Foro, Nueva época, núm. 3/2006: 397-465 ISSN:1698-5583

EN LA LEY 59/2003, DE 19 DE DICIEMBRE, DE FIRMA ELECTRÓNICA

Ana I. BERROCAL LANZAROT
Profesora Contratada
Doctora de Derecho Civil
Universidad Complutense de Madrid
anaberrocal548@hotmail.com

RESUMEN

La nueva Ley 59/2003, como respuesta a la necesidad de conferir seguridad a las comunicaciones por Internet y reforzar el marco jurídico existente, incorpora una serie de novedades en la regulación de la firma electrónica. Así se crea un concepto nuevo de firma electrónica demandado por el sector, la firma electrónica reconocida, que se equipara funcionalmente a la firma manuscrita; se exigen una serie de garantías a cumplir por los dispositivos de creación de firma; se incluye dentro de la modalidad de prueba documental al soporte en que figuran los datos firmados electrónicamente; se exige una especial legitimación a las personas físicas solicitantes de responsabilizarse de la custodia de tales datos, y se establece un régimen aplicable a la actuación de las personas jurídicas firmantes.

Palabras clave: firma electrónica, firma digital, documento electrónico, firma manuscrita, prueba documental, firmante, persona jurídica, certificado reconocido, claves.

ABSTRACT

The new Law 59/2003, as a response to the need to award safety to communications in the Internet and to reinforce the existing legal frame, incorporates several innovations related to the regulation of the electronic signature. So it is created a new concept of electronic signature demanded by the sector, the electronic qualified signature, which is compared functionally to the manuscript signature; a series of guarantees are demanded to expiring for the devices of creation of electronic signature; it is included inside the modality of documentary evidence to the support in which the signed information appears; a special legitimation is demanded to solicitors of taking responsibility of the custody of such information; and, there is established a regime applicable to the performance of legal persons signatories.

Keywords: electronic signature, digital signature, electronic document, manuscript signature, documentary evidence, signatory, legal person, qualified certificate, keys.

ZUSAMENFASSUNG

Das neue Gesetz 59/2003, als Antwort auf die Notwendigkeit, den Komunikationen im Internet Sicherheit zu leisten und den bestehenden juristichen Rahmen zu verstärken, nimmt eine Reihe der Neuigkeiten in der Regelung der elektronischen Signatur auf. Auf diese Weise wird ein neuer, vom Sektor verklagter Begriff von der elektronischen Signatur erschaffen - die anerkannte elektronische Signatur, die sich zweckmässsig zur eigenhändigen Unterschrift ausstattet. Es werden eine Reihe von Garantien, die man ausführen muss, für die Vorrichtung der Unterschriftschaffen gefordert; dies wird als belegte Beweisart dorthin eingeschlossen, wo die elektronisch unterschriebene Daten erscheinen. s wird eine espezielle Beglaubigung von der Antragsteller und zwar, dass sie die Verantwortung für die Verwahrung diesen Daten übernehmen.Und es wird ein verwendbares Regim auf die unterschriebene juristiche Personen eingeführt.

Schlüsselwörter: elektronische Signatur, digitale Unterschrift, elektronisches Dokument, eigenhändige Unterschrift, belegte Beweis, juristische Person, Signaturprüfschlüssel.

I. CONSIDERACIONES GENERALES

La regulación de la firma electrónica en España se encuentra actualmente en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica (en adelante, LFE)[1]. Su entrada en vigor ha tenido lugar el 20 de marzo de 2004, a los tres meses de su publicación[2]. Una *vacatio legis* que a buen seguro tiene su razón de ser en la necesaria adaptación de todos los agentes afectados por la norma a los notables cambios de fondo que se contienen en la misma y a las disposiciones novedosas que viene a introducir en lo que constituye el procedimiento de autenticación electrónica[3]. Supone

[1] *BOE*, núm. 304, de 20 de diciembre de 2003, pp. 45329 a 45343.

[2] Véase Disposición Final tercera.

[3] En este sentido, G. GÁLLEGO HIGUERAS, «Comentarios a la reciente Ley 59/2003, de 19 de diciembre, de Firma electrónica: algunas novedades al marco regulador existente», en *Revista Aranzadi de Derecho y Nuevas Tecnologías,* año 2004-3, número 6, p. 22.

la derogación de la normativa hasta esas fechas existente, el Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica[4] (en adelante, RDL 14/1999), primera norma legal que, con un ámbito de aplicación general y no meramente sectorial, reguló, en el Derecho español, la firma electrónica, los certificados y los prestadores de servicios de certificación. Su publicación, que mereció en su momento una valoración positiva, resultó esencial para fomentar el progreso de las transacciones electrónicas en España, para la difusión del concepto de firma electrónica, si bien no se desarrolló de forma completa (quedando pendiente, entre otras materias: la acreditación de prestadores, la certificación de dispositivos, registro de prestadores), de ahí la consecuencia de su escasa aplicación efectiva y utilidad real[5]. Fue, asimismo, objeto de duras críticas no sólo por el procedimiento empleado para su aprobación, pues se entendía discutible que concurrieran los presupuestos de extraordinaria y urgente necesidad que exige el art. 86 de la Constitución española de 1978 para otorgar dicha facultad extraordinaria de dictar normas con rango de ley al Gobierno (siguiendo este camino, se trataba de evitar la tramitación parlamentaria del texto), sino también por el tiempo en que se aprobó, en concreto, con anterioridad a la Directiva comunitaria 1999/93/CE, de 13 de diciembre, del Parlamento Europeo y del Consejo, por la que se establece un marco comunitario para la firma electrónica, Directiva que buscaba armonizar y reforzar el marco jurídico de la firma electrónica y la prestación de servicios de certificación[6].

Y aunque es cierto que estaba en fase avanzada la tramitación del proyecto de directiva sobre firma electrónica, al haber sido ya informada favorablemente en la sesión del Consejo de Ministros de Telecomunicación de

---

[4] Y de Cuentas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley. Véase Disposición Derogatoria única.

[5] En el apartado IV de su Exposición de Motivos se señala como justificación para su existencia que «*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*».

[6] Véanse G. MEDINA ORS y J. RIUS GARRETA, «La firma electrónica: su relevancia jurídica y su tratamiento en el Real Decreto-ley 14/1999», *CM,* núm. 9, 20 de enero de 2000, p. 27; A. MARTÍNEZ NADAL, «Comentario de urgencia al urgentemente aprobado Real Decreto-ley, de 17 de diciembre, sobre firma electrónica (I)», *La Ley,* núm. 4939, 1 de diciembre de 1999, p. 1; M.ª I. HUERTA VIESCA, «La firma electrónica en la regulación española: valoración crítica», en *Los prestadores de Servicios de Certificación en la Contratación Electrónica*, M.ª I. HUERTA VIESCA y RODRÍGUEZ-RUIZ DE VILLA (coords.), Aranzadi, 2001, p. 21; G. ALCOVER GARAU, «EL Real Decreto-ley sobre firma electrónica», *Revista de la Contratación Electrónica,* núm. 1, 2000, pp. 26-27.

la Unión Europea, celebrada el 22 de abril de 1999, por lo que los contenidos básicos estaban ya establecidos, no por ello es menos cierto que lo que se estaba llevando a cabo por el citado Real Decreto era una incorporación *ex ante* del contenido de la Directiva susceptible de alguna variación, que no podrían ser tenida en cuenta por las autoridades españolas, y que exigiría una necesaria adaptación ulterior, como así tendría lugar. Si bien, en su Exposición de Motivos se indicaba que *«este Real Decreto-ley persigue, respetando el contenido de la posición común respecto de la Directiva sobre firma electrónica, establecer una regulación clara del uso de ésta, atribuyéndole eficacia jurídica y previendo el régimen aplicable a los prestadores de servicios de certificación»,* hubiera resultado más lógico para tal propósito con esperar a la aprobación de la propuesta de directiva apenas tres meses después.

Tras su ratificación por el Congreso de los Diputados [7], se acordó proceder a su tramitación como proyecto de ley, con el fin de someterlo a una más amplia consulta y al posterior debate parlamentario para perfeccionar su texto. Sin embargo, esta iniciativa decayó al expirar el mandato de las Cámaras en marzo de 2000.

Posteriormente, con el inicio de una nueva Legislatura se presentaron dos anteproyectos (en adelante, BALFE), el primero a principios de 2002 por parte del Ministerio de Ciencia y Tecnología, con el que se pretendía dar cumplimiento precisamente al compromiso adquirido por el Gobierno de tramitar como ley ordinaria el citado Real Decreto 14/1999, y de eliminar las posibles divergencias que la anticipación en la aprobación de éste habían provocado con respecto a la Directiva comunitaria de firma electrónica; y el segundo de fecha 26 de julio de 2002, que fue resultado de una amplia consulta a la que se sumaron más de cincuenta entidades del sector, la Agencia de Protección de Datos, la Comisión del Mercado de Telecomunicaciones, el Consejo de Consumidores y Usuarios, el Consejo Asesor de las Telecomunicaciones y de la Sociedad de la Información, el Colegio de Registradores de la Propiedad y Mercantiles de España y el Consejo General del Notariado. Participó en su elaboración el Ministerio de Ciencia y Tecnología en estrecha colaboración con los Ministerios de Administraciones Públicas, Economía, Interior y Justicia y la Agencia Tributaria; y, tras su aprobación en 2003 por el Consejo de Ministros, inicia su tramitación parlamentaria como proyecto de ley [8], a cuyo texto articulado se presenta-

[7] Resolución de 21 de octubre de 1999 (*BOE,* 27 de octubre de 1999).

[8] Proyecto de Ley 121/000158, de 20 de junio de 2003. *BOCG*, Congreso de los Diputados, núm. 158-1, Serie A, 20 de junio de 2003, pp. 1 a 17.

ron un total de 234 enmiendas en el Congreso y de 289 en el Senado, que culmina, con su aprobación el 11 de diciembre de ese mismo año por el pleno del Congreso, en la actual Ley.

Una Ley que, por un lado, como indica su Exposición de Motivos, *«es el resultado del compromiso asumido en la VI Legislatura (de tramitar como proyecto de ley el Real Decreto-ley 14/1999), actualizando a la vez el marco establecido en el Real Decreto 14/1999, mediante la incorporación de las modificaciones que aconseja la experiencia acumulada desde su entrada en vigor en nuestro país, como en el ámbito internacional»*. De esta forma se consigue una mayor transparencia en su tramitación y debate en una materia que por su especial trascendencia lo demanda. Debate público llevado a cabo no sólo en la fase parlamentaria, sino también en las fases previas a su elaboración y presentación, a través de una ronda de consultas a expertos en la materia y un período de exposición pública, cuyo resultado, como hemos señalado, fue la redacción de la segunda versión del proyecto de ley sobre firma electrónica citado [9].

Y, por otro, supone la incorporación al ordenamiento interno de la regulación contenida en la Directiva 1999/93/ CE, de 13 de diciembre de 1999, del Parlamento Europeo y del Consejo, y no, como erróneamente se pretende en la citada Exposición de Motivos de la Ley, que dicha incorporación tuviera lugar con el Real Decreto 14/1999, pues, desde un punto de vista formal, la propia fecha de aprobación del mismo sólo le permitió atender a la propuesta de directiva. Por ello, ha de considerarse que la transposición formal de la Directiva la lleva a cabo la actual Ley. De hecho, en la misma se eliminan algunas de las divergencias existentes entre el texto legal español hasta entonces en vigor y el de la Directiva.

Asimismo, esta nueva Ley parece tener presente en la elaboración de su contenido la Ley Modelo para las firmas electrónicas de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI/ UNCITRAL), aprobada, junto a su Guía, el 5 de julio de 2001.

Consta de 36 artículos agrupados en seis títulos, diez disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria y tres disposiciones finales.

Tiene como principal finalidad reforzar el marco jurídico existente, incorporando a su texto «algunas novedades respecto del Real Decreto 14/1999, que contribuirán a dinamizar el mercado de la prestación de ser-

---

[9] A. MARTÍNEZ NADAL, *Comentarios a la Ley 59/2003, de firma electrónica,* Madrid, Thomson-Aranzadi, 2004, p. 28.

vicios de certificación, confiriendo seguridad a las comunicaciones a través de internet, y configurando la firma electrónica como instrumento capaz de generar confianza en las transacciones telemáticas, además de agilizar el comercio electrónico. Se permitirá, en consecuencia, una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas»[10].

Constituye su objeto, conforme dispone el art. 1, tanto la regulación de la firma electrónica, como elemento de seguridad de las comunicaciones en sus diversos aspectos, y su eficacia jurídica, como la prestación de servicios de certificación en sus diversos aspectos (objetivo: certificados, y subjetivo: prestadores de servicio de certificación).

Desde tal perspectiva, el presente estudio se va a centrar precisamente en un análisis exhaustivo de lo que constituye el ámbito de aplicación objetivo de la Ley 59/2003, más en concreto, en la regulación de la firma electrónica y su eficacia jurídica, destacando las novedades que la misma aporta frente a la anterior regulación del RDL 14/1999. Para su realización se tendrá en cuenta el antecedente más inmediato de esta regulación, representado en el citado Real Decreto 14/1999, como en la legislación comunitaria contenida en la mencionada Directiva sobre firma electrónica. Asimismo, tendremos presente los trámites parlamentarios de la norma, como las aportaciones numerosas de la doctrina sobre esta materia.

Ahora bien, sobre el contexto global en que se desarrolla el mundo de internet y, por tanto, la materia objeto de análisis, no sería completo nuestro estudio si no incorporásemos al mismo una mención de la normativa existente en el ámbito europeo[11], como fuera del mismo[12], sobre firma

---

[10] Apartado II de la Exposición de Motivos de la Ley.

[11] Al igual que en España, antes de la Directiva, algunos Estados habían procedido a aprobar su propia normativa en esta materia, otros tenían proyectos en fase de tramitación. Así, en *Alemania,* la regulación sobre firma electrónica se contenía en la *Gesetz zur Regelung der Rahmenbedingungen für Informations –und Kommunikationsdients (Informations –und Kommunikationsdienste– Gesetz-IukDG),* de 13 de junio de 1997 (*BGBI, I,* de 28 de junio), y en *Italia,* en el art. 15, *comma* 2, Ley de 15 de marzo de 1997, núm. 59, de *Delega al Governo per il conferimento di funzioni e compiti alle Regione ed enti locati, per la reforma della Publica Amministrazione e per la semplificazione administrativa* (*Gazzetta Ufficiale*, núm. 63, suppl. ord., 17 de marzo de 1997), y el Decreto del Presidente de la Republica Italiana núm. 513, de 10 de noviembre de 1997, *Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informaticie e telematici, a norma dell'articolo 15, comma 2,* de la Ley núm. 59, 15 de marzo de 1997 (*Gazzetta Ufficiale*, núm. 60, 13 de mazo de 1998). Ambas normativas han tenido que ser modificadas para adaptarse a la Directiva comunitaria. La *Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften (Signaturgesetz),* de 16 de mayo de 2001

(*BGBI, I,* núm. 22, 21 de mayo de 2001, pp. 876 y ss.), que reemplaza a la Ley 1997, e, igualmente el anterior *Verordnung zur digitalen Signatur (SigV)* (Reglamento de firma electrónica), de 22 de octubre de 1997 (*BGBI, I,* 26 de octubre, pp. 2498 y ss.) ha sido sustituido por *Verordnung zur elektronischen Signatur (Signaturverordnung-SigV),* de 24 de octubre de 2001, publicado el 16 de noviembre de 2001 (*BGBI, I,* 16 de noviembre de 2001, pp. 3074 y ss.) Y el Decreto italiano de 28 de diciembre de 2000, núm. 445 *(Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa– Testo A),* que, igualmente reemplaza a la regulación existente en el Reglamento de 1997, modificado parcialmente por Decreto Legislativo de 23 de enero de 2002, núm. 10, «*Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche»,* publicado en la *Gazzetta Ufficiale,* núm. 39, de 15 de febrero de 2002, que ha introducido, asimismo, nuevos artículos sobre la materia. Y modificado, nuevamente, este Decreto de 28 de diciembre de 2000, por Decreto de 7 de abril de 2003, núm. 137, publicado en la *GU,* núm. 138, 17 de junio de 2003.

