sobre la Renta de las Personas Físicas <sup>152</sup>. La Orden regula el empleo de firma electrónica avanzada basada en tecnología de cifrado asimétrico y un certificado de usuario emitido por la FNMT conforme al estándar X-509 del ITU-I, cuyo contenido establece. La emisión del certificado de usuario por la FNMT requerirá la intervención, como autoridad de registro, de alguna Delegación de la AEAT, ante la que el usuario se identificará.

---

<sup>150</sup> El Código Electrónico al que se hace referencia es definido en el Apartado Primero.Tres como « Código formado por 16 caracteres alfanuméricos, enterados por la AEAT en función de los datos incluidos por los declarantes a través de Internet/infovía y que dan validez a la autenticidad de la presentación.». Como puede observarse, se trata una vez más de la generación de un «hash» o compendio o resumen, análogo a la huella digital de la que hablaba la regulación de la Seguridad Social, base para la garantía de la integridad del documento durante la transmisión. La identificación del usuario se basa en el NRC.

<sup>151</sup> Aparte de las referencias genéricas a las disposiciones habilitantes de la LRJPAC y del RTEIT, cabe citar el art. 96 de la Ley del Impuesto sobre la Renta de las Personas Físicas; el art. 79.5 de la Ley del mismo impuesto, según reforma operada por la Ley 40/1988, de 9 de diciembre; el art. 59.3 del Reglamento del IRPF, aprobado por RD 214/1999, de 5 de febrero; y la disposición final 2ª de la Ley 50/1998, de Medidas Fiscales, Administrativas y del Orden Social.

<sup>152</sup> La regulación del procedimiento de renovación y revocación de los certificados de usuario X-509.V3 emitidos con fines tributarios fue objeto de regulación por la Orden del Ministerio de Economía y Hacienda de 28 de febrero de 2000. El procedimiento se podrá efectuar desde un ordenador personal con un navegador web, en el que se hayan incorporados las claves de firma y el certificado que se pretende renovar o revocar.

El ampararse en una firma electrónica avanzada y en un certificado no confiere la condición de firma equivalente a la manuscrita a la que se refiere el art. 3.1 RDLFE, por cuanto ésta exige que el certificado sea «reconocido», y éste sólo puede serlo – de conformidad con la definición del mismo recogida en el art. 2.j)– el que contiene la información descrita en el art. 8, además de ser emitido por un prestador de servicios de certificación que cumple los requisitos establecido en el art. 12 <sup>153</sup>. Existe una gran similitud en el contenido de los certificados reconocidos con el descrito en el apartado Primero, Quinta. Sólo se diferencia del contenido del art. 8 RDLFE en la ausencia de declaración de que el certificado se emite como tal, así como la identificación del prestador de servicios de certificación. El primero de los requisitos entendemos que es implícito al propio certificado, puesto que no induce a dudas el motivo de su expedición –amparada en una normativa legal-. Lo mismo cabe decir de la identificación del prestador de servicios, a quien no hace falta identificar por cuanto que la identificación es realizada *ope legis* por las disposiciones normativas que permiten y describen el empleo de la firma electrónica en el ámbito tributario. Con todo, la objeción acerca de la condición del prestador de servicios sigue en pie, con arreglo a la letra de la ley, por más que el régimen de FNMT sea el más fiel al espíritu de ésta.

En caso de impugnación de la realidad y seguridad de los mecanismos empleados, descritos por las normas, deberá ser acreditado mediante la correspondiente pericia en el seno de un proceso judicial. El sometimiento de estos procedimientos a estándares internacionales hace temerario tal intento <sup>154</sup>.

La regulación de la firma electrónica en el RD Ley 14/1999, de 17 de septiembre

---

<sup>153</sup> Que, a su vez, hace referencia a los requisitos determinados en el art. 7 (registro del prestador en el Registro de Entidades de Certificación mantenido por el Ministerio de Justicia –inexistente en la actualidad–) y en el art. 11 (los requisitos genéricos de cualquier prestador de servicios de certificación).

<sup>154</sup> No obstante, es posible la producción de errores en la transmisión telemática que pueden influir en la validez de la declaración presentada. Así, en la Orden de 20 de enero de 1999 se prevé un procedimiento de subsanación de dicha eventualidad.

Adelantándose a la aprobación de la Directiva de firma electrónica –como también sucediera en la regulación del tratamiento automatizado de datos personales entre la LORTAD y la Directiva 95/46/CE– el legislador español ha optado por dar carta de naturaleza, como hicieron antes sus homólogos alemanes e italianos, a la disposición básica de regulación de la firma electrónica.

El RD-Ley 14/1999, de 17 de septiembre (RDLFE) se propone regular el uso de la firma, el reconocimiento de su eficacia jurídica y el régimen la prestación al público de los servicios de certificación y de los prestadores de los mismos.

Siguiendo la Posición Común de 22 de abril de 1999, se ha considerado conveniente adelantarse a la regulación comunitaria por el propósito de favorecer la implantación y difusión de este tipo de servicios –por otra parte ya empleados– en el mercado español <sup>155</sup>. Ello se manifiesta a lo largo de su articulado, donde la perspectiva empleada se dirige fundamentalmente al sector empresarial y al empleo en el mismo de estos servicios, haciéndose difícil en ocasiones su aplicación en el sector público <sup>156</sup>.

No obstante, esta aprobación previa a la de la Directiva ha ocasionado la divergencia de algunos aspectos de la regulación, que obligarán en el futuro a la revisión del RDLFE, o bien a su interpretación modificada con arreglo a lo dispuesto en la Directiva 1999/93/CE.

---

<sup>155</sup> A ello se alude expresamente en la Exposición de Motivos de la norma, cuando manifiesta que «Existe, además, en España, un sector empresarial que podría prestar un servicio de certificación de la firma electrónica con suficiente calidad [...] La urgencia de la aprobación de esta norma deriva, también, del deseo de dar, a los usuarios de los nuevos servicios, elementos de confianza en los sistemas, permitiendo su introducción y rápida difusión.»