Asimismo, con posterioridad a la aprobación de la Ley de Firma Electrónica, en Alemania se ha dictado la importante Ley de 13 de julio de 2001, de adaptación de las formalidades del Derecho privado y de otras disposiciones al moderno tráfico de actos jurídicos, en virtud de la cual se intenta introducir el concepto y la terminología de la firma electrónica a determinados textos legales de carácter sustantivo. Se produce, así, modificaciones esenciales en el Código Civil y en la Ley de Enjuiciamiento Civil. Respecto al primero, se añade un nuevo apartado 3 al parágrafo 126, en el que se dispone expresamente que la forma escrita puede ser sustituida por la forma electrónica, y se crean dos nuevos parágrafos, el parágrafo 126.*a),* en donde se regula la forma electrónica, y el parágrafo 126.*b)* referido al *Text form* (art. 1 de la Ley), y con respecto a la Ley de Enjuiciamiento Civil que se pretende su adaptación a las nuevas tecnologías, y, en concreto, se constata la existencia del documento electrónico como prueba, se habla de documentos electrónico en el parágrafo 130.*a)* y se regula la prueba de apariencia en caso de firma electrónica cualificada en el parágrafo 292.*a)* (art. 2 de la Ley).

Hay que destacar también en este *iter* legislativo europeo la regulación existente en *Francia* representada por la Ley núm. 2000-230, de 13 de marzo de 2000, sobre adaptación del derecho de prueba a las nuevas tecnologías de la información y relativas a la firma electrónica (publicada en el *Boletín Oficial, JO,* núm. 62, de 14 marzo de 2000, p. 3968) en la que se introduce una modificación al Capítulo VI, «De la prueba de las obligaciones y del pago», concretamente a los arts. 1315, inciso 1, y 1316, incisos 1 al 4, del *Code*, y el Decreto núm. 2001-272, de 30 de marzo de 2001, para la aplicación del art. 1316.4 del *Code* y relativo a la firma electrónica, modificado a su vez por Decreto 2002-535, de 18 de abril de 2002.

En *Bélgica*, con la Ley belga de 9 de julio de 2001 (*Moniteur Belgue du 29 de septembre 2001*) en la que se fijan ciertas reglas relativas al régimen jurídico de las firmas electrónicas y de servicios de certificación y, asimismo, en *Luxemburgo*, con el Reglamento de 1 de junio de 2001 relativo a las firmas electrónicas, al pago electrónico y a la creación del Comité de Comercio electrónico.

Por su parte, en *Portugal*, hay que mencionar el Decreto-ley portugués 290-D/99, de 2 de agosto, que aprueba el régimen jurídico de los documentos electrónicos y de firma digital, y que aún no ha adaptado su contenido a la normativa comunitaria.

[12] Así, habrá de tenerse igualmente presente, por un lado, la primera Ley de firma digital (la *Utah Digital Signature Act,* publicada en mayo de 1995), y la «*Federal Electronic Signatures in Global and Nacional Comerse Act» (E-Sing Act)*, cuya aprobación tuvo lugar el 30 de junio de 2000, vigente desde el 1 de octubre de 2000, fue precisamente debida a la fragmentación, dispersión y heterogeneidad existente en la regulación sobre firma electrónica en Estados Unidos ante la actuación legislativa asumida y llevada a efecto por prácticamente todos los Estados de la Unión.

electrónica, y llevásemos a cabo un enfoque comparativo de la misma con nuestra legislación.

Como, igualmente, no lo sería si no se tuviese en cuenta la normativa contenida en la Ley de Enjuiciamiento Civil 1/2000, de 7 de enero, que regula la eficacia del documento electrónico en el proceso civil; en la Ley 24/2001, de 27 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, abreviadamente Ley de Acompañamiento, por la que se disipan todas las dudas sobre la validez y eficacia del «documentos público electrónico», al permitir la plena operatividad de la firma electrónica y del documento público electrónico y su uso por Notarios y Registradores [13], recientemente modificada por la Ley 24/2005, de 18 de noviembre, de reformas para el impulso de la productividad [14]; y, en sede de comercio electrónico, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del comercio electrónico (en adelante, LSSI), y la Directiva 2000/31/CEE, de 8 de junio de 2000, del Parlamento Europeo y del Consejo, sobre aspectos jurídicos de los servicios de sociedad de la información, en particular el Comercio Electrónico en el mercado interior (Directiva sobre comercio electrónico).

II. FIRMA ELECTRÓNICA Y SU EFICACIA JURÍDICA

El art. 3 de la LFE, bajo la rúbrica «Firma electrónica y documentos firmados electrónicamente», dedica su contenido, de forma novedosa, tanto a la regulación de la firma electrónica, a su concepto, clases y efectos y su incorporación al proceso judicial, como a los documentos firmados electrónicamente, sus clases y efectos, y su aprobación como prueba documental en juicio. Del primero de los aspectos de la regulación nos vamos a ocupar en este apartado, como asimismo de una serie de elementos de naturaleza técnica también regulados en la LFE que están relacionados con el funcionamiento de la firma electrónica, como son los datos de creación y verificación de firma y los dispositivos de creación y verificación de firma.

Ahora bien, como hemos señalado de forma novedosa, se presenta la actual regulación, pues lo cierto es que en la evolución normativa del texto

---

[13] *BOE*, núm. 313, fascículo segundo, año CCXLI, de 31 de diciembre de 2001, pp. 50494 a 50619 (específicamente, pp. 50604 a 50606).

[14] *BOE*, núm. 277, de 19 de noviembre de 2005, pp. 37846 a 37868 (especialmente, pp. 37860 a 37862).

legal encontramos cómo en las versiones iniciales del BALFE no existía un precepto unitario semejante, ya que se destinaban dos preceptos a la regulación de parte de esta materia, en concreto, el art. 2, donde se contenían las distintas definiciones de firma electrónica y un art. 3, donde se regulaba la cuestión de los efectos y el valor procesal de la firma electrónica; si bien sólo a partir de la segunda versión del BALFE es cuando aparece la nueva categoría de firma electrónica reconocida, que constituye una de las principales novedades de la LFE. Y es en el proyecto de ley presentado para su tramitación parlamentaria donde ya se destina un único precepto a la materia (art. 3), y donde se contiene asimismo referencia a la firma electrónica reconocida; sin embargo, no se regula tampoco la materia relativa a los documentos firmados electrónicamente, sino que la referencia a su tratamiento jurídico tiene lugar posteriormente, con la presentación en el Senado de la enmienda número 275 por el Grupo Parlamentario Popular, y de su posterior admisión e incorporación al texto [15], que añade tres nuevos apartados (5 al 8) al art. 3, y varía el título inicial bajo el que se rubrica el precepto: «Concepto, clases y efectos de la firma electrónica», que pasa a ser el ya mencionado de «Firma electrónica y documentos firmados electrónicamente».

Precedente normativo en el Derecho español de esta materia se encuentra, no obstante, en la doble regulación contenida en los arts. 2 y 3 del RDL 14/1999, que regulan, respectivamente, el concepto y las clases (art. 2) y los efectos (art. 3) de la firma electrónica; y en el ámbito comunitario, en la Directiva, que igualmente dedica dos preceptos a la materia, el art. 2 a definir la firma electrónica, y el art. 5 a los efectos jurídicos de la firma electrónica. Aun cuando ambas regulaciones coincide sustancialmente en los términos sobre los que se pretende sustentar la materia con la nueva LFE, sin embargo, presentan alguna diferencia con la nueva normativa, en concre-

---

[15] *BOCG*, Senado, núm. 158, Serie II, 21 de octubre de 2003, pp. 108-109. La *justificación* a tal enmienda se basa en los siguientes argumentos: «*La propuesta normativa se basa, si se quiere que la firma electrónica sea útil y operativa, en la necesidad de reconocer eficacia probatoria a los documentos firmados electrónicamente, públicos y privados, como consecuencia de atribuir al soporte material firmado electrónicamente la cualidad de documento, y todo ello con la finalidad de potenciar la sociedad de la información mediante el rápido establecimiento de un marco jurídico para la utilización de una herramienta que aporta confianza en la realización del comercio electrónico en redes abiertas como es el caso de Internet.*

La propuesta normativa no entra a determinar el valor probatorio de los documentos públicos y privados, por cuanto dicho valor y eficacia vendrá establecido por la legislación que resulte de aplicación, deteniéndose tan sólo en los singulares efectos que la incorporación de un dispositivo de firma electrónica reconocida o avanzada pueda producir.»

to, carecen de lo que viene a constituir una novedad más formal que real, como es la creación de una nueva clase de firma electrónica, la firma electrónica reconocida, existente en el ámbito del Derecho comparado; de la consideración del soporte en el que se incorpora la firma como prueba documental a efectos de aportación en el proceso, y de una regulación exhaustiva de los documentos firmados electrónicamente.

1. Concepto y clases

Sobre la premisa que en el comercio electrónico, el clásico documento en soporte papel es sustituido por el novedoso documento electrónico, el apartado 1 del art. 3 de la LFE define de forma general la firma electrónica como «*el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante*».

Se trata de una definición amplia que puede englobar a todo conjunto de firmas electrónicas, desde aquellas más complejas, como la firma digital basada en la criptografía asimétrica, pasando por las firmas basadas en sistemas biométricos como el iris, la propia palma de la mano, la huella dactilar, etc. [16], hasta la más simples, como un nombre u otro elemento identificativo (por ejemplo, la firma manual digitalizada, o un *password* o contraseña), incluido al final del mensaje electrónico, o la existencia de una pregunta-respuesta, y un *pin* de acceso, lo que se denomina tecnología de secreto compartido, de tan escasa seguridad que plantean la cuestión de su valor probatorio a efectos de autenticación o identificación del autor [17].

Asimismo, de este concepto amplio y tecnológicamente indefinido de firma que nos ofrece el citado precepto podemos resaltar las siguientes características de la firma electrónica:

---

[16] A estos sistemas biométricos se refiere expresamente el Decreto italiano de 28 de diciembre de 2000, en cuyo art. 22 dedicado a la firma electrónica, y reformado en parte de su contenido por el Decreto de 7 de abril de 2003, en su letra *e),* define la clave biométrica como «*la secuencia de códigos informáticos utilizados en los mecanismos de seguridad que emplean métodos de verificación de la identidad personal basados en específicas características físicas del usuario*».

[17] Fco. J. GARCÍA MAS, «El documentos público electrónico (I)», en *Nuevas Tecnologías en la contratación: Sociedad Nueva Empresa e Hipoteca Electrónica*, Thomson-Civitas, 2005, p. 127; A. MARTÍNEZ NADAL, «Comentario al art. 3 de la LFE», en *Comentarios a la Ley 59/2003..., op. cit.,* p. 63, quien añade que incluso puede dudarse de la condición de firma, por su utilidad más bien escasa o inexistente, estas firmas tan simples.

La firma electrónica es un conjunto de datos y no un símbolo, sello o grafía electrónica que sirve para identificar al firmante de un mensaje y para acreditar la identificación del mismo, como la integridad del contenido del mensaje.

Se trata de una técnica para identificar al firmante de un documento electrónico.

Los datos de firma electrónica puede forma parte del documento o ir asociados funcionalmente con ellos o, lo que es lo mismo, pueden aparecer como un conjunto independiente. El modo concreto en que en cada momento se manifieste la firma electrónica dependerá del sistema técnico que se elija y de las aplicaciones prácticas que ofrezca cada modalidad.

Por su parte, esta definición era la misma que contenía el proyecto de ley que se presentó a las Cortes para su posterior tramitación parlamentaria, pero no así de las dos versiones que le precedieron [18].

Su antecedente se encuentra en el art. 2 del RDL 14/1999, que establecía en su apartado *a)* un concepto general de firma electrónica —coincidente básicamente con el contenido en el art. 2.1 de la Directiva y muy similar al que posteriormente se ofreció por la primera versión del borrador de anteproyecto de firma electrónica—, se expresaba en estos términos: *«es el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o los autores del documento que los recoge»*.

El art. 2.1 de la Directiva conceptúa, asimismo, la firma electrónica como: *«los datos en forma electrónica anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio de autenticación»*.

Y, en similares términos, la Ley CNUDMI/UNCITRAL de firma electrónica en su art. 2 la define como: «*los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en los mensajes de datos*» [19].

---

[18] La versión primera del BALFE definía 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 al autor o a los autores del documento que la recoge*».

La versión segunda del BALFE establecía la siguiente definición, en el que se sustituye el término identificación por el de autenticación, también utilizado en la normativa comunitaria: «*el conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio de autenticación*».

[19] De las definiciones expuestas (RDL 14/1999, LFE, Directiva, Modelo UNCITRAL) coinciden únicamente en el reconocimiento de la firma electrónica como datos en forma

De las funciones que se exige a la firma electrónica que garantiza la seguridad de las transacciones electrónicas como son: 1) la integridad —garantía de que los datos originales no han sido modificados, si la firma se verifica correctamente por el destinatario—; 2) la autenticidad —garantía de que el firmante de un documento electrónico está identificado a través del certificado emitido por el prestador de servicios de certificación—; 3) confidencialidad; 4) no repudio —la firma está asociada unívocamente a la clave privada del firmante, por lo que mediante el uso de la clave pública correspondiente, la firma puede serle atribuida directamente a éste—; para la firma electrónica simple el art. 3.1 sólo exige la relativa a la identificación del firmante, no siendo necesario que la firma dé también integridad al mensaje. Identificación que también, como veremos, se predica de la firma avanzada y reconocida, y que ha sido discutida por la doctrina en el sentido, de que lo único que puede determinar, sobre todo para la firma reconocida, es que esa firma está vinculada o pertenece a un titular, pero no que efectivamente haya sido utilizada por el mismo, ni su nexo, por tanto, con el documento [20]. A diferencia de la firma en los documentos cartáceos de contenido negocial, que consiste en declarar la voluntad del autor del mensaje, y precisa, por eso, de una actuación personal del mismo; la llamada firma electrónica, por el contrario, es escindible o separable de la persona, pudiendo accionar la misma, su mismo titular o un tercero, con o sin el consentimiento de aquél [21].

Sobre esta función identificativa del titular de la firma se refiere también el art. 1.316-4 del *Code Civil*, cuando establece que: «*la signatura nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste la consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officer public, elle confère l'authenticité à cet acte*» [22]. El parágrafo 2 de la Ley alemana 2001, al definir la *elektronische signaturen* como «*daten in elektronischer forma, die anderen elektronischen daten beigefügt oder logisch mit ihnen verknüpft sind und die zur*

---

electrónica, consignados o asociados a otros datos electrónicos y que sirven para identificar al que firma.

[20] Véanse Fco. J. GARCÍA MAS, *Comercio y firma electrónicos (Análisis jurídico de los servicios de la sociedad de la información),* 2.ª ed., Valladolid, Lex Nova, 2004, p. 57; A. RODRÍGUEZ ADRADOS, *Firma electrónica y documento electrónico, Escritura Pública. Ensayos de Actualidad,* Madrid, Colegios Notariales de España, 2004, p. 54.

[21] A. RODRÍGUEZ ADRADOS, *Firma electrónica y documento electrónico..., op. cit.,* p. 49.