<sup>156</sup> No obstante la dificultad, el propósito de la Directiva y del RDLFE es conferir validez a las firmas emitidas por los organismos administrativos en el seno de sus organizaciones y en las relaciones que éstas mantengan con los ciudadanos. Así, el Considerando 12 habla de la posibilidad de que los servicios de certificación y asociados puedan ser prestados por entidades públicas o privadas; y en el Considerando 19 se prevé expresamente su uso en el sector público, con la posibilidad de establecer nacionalmente requisitos adicionales a los exigidos en la Directiva (art. 3.7). En el Anexo II se listan las condiciones requeridas para poder ser considerado prestador de servicios de certificación reconocidos, que, por su redacción, permiten –a pesar de las referencias de claro contenido contractual– ser aplicadas a los prestadores públicos, lo que no sucede con la dición del art. 12 del RDLFE.



#### ❖ Diversidad de firmas electrónicas

Lo primero que ha de quedar claro es que el empleo de la firma digital no se halla sometido a un único bloque normativo. La finalidad del RDLFE era, como hemos indicado, fomentar su uso y garantizar el reconocimiento legal del mismo mediante la prohibición de negarle condición probatoria; lgo innecesario pues, como indica ORMAZÁBAL <sup>157</sup>, la firma electrónica avanzada sería igualmente admisible como prueba aunque no existiese el art. 3 RDLFE al establecer la LEC un *numerus apertus* de medios probatorios y reconocer expresamente a los medios o instrumentos que permiten reconocer datos, cifras o números en el art. 384.

La norma del art. 3.2 que establece que «A la firma electrónica que no reúna todos los requisitos previstos en el apartado anterior, no se le negarán efectos jurídicos ni será excluida como prueba en juicio, por el mero hecho de presentarse en forma electrónica» permite la admisión de otras modalidades de firma electrónica, si bien no podrán gozar de los beneficios procesales de la presunción de equivalencia funcional con la firma manuscrita prevista en el apartado 1º del mismo artículo para las que sí cumplan las prescripciones del RDLFE. Será obligación de la parte acreditar la autenticidad e integridad del documento con ella firmado mediante los correspondientes medios probatorios (algo determinado por el art. 384.2 LEC), y supondrá la negación *ab initio* de la equiparación del documento electrónico firmado con los documentos públicos o privados establecidos en la LEC. Pero, obviamente, el cumplimiento de los requisitos establecidos en la legislación administrativa para el empleo de estos medios de firma, y la similitud funcional de éstos con los establecidos en el RDLFE (como es el caso de los documentos fiscales sometidos al régimen anteriormente examinado) tendrá una relevancia concluyente para el tribunal de cara a otorgarles credibilidad probatoria.

---

<sup>157</sup> ORMAZÁBAL SÁNCHEZ, Guillermo, *op.cit.* pág. 225

La primera excepción deriva de la interpretación del ámbito de aplicación del RDLFE y la Directiva comunitaria. Ambas introducen una regulación para la prestación *al público* de este tipo de servicios (art. 1.1 RDLFE); pero la Directiva –que en su art.1.1 sólo habla como objetivo de «facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico» es más explícita en esta exclusión al establecer el respeto a los acuerdos de derecho privado celebrados entre un número determinado de participantes (Considerando 16)<sup>158</sup>. Como refleja DÍAZ FRAILE<sup>159</sup>, cabe plantearse la aplicación analógica en estos casos del art. 51 del Código de Comercio cuando una de las partes contratantes sea comerciante, al establecer este precepto que «La correspondencia telegráfica sólo producirá obligación entre los contratantes que hayan admitido este medio previamente y en contrato escrito, y siempre que los telegramas reúnan las condiciones o signos convencionales que previamente hayan establecido los contratantes, si asó lo hubiesen pactado»; norma por lo demás aplicable dado que el RDLFE deja subsistentes todas las disposiciones relativas a la celebración, formalización, validez y eficacia de los contratos y otros actos jurídicos (art.1.1).

La segunda excepción normativa vendrá determinada por el bloque normativo expuesto anteriormente relativo al empleo de firmas electrónicas en la Administración Pública. Si bien el art.5 parece querer establecer el empleo de este tipo de firmas a la Administración Pública al establecer que se podrán *añadir* requisitos o condiciones adicionales<sup>160</sup>, estimamos que lo que el RDLFE ha establecido ha sido sólo la regulación de la prestación al público de este servicio, no del régimen jurídico de todas las firmas electrónicas. Y ello es evidente. La prueba de la validez de los mecanismos técnicos y organizativos que amparan una firma electrónica empleada en la Administración Pública vendrá determinada por la comprobación de los requisitos establecidos por la legislación sectorial que la

---

<sup>158</sup> Considerando 16: «[...] En la medida en que lo permita la legislación nacional, ha de respetarse la libertad de las partes para concertar de común acuerdo las condiciones en que aceptarán las firmas electrónicas; no se debe privar a las firmas electrónicas utilizadas en estos sistemas de eficacia jurídica ni de su carácter de prueba en los procedimientos judiciales».

<sup>159</sup> DÍAZ FRAILE, *op.cit.*

<sup>160</sup> El empleo de la firma electrónica en el sector público se halla expresamente recogido en la Directiva (Considerando 19), cuyo art. 3.7 autoriza a los Estados a «supeditar el uso de la firma electrónica en el sector público a posibles prescripciones adicionales»

impone, y no por el cumplimiento de los requisitos que se establecen para las empresas en el RDLFE <sup>161</sup>. Eventualmente, las Administraciones gozan de una facilidad probatoria de la fiabilidad técnica de sus medios de firma al contar con el soporte técnico profesional de los funcionarios encargados de tales servicios, que le proporcionarían una prueba pericial sin coste alguno. Es lógico que los particulares y las empresas no gozan de la misma posibilidad respecto de sus instrumentos signados digitalmente, por lo que es la ley –con su propósito de favorecer el uso de la firma electrónica– la que se encarga de facilitar su empleo otorgándoles presunciones de validez en función del cumplimiento de un determinado régimen.

La tercera excepción, especialidad de la anterior, viene determinada por el art. 5.3 RDLFE, al aceptar que « Podrá someterse a un régimen específico, la utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa». Será el cumplimiento de su normativa específica la que determine el valor a conferir a las firmas digitales en tal campo <sup>162</sup>.

#### ❖ Consecuencias legales del empleo de la firma digital

---

<sup>161</sup> Algunos de difícil o imposible cumplimiento desde la perspectiva pública. Es el caso de la exigencia de garantías económicas a las autoridades de certificación que se establezcan en el seno de una Administración; o que ésta proporcione información sobre las condiciones del servicio a los usuarios; requisitos estos exigidos por el art. 12 para poder emitir certificados reconocidos. O el de requerir el consentimiento del usuario para la inclusión en certificado de algún atributo distinto de su propia identificación, como el cargo ocupado, del art. 11 para el certificado reconocido. En estos casos se hace necesario una interpretación correctora basada en la legislación administrativa y en la legislación de protección de datos personales.

<sup>162</sup> Qué duda cabe que el sometimiento a juicio de un documento de esta naturaleza podrá dar lugar a la aplicación del novedoso régimen de restricción a la publicidad de las actuaciones previsto en los arts. 138.2 y 140.3 LEC.

El primero, referido a la publicidad de las actuaciones orales, establece que «Las actuaciones a que se refiere el apartado anterior podrán, no obstante, celebrarse a puerta cerrada cuando ello sea necesario para la protección del orden público o la seguridad nacional de una sociedad democrática [...]».

El art. 140.3 por su parte permite que «No obstante lo dispuesto en los apartados anteriores, los tribunales por medio de auto podrán atribuir carácter reservado a la totalidad o parte de los autos cuando tal medida resulte justificada en atención a las circunstancias expresadas por el apartado 2 del art. 138. Las actuaciones de carácter reservado sólo podrán ser conocidas por las partes y por sus representantes y defensores, sin perjuicio de lo previsto respecto de hechos y datos con relevancia penal, tributaria o de otra índole.»

Aunque ya hemos hablado *in extenso* de las consecuencias procesales del empleo de la firma digital en los documentos electrónicos asociados a las mismas, no nos resulta inadecuado resumir los efectos procesales y legales en los siguientes:

- a) Todas las firmas electrónicas gozarán de valor probatorio, quedando éste supeditado:
  1. Bien al cumplimiento de los requisitos establecidos para la firma electrónica empleada (que se pueda considerar avanzada, y que haya sido creada con un dispositivo seguro), para el certificado (que pueda ser considerado como reconocido, en función de un contenido determinado por la ley, y por las características del prestador de servicio de certificación), y para el prestador de servicios de certificación (que esté acreditado por los procedimientos establecidos por la legislación).
  2. Bien a la prueba de la integridad y de la autenticidad proporcionada por los mecanismos empleados respecto del documento firmado y de la identidad de su autor, a través de la actividad probatoria que emplee la parte que los alegue.
- b) El valor legal de los certificados emitidos por prestadores de servicio con anterioridad a la entrada en vigor de la norma conservarán su validez de acuerdo con las normas que rigieran la actividad de aquéllos, la que no obstante, deberá adaptarse a lo dispuesto en el RDLFE en el plazo de un año (Disposición Transitoria única).
- c) El valor probatorio indicado podrá suplirse por una presunción probatoria amparada en normas establecidas por el RDLFE y su regulación complementaria.
- d) La presunción de equivalencia funcional con la firma manuscrita admite prueba en contrario
- e) Quedan subsistentes todos los requisitos formales y materiales exigidos para la celebración de obligaciones y contratos suscritos mediante firma electrónica.

- f) El empleo de servicios prestados por las entidades de certificación no sustituye la intervención de fedatarios públicos respecto de los documentos signados, ni impone una determinada concepción pública o privada a los documentos electrónicos.
- g) El cauce procesal de admisión de los documentos firmados electrónicamente será:
1. El determinado por los arts. 299.2 y 384 LEC para los documentos firmados con firma que no tenga la condición de avanzada basada en certificado reconocido
  2. El determinado por el art. 324 LEC para los documentos firmados con firma electrónica avanzada basada en un certificado reconocido, que podrán equipararse a los documentos manuscritos privados.
- h) En cuanto a los documentos públicos administrativos y judiciales, si cumplen los requisitos previstos en el art. 45.2 LRJPAC y los establecidos en el RD 263/1995, de 16 de febrero (RTEIT) y 230.2 LOPJ, respectivamente, tendrán la condición de documentos públicos establecida en los art. 317 y ss LEC. Ello no supone el cumplimiento de lo establecido en el RDLFE, si bien sólo una firma electrónica avanzada podrá dar satisfacción a los requisitos establecidos por la legislación sectorial.
- i) Se admite la posibilidad de que las personas jurídicas tengan firma propia en el ámbito de la gestión de tributos, y no sólo a través de sus representantes legales <sup>163</sup>; condicionado a la publicación de una regulación específica por el Ministerio de Economía y Hacienda (art. 5.3.in fine).

A estas reflexiones cabría añadir una más. Si la validez y eficacia de una firma electrónica administrativa o judicial depende del cumplimiento de los requisitos que

---

<sup>163</sup> Uno de los contenidos del certificado reconocido es, precisamente, la inclusión de la referencia a los documentos que acrediten las facultades del signatario para actuar en nombre de la persona física o jurídica a la que represente (art. 8.1.f).

establezca su legislación sectorial y no el RDLFE, ¿podría plantearse una aplicación analógica de la presunción del art. 3.1.II si las firmas reguladas sectorialmente cumplen los requisitos de la firma electrónica avanzada basada en un certificado reconocido? Esto sucede con los documentos de la Administración Tributaria y de la Seguridad Social, que han establecido el empleo de la tecnología de cifrado asimétrico –firmas electrónicas avanzadas- y la utilización de los servicios de la FNMT –prestador acreditado-. Si el contenido de los certificados establecidos particularmente coincide con el contenido previsto en el art. 11 para los certificados comerciales, no vemos obstáculo para que puedan beneficiarse de dicha presunción probatoria en el improbable caso de que fueran cuestionados en juicio o en un procedimiento administrativo.

Una característica que sí pone en cuestión el régimen previsto en la Directiva comunitaria, y constituye uno de los puntos de divergencia con esta– lo constituye la posibilidad abierta en el art. 11.c) al prestador de servicios de certificación de poder ofrecer como servicio el almacenamiento de los datos de creación de firma, uesta de relieve por MARTÍNEZ NADAL <sup>164</sup>. Según se manifestó, la Directiva advertía del peligro que toda actividad de copia o almacenamiento de claves podría suponer en el esquema de confianza que requiere el empleo de esta técnica de autenticación documental, por lo que consideraba como exigencia para todo proveedor de servicios de certificación que emitiera certificados reconocidos la prohibición de realizarlos. Ciertamente, al establecerse la prohibición en el Anexo II, relativo a condiciones de los proveedores que emitan certificados reconocidos, dejaba abierta la posibilidad de que los que no emitieran este tipo de certificados sí pudieran hacerlo.