[22] Art. 1316-4 (L.n. 2000-230, 13 de marzo de 2000, art. 4): «*la firma necesaria para la perfección de un acto jurídico identifica a quien la fija. Manifiesta el consentimiento de las partes a la obligación que se derivan de este acto. Cuando la firma es electrónica, consiste en el uso de un proceso fiable de identificación que garantiza su unión con el acto al que se vincula. Cuando la firma es puesta por una autoridad pública, confiere autenticidad a este acto*».

authentifizierung dienen» [23]. Y el art. 2 del Decreto-ley núm. 290-D/99 portugués [24].

1.1. *Firma electrónica avanzada*

El art. 3.2 de la LFE da un nuevo concepto de firma electrónica, el correspondiente al de firma electrónica avanzada: «*La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control*» [25].

Se trata de una clase de firma ya prevista en el RDL 14/1999, cuyo art. 2, apartado *b),* coincidente con el contenido del art. 2.2 de la Directiva, la definía como: «*La firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo*

---

[23] Parágrafo 2 de la Ley: *Firma electrónica* «*son los datos en forma electrónica, unidos a otros datos electrónicos o asociados de forma lógica y que sirven como medio de autenticación*».

[24] Art. 2.*b)*: «*Assinatura electrónica: resultato de um processamento electrónico de dados susceptible de constituir objecto de directo individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento electrónico ao qual seja aposta, de modo que:*

i. Identifique de forma unívoca o titular como autor do documento.

ii. A sua aposição ao documento dependa apenas da vontate do titular.

iii. A sua conexao com o documento permita detectar toda e qualquer alteraçao superveniente do conteúdo deste».

(Firma electrónica es el resultado de un proceso electrónico de datos susceptible de constituir objeto de derecho individual y exclusivo, y de ser utilizado para dar a conocer la autoría de un documento electrónico al que se pone, de modo que: 1. Identifique de forma única al titular como autor del documento. 2. Su fijación en el documento dependa sólo de la voluntad del titular. 3. Su conexión con el documento permita detectar cualquier alteración sobrevenida al contenido de éste.)

[25] Es la misma definición contenida en el proyecto de ley y coincide, asimismo, sustancialmente, si bien con algunos cambios de carácter formal con las definiciones contenidas en las dos versiones del BALFE.

El art. 2.*b)* de la versión primera del BALFE se conceptuaba la firma electrónica avanzada como «*la firma electrónica que permite la identificación del firmante y ha sido creada por medios que éste puede mantener 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*».

Por su parte, el art. 2.*b)* de la segunda versión del BALFE la definía como «*la firma electrónica que está vinculada únicamente al firmante, permitiendo su identificación, ha sido creada por medio que éste puede mantener bajo su exclusivo control, y está vinculada a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación de éstos*».

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.»

El art. 2.2 de la Directiva señala en esta línea que la firma electrónica avanzada es: «*La firma electrónica que cumple los siguientes requisitos:* a) *estar vinculada de manera única al firmante;* b) *permitir la identificación del firmante;* c) *haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control;* d) *estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable*»[26].

Es una firma que, en los tres textos legales expuestos, se le exige el cumplimiento de una serie de requisitos: 1) Debe ser suficiente para identificar al firmante y detectar cualquier cambio ulterior de los datos firmados; 2) Estar vinculada al firmante de manera única y a los datos a los que se refiere; y 3) Haber sido creada por medios que el firmante tiene bajo su exclusivo control[27].

---

[26] No obstante, en la propuesta inicial presentada por la Comisión (art. 2.1), se establecía un concepto de firma electrónica donde se exigía que toda firma cumpliera los requisitos ahora sólo exigidos para la firma electrónica. Así, definía en un primer momento la firma electrónica como «*la firma en forma digital integrada en unos datos, anexa a los mismos o asociada con ellos, que utiliza un signatario para expresar conformidad con su contenido y que cumple los siguientes requisitos:* a) *estar vinculada al signatario de manera única;* b) *permitir la identificación del signatario;* c) *haber sido creada por medios que el signatario puede mantener bajo su exclusivo control;* d) *estar vinculada a los datos relacionados de modo que se detecte cualquier alteración ulterior de los mismos*».

Si embargo, en la Propuesta modificada de la Directiva la situación varía, pues en el art. 2.1 se ofrece un concepto general de firma electrónica desprovisto ya de la exigencia de los requisitos mencionados: «*los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación*»; a este precepto se le añade otro, el art. 2.1 *bis*, que se convierte con posterioridad en el art. 2.2 de la Posición Común y del texto aprobado definitivamente, donde se da un nuevo concepto, el de firma electrónica avanzada, siendo en ésta ahora donde se exigen aquellos requisitos que en un principio, se aplicaban y alcanzaban a todas las firmas electrónicas de la clase que fueran.

[27] Tales requisitos también se exigen en el parágrafo 2.2 de la Ley alemana de Firma Electrónica de 2001 al expresarse en los siguientes términos: *Fortgeschrittene elektronische signaturen elektronische signaturen nach nummer 1 die*

a) *ausschlieblich dem signaturschlüssel-inhaber zugeordnet sind,*

b) *die identifizierung des signaturschlüssel-inhabers ermöglichen,*

c) *mit mitteln erzeugt werden, die der signaturschlüssel-inhaber unter seiner alleinigen kontrolle halten kann, und*

d) *mit den daten, auf die sie sich beziehen, so verknüpft sind, dass, eine nachträglich veränderung der daten erkannt werden kann».* [Firma electrónica avanzada es la firma electrónica que cumple los siguientes requisitos: *a)* estar vinculada de manera exclusiva al firmante, *b)* permite la identificación del firmante, *c)* haber sido creada utilizando medios que el firmante mantiene bajo su exclusivo control, y *d)* que los datos a los que se refiere, son utilizados, de modo que cualquier cambio posterior pueda ser detectable.]

El firmante tiene, por tanto, unos datos de creación de firma, que son suyos únicamente, con unos medios —programa o sistema informático— que aplican esos datos sobre el mensaje y, que él solo controla; y, que generan una firma que es distinta cada vez que se firma un documento.

Frente a los riesgos ya señalados existentes en el mundo de las comunicaciones electrónicas, esta firma garantiza la autenticación del autor (identificación); evita el rechazo en origen de los mensajes electrónicos, y salvaguarda la integridad de los documentos electrónicos. Cumple, por tanto, en relación con los documentos electrónicos, las dos principales funciones que se atribuyen a la firma manuscrita sobre un documento papel, como es permitir identificar al autor del escrito (autenticación) y constatar que el mensaje no ha sido alterado después de la firma (integridad) [28].

Ahora bien, esta Ley, al igual que el RDL 14/1999, siguiendo las directrices marcadas por la Directiva comunitaria, opta por una neutralidad tecnológica que, sin embargo, es más formal y aparente que real, pues, en el fondo, el legislador, tanto ahora como antes, está pensando —y así, como veremos en alguna ocasión, además lo ha plasmado en el articulado—, cuando se refiere a la firma electrónica, en una clase particular de firma que puede ofrecer la misma seguridad que proporciona las firmas electrónicas avanzadas, por cuanto puede cumplir los requisitos establecidos en el art. 3.2 de la LFE, como es la *firma digital*. Estas firmas se crean usando una tecnología específica, el llamado sistema de criptografía asimétrica o de clave pública.

El *sistema criptográfico* es un sistema de tratamiento de la información que transforma un mensaje, de manera que sólo las personas en posesión de algoritmos (procedimiento matemático) y claves (conjunto de dígitos alfanuméricos) adecuados pueden acceder a su contenido de manera correcta [29].

Estos sistemas criptográficos por tipo de clave se pueden clasificar en sistemas simétricos o asimétricos. En los *simétricos*, la misma clave es compartida en origen y en destino, de forma que el emisor y receptor del mensaje debe conocer la clave —uno para cifrar y el otro para descifrar—; y en los *asimétricos*, desarrollado como tal sistema a mediados de los setenta, existen dos claves complementarias, una de ellas privada en poder del emisor, y otra pública en poder de uno o varios receptores. Consiste en un par

---

Y, asimismo, en el art. 2.2 de la Ley belga de 2001, y en el art. 1.9 del Reglamento luxemburgués de 2001.

[28] Fco. J. GARCÍA MAS, *Comercio y firma electrónicos, op. cit.,* p. 59; del mismo autor, «El documento público electrónico (I)», *op. cit*., p.129.

[29] Fco. J. GARCÍA MAS, *Comercio y firma electrónicos, op. cit.,* p. 57.

de claves basadas en algoritmos matemáticos. Sobre lo expuesto está claro que el sistema más seguro es el asimétrico, al existir dos claves complementarias que evitan en gran medida la ruptura de una de ellas y que garantizan, al ser complementarias, la seguridad del sistema [30].

En este sistema, aplicando una de las claves, la clave privada sobre el mensaje o conjunto de datos a transmitir utilizando un algoritmo criptográfico, se encripta (se codifica) hasta hacerlo incomprensible, aplicando después en destino, cuando se recibe el mensaje, la otra clave, la clave pública, precisamente al mensaje codificado, el receptor que tiene en su poder la clave pública correspondiente que le ha proporcionado el emisor, puede proceder a la correcta desincriptación de los datos transmitidos, y retroceder, por tanto, hasta el mensaje inicial en claro.

Estas claves que funcionan siempre de forma complementaria, tienen las siguientes características: «1) Ambas claves son aptas tanto para codificar como para descodificar, pero, si se codifica con la clave 1, solamente se puede descodificar con la clave 2, y viceversa. En definitiva, un mensaje no se puede descodificar y codificar con la misma clave, sino que para lo segundo precisa de la clave complementaria; 2) El conocimiento de una de las dos claves no permite desvelar cuál es la otra. Es decir, si una persona conoce cuál es la clave A, por esa sola información no puede llegar a descifrar cuál es la clave B» [31].

Para que este par de claves puede ser usado adecuadamente a fin de proporcionar la tan ansiada seguridad, es precio que una de las dos sea secreta, es decir, que el titular de la misma la tenga guardada, oculta, en secreto, de manera que nadie más que él pueda tener acceso a la misma (puede ocurrir, incluso, que ni siquiera el titular la conozca, pues probablemente se mantendrá en una tarjeta inteligente, o se podrá acceder a ella mediante un número de identificación personal o a través del reconocimiento de la huella dactilar). Es la llamada clave privada. Por el contrario, la clave complementaria debe ser de general conocimiento, a disposición de cualquiera. Precisamente por ello recibe el nombre de clave pública o clave de verificación matemática [32].

Éstas son las bases técnicas de la firma electrónica avanzada como firma digital, en la que existe también, antes del envío de cualquier mensaje, la

---

[30] Fco. J. GARCÍA MAS, *Comercio y firma electrónicos, op. cit.,* p. 58.

[31] F. GOMÁ LANZÓN y C. GARCÍA VIADA, *Libro Blanco de la firma electrónica notarial,* Consejo General del Notariado, 2000, p. 16.

[32] F. GOMÁ LANZÓN y C. GARCÍA VIADA, últ. lug. cit.

función algorítmica, denominada *hash* que extrae de cada mensaje específico un resumen de longitud fija, sea cual sea la extensión del mensaje inicial. Este resumen o extracto, que normalmente se conoce como «huella digital» se compone de un listado de letras y números completamente incomprensibles, resultado de aplicar el algoritmo al mensaje que se quiere enviar, y tiene como características: su irreversibilidad, pues de la huella digital (o *hash*) no es posible ascender al mensaje en claro y descifrarlo, y su exclusividad para cada mensaje, de modo que si cambiáramos en el mismo una sola letra, una coma o simplemente un acento, la huella digital resultante sería completamente diferente a la del primero. Resultado, en fin, de esta transformación matemática sobre un documento es una cadena de *bits* de tamaño predeterminado denominado *hash* o huella digital, que es representativa de cada documento, de tamaño constante y habitualmente menor que el documento original, no siendo reconstruible el documento original a partir de ella.

Por tanto, la firma digital es el resultado de aplicar la clave privada a un resumen o *hash* previamente obtenido del documento que se quiere enviar por el procedimiento siguiente: se aplica una función *hash* sobre tal documento y se extrae su huella digital. A continuación se encripta la huella digital extraída, aplicando la clave privada del firmante (datos de creación de firma) mediante un sistema informático denominado dispositivo de creación de firma. En este momento tenemos un mensaje y una huella digital del mismo, esta última encriptada con la clave privada. A esta huella digital encriptada es lo que se suele llamar *«firma electrónica del mensaje»*, que será diferente para cada mensaje, pues depende esencialmente de éste. Ambos mensajes, el inicial, total y en claro, y resumen cifrado o huella digital encriptada son remitidos conjuntamente al destinatario y la clave pública del firmante. El receptor del mensaje, que cuenta con dos elementos (el mensaje inicial y el resumen del mensaje o huella digital) debe proceder a la verificación de la firma. Se trata tal verificación de un proceso de comprobación de esa firma por referencia al mensaje original y a una clave pública dada, determinando de esta forma que la firma digital fue creada para este mismo mensaje utilizando la clave privada, que corresponde a la clave pública referida. Para ello, el receptor del mensaje llevará a cabo dos operaciones: descodificará la huella digital firmada con la clave privada del emisor aplicando su clave pública; y aplicará de nuevo la función *hash* al mensaje recibido para obtener otra huella digital del mismo. Si son iguales, significa que el mensaje que se ha enviado es el mismo que se ha recibido, pero si son diferentes —sea cual sea la diferencia—, supone que ha habido

cambios y probablemente alguna manipulación en el camino y, por tanto, no hay que confiar en el mensaje. Todo depende, en consecuencia, de que las huellas digitales o el *hash* recibido y descifrado y segundo *hash* obtenido coincidan o sean diferentes. Si ambos son coincidentes, el destinatario tiene la seguridad de que el mensaje recibido ha sido firmado por el emisor con ese contenido y, en consecuencia, no ha sido manipulado en el camino desde el emisor hasta el receptor del mismo, quedando identificado el titular de las claves privadas y públicas utilizadas para la firma electrónica. Si son diferentes, podrá suponer alteración de uno u otro de los elementos en cualquier momento, con lo que el receptor no tiene seguridad en el mensaje recibido.

De forma que, sólo en el primer caso, es decir, si coinciden ambas huellas digitales, quedan cumplidos por las firmas basadas en la criptografía de clave pública los conceptos de seguridad característicos de la firma electrónica: *autenticación*, pues ofrece seguridad en relación con la identidad del emisor del mensaje (titular); si bien, no necesariamente, identificará la persona o personas que en un futuro accionarán el dispositivo de creación de firma, ni, en suma, quien preste el consentimiento; *integridad* de éste, es decir, que el mensaje recibido es el mismo que el que se envió, o que si ha sido modificado, esta modificación va a ser detectada; y *no repudio en origen*, al impedir que el que envió un determinado mensaje pueda negar haberlo hecho [33], cumpliéndose, asimismo, los requisitos legalmente exigidos para la firma electrónica avanzada.

---

[33] No resuelve, en cambio, la firma digital el *no repudio en destino*, aunque en la Exposición de Motivos de la LFE puede parecer que sí, cuando alude al uso del sello de tiempo. En su apartado II se dispone «*como respuesta a esta necesidad de conferir seguridad a las comunicaciones por Internet surge, entre otros, la firma electrónica. La firma electrónica constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas, basándose en fechas electrónicas*».