En la legislación española la posibilidad se supedita al consentimiento del interesado, tratando de este modo el dato de creación de firma únicamente en su dimensión de dato de carácter personal, a los fines de aplicación del régimen disciplinario de la LOPDP (art. 15) <sup>165</sup>. Como pone de relieve la autora citada, el bien

---

<sup>164</sup> Martínez nadal, *op.cit.*

<sup>165</sup> Art. 15 RDLFE: «1. El tratamiento de los datos personales que precisen los prestadores de servicios de

jurídico protegido con la normativa de protección de datos no coincide con el de las normas del RDLFE, que pretenden garantizar el no repudio de las firmas emitidas mediante el establecimiento del requisito del control exclusivo del firmante de sus datos de creación de firma <sup>166</sup>. Su admisión deberá ser sometida a revisión en el proyecto de ley que pretende desarrollar el Gobierno en fechas próximas, que sustituirá al actual RDLFE.

Por último, en relación con este apartado, hemos de resaltar –junto con MARTÍNEZ NADAL y ORMAZÁBAL– que actualmente la presunción conferida por el art. 3.1.11 carece de virtualidad, al requerirse la aprobación de normas de homologación para los dispositivos de creación de firmas'; la acreditación del prestador de servicios –en función de un procedimiento y unas entidades que todavía no existen–; y el registro del prestador de servicios en un Registro Público dependiente del Ministerio de Justicia, regulado en el ar. 7 RDLFE, que actualmente no existe.

#### ❖ Los prestadores de servicios de certificación

---

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. El mismo régimen será de aplicación a los datos personales que se conozcan en el órgano que, en el ejercicio de sus funciones, supervisa la actuación de los prestadores de servicios de certificación y el competente en materia de acreditación.

2. Los prestadores de servicios de certificación que expidan certificados a los usuarios, únicamente pueden recabar datos personales directamente de los titulares de los mismos o con su consentimiento explícito. Los datos requeridos serán, exclusivamente, los necesarios para la expedición y el mantenimiento del certificado.

3. Los prestadores de servicios de certificación que hayan consignado un seudónimo en el certificado, a solicitud del signatario, deberán constatar su verdadera identidad y conservar la documentación que la acredite.

Dichos prestadores de servicios estarán obligados a revelar la identidad de los titulares de certificados cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el art. 11.2 de la Ley Orgánica 5/1992, de 29 de octubre. Ello se entiende sin perjuicio de lo que, en la legislación específica en materia tributaria, de defensa de la competencia y de seguridad pública, se disponga sobre la identificación de las personas.

En todo caso, se estará a lo previsto en las normas sobre protección de datos indicadas en el apartado 1 de este artículo.»

<sup>166</sup> Ese es precisamente uno de los requisitos de la firma electrónica avanzada. Véase definición ex art. 2.b).

### *Régimen general*

Los prestadores de servicios de certificación, o proveedores de servicio de certificación en la terminología comunitaria, han sido objeto de regulación de desarrollo tanto en el RDLFE como por normas posteriores.

EL RDLFE sigue, como no cabía esperar, el régimen implantado por la Directiva. Como mecanismo propio de supervisión, más orientado no obstante hacia el reconocimiento cruzado de certificados, se prevé un Registro de Prestadores de Servicios de Certificación en el art. 7. Dicho registro dependerá del Ministerio de Justicia, y tendrá por objeto identificar al prestador de servicios y justificar que reúne los requisitos necesarios <sup>167</sup>.

Plantea problemas entender el carácter obligatorio o no del registro. El art. 7.1 establece que los prestadores de servicios de certificación «deberán solicitar su inscripción con carácter previo al inicio de su actividad». El art. 11.g) convierte la solicitud de inscripción en un requisito a cumplir por cualquier prestador de servicios de certificación, sancionándolo disciplinariamente en el caso de los que emitan certificados ordinarios como infracción leve en el art. 25.3.a) –no se prevé su incumplimiento por el prestador que sí los emita–. El art. 12 hace referencia a este artículo como de cumplimiento obligado por los que deseen emitir certificados reconocidos. Por su parte, el párrafo 2.2 del art. 7 alude a que «La formulación de la solicitud de inscripción les permitirá iniciar o continuar su actividad, sin perjuicio de la aplicación del régimen sancionador correspondiente». De todo ello se infiere, a la luz de los reiterados pronunciamientos de la Directiva, que la inscripción registral no opera como autorización previa de funcionamiento, sino como instrumento que

---

<sup>167</sup> La prueba a la que hemos aludido del cumplimiento de los requisitos del prestador se verá así favorecido mediante este mecanismo de publicación. Con arreglo al art. 7.3 el registro será público y podrá ser consultado por vía telemática o mediante certificación registral. La información que proporcionará hará referencia a su identificación, dirección de correo electrónico, la clave pública así como la información acerca de su condición de acreditado o de la posibilidad de emitir certificados reconocidos.



facilita la prueba de las condiciones exigidas a la firma para lograr eficacia legal, de acuerdo con el régimen del art. 3 <sup>168</sup>.

El control o supervisión regulado en la Directiva comunitaria (art. 3.3) se materializa en un régimen de inspección y control de los prestadores, a desarrollar por la Secretaría General de Comunicaciones, del Ministerio de Ciencia y Tecnología <sup>169</sup>; y en un régimen disciplinario doble: el propio del RDLFE por incumplimientos a su articulado, de acuerdo con los tipos, sanciones y procedimiento establecido en el Título V, y el de protección de datos personales en cuanto a la violación de la LOPDP en relación al empleo indebido de datos personales en los procesos de creación, verificación o de prestación de servicios añadidos a los de firma electrónica, de conformidad con el art. 16.3.

Como se establecía en el marco comunitario, España ha regulado un régimen de acreditación voluntario en el art. 6, que favorece tanto a los prestadores como a los productos de firma electrónica <sup>170</sup>. Es más; la legislación española ha propiciado el sometimiento a dichos regímenes de acreditación mediante la incorporación de una presunción probatoria al artículo 3 ya muchas veces aludido. La posesión de la acreditación será objeto de inscripción en el Registro de Prestadores de Servicio de Certificación, favoreciendo con ello el empleo, confianza y seguridad de los

---

<sup>168</sup> MARTÍNEZ NADAL opina, por el contrario, que para el caso de los prestadores de estos servicios que emitan certificados reconocidos es un requisito de funcionamiento, al considerar que es ilógico su existencia sin el cumplimiento de un requisito que es sancionable para otros prestadores. No compartimos esta opinión amparándonos en el art. 25.1.a), que establece expresamente como infracción muy grave el incumplimiento por los prestadores de servicios que emitan certificados reconocidos de las obligaciones del ar. 11 «salvo la c), g) y h)», siendo precisamente la g) la que ahora nos ocupa. No es que no exista previsión especial para este tipo de prestadores; es que la propia ley excluye este incumplimiento de la condición de infracción. De ser un requisito imprescindible de existencia no se habría realizado esta exclusión expresa. Y como quiera que el art. 12 remite al cumplimiento del art. 7, que prevé la posibilidad de solicitud ulterior, lo único que podemos deducir es que no se trata de un requisito esencial y que constituye una laguna legal sancionadora criticable, por cuanto si constituye un medio privilegiado de favorecimiento de la prueba de los requisitos de la firma para acogerse a la presunción legal y el certificado reconocido precisamente pretende conferir seguridad y confianza a los que confían en estas firmas por ellos avalados, su incumplimiento contraría la finalidad y especial confianza que merecen estos certificados, debiendo por ello ser objeto de sanción –como se postula de los incumplimientos del art. a que se refiere el art. 25.1.b) si se afecta a la seguridad de los servicios de certificación.

<sup>169</sup> Aunque el art. 16.1 la radica en el Ministerio de Fomento, este organismo fue transferido al Ministerio de Ciencia y Tecnología en la última reorganización departamental operada en 2000.

<sup>170</sup> Al régimen de evaluación de la conformidad con la normativa aplicable de los dispositivos seguros de creación de firma electrónica alude el art. 21.

certificados, que sólo con la consulta al Registro citado, en las dos vías propuestas, podrán acreditar dicho cumplimiento.

El régimen de acreditación ha sido desarrollado por el la Orden del Ministerio de Fomento de 21 de febrero de 2000, por la que se aprueba el Reglamento de Acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica.

Es curioso la escasa, por no decir casi testimonial, regulación que merecen las denominadas autoridades de registro, que sólo son aludidas en el art. 11.a) <sup>171</sup>. MARTÍNEZ NADAL <sup>172</sup> la define como «una entidad que proporciona servicio local a un conjunto de suscriptores de una autoridad de certificación».

Entre las funciones de una autoridad de registro local cabe citar, como señala la autora citada, las de registro, baja y cambio de atributos de los usuarios, identificación y autenticación de éstos, y autorización de solicitudes de emisión de los certificados, o de suspensión y revocación de los mismos.

Su labor es vital para la vida y confianza del certificado. si éste se caracteriza por vincular unos datos de verificación de firma a un signatario y confirmar su identidad (art. 2.i RDLFE), es esencial identificar a dicho usuario, siendo muy posible que éste no se encuentre cercano al prestador de servicios de certificación.

La función de registro local es una misión que le compete al prestador de servicios de certificación, de acuerdo con el art. 11.a), dado que constituye una fase del propio proceso de generación de la firma electrónica y del certificado que la acompaña.

---

<sup>171</sup> Art. 11 RDLFE: «Todos los prestadores de servicios de certificación deben cumplir las siguientes obligaciones: a) Comprobar por sí o por medio de una persona física o jurídica que actúe en nombre y por cuenta suyos, la identidad y cualesquiera circunstancias personales en los solicitantes de certificados relevantes para el fin propio de éstos, utilizando cualesquiera de los medios admitidos en derecho.»

<sup>172</sup> MARTÍNEZ NADAL, Apolonia, *Comercio Electrónico, Firma digital y Autoridades de Certificación*, Madrid, 2000, págs. 140-141.

Este podrá hacer uso de los servicios de otras personas físicas o jurídicas, para lo que deberá establecer una estructura organizativa propia o concertar los correspondientes contratos de arrendamientos de servicios, sin que ello suponga exoneración de responsabilidad por su parte, dado que es él el último responsable de la función descrita.

Como establece el art. 11.a), la identificación se realizará mediante cualquier medio admitido en derecho.

La excepción a esta obligación –que, recordemos, se impone a todo prestador de servicios de certificación, con independencia del tipo de certificado que emita– deriva de la emisión de certificados no reconocidos «que se limiten a constatar determinadas circunstancias específicas de los solicitantes de aquellos». Causa, en opinión de la autora citada <sup>173</sup> sorpresa la referencia que hace el precepto glosado a la excepción a la obligación de identificación cuando el certificado, por definición del art. 2.i citado, consiste precisamente en la confirmación de la identidad del usuario. En estos supuestos no existirá certificado *strictu sensu*. No obstante, y como la misma autora reflejaba en otra de sus obras <sup>174</sup>, existen certificados de atributos, reflejados en algunas legislaciones extranjeras <sup>175</sup>, a los que parece haberse referido el RDLFE al asociarlos a la certificación de circunstancias específicas del solicitante. Pero, al no distinguir la Directiva ni el RDLFE entre unos y otros certificados, y determinar como objeto de éstos la identificación del firmante, convenimos con ella en la imposibilidad de existencia con efectos de certificado de este tipo en nuestro Derecho. Su aposición a una firma digital no supondrá más efecto legal que el que derive de las pruebas complementarias que se aporten con el documento firmado digitalmente.

---

<sup>173</sup> MARTÍNEZ NADAL, «Comentarios de urgencia al urgentemente aprobado Real Decreto-Ley 14/1999 de 17 de septiembre, sobre firma digital», en *Revista La Ley-Actualidad* nº 4939, 1 diciembre 1999.

<sup>174</sup> MARTÍNEZ NADAL, Comercio electrónico... op.cit. pág. 124.