Tampoco un cuarto concepto de seguridad, el de la *confidencialidad*, cuyo significado no es otro que los mensajes que viajan a través de la Red, no puedan ser conocidos más que por el destinatario natural de los mismos, lo proporciona por sí mismo la firma digital. Se obtiene utilizando de otra manera la infraestructura de clave pública. Así para conseguir que un documento sea secreto o confidencial salvo para su receptor natural hay que codificar (encriptar o cifrar) el mensaje que se envía. Y nuevamente hay que utilizar el sistema de claves asimétricas, como en el caso de la firma electrónica, pero con una diferencia, pues mientras en ésta el par de claves que entran en acción son las del emisor del mensaje, para cifrar y codificar un mensaje se usa el par de claves del receptor del mismo. Se codificará el envío global del mensaje con la clave pública del receptor del mismo. De forma que el mensaje solamente podrá ser descodificado con la clave complementaria, pero esa clave es la privada de receptor, luego sólo el receptor y nadie más podrá llegar a conocer el contenido del men-

En este contexto —y, pese a resultar lógico el fundamento sobre el que se sustenta la pretendida neutralidad tecnológica, como es la rápida evolución de la técnica y la necesidad de dejar abierta la norma a cualquier futuro desarrollo tecnológico que pueda surgir—, lo razonable hubiera sido, partiendo de la consideración de una clase particular de firma electrónica avanzada como puede ser la firma digital, centrarse en la regulación de la misma, dada la función predominante que la criptografía de clave pública desempeña aparentemente en la práctica más reciente del comercio electrónico actual, sin dejar por ello de alentar, asimismo, en el propio contenido de la norma, el recurso a otras técnicas futuras y seguras; evitando con ello el dar cabida a técnicas inseguras como está sucediendo con la normativa sustentada en la nueva LFE, y ya ocurriera en anteriores regulaciones.

No obstante, la propia LFE, aunque no menciona expresamente la firma digital, por un lado, en la definición de firma electrónica en general que ofrece en su Exposición de Motivos, se está refiriendo a la firma electrónica avanzada, más en concreto, en su modalidad de firma digital, por cuanto hace referencia a las exigencias de autoría e integridad predicable de ésta, frente a la sólo exigencia de autenticación que en el articulado se destina a la firma electrónica en general: «*la firma electrónica constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas en fechas electrónicas*» [34].

Y, por otro, incidentalmente, y como apuntamos al inicio de este epígrafe, aparecen en su articulado alguna referencia a la criptografía asimétrica, así en el art. 24.1, al definir «*los datos de creación de firma*», como «los datos únicos, como códigos o *claves criptográficas privadas*, que el firmante utiliza para crear la firma electrónica»; y en el art. 25.1, al referirse al concepto de «*datos de verificación de firma*» como «los datos, como códigos o *claves criptográficas públicas* que se utilizan para verificar la firma electrónica».

En esta línea, si bien constatado de forma expresa, el Decreto italiano de firma electrónica de 2000, reformado por Decreto de 7 de abril de 2003,

---

saje. Esto significa que es confidencial y secreto para él. Véanse F. GOMÁ LANZÓN y C. GARCÍA VIADA, *Libro Blanco de la firma electrónica notarial, op. cit.,* p. 24. Más extensamente, A. MARTÍNEZ NADAL, *Comercio electrónico, certificados y autoridades de certificación,* 3.ª ed., Madrid, Civitas, 2001, pp. 45 a 63.

[34] Apartado II de la Exposición de Motivos de la LFE.

suprime la definición de firma electrónica avanzada y mantiene sólo la conceptuación de firma digital[35].

---

[35] Art. 1.1.*n)* firma digital: «*è un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare 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*» (firma digital «es un particular tipo de firma electrónica cualificada basada en un sistema de claves asimétricas en pareja, una pública y otra privada, que respectivamente permiten al titular mediante clave privada, y al destinatario mediante la clave pública hacer manifiesta y verificar la proveniencia y la integridad de un documento informático o de un conjunto de documentos informáticos»).

Por su parte, el art. 22, reformado, en parte, por el Decreto citado de 7 de abril de 2003, define que se entiende: «b) *por claves asimétricas, el sistema de claves criptográficas, una privada y una pública, correlativas entre sí, utilizadas en el ámbito de los sistemas de validación de documentos informáticos;* c) *por clave privada, elemento del sistema de claves asimétricas, destinado a ser conocido solamente por el sujeto titular, mediante el cual se pone la firma digital sobre el documento informático;* d) *por clave pública, el elemento del sistema de claves asimétricas destinado a ser conocido por el público en general, con el que se verifica la firma digital puesta sobre el documento del titular de la clave asimétrica;* f) *por certificación, el resultado del procedimiento informático, aplicada a la clave pública y puesta de manifiesto por el sistema de validación, mediante el cual se garantiza la correspondencia biunívoca entre la clave pública y el sujeto titular al que le pertenece, se identifica a este último, y se atestigua el período de validez de la susodicha clave y el término de validez del certificado, en todo caso no superior a tres años*». Y en su art. 23, referido de nuevo a la firma digital, señala que: «*1. La firma digital debe referirse de manera unívoca a un solo sujeto y al documento o al conjunto de documentos a los que se acopla o asocia; 2. Para la generación de la firma digital debe emplearse una clave privada que se corresponde con una clave pública, que ha sido objeto de emisión de un certificado cualificado que, en el momento de su suscripción, no ha resultado falto de validez o bien no ha resultado suspendido o revocado.*»

En similares términos, se pronuncia el Decreto-ley núm. 290-D/99 de documento electrónico y firma digital portugués, cuando define la firma digital en el art. 2.*c):* «Assinatura digital: *processo de assinatura electrónica baseado em sistema criptográfico asimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é egenerado um par des chaves asimétricas exclusivas e interdependentes, uma das quais privada e otra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento electrónico ao qual a assinatura é aposta e concordancia como o seu contenido, e ao declaratário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente clave privada e se o documento electrónico foi alterado depois de aposta a assinatura*» («firma digital: proceso de firma electrónica basado en un sistema criptográfico asimétrico, compuesto por un algoritmo o serie de algoritmos, mediante el cual se genera un par de claves asimétricas, exclusivas e interdependientes, una de ellas privada y otra pública, y que permite al titular usar la clave privada para declarar la autoría del documento electrónico al que la firma ha sido puesta y, en concordancia con su contenido, y al destinatario usar la clave pública para verificar si la firma ha sido creada mediante el uso de la correspondiente clave privada, o si el documento electrónico ha sido alterado después de puesta la firma»).

1.2. *Firma electrónica reconocida*

Frente al dualismo en la clasificación de las firmas tanto del RDL 14/1999 como de la Directiva, la LFE introduce un tercer tipo de firma, de mayor calidad y seguridad, como es la firma electrónica reconocida, definida en el art. 3.3 como «*la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma*».

Constituye una aportación novedosa del legislador su mención expresa en la norma, pues su calificación como tal no se contiene ni en el RDL 14/1999 ni en la Directiva. Tampoco en la primera versión del BALFE, aunque sí en la segunda, donde aparece por primera vez definida esta clase de firma [36].

Supone, como señala la Exposición de Motivos de la Ley, «*la creación de un concepto nuevo demandado por el sector, sin que ello implique modificación alguna de los requisitos sustantivos que tanto la Directiva 1999/93/CE como el propio Real Decreto Ley 14/1999 venían exigiendo*» [37].

Los requisitos, precisamente, que la Ley establece para la calificación de una firma electrónica como «reconocida» son: la firma electrónica avanzada, un certificado reconocido sobre el que se basa ésta y un dispositivo seguro de creación de firma mediante el que se genera aquélla. Tratado en el apartado anterior el primero de los requisitos mencionados, sólo nos ocuparemos del análisis de este último, destinando un epígrafe a tal finalidad. No obstante, hemos de mencionar que la LFE define en su art. 6.1 que un certificado electrónico «*es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad*». Y entiende que son certificados reconocidos «*los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten*» (art. 11.1 LFE).

Cumplidos los requisitos mencionados, determina la Ley en su art. 3.4 la equivalencia funcional a efectos de validez y eficacia de la firma recono-

---

[36] En el art. 2, apartado *c),* de la segunda versión del BALFE es donde, en efecto, aparece por primera vez la noción de «*firma electrónica reconocida*» definida como «*la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma*».

[37] Apartado I de la Exposición de Motivos de la LFE.

cida con la firma manuscrita, así dispone el citado precepto que: «*la firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel*».

Ahora bien, estos requisitos son exactamente los mismos que el art. 3.1 del RDL 14/1999 exigía para dotar a la firma electrónica avanzada de una equivalencia igualmente funcional a la firma manuscrita, pues, para que tal equivalencia pudiera tener lugar, la firma electrónica avanzada debía estar basada en un certificado reconocido y producido por un dispositivo seguro de creación de firma.

En este contexto, esta tercera categoría de firma electrónica no supone en sí misma una creación del todo original, pues la previsión de la firma electrónica reconocida en la LFE no implica por sí sola en los términos vistos la exigencia de nuevos requisitos ni la determinación de un sistema de equivalencia funcional de la firma electrónica que sea innovador con respecto al consagrado en el RDL 14/1999, sino sólo la de dotar de una nueva denominación jurídica a una categoría de firma hasta ahora no recogida por el legislador español como tal en un texto legal. Estamos, pues, ante una innovación que podemos calificar más de formal que de sustantiva, ya que simplemente se está creando una nueva categoría de firma a la que se va a dotar de un *nomen iuris*, respecto del que se va asociar un concepto preciso contenido en la propia norma, ya existente, no obstante, en los términos jurídicos en que se expresa, en una regulación precedente como es el RDL 14/1999.

Este formalmente nuevo concepto de firma electrónica reconocida tiene, en esencia, más un valor comercial, responde a un nuevo producto de firma electrónica, que ya había sido asimilado por el mercado —de ahí los términos en que se expresa la propia Exposición de Motivos de la Ley—, en unos términos sustancialmente ya previstos en la normativa española, e incluso introducidos en su configuración como tal en el mundo del Derecho por la doctrina representada en los autores Rubio Velázquez y Alamillo Domingo, los cuales, al tratar de esta clase de firma, entendían que «*la denominación de firma electrónica reconocida se refiere a la cualificación de la calidad de la firma, de modo que no es necesario ni un contrato privado ni una norma jurídica para "reconocer" la firma*» [38].

De verdadera novedad de la Ley con respecto al RDL 14/1999, en todo caso, se puede hablar en lo que atañe a la equivalencia funcional de la firma

---

[38] R. RUBIO VELÁZQUEZ y I. ALAMILLO DOMINGO, «Firma electrónica y certificado digital», en *Internet: Claves legales para la empresa*, Madrid, Civitas, 2002, pp. 636-637.

electrónica, del extenso apartado 8 del art. 3. Dicho apartado —introducido en el trámite del Proyecto de LFE en el Senado— atiende a la vocación esencialmente probatoria que tiene todo tipo de firma —electrónica o no— y regula algunas de las vicisitudes que pueden acontecer ante la aportación de un documento firmado electrónicamente como prueba en un proceso y, en particular, uno de los escenarios más adversos como es la impugnación de la firma electrónica por la otra parte.

Ahora bien, sobre la base de los requisitos mencionados y del sistema de criptografía asimétrica aludido en líneas precedentes, que nos ha permitido determinar la firma digital como firma electrónica avanzada —todo ello, pese al principio neutralidad tecnológica que, en principio, preside la actual regulación—, esta firma permite al destinatario de un mensaje tener la seguridad de que la clave pública pertenece de verdad al emisor y no a otra persona que se ha hecho pasar por él. Desde luego, no por la simple declaración o manifestación del emisor del mensaje, por muy extendida que sea esa declaración, dado que puede ser falsa o manipulada. Es necesaria la intervención de un tercero imparcial que lo confirme, son los llamados prestadores de servicios de certificación. Son entidades que, previa identificación del solicitante, le expiden un par de claves criptográficas, y una vez hecho esto, emiten un certificado electrónico en el que se enlaza y se identifica una determinada clave pública (datos de verificación de firma) con una persona concreta, cuyos datos aparecen asimismo en el certificado[39]. Por eso se le suele denominar también certificado de claves públicas. De este modo, el receptor del mensaje tiene la seguridad de que la clave pública pertenece al emisor, no porque éste se lo diga, sino porque puede consultar el certificado electrónico que así lo acredita, expedido por un prestador de servicio de certificación, en el que no solo podrá comprobar la titularidad del par de claves, sino también la vigencia de las mismas y que no hayan sido revocadas. El sistema conjunto de clave privada + clave pública + certificado electrónico emitido por un prestador de servicio de certificación, es lo que se denomina «*infraestructura de clave pública o PKI*»[40].

Esta infraestructura de clave pública sobre la que hoy por hoy se sustenta la configuración de la firma electrónica permite garantizar los con-

---

[39] Define el art. 2.2 de la LFE por prestador de servicios de certificación «*la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica*».

[40] F. GOMÁ LANZÓN y C. GARCÍA VIADA, *Libro Blanco de la firma electrónica notarial, op. cit.,* p. 16.

ceptos de seguridad ya mencionados de autentificación, integridad y no repudio, esto es, ofrecer seguridad en el sentido de identificar al emisor (firmante); a que el mensaje no ha sido manipulado en el trayecto del emisor al receptor y a que no pueda rechazar aquél haberlo emitido. No obstante, García Mas advierte de la necesidad de ser más humilde y prudente, cuando se dice de manera grandilocuente que este tipo de firma garantiza la identidad del firmante, pues, aunque todo el proceso se haya desarrollado perfectamente y no se detecte ninguna alteración en el mecanismo, aquella identidad no queda garantizada al cien por cien, pues el titular de la firma puede no haber sido quien ha firmado, sino un tercero, bien porque voluntariamente el titular le ha dado el *pin* de acceso, o bien éste ha sido extraviado, o bien ha sido observado o copiado por un tercero. Otra cosa será la asunción o no de responsabilidades por parte del titular de la firma, que por su falta de diligencia en todos los sentidos deba asumir las consecuencias de la utilización de la firma por un tercero. Pero en sentido estricto, «si una de las partes contratantes no ha sido quien ha firmado el documento, sino un tercero, no podemos decir que ha prestado su consentimiento en el contrato; podremos decir cualquier otra cosa, que asuma las obligaciones derivadas del mismo, que existe un principio general en la firma electrónica sobre asunción de lo que se firma, y un largo etcétera, pero nunca que efectivamente ha prestado el consentimiento» [41].

En el Derecho comparado, el Derecho francés y la Ley Modelo CNUDMI/UNCITRAL se limitan a señalar requisitos complementarios a sus firmas «asegurada» y «fiable», respectivamente [42], mientras que el Derecho alemán primero [43], y después el italiano, acuñan un nuevo concepto, el de

---

[41] Fco. J. GARCÍA MAS, *Comercio y firma electrónicos, op. cit.,* pp. 59-61.

[42] El art. 2 del Decreto 2001-272, de 30 de marzo de 2001, *relatif à la signature électronique,* dispone que «*la fiabilidad de un proceso de firma electrónica se presume salvo prueba en contrario cuando este proceso emplea una firma electrónica segura, establecida mediante un dispositivo seguro de creación de firma electrónica y que la verificación de esta firma descanse sobre un certificado electrónico cualificado*».

[43] El parágrafo 2 de la *Gesetz* de 2001 después de definir tanto la firma electrónica (núm. 1), como la firma electrónica avanzada (núm. 2), conceptúa firma electrónica cualificada como aquella firma que cumple los requisitos del número 2, por tanto, una firma electrónica avanzada que: *a)* esté basada en un certificado cualificado válido en el momento de su creación; *b)* que haya sido producida por un dispositivo seguro de creación de firma [*«qualifizierte elektronische signaturen» elektronische signaturen nach nummer 2 die* a) *auf einem zum zeitpunkt ihrer erzeugung gültigen qualifizierten zertifikat beruhen und* b) *mit einer sicheren signaturerstellungseinheit erzeugt werden*].