<sup>175</sup> Es el caso del §2 (3) de la Signaturgesetz –SigG , de 1 Agosto 1997. Disponible en Internet en <http://www.iid.de/rahmen/iukdgeb.htm>

Por último, en cuanto al régimen general de los prestadores de servicios de certificación, ha de ser citado el establecimiento –conforme a las pautas comunitarias– de un régimen de responsabilidad civil, caracterizado por las siguientes notas:

- a) El hecho generador de la responsabilidad es el mero incumplimiento de las obligaciones legales o la actuación negligente. A pesar de esta dicción, y confrontando el precepto con las disposiciones sancionadoras del Título V, entendemos que no cabrá una exacción de responsabilidad por cualquier incumplimiento de las obligaciones establecidas por la norma, sino que se requerirá que, además, dicho incumplimiento haya originado un daño grave al usuario <sup>176</sup>
- b) En favorecimiento de la reclamación, se establece una inversión de la carga de la prueba de la diligencia (art. 14.1 in fine)
- c) Los prestadores de certificados reconocidos responderán por su uso indebido si no consignaron de forma clara para terceros el límite de uso o de valor de las transacciones para los que podía emplearse <sup>177</sup>. Esta es una concreción de la obligación de mantener un registro de certificados con rapidez y seguridad, a las que se refieren los art.s 11.e) y 12.c). No obstante, el panorama se complica al determinar el art. 11.e) que «A dicho registro podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten, cuando así lo autorice el signatario», puesto que en este caso se condiciona el cumplimiento por el prestador de servicios de su obligación a un consentimiento del propio firmante. Si la norma obedece al principio del consentimiento para el tratamiento de datos personales en ficheros automatizados –en lo que básicamente consiste

---

<sup>176</sup> Este criterio de la generación de daños es lo que determina la consideración como falta muy grave de determinados incumplimientos formales para los que emitan certificados reconocidos, o meramente grave si los certificados expedidos son no reconocidos. Véase art. 25.1.b) y 2.a)

<sup>177</sup> No puede entenderse este artículo de forma literal, de forma tal que sólo cabrá hablar de responsabilidad por el prestador de certificados reconocidos en estos dos casos. La mala redacción debe referirse a los supuestos de negligente información sobre los límites de uso y de valor de las transacciones, y no al resto de posibles causas de negligencia.

el registro de certificados–, de acuerdo con el art. 6.1 LOPDP, deberá entenderse tácitamente consentido por cuanto el mantenimiento del servicio de directorio es necesario para el desarrollo del servicio de firma contratado, acogiéndose por ello a la excepción prevista en el art. 6.2 LOPDP. Otra forma de eludirlo será, obviamente, el establecimiento de una cláusula específica de autorización a dicho tratamiento en el contrato de arrendamiento de servicios de firma electrónica, que no obstante requerirá aprobación expresa del contratante-usuario, al ser restrictiva de derechos –a la autodeterminación informativa, en este caso–.

- d) La responsabilidad podrá ser contractual o extracontractual, exigible de acuerdo con el CC, con las especialidades del RDLFE.
- e) La exigencia de fianza o aval por mil millones de pesetas, o por los importes definidos en el art. 12.g) no han de entenderse como límites máximos de exigibilidad, sino como requisitos mínimos de solvencia. El régimen aplicable seguirá siendo el derivado del art. 1911 CC.
- f) La normativa sobre responsabilidad del art. 14 deberá completarse con las normas sobre protección de consumidores y usuarios <sup>178</sup>

*En especial, los prestadores de servicio de certificación públicos*

Como ya se dijo, los prestadores de estos servicios pueden ser personas físicas o jurídicas, tanto públicas como privadas.

En el caso de ser personas jurídicas públicas (Administraciones, organismos o sociedades de ellas dependientes) el art. 4.2 exige que lleven cuentas separadas y actúen bajo los principios de objetividad, transparencia y no discriminación.

---

<sup>178</sup> Leyes 26/1984, de 19 de julio, General para la defensa de consumidores y usuarios ; y Ley 7/1998, de 13 de abril, de condiciones generales de contratación.

La duda que surge al interpretar este artículo en combinación con el art. 1.1, en el que se establece como ámbito de la norma el de la «prestación al público de servicios de certificación» es si estos servicios, prestados por entes públicos, son los que se prestan al ciudadano como consecuencia de un contrato de arrendamiento de servicios regulado por el Derecho Privado o también incluye la certificación de los órganos públicos a los que presta servicio en exclusiva, siendo entonces la certificación el resultado del cumplimiento del ejercicio de funciones públicas. La consecuencia de esta cuestión será que el régimen de prestación de certificación de la firma electrónica avanzada empleada como requisito de validez del acto administrativo o judicial, realizada por los entes públicos a los que se encomiende tal función, no quedará sometido al régimen de los arts. 7, 11 y 12 del RDLFE, sino al que establezca la normativa que expresamente los regule <sup>179</sup>.

Nos decantamos por esta opinión sobre la base de los siguientes argumentos:

- a) Las normas que regulan la validez de los documentos administrativos y judiciales no exigen el empleo de la firma electrónica, sino la consecución de determinados resultados (conservación, integridad, disponibilidad, autenticidad, constancia del envío y recepción), que pueden conseguirse simplemente mediante el empleo de una firma electrónica avanzada sin que ésta tenga que venir amparada en un certificado reconocido o no. Qué duda cabe de que la adopción del esquema firma electrónica avanzada-certificado reconocido acrecienta la confianza en el requisito formal de la firma, pero la publicación de la identidad del firmante (en este caso la Administración), vendrá determinada por la propia ley y por el hecho de que previamente habrá

---

<sup>179</sup> Ello sin perjuicio de que se sometan, por aplicación analógica, al régimen del RDLFE en todo cuanto les sea aplicable, lo que no siempre será posible, dada la orientación empresarial que subyace en el RDLFE. Así parece haberlo entendido la DGRN, al haber regulado por medio de la Instrucción de 19 de octubre de 2000 el uso de la firma de los fedatarios públicos, en la que ordena a los Consejos Nacionales del Notariado y al Colegio de Registradores de la Propiedad y Mercantiles de España su constitución como prestadores de servicio de certificación acreditados, conforme a lo dispuesto en el RDLFE, «a los únicos efectos de expedir certificados electrónicos mediante los que se vinculen unos datos de verificación de firma a la identidad, cualidad profesional y situación administrativa de los miembros en activo integrados en las respectivas corporaciones.»

de haberse admitido por el administrado o justiciable el empleo de estos medios de comunicación <sup>180</sup>

- b) Para el cumplimiento de estos requisitos en un esquema técnico-organizativo análogo al empleado por el RDLFE, han sido dictadas normas específicas para los prestadores de servicios de certificación en la Administración Pública. Por su interés, nos referiremos posteriormente a este argumento.
- c) No es posible el cumplimiento de los requisitos exigidos por el RDLFE para que los certificados asociados a las firmas electrónicas avanzadas que emplee la Administración tenga el valor determinado por el art. 3.1. Si la firma avanzada ha de basarse en un certificado reconocido, que ha de incluir el contenido especificado en el art. 8, no se entiende cómo va a tener que contarse con el consentimiento expreso del funcionario a quien se atribuye la firma para incluir el puesto o cargo que ocupa o cualquier otra circunstancia personal que sea significativa en función del fin propio del certificado (aptdos. 1.e) y 2). O bien se entiende en este caso que se aplicaría analógicamente lo dispuesto en el apartado siguiente, relativo a la actuación en nombre de personas físicas o jurídicas, o bien se consideraría que no haría falta contar con el consentimiento del funcionario al constituir su cargo un dato público que excluye la necesidad de consentimiento para su tratamiento en virtud de las exclusiones previstas en la LOPDP <sup>181</sup>. El

---

<sup>180</sup> En el ámbito administrativo viene exigido por el art.7.2.c) RTEIT: «Las comunicaciones y notificaciones efectuadas en los soportes o a través de los medios y aplicaciones referidas en el apartado anterior serán válidas siempre que: [...] c) En los supuestos de comunicaciones y notificaciones dirigidas a particulares, que éstos hayan señalado el soporte, medio o aplicación preferente para sus comunicaciones con la Administración General del Estado en cualquier momento de la iniciación o tramitación del procedimiento o del desarrollo de la actuación administrativa.»

En el ámbito judicial, el art. 162.1 LEC: «Cuando los juzgados y tribunales y las partes o los destinatarios de los actos de comunicación dispusieren de medios electrónicos, telemáticos, infotelecomunicaciones, o de otra clase semejante, que permitan el envío y la recepción de escritos y documentos, de forma tal que esté garantizada la autenticidad de la comunicación y de su contenido y quede constancia fehaciente de la remisión y recepción íntegras y del momento en que se hicieron, los actos o comunicación podrán efectuarse por aquellos medios, con el acuse de recibo que proceda. Las parte sy profesionales que intervengan en el proceso deberán comunicar al tribunal el hecho de disponer de los medios indicados y su dirección.»

<sup>181</sup> Esta norma, al fin y al cabo, protege el principio del consentimiento del art. 6 LOPDP. Si la entendemos así, habremos de hacer referencia a dicho precepto en toda su integridad, siendo así que el mismo excluye tal requisito en determinados supuestos: «2.No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el

cargo del funcionario es un dato exigido por las normas de procedimiento administrativo y judicial para identificar al órgano del que emanan y el ejercicio por él de la competencia, razón por la que puede ampararse en el régimen de excepción del principio de consentimiento de la LOPDP aunque sea negando la aplicación en estos casos del cumplimiento de los preceptos del art. 8 RDLFE.

- d) Los prestadores de servicio de certificación *internos* de la Administración están exentos de la prestación de la garantía o fianza establecida en el art. 12. g). En este caso, o bien presumimos que estos recursos en los entes públicos que realizan esta función *ad intra* de la propia organización administrativa por aplicación directa del art. 44 de la Ley General Presupuestaria <sup>182</sup>; o bien, nuevamente, habremos de entender que no es de aplicación a estos casos, con la nueva quiebra de la dicción literal del art. 3.1.
- e) Igual cabe decir de la información al usuario (en este caso el funcionario administrativo o judicial al que se atribuye el uso de la firma electrónica) sobre las condiciones de utilización del certificado, así como de la información al público en general de las condiciones y criterios que se comprometen a seguir. En este supuesto el defecto proviene de la dicción del RDLFE, puesto que la Directiva deja, al regular estos requisitos, abierta la posibilidad a que no sean de aplicación a todos los casos al referirse en el Anexo II.k) a «Antes de entrar en una relación contractual con una persona que solicite un certificado para apoyar a partir del mismo su firma electrónica...». Sólo con una interpretación correctora sobre la base de este requisito tal y

---

ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento»

<sup>182</sup> Art. 44 LGP: «1. Los Tribunales, Jueces y Autoridades administrativas no podrán despachar mandamientos de ejecución ni dictar providencias de embargo contra los derechos, fondos, valores y bienes en general de la Hacienda Pública. 2. El cumplimiento de las resoluciones judiciales que determinen obligaciones a cargo del Estado o de sus Organismos Autónomos corresponderá , exclusivamente, a la Autoridad administrativa que sea competente por razón de la materia, sin perjuicio de la posibilidad de instar, en su caso, otras modalidades de ejecución de acuerdo con la Constitución y las Leyes. 3. La Autoridad administrativa encargada del cumplimiento acordará el pago en la forma y con los límites del respectivo presupuesto. Si para el pago fuera necesario un crédito extraordinario o un suplemento de crédito, deberá solicitarse de las Cortes Generales de acuerdo uno u otro dentro de los tres meses siguientes al de notificación de la resolución judicial.»



como lo establece la Directiva sería posible entender cumplido el art. 12 en este extremo informativo.

El art. 81 de la Ley 66/1997, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, autorizó a la FNMT para prestar 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 (EIT) en las relaciones entre órganos de la Administración General del Estado entre sí o con órganos vinculados a ella, y las mantenidas entre personas físicas o jurídicas y aquélla. Para tal función contaría con la colaboración de la entidad pública empresarial Correos y Telégrafos, que actuará como autoridad de registro local <sup>183</sup>. Estos servicios podrán acoger las relaciones de los administrados con las Administraciones Autonómicas y Local, siempre que se suscriba el correspondiente convenio de colaboración. Las normas de desarrollo serán dictadas en el plazo de un año por el Gobierno

Del art. 81 citado puede desprenderse que pretende regular todas las condiciones adicionales a las previstas por el art. 45 LRJPAC y el RTEIT precisas para el cumplimiento de los fines allí propuestos. El régimen de estas firmas no pasa, por tanto, por el contenido del RDLFE, referido a la prestación al público de estos servicios <sup>184</sup>, sino por las normas de desarrollo de este precepto <sup>185</sup>.