Por su parte, el nuevo parágrafo 126.*a)* BGB tras la reforma por Ley de 13 de julio de 2001, señala que «*si la forma escrita legalmente prescrita se sustituye por la forma electrónica, el emisor de la declaración deberá añadir su nombre, y el documento electrónico deberá ir pro-*

firma cualificada («*qualifizierte*»/«*qualificata*»), que supone también una mera modalidad de la firma electrónica avanzada al que se le añaden una serie de requisitos. Si bien conviene precisar que tras la reforma por Decreto de 2003, del Decreto italiano de 2000, se ha suprimido la mención de firma electrónica cualificada y se ha sustituido por una definición única de firma digital en los términos vistos en otro apartado de nuestro estudio [44].

2. Datos y dispositivos de creación y verificación de firma

Junto con la firma electrónica es necesario hacer referencia a unos elementos técnicos complementarios que permiten precisamente la creación y verificación de las firmas electrónicas. En este sentido, el Título IV de la LFE con la denominación «Dispositivos de firma y sistemas de certificación de prestadores de servicios de certificación y de dispositivos de firma electrónica» regula, en el Capítulo I, por una parte, los «Dispositivos de firma electrónica», destinando dos preceptos a la materia, el art. 24 a los «Dispositivos de creación de firma electrónica», donde se desarrollan las nociones de datos de creación de firma, dispositivos de creación de firma y dispositivo seguro de creación de firma, y el art. 25 a los «Dispositivos de verificación de firma electrónica», donde se desarrollan igualmente las nociones de datos de verificación de firma, dispositivos de verificación de firma y las garantías que, siempre que sea técnicamente posible, deben cumplir estos dispositivos. Y, por otra parte, en el Capítulo II regula la «Certificación de prestadores de servicios de certificación y dispositivos de creación de firma electrónica», dedicando tres preceptos a la materia, el art. 26 a la «Certificación de prestadores de servicios de certificación», el art. 27 a la «Certificación de dispositivos seguros de creación de firma elec-

---

visto de una firma electrónica cualificada de acuerdo con la Ley de firma, y si se trata de un contrato, las partes deberán firmar electrónicamente en cada caso un documento del mismo tenor de la forma establecida en el apartado 1» («Soll die gesetzlich vorgeschriebene schriftliche Form duch die lektroniche Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen signatur nach dem signaturgesetz versen.

Bei einem Vertrag müssen die Parteien jeweils ein gleichlautendes Dokument in der in Absatz 1 bezaeichneten Weise elektronisch signieren»).

[44] Disponía el art. 1, ee del Decreto 2000 [reformado por el art. 2.*g)* del Decreto Legislativo 2002 y suprimido por el art. 1 del Decreto de 7 de abril de 2003] que firma electrónica cualificada es «*la firma electrónica avanzada que se basa en un certificado cualificado y creada mediante un dispositivo seguro de creación de firma*».

trónica» y, finalmente, el art. 28 al «Reconocimiento de la conformidad con la normativa aplicable a los productos de firma electrónica».

Tanto de los dispositivos de creación y de verificación de firma electrónica como de la certificación de los dispositivos de creación de firma, y del reconocimiento de su conformidad con la normativa aplicable, nos vamos a ocupar en este apartado.

2.1. *Datos de creación y verificación de firma*

El art. 24 de la LFE, bajo el título «Dispositivo de firma electrónica», define los datos de creación de firma como *«los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica».* Esta definición coincide con la del art. 2, apartado *d),* del RDL 14/1999, con la única salvedad meramente formal, de una diferente denominación del creador de la firma, que en vez de firmante como ahora, se le calificaba de signatario. En esta línea, se conceptuaba los datos de creación de firma como *«los datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la firma electrónica»*. Del mismo modo, la Directiva comunitaria define en su art. 2.4 tales datos como *«los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica»*. Definición que en sus términos es exactamente igual que la empleada por el legislador de la actual LFE [45].

Se trata de datos que se incorporan a un chip electrónico, banda magnética o disco duro de un ordenador y mediante un algoritmo de *hash* o

---

[45] Y, también, por el parágrafo 2.4 de la Ley alemana de 2001: «*Signaturschlülssel einmalige elektronische Daten wie private kryptographische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden.»*

En similares términos, por su parte, se pronuncia, el art. 22.*b)* del Decreto italiano de 28 de diciembre de 2000, cuando define por clave privada «*l'elemento della coppia di chiavi asimmetriche, destinato al esesere conosciuto soltando dal soggetto titolare, mediante il quale si appone la firma digitale sul documento informatico»* («el elemento de la copia de clave asimétrica, destinado a ser conocido solamente por el sujeto titular, mediante la cual se fija la firma digital sobre el documento informático»). Y el art. 2.*d)* del Decreto portugués núm. 290-D/99: «*Chave privata: elemento do par de chaves asimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apöe a assinatura digital no documento electrónico, ou se descifra um documento electrónico previamente cifrado com a correspondente chave publica»* («clave privada: elemento del par de claves asimétricas destinado a ser conocido sólo por su titular, mediante el cual se fija la firma digital al documento electrónico, o se descifra un documento electrónico previamente cifrado con la correspondiente clave pública»).

algoritmos resumen se extraen elementos característicos del mensaje que conforman un resumen de longitud fija, al que se aplica la clave privada, que será un par de valores calculados a partir de la elección de dos números primos y, quedando el mensaje que se va a enviar, de este modo, encriptado. Tales datos que corresponden a la clave privada los utiliza el firmante para codificar el *hash* que corresponde al documento a firmar.

Como elemento característico de los mismos viene a establecerse el que éstos deben ser únicos y, por tanto, debe ser posible garantizar razonablemente en base a criterios matemáticos o estadísticos que la clave privada no puede ser duplicada [46]. Sirven para generar la firma.

Por su parte, el art. 25 de la LFE, bajo el título «Dispositivos de verificación de firma electrónica», define los «datos de verificación de firma» como «*los datos, códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica*». Esta definición coincide con la del apartado *g)* del art. 2 del RDL 14/1999, que conceptuaba los «datos de verificación de firma» como «*los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica*», y con la que ofrece la Directiva comunitaria, al establecer en su art. 2.7 que los datos de verificación de firma son «*los datos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar una firma electrónica*» [47].

Se trata de datos con los que va a tener lugar la operación inversa a la encriptación, se va a verificar la firma que corresponde a la clave privada

---

[46] R. RUBIO VELÁZQUEZ y C. RODRÍGUEZ SAU, «I Parte. Aspectos Legales», en *La firma electrónica. Aspectos legales y técnicos,* de R. RUBIO VELÁZQUEZ, C. RODRÍGUEZ SAU y R. MUÑOZ MUÑOZ, Barcelona, Ediciones Experiencia, 2004, p. 133.

[47] Véase en estos términos el art. 22.*d)* del Decreto italiano de 28 de diciembre de 2000, al entender «*per chiave pubblica, l'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale aposta sul documento informatico dal titolare delle chiavi asimmetriche*» («clave pública, el elemento de la copia de claves asimétricas destinadas a ser conocida por el público, con la que se verifica la firma digital fijada sobre el documento informático por el titular de la clave asimétrica»); el art. 2.*e)* del Decreto núm. 290-D/99: «*Chave publica: elemento do par de chaves asimétricas destinado a ser divulgado, com o qual se verifica assinatura digital aposta no documento electrónico pelo titular do par de chaves asimétricas, ou se cifra um documento electrónico a transmitir ao titular do mesmo par de chaves*» («clave pública, el elemento del par de claves asimétricas destinado a ser divulgado, con el cual se verifica la firma digital fijada en el documento electrónico por el titular del par de claves asimétricas, o se cifra el documento electrónico a transmitir al titular del mismo par de claves»), y el parágrafo 2.5 de la Ley alemana de 2001 «Signaturprüfschülssel elektronische Daten wie offentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden» («Datos de verificación de claves de firma como claves criptográficas públicas, que comprueban la firma electrónica utilizada»).

del firmante, aplicando la clave pública a la huella digital para descodificar el mensaje encriptado con la clave privada, con el objeto que posteriormente el destinatario del mensaje vuelva de nuevo a aplicar la función *hash* al mensaje recibido y obtenga otra huella digital del mismo. Verificar una firma electrónica es culminar la función de la firma electrónica, pues la verificación tiene lugar cuando el destinatario emplea la clave pública.

Por tanto, bajo el Título «Dispositivos de firma electrónica» se regula como nociones previas tanto para la aplicación del dispositivo de creación como para el de verificación los datos de creación y verificación de firma, respectivamente, que desde un punto de vista técnico constituyen además elementos que posibilitan la creación de una firma (clave privada de la criptografía asimétrica) o su verificación (clave pública de la criptografía asimétrica).

Pese al principio de neutralidad tecnológica tantas veces mencionado que tanto antes como ahora preside la regulación de la firma electrónica en España como en el ámbito comunitario, el legislador en tales instancias normativas, sin embargo, opera en los términos vistos implícitamente bajo la perspectiva de la criptografía asimétrica en la que se basa la firma digital como modalidad de firma electrónica avanzada, pues, por una parte, se refiere a la clave criptográfica privada (*datos de creación de firma*), que se aplica sobre un documento y permite la firma del mismo por medios electrónicos, siendo esencial para la propia seguridad del sistema que esté bajo el control único y exclusivo de su titular y permanezca en secreto, pues, en caso contrario, existe el riesgo de que sea utilizada a efectos de firma por quien no es titular legítimo con los consiguientes problemas de responsabilidad y, por otra, se hace referencia a la clave criptográfica pública (*datos de verificación de firma*), libremente accesible para cualquier persona, que se aplica sobre un documento electrónico firmado previamente de forma electrónica, y que permite al destinatario del mensaje verificar que ha sido firmada por el titular de la clave privada. De forma que si el resultado de la verificación es positivo se tiene la garantía de la autenticación e integridad del mensaje, lo que supone que el mensaje verificado con la clave pública sólo puede haber sido firmado con la clave privada correspondiente, que en principio se atribuye a su titular y que no ha sido aquél alterado en tránsito. Si el resultado es negativo, no se tiene ninguna garantía y, por tanto, no se tiene la certeza de que haya sido firmado por el titular de la clave privada, o que no haya resultado manipulado el mensaje en su tránsito al destinatario.

En cualquier caso, desde la perspectiva descrita, los datos de creación y verificación de firma, en los términos descritos como par de claves (privada y pública) asociadas, nos sitúan ante los que se denomina infraestructura de clave pública.

Ahora bien, para la validez y eficacia de la firma es necesario que en el proceso de generación del par de claves en cuestión se cumplan una serie de características y requisitos que doten a las mismas de una mínima calidad y ofrezcan igualmente unas mínimas garantías en el desarrollo de aquél. Lo que nos sitúa ante la exigencia de que tanto los datos de creación como de verificación de firma sean seguros y de calidad en su generación, evitando, de esta forma, la existencia de claves poco fiables, que sean fácilmente rompibles (en el sentido de que a partir de la clave pública, pudiera obtenerse la privada), previsibles (fácilmente conocibles por el proveedor de «software» o «hardware» de generación de claves reconstruyendo el proceso de creación) o se trate, simplemente, de claves repetidas (por la no introducción de los adecuados correctores de aleatoriedad en los procedimientos de generación) [48].

Las características que debe cumplir el par de claves son [49]:

1.º Ha de tratarse de un par de claves seguras, claves no reproducibles, de forma que no sea posible obtener la clave privada (los datos de creación de firma) del firmante —que ha de ser secreta— a partir de la clave pública, lo que se denomina la «no viabilidad computacional», que dependerá en gran medida de determinados factores, como la longitud de la clave que puede establecerse de tal forma que no pueda romperse en un período de tiempo viable o realizable; de los avances de la técnica, de los datos protegidos, de la capacidad computacional general requerida para protegerlos, del costo y del tiempo necesario para atacar dichos datos.

2.º El par de claves ha de ser único, es decir, que no debe existir una misma clave para dos o más personas.

3.º El procedimiento de generación ha de ser adecuado, que impida la posibilidad de obtener la clave privada del firmante reproduciendo el procedimiento de generación de claves.

---

[48] A. MARTÍNEZ NADAL, «Comentario al art. 24 de la LFE», en *Comentarios a la Ley 59/2003..., op. cit.,* p. 406.

[49] A. MARTÍNEZ NADAL, «Comentario al art. 24 de la LFE», en *Comentarios a la Ley 59/2003..., op. cit.,* pp. 406-408.

No obstante, como bien señala Martínez Nadal, estos requisitos de calidad que deben cumplir las claves criptográficas pueden variar en función del sistema de creación. Así, para esta autora «existen dos alternativas básicas en función de dónde se genera el par de claves, bien por el propio titular, bien por una entidad distinta. A favor del sistema central de creación de claves por una entidad distinta del titular (por ej., una entidad de certificación) se alega que ofrece la ventaja de que los instrumentos de generación utilizados por la entidad serán de mayor calidad y ofrecerán mayores garantías de las que pueda utilizar un simple titular. El inconveniente de este sistema central frente al sistema local de creación por el propio titular es que no existe garantía de la destrucción efectiva, por parte de la entidad de certificación, de la clave privada de firma, dando pie a posibles utilizaciones fraudulentas». En definitiva, concluye la autora, «si se quiere que la criptografía asimétrica proporcione una firma digital válida y eficaz, es necesario que, sea cual sea el sistema de generación, las claves certificadas tengan la calidad suficiente, sean únicas y estén a prueba de manipulaciones» [50].

En todo caso, además, de los requisitos de calidad y seguridad reseñados necesarios en el proceso de generación de las claves, para dotar de validez y eficacia a la firma resulta también exigencia necesaria un adecuado control y custodia por el titular de la clave privada, de forma que no sea posible la utilización por terceros, que podían suplantar su personalidad y falsificar la firma. En este sentido, el art. 18.*b)*.1.º de la LFE obliga a los prestadores de servicios de certificación a informar al solicitante de un certificado de las obligaciones del firmante de la forma en que han de custodiarse los datos de creación de firma y la protección que ha de seguirse para comunicar la pérdida o la posible utilización fraudulenta de dichos datos.

2.2. *Dispositivos de creación y verificación de firma*

Tras fijar los conceptos de datos de creación y verificación de firma, la LFE da una definición de dispositivo de creación y verificación de firma, conceptuándolos ambos, respectivamente, como *«un programa o sistema informático que sirve para aplicar los datos de creación de firma»* (art. 24.2),

[50] A. MARTÍNEZ NADAL, «Comentario al art. 24 de la LFE», en *Comentarios a la Ley 59/2003..., op. cit.,* pp. 408-409.

y como «*un programa o sistema informático que sirve para aplicar los datos de verificación de firma*» (art. 25.2).

Ambas definiciones tienen su origen más inmediato en la regulación que ofrece la Directiva comunitaria de firma electrónica que define el dispositivo de creación de firma como «*un programa informáticos configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma*» (art. 2.5), y dispositivo de verificación de firma electrónica como «*un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de verificación de firma*» (art. 2.8), y, asimismo, coinciden sustancialmente con las que el RDL 14/1999 proporcionaba en el art. 2, apartados *e)* y *h).*

Por tanto, según la definición dada por la LFE, dispositivo de creación de firma sería tanto las aplicaciones de *software* como el *hardware* necesarios para generar firmas, permitiendo de este modo la aplicación de la clave privada sobre un mensaje electrónico por parte de su autor y remitente para la creación de una firma electrónica, y la aplicación de la clave pública por parte del destinatario para la verificación de ese mensaje firmado. El propio certificado formaría parte del concepto de dispositivo de creación de firma. Gráficamente, los datos de creación de firma (clave privada), que son datos únicos, actúan sobre el mensaje aplicando el algoritmo correspondiente, de manera que un programa (o dispositivo o sistema informático) llega a crear la firma electrónica para ese mensaje[51].