---

<sup>183</sup> La FNMT recibió un nuevo Estatuto y Denominación (Real Casa de la Moneda) por virtud el RD 114/1999, de 25 de junio, cuyo art. 2.1.g) y h), respectivamente, le autorizan a prestar los servicios de entidad de certificación en el ámbito de las Administraciones Públicas y a personas físicas y jurídicas, públicas y privadas, actuando en este último caso con arreglo al Derecho Privado.

La regulación ha de complementarse con la Orden de 26 de julio de 1999, del Ministerio de Economía y Hacienda, por la que se regulan las bases de datos y ficheros automatizados de carácter personal existentes en la FNMT-RCM.

<sup>184</sup> Sin perjuicio de que puedan ser prestados por entes públicos empresariales con arreglo al Derecho Privado, en cuyo caso sí será de aplicación el RDLFE.

<sup>185</sup> A pesar de ello, y como venimos manteniendo, las relaciones son grandes, y no dejan de ser reflejadas en las propias normas regulatorias. La Exposición de Motivos del RD 1290/1999 justifica el carácter no exhaustivo del mismo, en desarrollo de este art. 81, precisamente por estar pendiente la aprobación de la Directiva comunitaria sobre firma digital, «con la que este Real Decreto está íntimamente relacionado». Lo que realiza el RD es una regulación paralela a la de la Directiva, acogiéndose al mismo esquema técnico y organizativo de firma electrónica avanzada-certificado reconocido-prestador de servicios de certificación acreditado, como posteriormente admite el mismo párrafo. Así, se condicionan los requisitos de validez establecidos a lo que posteriormente estableciera la Directiva, de acuerdo con la Disposición Adicional Tercera.

La norma de desarrollo está constituida por el RD 1290/1999, de 23 de julio, que desarrolla el art. 81 de la Ley 66/1997. El mismo no afecta al régimen de aplicación de medios telemáticos para la generación de documentos electrónicos establecido por el RTEIT, según declara el art. 2.3, ni a los relativos a información clasificada, a la Defensa Nacional o a la seguridad el Estado.

El art. 7 declara autoridad de registro local a Correos y Telégrafos, al asignarle las funciones de recibir las solicitudes de inscripción en el Registro de usuarios, la acreditación de su identidad y la entrega de los títulos de usuarios, y, eventualmente, en las operaciones de sellado temporal (timestamping).

Los usuarios físicos o jurídicos, públicos o privados, deberán solicitar su inscripción en el Registro de Usuarios regulado en el art. 11, actuando como condición legal de empleo de los certificados, que no les serán entregados hasta que se verifique.

La Disposición Adicional Cuarta aprobaba el Anexo de condiciones técnicas de desarrollo y prestación del servicio. Este anexo cobró especial interés en virtud del art. 51 de la Ley 50/1999, de 30 de diciembre, que modificó el art. 81 de la Ley 66/1997, puesto que, aparte de ampliar las facultades de intervención como entidad certificadora al ámbito de la Administración de Justicia, determinaba la aplicación temporal de dicho anexo a cualesquiera otros proveedores de servicios de certificación electrónica distintos de la FNMT-RCM que prestaran los servicios a la Administración de Justicia. Este precepto suscita la duda de si se refiere a las entidades o empresas que prestaran sus servicios a la Administración de Justicia o a todo prestador de servicios de certificación electrónico, en tanto no fuera desarrollado el RDLFE. Creemos que debe dirigirse únicamente a los que prestan estos servicios a la Administración de Justicia, pues la Directiva y el RDLFE no regula requisitos técnicos obligatorios para los que se dediquen a estos servicios, por aplicación del principio de neutralidad tecnológica. Tampoco creemos que la asunción de este Anexo confiera a la empresa o entidad que los cumpla la condición de prestador acreditado, a los efectos del RDLFE, dado que la legislación de la

FNMT no le confiere ese carácter en ningún momento por el cumplimiento de estos requisitos <sup>186</sup>.

#### 1.2.d) Conclusión

La variedad de regímenes legales aplicables a la firma electrónica, así como las divergencias halladas en el RDLFE en relación con el tenor de la Directiva, hacen aconsejable la elaboración de un texto único que refunda y aclare las normas relativas al uso de la firma electrónica tanto en el sector público como privado.

Igualmente es de exigir el pronto desarrollo reglamentario del RDLFE (establecimiento del Registro de Certificadores, del Registro de Usuarios de FNMT-RCM, etc, aprobación de las normas de homologación de los productos de firma electrónica), con el fin de poder hacer uso de la presunción probatoria incluida en el RDLFE. Entre tanto, desde el punto de vista procesal, no podrá admitirse la equiparación de los documentos electrónicos a los documentos públicos o privados sino para los documentos judiciales y administrativos, y en el caso de los primeros únicamente cuando el Consejo General del Poder Judicial, en virtud de lo establecido en el art. 230.3 LOPJ, apruebe los programas a emplear con tal fin.

---

<sup>186</sup> El sentido del Anexo de condiciones técnicas y administrativas se relaciona con el art. 1 del RD 1290/1999, en el que se declara el objeto de la norma: «La presente disposición tiene por objeto desarrollar reglamentariamente la prestación, por la FNMT-RCM, en colaboración con la entidad pública empresarial Correos y Telégrafos, de los servicios técnicos y administrativos necesarios para garantizar la seguridad, la validez y eficacia de las comunicaciones de la Administración General del Estado y sus organismos públicos, a través de técnicas y medios electrónicos, informáticos y telemáticos (EIT), en los términos establecidos en el art 81 de la Ley 66/1997, de 30 de diciembre, de Medidas fiscales, administrativas y del orden social». Como señala BONET COMPANYY [*op.cit.* pág. 231], lo que realiza el art. 81 es la integración de la actuación de la FNMT entre los requisitos exigidos por la LRJPAC para la validez y eficacia de los documentos electrónicos administrativos. El anexo cumple la misión de concretar

la actuación requerida de la FNMT como entidad certificadora, lo que ha de predicarse de cualquier otro prestador que preste los mismos servicios a la Administración de Justicia.