De forma análoga a estos dispositivos de creación, los dispositivos de verificación de firma serían programas o sistemas informáticos que sirven para aplicar los datos de verificación de firma que permiten la aplicación de la clave pública por parte del destinatario para la verificación del mensaje firmado.

Ahora bien, junto a la determinación del concepto básico de dispositivo de creación de firma, la LFE introduce la noción de dispositivo seguro de creación de firma. Un dispositivo seguro de creación de firma es un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías (art. 24.3):

---

[51] En este sentido, el parágrafo 2.11 de la Ley alemana de 2001 dispone: «*Signaturanwendungskomponenten Software– und Hardwareprodukte, die dazu bestimmt sind,* a) *Daten dem Prozess der Erzeugung oder Prüfung qualifizierter elektronischer Signaturen zuzuführen oder* b) *qualifizierte elektronische Signaturen zu Prüfen oder qualifizierte Zertifikate nachzuprüfen und die Ergebnisse anzuzeigen*».

a) *Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto*[52].

Se determina expresamente, por una parte, que no sea posible la reproducción de las claves. Ya hemos mencionado en líneas precedentes la necesaria unicidad de la clave privada, a fin de evitar que una misma clave sea atribuida a dos o más personas. Ahora bien, esta exigencia parece alcanzar, como se desprende del tenor literal de la norma, a los datos utilizados para la generación de la firma, a diferencia del RDL 14/1999, donde se hacia referencia sólo a los dispositivos de creación de firma. Pese al tenor literal, el legislador de la LFE a la hora de exigir el requisito de unicidad en el proceso de generación de claves, está pensando no sólo en los datos de creación de firma y los dispositivos que permiten su aplicación, sino también en los dispositivos de generación de claves de firma, que, aplicándose éstas sobre un mensaje electrónico, queda éste firmado.

b) *Que existe una seguridad razonable de que los datos utilizados para la generación de la firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento*[53].

Se exige que las claves no puedan ser deducibles una de otra, aunque matemáticamente ambas estén relacionadas. Se ha de procurar para ello que el procedimiento de generación de claves debe estar correctamente configurado y, en especial, las claves han de tener la longitud suficiente para impedir la denominada ruptura de la clave privada que consiga a partir de la clave pública[54]. Actualmente, la tecnología utilizada en el ámbito de la certificación digital y, en concreto, los algoritmos matemáticos emplea-

---

[52] Coincide con lo dispuesto en el Anexo III, punto 1, apartado *a),* de la Directiva, que exige «*que los datos utilizados para la generación de firma sólo puedan producirse una vez en la práctica y se garantice razonablemente su secreto»,* y, asimismo, con el art. 19.1.º del RDL 14/1999, que señala: «*Que los datos utilizados para la generación de firma puedan producirse sólo una vez y que asegure razonablemente su secreto*».

[53] Coincide con el Anexo III, punto 1, apartado *b),* de la Directiva, que exige que los dispositivos seguros garanticen que «*existe la seguridad razonable de que los datos utilizados para la generación de firma no pueden ser hallados por deducción y la firma será protegida contra la falsificación mediante la tecnología existente en la actualidad*». Sin embargo, presenta con el art. 19.2 del RDL diferencias sustanciales, concretamente con lo que dispone tal precepto en su inciso segundo, así determina «*que exista seguridad razonable de que dichos datos no puedan ser derivados de los de verificación de firma o de la propia firma y de que la firma no pueda ser falsificada con la tecnología existente en cada momento*».

[54] A. MARTÍNEZ NADAL, «Comentario al art. 24 de la LFE», en *Comentarios a la Ley 59/2003..., op. cit.,* p. 414.

dos, vienen a garantizar razonablemente la imposibilidad de deducción de la clave privada a partir de la clave pública. Lo cierto es que sobre la base de las capacidades actuales de proceso de que disponen los ordenadores y teniendo en cuenta el tipo de algoritmos matemáticos y la longitud de las claves resulta muy difícil la deducción de éstas, pues se tardará un tiempo desproporcionado en conseguir averiguar la clave privada frente a «ataques basados en la fuerza bruta», consistentes principalmente en probar una tras otras las posibles combinaciones, hasta encontrar la correcta[55].

No obstante, la constante evolución propia de un sector como el informático puede llegar a determinar que en un futuro las claves utilizadas en la actualidad para firmar electrónicamente documentos puedan ser deducibles; determinando que la seguridad en este punto es un concepto relativo, al depender en buena parte del estado de la técnica existente en cada momento. De ahí que, periódicamente los algoritmos deban ser sustituidos, de acuerdo con el estado de la técnica vigente. Al respecto, existen para evitar que en un momento futuro se pudieran poner en duda documentos firmados con claves actuales, existen servicios como el *archiving*, donde un tercero independiente de las partes que han firmado el documento, lo almacena protegiéndolo con su propia firma, la cual se incorpora al documento sucesivamente en atención a la periódica actualización de los dispositivos de creación de firma que realice el prestador de servicio de *archiving*[56]. En cualquier caso, y nuevamente, se trataría de una exigencia relativa a los dispositivos de generación de datos de firma, más que a los dispositivos de creación de firma.

Por otra parte, la necesidad de proteger la firma contra la falsificación con la tecnología existente en cada momento determina que el mensaje una vez firmado no sea susceptible de modificaciones, o que se pueda obtenerse fraudulentamente la firma atribuida al titular de la clave privada.

c) *Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros*[57].

---

[55] R. RUBIO VELÁZQUEZ y C. RODRÍGUEZ SAU, «I Parte. Aspectos Legales», en *La firma electrónica..*, *op. cit.,* p. 134.

[56] R. RUBIO VELÁZQUEZ, últ. lug. cit.

[57] Coincide con lo dispuesto en el Anexo III, punto I, apartado *c),* que exige que: «*Los datos utilizados para la generación de firma pueden ser protegidos de forma fiable por el firmante legítimo contra su utilización por otros.*»

Resulta necesario para el buen funcionamiento del sistema de certificados que, además de la identificación del titular de la clave privada, ésta se halle bajo su control y sea adecuadamente custodiada por el mismo.

Ahora bien, la seguridad de un dispositivo de creación de firma puede faltar si cualquiera puede acceder a los datos de creación de firma (clave privada), y utilizarlos, suplantando de esta manera al firmante. Existen prestadores que suministran certificados digitales en *software* sin ninguna medida ni barrera de control que impida el acceso a los mismos. Se almacenan en el disco duro de un ordenador, y cualquiera que tenga acceso al mismo puede hacer uso de las claves y falsear la firma. Una medida de protección de los certificados en *software* es la colación de claves o *PINs* de acceso a los mismos, de tal manera que sólo el que conozca el *PIN* puede utilizar el dispositivo de creación de firma.

Tratándose de certificados almacenados de *hardware* (*UBS keys*, tarjetas inteligentes, etc.), además de las claves de acceso a los mismos, el tipo de almacenamiento permite otorgar mayores garantías de protección de los datos de creación de firma al evitar el duplicado del certificado, y, en el caso de las tarjetas criptográficas, esas mayores garantías de protección se consiguen incorporando un microprocesador independiente que gestiona de manera avanzada el acceso a los datos almacenados [58].

d) *Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.*

Resulta necesario garantizar la integridad del documento firmado, para ello se debe utilizar aquellas herramientas que aseguren que el documento no haya sido alterado en el paso intermedio entre la declaración de voluntad del firmante y la generación del documento firmado. De forma que, para que un dispositivo de creación de firma pueda ser considerado seguro, deben existir precisamente mecanismos que garanticen que el documento presentado para la firma sea el mismo que finalmente va a ser firmado. Esto es, la necesidad de que la aplicación de clave privada sobre un mensaje a efectos de firma no altere su contenido y que el firmante pueda conocer efectivamente lo que va a firmar [59].

---

[58] R. RUBIO VELÁZQUEZ, últ. lug. cit.

[59] Por su parte, el Decreto italiano de 28 de diciembre de 2000 exige en el art. 29-*sexies* que los dispositivos seguros y el procedimiento para generación de firma deben presentar unos requisitos de seguridad suficientes para garantizar que la clave privada: «a) *sia riservata;* b) *non possa essere derivata e che la relativa firma sia protesta da contraffazioni;* c) *possa*

Por tanto, el dispositivo seguro de creación de firma será aquel programa o aparato informático que aplica el dato de creación de firma (clave privada) sobre un mensaje electrónico cumpliendo una serie de requisitos que fija la ley expresamente y que permiten calificarlo como seguro [60]. Tal dispositivo junto al certificado electrónico reconocido sobre el que se basa la firma electrónica avanzada, conforman una firma electrónica reconocida [61], la cual tendrá respecto los datos consignados en la misma, el mismo valor jurídico que la firma manuscrita (art. 3.5 LFE).

El origen de esta noción de dispositivo seguro de creación de firma lo encontramos en el art. 2.6 de la Directiva comunitaria, y su antecedente normativo en el Derecho español lo hallamos en el art. 2.*f)* RDL 14/1999, si bien, a diferencia del art. 24 LFE, aquél efectúa una remisión a otro precepto.

Ahora bien, una vez establecidas de forma genérica y en abstracto estas exigencias, resulta necesario determinar en la práctica cuándo un dispositivo de creación de firmas cumple tales requisitos y se considera seguro. Para ello se regula la certificación técnica de tales dispositivos seguros de creación de firma electrónica en el art. 27 de la LFE, bajo la rúbrica «Certificación de los dispositivos seguros de creación de firma», dentro del Título IV bajo la denominación de «Dispositivos de firma electrónica y sis-

---

essere suficientemente protesta dal titolare dall'uso da parte di terzi. 2. I dispositivi sicuri di cui ai comma 1 devono garantire l'integrità dei dati elettronici a cui la firma si riferisce. I dati devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguitá, e si debe richiedere conferma della volontà di generare la firma. 3. Il secondo periodo del comma 2 non si aplica alle firme aposte con procedura automatica, purché l'attivazione della procedura sia chiaramente riconducibile alla volontà del titolare. 4. I dispositivi sicuri di firma sono sottoposti alla valutazione e certificazione di sicurezza nel settore della tecnologia dell'informazione di cui all'art. 10 comma 1, del decreto legislativo 23 gennaio 2002, n.º 10». [«*a)* sea reservada; *b)* no pueda ser derivada y que la firma sea protegida contra su falsificación; *c)* pueda ser suficientemente protegida por el titular frente a su uso por parte de terceros. 2. Los dispositivos seguros del apartado primero deben garantizar la integridad de los datos electrónicos a los que la firma se refiere. Los datos deben ser presentados al titular, antes de su fijación en la firma, claramente y sin ambigüedad, y se debe requerir confirmación de su voluntad para generar firma. 3. El apartado segundo no se aplica a la firma fijada con procedimiento automático, con tal que la activación del procedimiento sea claramente reconducible a la voluntad del titular. 4. Los dispositivos seguros de firma son presentados a la valoración y certificación de seguridad del sector de la tecnología de la información del art. 10, apartado 1, del Decreto Legislativo de 23 de enero de 2002, núm. 10»).

En sentido similar, se expresa el art. 2.7 con las exigencias previstas en el Anexo III de la Ley belga de 2001, y el art. 4 del Reglamento luxemburgués de 2001.

[60] A. MARTÍNEZ NADAL, «Comentario al art. 24 de la LFE», en *Comentarios a la Ley 59/2003..., op. cit.,* p. 411.

[61] En este sentido, se expresa también la Exposición de Motivos de la LFE, en su apartado II.

temas de certificación de prestadores de servicios de certificación y de dispositivos de firma electrónica» [62].

El precedente de esta norma se halla en los apartados 4 y 5 del art. 3 de la Directiva, y en los arts. 20 y 21 del RDL 14/1999, dedicados al establecimiento de un procedimiento de evaluación y certificación de la seguridad de los dispositivos de firma.

Se define en el apartado 1 del citado art. 27 la certificación de dispositivos seguros de creación de firma electrónica como *«el procedimiento por el que se comprueba que un dispositivo cumple los requisitos establecidos en esta Ley para su consideración como dispositivo seguro de creación de firma»*. Se trata, pues, de un procedimiento cuya finalidad reside en la comprobación del cumplimiento de los requisitos de seguridad previstos en el mencionado art. 24.3.

Podrá ser solicitado, tal como dispone expresamente el apartado 2 del art. 27, *«por los fabricantes o importadores de dispositivos de creación de firma y se llevará a cabo por las entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria, y en sus disposiciones de desarrollo»*.

La certificación se debe llevar a cabo por las entidades de certificación que hayan sido, asimismo, reconocidas por una entidad de acreditación establecida conforme a la Ley de Industria. Mientras no sean aquellas entidades de certificación reconocidas, no podrá procederse a la certificación de dispositivos seguros de creación de firma.

Existentes tales entidades de certificación, las normas que han de aplicarse para llevar a cabo la correspondiente certificación de los dispositivos las establece el art. 27.3 cuando dispone que *«en los procedimientos de certificación se utilizarán las normas técnicas cuyos números de referencia hayan sido publicados en el* "Diario Oficial de la Unión Europea" *y, excepcionalmente, las aprobadas por el Ministerio de Ciencia y Tecnología que se publicarán en la dirección de Internet de este Ministerio»*. En este sentido, el art. 28 de la LFE, bajo el título «Reconocimiento de la conformidad con la normativa aplicable a los productos de firma electrónica», establece en su

---

[62] En la Exposición de Motivos de la LFE, apartado II, se contempla la certificación técnica de los dispositivos seguros de creación de firma electrónica: «*La certificación técnica de los dispositivos seguros de creación de firma electrónica se basa en el marco establecido por la Ley 21/1992, de 16 de julio, de Industria, y en sus disposiciones de desarrollo. Para esta certificación se utilizarán las normas técnicas publicadas a tales efectos en el Diario Oficial de las Comunidades Europeas*, *o, excepcionalmente, las aprobadas por el Ministerio de Ciencia y Tecnología.*»

apartado 1 que «*se presumirá que los productos de firma electrónica aludidos en la letra* d) *del apartado primero del art. 20, y en el apartado tercero del art. 24 son conformes con los requisitos previstos en dichos artículos si se ajustan a las normas técnicas correspondientes cuyos números de referencia hayan sido publicados en el* "Diario Oficial de la Unión Europea"».

Tales previsiones normativas responden a la uniformidad técnica que desde instancias europeas se predica para la certificación de dispositivos de seguros de creación de firma que se desarrollen en el ámbito de la Unión europea, a lo que se ha de añadir, una uniformidad interna derivada de las normas técnicas que, a su vez, se publiquen en la dirección de Internet del Ministerio de Ciencia y Tecnología.

Desde la perspectiva expuesta, básicamente este procedimiento de certificación es un procedimiento voluntario cuyo alcance es meramente comercial, pues el fabricante o importador de tales productos de firma electrónica que hayan solicitado y obtenido la correspondiente certificación tendrán sobre los demás competidores una ventaja, derivada del plus de calidad y de seguridad que le proporciona el haber obtenido la correspondiente certificación.

No obstante, aun siendo un dispositivo de creación de firma seguro, no impide su modificación o revocación, si precisamente sus titulares dejan de cumplir las condiciones iniciales de obtención, tal como dispone el art. 27.4 de la LFE.

Ahora bien, aunque la obtención de la certificación por los interesados conforme dispone el art. 27 de la LFE, no hace presumir que el dispositivo es seguro, a diferencia de lo establecido de forma genérica en el art. 20 y de forma específica en el art. 3.1, ambos del RDL 14/1999. El art. 28 de la LFE, sin embargo, en su apartado 1, parte de una presunción genérica de cumplimiento de determinados requisitos legales por parte de los productos de firma electrónica, en concreto los aludidos en el párrafo *d)* del art. 20, que impone al prestador de servicios de certificación que expida certificados reconocidos la obligación de «*utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirve de soporte*», y los previstos en el apartado 3 del art. 24, que, como bien sabemos, establece las exigencias que deben cumplir los dispositivos seguros de creación de firma para ser considerados como tales [63].

[63] Tiene su origen esta previsión en el art. 3.5 de la Directiva, que dispone que «*la Comisión, con arreglo al procedimiento del art. 9, podrá determinar y publicar en el* Diario Oficial de las Comunidades Europeas *los números de referencia de las normas que gocen de reconoci-*

Mientras que el mencionado art. 28 en su apartado segundo aborda la cuestión del reconocimiento de la eficacia de los certificados sobre dispositivos seguros de creación de firma expedidos en otros Estados miembros, disponiendo al efecto, en cumplimiento precisamente de lo previsto en el art. 3.4 de la Directiva, que «*se reconocerá eficacia a los certificados de conformidad sobre dispositivos seguros de creación de firma que hayan sido otorgados por los organismos designados para ello en cualquier Estado miembro del Espacio Económico Europeo*» [64]. Con esta previsión se viene a reconocer la interoperabilidad de los dispositivos de firma electrónica certificados entre los distintos Estados miembros, partiendo de la idea no sólo de nuestra pertenencia a la Unión Europea, sino también al mercado transfronterizo de las comunicaciones electrónicas, en el seno de la Unión, como fuera de la misma.

Una vez establecidos los requisitos que deben cumplir los dispositivos de creación de firma para ser considerados seguros, y determinar, asimismo, la posibilidad de certificación de los mismos por una entidad de certificación que así lo acredite, como el reconocimiento de aquellos que se expidan en otros Estados miembros, corresponde referirse en este momento, respecto a los dispositivos de verificación de firma, y a partir de la definición legal dada de los mismos al inicio de este apartado, a los requisitos que la LFE en su art. 25.3 señala que deben cumplir estos dispositivos así; se dispone que «*los dispositivos de verificación de firma electrónica garanti-*

---

miento general para todos los productos de firma electrónica. Los Estados miembros presumirán que los productos de firma electrónica que se ajusten a dichas normas son conformes con lo prescrito en la letra f) *del anexo II ("utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procedimientos con que trabajan") y en el anexo III de la presente Directiva ("requisitos de los dispositivos seguros de creación de firma")».*

[64] El art. 3.4 de la Directiva establece que «*la conformidad de los dispositivos seguros de creación de firma con los requisitos fijados en el anexo III ("Requisitos de los dispositivos seguros de creación de firma") será determinada por los organismos públicos o privados pertinentes, designados por los Estados miembros. La Comisión, con arreglo al procedimiento del art. 9, establecerá los criterios para que los Estados miembros determinen si procede designar un determinado organismo. La conformidad con los requisitos del anexo III establecida por dichos organismos será reconocida por todos los Estados miembros».*

Por su parte, de forma similar se pronunciaba el art. 21.1 del RDL 14/1999, al señalar que: «*1. Los órganos de certificación a los que se refiere el art. 6 podrá certificar los dispositivos seguros de creación de firma electrónica, previa valoración de los informes técnicos emitidos sobre los mismos, por entidades de evaluación acreditadas.*

En la evaluación del cumplimiento de los requisitos previstos en el art. 19, las entidades de evaluación podrán aplicar las normas técnicas respecto de los productos de firma electrónica a las que se refiere el artículo anterior u otras que determinen los órganos de acreditación y de certificación, y cuyas referencias se publiquen en el Boletín Oficial del Estado.»

zarán, siempre que sea técnicamente posible, que el proceso de verificación de una firma electrónica satisfaga, al menos, los siguientes requisitos:

a) *Que los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma.*

b) *Que la firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente.*

c) *Que la persona que verifica la firma electrónica pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.*

d) *Que se muestren correctamente tanto la identidad del firmante o, en su caso, consten claramente la utilización de un seudónimo, como el resultado de la verificación.*

e) *Que se verifiquen de forma fiable la autenticidad y la validez del certificado correspondiente.*

f) *Que pueda detectarse cualquier cambio relativo a su seguridad*».

Estos requisitos coinciden básicamente con los que dispone la Directiva comunitaria en el art. 3.6, y se trata simplemente de exigencias destinadas tanto a garantizar la seguridad y fiabilidad de los productos (de los datos mostrados a la persona que verifica la firma), y del procedimiento de verificación de un mensaje firmado electrónicamente para detectar si ha sido modificado, como de la comprensión del procedimiento, sus elementos básicos y su resultado por el verificador[65]. La LFE, no obstante, no contempla, a diferencia de para los dispositivos seguros de firma electrónica, la posibilidad de certificación de estos dispositivos por parte de una entidad de certificación.

Finalmente, de forma novedosa, y sin que exista precedentes ni en la normativa comunitaria, ni en el RDL 14/1999, se refiere la LFE en el art. 25.4 al almacenamiento de datos de verificación de firma[66]. Alude tanto al momento en que la firma se produce como a la constatación de la validez del certificado electrónico en el momento de la verificación —ante la posibilidad de revocación de éste—, y a las circunstancias, no sólo relevantes para la determinación de la validez y eficacia de la firma, sino también para

---

[65] A. MARTÍNEZ NADAL, «Comentario al art. 25 de la LFE», en *Comentarios a la Ley 59/2003..., op. cit.,* p. 422.

[66] Art. 25.4 de la LFE dispone: «*Asimismo, los datos referentes a la verificación de la forma, tales como el momento en que ésta se produce o una constatación de la validez del certificado electrónico en ese momento, podrá ser almacenados por la persona que verifica la firma electrónica o por terceros de confianza.*»

constatar cuándo deben almacenarse los datos de verificación de firma. Tal función de almacenamiento o custodia puede recaer tanto en la persona que verifica la firma, como en un tercero, bien la propia entidad de certificación, o bien, un notario, siendo quizá esta segunda posibilidad más adecuada que la primera a los efectos de dotar a la actuación de más independencia y objetividad.

3. Efectos jurídicos de la firma electrónica

A la validez y eficacia de la firma electrónica dedica la LFE los apartados 4, 8, 9 y 10 del art. 3, que coincide sustancialmente con lo dispuesto en el art. 5 de la Directiva comunitaria, y en los que se equipara la firma electrónica reconocida a la firma manuscrita, se determina las consecuencias de la impugnación de la autenticidad de la firma electrónica reconocida por la otra parte no firmante, se reconoce valor jurídico a la autonomía de la voluntad de las partes para dotar de eficacia a la firma electrónica y se especifica la admisibilidad de los datos firmados electrónicamente como prueba documental en juicio; del análisis de todas estas materias nos ocuparemos en este apartado.

Como mencionamos en líneas precedentes, el art. 3.4 de la Ley establece la regla del equivalente funcional entre la firma electrónica reconocida y la firma manuscrita, al disponer que *«la firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel»* [67]. Esta regla ya

[67] De la misma forma, se pronuncia el art. 7 del Decreto-ley portugués núm. 290-D/99 al disponer: «*1. A aposiçao de una assinatura digital a um documento electrónico ou a uma cópia deste equivale à assinatura autógrafa dos documentos com forma escrita sobre suporte de papel e cria a presunçao de que:* a) *a pessoa que apôs a assinatura digital é o titular desta ou é representante, com poderes bastantes, da pessoa colectiva titular da assinatura digital;* b) *a assinatura digital foi aposta com a intençao de assinar o documento electrónico;* c) *o documento electrónico näo sofreu alteraççäo desde que ihe foi aposta a asssinatura digital, sempre que seja utilizada para verficaçäo uma chave pública contida em certificado válido emitido por entidade certificadora credenciada nos termos deste diploma*» (La fijación de una firma digital a un documento o a una copia de éste equivale a firma autógrafa de documentos con forma escrita sobre soporte papel y determina la presunción de que: *a)* la persona que fija la firma digital es titular de ésta o es representante, con poderes bastantes, de persona jurídica titular de la firma digital; *b)* la firma digital fue puesta con la intención de firmar un documento electrónico; *c)* o el documento electrónico no ha sufrido alteración desde que fue puesta la firma digital, siempre que se haya utilizado para verificarla una clave pública contenida en un certificado válido emitido por una entidad certificadora acreditada en los términos de esta norma»).

se contenía en el art. 3.1, párrafo 1.º, del RDL 14/1999, que establecía asimismo que: «*La firma electrónica avanzada, siempre que esté basada en un certificado reconocido y haya sido producida por un dispositivo seguro de creación de firma, tendrá respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel...*» Lo cierto es que, como ya indicamos, las diferencias existentes entre ambas regulaciones son más formales que reales en este punto, pues lo dispuesto en el art. 3.3 de la LFE cuando define qué se entiende por firma electrónica reconocida viene a coincidir sustancialmente con los términos contenidos en el art. 3.1, párrafo 1.º, del RDL 14/1999, y, en consecuencia, cuando se dota de plena eficacia y de equivalencia funcional con la firma manuscrita a la firma electrónica avanzada que cumpliera con los requisitos mencionados en el citado art. 3.1, éstos vienen a ser los mismos que son exigibles en la regulación actual para la firma electrónica reconocida. Recordemos que el art. 3.3 de la LFE considera firma electrónica reconocida «*la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma*» [68].

El art. 4, parágrafo 4, de la Ley belga de 2001 «*sans préjudice des articles 1323 et suivants du Code Civil, une signatura électronique avancée realisée sur la base d'un certificar qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, est assimilée à une signatura manuscrite, qu'elle sois réalisée par une personne physique ou morale*» (sin perjuicio de los arts. 1.323 y siguientes del Código Civil, una firma electrónica avanzada realizada sobre la base de un certificado cualificado y establecida por medio de un dispositivo seguro de creación de firma electrónica, se asmila a una firma manuscrita, sea realizada por una persona física o moral).

El art. 7.1 del Decreto portugués núm. 290-D/99: «*A aposição de uma assinatura digital a um documento electrónico ou a uma cópia deste equivale à assinatura autógrafa dos documentos com forma escrita sobre suporte de papel.*» Y el parágrafo 6.2 de la Ley alemana de 2001 dentro del Capítulo II referido a los denominados ofertantes de servicios de certificación, esto es, a los prestadores de servicios de certificación, establece que éstos deben informar y advertir al solicitante que la firma electrónica cualificada tiene en el tráfico jurídico el mismo efecto que la firma manuscrita, si la ley no establece otra cosa *[«(2) Der Zertifizierungsdiensteanbieter hat den Antragsteller darüber zu unterrichten, dass eine qualifizierte elektronische Signatur im Rechtsverkehr die gleiche Wirkung hat wie eine eigenhändige Unterschift, wenn durch Gesetz nicho ein anderes bestimmt ist»]*.

Fuera de Europa, tanto la Ley de Firma Digital de Utah (en el Título III, sección 403), como *E-Sign Act* (sección 101) otorgan a la firma y al documento electrónico un *status* legal equivalente a la firma en soporte autógrafo y al documento en papel.

[68] El Código francés, aunque ha tomado un camino diferente, pues ha modificado el concepto de «escritura» para que quepa en él la firma electrónica, y en su reforma por Ley 465/2000, incluye una definición de «prueba literal» o «prueba por escrito», como «serie de letras, de caracteres, de cifras, o de cualesquiera otros signos o símbolos dotados de caracteres, de cifras o de cualesquiera otros signos o símbolos dotados de significado inteligible», lo

En consecuencia, sobre lo expuesto, para la plena operatividad de la regla de la equivalencia funcional de la firma electrónica reconocida con la firma manuscrita, que dispone el art. 3.4 de la LFE, en una interpretación conjunta con el art. 3.3 de esta misma Ley, es necesario el cumplimiento de los siguientes requisitos:

1.º Debe tratarse de una firma electrónica avanzada (art. 3.2 de la LFE).

2.º Dicha firma electrónica avanzada ha de estar basada en un certificado reconocido, es decir, aquel que cumple los requisitos de los arts. 11, 12 y 13 de la LFE, y que haya sido expedido por un prestador de servicios

---

que le permite conservar la rúbrica «De la prueba literal», para que la prueba pueda ser igualmente aquella que no consiste necesariamente en «letras».

Art. 1.316 del *Code* (L. n. 2000-230, 13 de marzo de 2000, art. 1-III): «*La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou des tous autras signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmision.*»

Sin embargo, precisa en el art. 1.316-1 del *Code* (L. n. 2000-230, 13 de marzo de 2000, art. 1-III): «*L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'integrité*» («Los escritos bajo forma electrónica son admitidos en el mismo título que los escritos sobre soporte papel, bajo la reserva que pueden ser debidamente identificada la persona del que emane y que han establecido y conservado las condiones innatas para garantizar la integridad.»)

Por su parte, el art. 10.3 del Decreto 445/2000, reformado por Decreto Legislativo de 23 de enero de 2002, núm. 10 (art. 6), sin utilizar la equiparación como hace la legislación española entre firma manuscrita y firma electrónica reconocida, no obstante, establece que ésta hace prueba plena de su existencia, por lo que en el fondo se mantiene en la misma línea. Así, dispone que «*3. Il documento informatico, quando è sottoscritto con firma digitale o con un altro tipo de firma elettronica avanzata, e la firma è basata su di un certificato qualificato ed è generata mediante un dispositivo per la creazione di una firma sicura, fa inoltre piena prova, fino a querela di falso, della provenienza delle dichiarazioni l'ha sottoscritto*» («3. El documento informático, cuando está suscrito con firma digital o con otro tipo de firma electrónica avanzada, y la firma está basada en un certificado cualificado y es generada mediante un dispositivo para la creación de una firma, hace, además, prueba plena, salvo querella de falsedad, de la procedencia de la declaración del que la ha suscrito»). Algún autor como G. BUONOMO, «Lo schema governativo stravolge il proceso civile», en *InterLex de 24 gennaio de 2002* (http.//www.interlex.it/docdigit/buonomo8.htm), se inclina por considerar que del texto del citado art. 10 el documento informático firmado con firma digital, es equivalente a la firma auténtica de notario, otorgándole, por tanto, un valor superior al del documento cartáceo, pues atribuye a esta firma el valor de certificación notarial. En contra y en la línea de la equiparación ya introducida con el d.P.R. 513/1997, se muestran M. CAMMARATA y E. MACCARONE, *La firma digitale sicura. Il documento informatico nell'ordinamento italiano,* Milano, Giuffrè, 2003, p. 93, quienes ponen de manifiesto el desastre normativo que puede ser adoptar tal posición, dada la adopción generalizada del documento informático, sobre todo en las relaciones privadas.

de certificación que cumpla con los requisitos previstos en el art. 20 de la LFE.

3.º Dicha firma electrónica avanzada, además, debe haber sido producida por un dispositivo seguro de creación de firma que cumpla con los requisitos del apartado 3 del art. 24 de la LFE.

Ahora bien, cumplidos los requisitos reseñados, y verificada la equivalencia funcional con la firma manuscrita, no existe, sin embargo, a diferencia del art. 3.1, párrafo 2.º, del RDL 14/1999, una presunción legal expresa de cumplimiento de tales requisitos en el art. 3 de la LFE. El citado art. 3.1, párrafo 2.º, del RDL 14/1999 disponía que *«se presumirá que la firma electrónica avanzada reúne las condiciones necesarias para producir los efectos indicado en este apartado, cuando el certificado reconocido en que se base haya sido expedido por un prestador de servicios de certificación acreditado y el dispositivo seguro de creación de firma con el que ésta se produzca se encuentre certificado, con arreglo a lo establecido en el artículo 21»*. Esta supresión de la presunción legal, que constituyó en su momento una aportación novedosa del RDL 14/1999 —al no exigirse en el Derecho comunitario—, no sólo alcanza al texto del art. 3 de la LFE, en el que no existe, como hemos indicado, referencia alguna a la misma, sino que también parece optarse por tal supresión al pronunciarse expresamente el art. 26.4 en los siguientes términos: *«la certificación de un prestador de servicios de certificación no será necesaria para reconocer eficacia a una firma electrónica»* [69]. Lo que va a exigir, en principio, la acreditación o demostración necesaria del cumplimiento de los requisitos reseñados por la parte interesada en la validez de la firma para que la equiparación funcional de la firma electrónica reconocida con la firma manuscrita resulte operativa. Y hará necesario acudir a complejas y dificultosas pruebas que nos permitan demostrar la existencia de los requisitos establecidos en el mencionado art. 3.3 [70].

Aunque pueda ser criticable la eliminación de la citada presunción legal del art. 3.1, párrafo 2, del RDL 14/1999, pues en ocasiones la prueba o pruebas que se practiquen ante el juez sobre la existencia de tales requisi-

---

[69] Y también en la Exposición de Motivos de la LFE en su apartado III, al disponer: «*Por otra parte, la Ley modifica el concepto de certificación de prestadores de servicios de certificación para otorgarle mayor grado de libertad y dar un mayor protagonismo a la participación del sector privado en los sistemas de certificación y eliminando las presunciones legales asociadas a la misma, adaptándose de manera más precisa a lo establecido en la Directiva.*» Lo que en ambos casos parece vincularse la eliminación de la presunción legal, con el cambio en la conceptuación de los prestadores de servicios de certificación.

[70] En este sentido, A. MARTÍNEZ NADAL, «Comentario al art. 3 de la LFE», en *Comentarios a la Ley 59/2003, de firma electrónica, op. cit.,* p. 78.

tos van a resultar prácticamente imposibles; lo cierto es, señala Martínez Nadal, que la tendencia a la privatización de los sistemas de certificación y, el riesgo de dotar de iguales efectos a distintos sistemas de certificación, sean públicos o privados, con diferente contenido, seguridad y fiabilidad, determinan que el legislador haya optado en la actual LFE por prescindir del beneficio de la presunción. No parece razonable que a una simple declaración de una entidad de naturaleza privada que no ofrezca una adecuada seguridad y fiabilidad en sus productos, sea beneficiada al mismo nivel —si resultará operativa la presunción legal—, que otra igualmente privada que, dotada, además, de la certificación expedida por una autoridad de certificación, ofrezca productos de firma más seguros y fiables [71].

No obstante, frente a tales argumentos, el art. 3.8 cuando se refiere a la impugnación de la autenticidad del documentos firmado con firma electrónica reconocida, dispone simplemente que *«se procederá a comprobar por el prestador de servicios de certificación...»* el cumplimiento de una serie de obligaciones que van a influir, entre otros extremos, en los relativos a la autoría, integridad y confidencialidad y no repudio del mensaje firmado electrónicamente. Lo que parece deducirse de esa simple comprobación de los extremos indicados es que por el hecho de tratarse de un documento firmado con una firma electrónica reconocida, ya se presumen existentes, salvo prueba en contrario, y siempre con una responsabilidad del cumplimiento de los mismos por parte de la entidad certificadora. De forma que, al no ser necesaria su prueba, pues se presumen, simplemente se exigirá la comprobación de su cumplimiento, lo que determinará que la carga de probar que la autoría e integridad del documento aparente no se corresponde con la realidad fáctica, recaiga en quien precisamente invoque tales hechos.

Desde tal planteamiento, si bien no en el propio texto legal, pero sí implícitamente, operaría la presunción; y, en consecuencia, alcanzaría la misma a la equiparación de efectos con la firma manuscrita. Pero siendo conscientes de la existencia de un sistema de certificación donde se da pleno protagonismo al sector privado, y en la línea doctrinal expuesta, aunque se emplee el término «comprobará», habrá de entenderse que en el fondo lo que el legislador está pensando es que se deberá «probar», si se quiere dotar, como parece ser también su intención, de las máximas garantías de seguridad y fiabilidad al consumidor final de los diferentes produc-

---

[71] En este sentido, A. MARTÍNEZ NADAL, «Comentario al art. 3 de la LFE», en *Comentarios a la Ley 59/2003, de firma electrónica, op. cit.,* p. 79.

tos de firma electrónica, frente a la existencia de diferentes prestadores con distinto nivel de calidad, seguridad y fiabilidad tanto en aquellos que ofrecen como en los servicios que prestan.

En cualquier caso, este reconocimiento legal de efectos del art. 3.3 de la LFE se establece sólo respecto de las firmas electrónicas reconocidas, pero que sucede con aquellas firmas electrónicas que no reúnen los requisitos para la equiparación. Al efecto, se establece en el apartado 9 del art. 3 que «*no se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de la firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica*»[72].

Al no beneficiarse de la equiparación, la eficacia de la firma en relación a la autoría e integridad del mensaje firmado exigirá la aportación de elementos probatorios, la mayoría de las veces difíciles y costosos en su ejecución.

Por otra parte, sin mención expresa ni el RDL 14/1999 ni en el texto articulado de la Directiva, el art. 3.10 de la LFE se da plena operatividad a la «firma electrónica convencional»[73]. Se reconoce, en virtud del principio

---

[72] Coincide con lo establecido en el art. 5.2 de la Directiva sobre firma electrónica: «*Los Estados miembros velarán por que no se niegue eficacia jurídica, ni a la admisibilidad como prueba en procedimientos judiciales, a la firma electrónica por el mero hecho de que:*

— *ésta se presente en forma electrónica, o*

— *no se base en un certificado reconocido, o*

— *no se base en un certificado expedido por un proveedor de servicios de certificación acreditado,*

— *o no esté creada por un dispositivo seguro de creación de firma.*»

Y con el art. 3.2 del RDL 14/1999 que disponía que: «*A la firma electrónica que no reúna los requisitos previsto 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.*»

Por su parte, en esta línea, el art. 10.4 del Decreto 445/2000 señala que: «*4. Al documento informatico, sottocristto con firma elettronica, in ogni caso no può essere negata rilevanza giuridica né ammissibilità come mezzo di prova unicamente a causa del atto che è sottoscritto in forma elettronica ovvero in quanto la firma no è basata su di un certificato qualificato rilasciato da un certificatore accreditato o, infine, perché la firma no è stata aposta avvalendosi di un dispositivo per la creazione di una firma ricura*» («Al documento suscrito con firma electrónica, en todo caso, no puede ser negada su relevancia jurídica ni admisibilidad como medio de prueba únicamente a causa del acto que ha sido suscrito en forma electrónica, o bien, en cuanto la firma no está basada en un certificado cualificado expedido por un certificador acreditado, o en fin porque la firma no haya sido producida valiéndose de un dispositivo para la creación de una firma segura».)

[73] Denominación aceptada por una parte importante de la doctrina. Véanse, entre otros autores, G. GÁLLEGO HIGUERAS, «Comentario a la reciente Ley 59/2003...», *op. cit.,* p. 25; R. RUBIO VELÁZQUEZ e I. ALAMILLO DOMINGO, «Firma electrónica y certificación digital», *op. cit.,* p. 641.

El art. 3.10 de la LFE dispone que «*a los efectos de lo dispuesto en este artículo, cuando una firma electrónica se utilice conforme a las condiciones acordadas por las partes para relacionarse entre sí, se tendrá en cuenta lo estipulado entre ellas*».

de autonomía de la voluntad, que las partes puedan fijar las condiciones sobre las que va a operar la firma electrónica en orden a su eficacia[74]. De forma que ésta no se hace depender de una ley, sino del acuerdo de voluntades que conforma el contenido del contrato, en el que se ha reconocido y dotado a la firma electrónica en los términos fijados contractualmente con eficacia vinculante *inter partes*. El despliegue de efectos de tal firma, por tanto, solo alcanza a determinados sujetos, en concreto a quienes han sido parte de un contrato y es por ello por lo que dicha firma y su eficacia deberá someterse al régimen acordado por la partes en el ejercicio de su autonomía de la voluntad, y no a los requisitos que marca la regulación que con alcance general determina una ley. Se prevé en los contratos previos consustanciales a los entornos cerrados de usuarios, que los documentos electrónicos que se intercambien los usuarios contengan una firma electrónica dotada de una serie de características previamente acordadas y que las partes la determinen como mecanismo adecuado para instrumentar su declaración de voluntad.

Sin embargo, para algún autor esta posibilidad que ofrece el legislador resulta altamente peligrosa, pues en ningún caso la equivalencia funcional, las garantías y los requisitos que la ley exige a los determinados tipos de firma electrónica pueden ser dejados a la autonomía de voluntad de las partes, por ser normas de derecho imperativo o de *ius cogens*[75].

Por otra parte, el Considerando 16 de la Directiva sobre firma electrónica, sobre el que probablemente se basa el contenido del citado art. 3.10, establece que «*la presente Directiva contribuye al uso y al reconocimiento legal de la firma electrónica en la Comunidad; no se precisa un marco reglamentario para las firmas electrónicas utilizadas exclusivamente dentro de sistemas basados en acuerdos voluntarios de derecho privado celebrado entre un número determinado de participantes; 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 se 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*».

[74] Estas condiciones, como señalan Rubio Velázquez y Rodríguez Sau, «podrán tener en cuenta, entre otros, los siguientes aspectos: 1. Selección del ámbito de uso de la firma electrónica. 2. Determinación del *significado* exacto del acto de firma. Atribuyéndole un valor concreto, no necesariamente como autor del documento, sino como revisor, testigo, etc. 3. Establecimiento de la necesidad de emplear ciertos *atributos* y de la fuente de obtención de los mismos, tales como poderes, autorizaciones, roles, cargos, etc. 4. Necesidad de emplear ciertos *mecanismos de verificación* de los certificados reconocidos, como listas de certificados revocados (CRLs). 5. Establecimiento de ciertos *requisitos adicionales* para considerar válida una firma electrónica entre las partes. Estos requisitos pueden ser técnicos, funcionales o subjetivos. 6. Establecimiento de *efectos adicionales* a los previstos por la ley para el tipo de firma empleada». Véase R. RUBIO VELÁZQUEZ y C. RODRÍGUEZ SAU, «Concepto legal de firma electrónica y de prestador de servicios de certificación», en *La firma electrónica..., op. cit.,* pp. 38-39.

[75] Fco. J. GARCÍA MAS, *Comercio y firma electrónicos, op. cit.,* p. 69.

No obstante, de ser problemática esta forma de dotar de eficacia a la firma, lo será sobre todo en aquellos supuestos en que la situación de igualdad no exista entre las partes y, por tanto, dé lugar a una situación de abuso que perjudique gravemente a una de ellas. En otros casos, al suplir la falta de presunción legal en los términos vistos, con respecto a lo previsto en la regulación anterior, a través de lo convenido por las partes, puede resultar positiva su utilización para evitar determinados resultados excluyentes [76].

3.1. *Aspectos procesales. La impugnación de la autenticidad de la firma electrónica*

Una importante novedad que contiene la LFE con respecto al RDL 14/1999, en lo que atañe a la equivalencia funcional de la firma electrónica, como indicamos en líneas precedentes, la encontramos en el apartado 8 del art. 3. Dicho apartado fue introducido durante la tramitación del proyecto de ley en el Senado a resultas de la enmienda número 275 propuesta por el Grupo Parlamentario Popular [77]. En su contenido se refiere a la eficacia probatoria que esencialmente tiene todo tipo de firma —electrónica o no—, regulando algunas de las vicisitudes que pueden derivarse ante la aportación de un documento firmado electrónicamente como prueba en un proceso y haciendo en particular referencia a la impugnación de la firma electrónica por la otra parte [78].

Únicamente de la impugnación de la firma nos vamos a ocupar en este apartado dejando el análisis de la eficacia probatoria del documento firmado electrónicamente, para el que dediquemos a los documentos electrónicos.

La norma diferencia dos escenarios distintos atendiendo al tipo de firma electrónica que sea objeto de impugnación. Así, establece que «*... si se impugnare la autenticidad de la firma electrónica reconocida, con la que se hayan firmado los datos incorporados al documento electrónico, se procederá a comprobar que por el prestador de servicios de certificación, que expide los certificados electrónicos, se cumple todos los requisitos establecidos en la ley en cuanto a la garantía de los servicios que presta en la comprobación de la eficacia de la firma electrónica, y en especial, las obligaciones de garantizar la*

---

[76] En este mismo sentido A. MARTÍNEZ NADAL, «Comentario al art. 3 de la LFE», en *Comentarios a la Ley 59/2003, de firma electrónica, op. cit.,* p. 81.

[77] *BOCG*, Senado, núm. 158, Serie II, 21 de octubre de 2003, pp. 108-109.

[78] G. GÁLLEGO HIGUERAS, «Comentarios a la reciente Ley 59/2003, de 19 de diciembre», *op. cit.,* p. 31.

confidencialidad del proceso, así como la autenticidad, conservación e integridad de la información generada y la identidad de los firmantes...».

Sobre tal base legal, para la impugnación de la firma electrónica reconocida, el legislador se centra en la comprobación del cumplimiento por parte del prestador de servicios de certificación de los requisitos que prevén los arts. 17 a 21 de la LFE, que pueden influir en la seguridad del certificado emitido y de la firma electrónica que la acompaña y en particular de todos aquellos que pueden afectar a la confidencialidad del proceso de generación de firma, a la autenticidad de la firma electrónica, a las garantías sobre la conservación e integridad de la información generada, así como también a la comprobación de la identidad de los firmantes.

Si bien, partiendo, como es sabido, que para que a una firma electrónica reconocida se la califique como tal, se requiere que además de garantizar la identidad del firmante y la integridad del documento firmado —esto es, ser una firma electrónica avanzada— esté soportada por un certificado reconocido y haya sido generada mediante un dispositivo seguro de creación de firma; su impugnación exigiría probar no sólo la naturaleza de avanzada de dicha firma, sino también la existencia, por un lado, de un certificado de firma que cumpla con los requisitos exigidos para ser calificado de reconocido previstos en el art. 11 de la LFE, y expedido por un prestador de servicios de certificación, que cumpla con los requisitos exigidos para este tipo de entidades de certificación en el art. 20 de esta Ley, y, por otro, la condición de «seguro» del dispositivo de creación de firma utilizado, y, en consecuencia, que en el mismo se den las características previstas en el art. 24.3. El hecho de que no se tenga presente algunos de estos extremos en la regulación del art. 3.8 la hacen a ésta insuficiente en su contenido y descuida que la impugnación de una firma electrónica reconocida pueda venir justificada por la existencia de vicios en otros elementos, ajenos al buen hacer de la entidad de certificación, pero necesarios para dotar a dicha firma electrónica de la condición de «reconocida», por ejemplo, la inexistencia de un certificado reconocido de firma o la no utilización de un dispositivo de creación de firma seguro [79]. Puede, no obstante, pensarse que la enumeración legal es simplemente ejemplificativa [80], lo que permite otros supuestos de impugnación centrados en la falta de alguno

[79] En esta línea, G. GÁLLEGO HIGUERAS, «Comentarios a la reciente Ley 59/2003, de 19 de diciembre», *op. cit.,* p. 32.

[80] En este sentido, A. MARTÍNEZ NADAL, «Comentario al art. 3 de la LFE», en *Comentarios a la Ley 59/2003 de firma electrónica, op. cit.,* p. 83.

de los requisitos que se exigen para que exista una firma electrónica reconocida [81].

Si de lo que se trata, es de la impugnación de una firma electrónica avanzada, establece el citado art. 3.8 que *«si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónicos se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil»*.

En este sentido, la autenticidad de la firma electrónica avanzada requerirá el cumplimiento de los requisitos dispuesto en el art. 3.2 de la LFE, que inciden en la autenticidad e integridad del mensaje firmado, atenientes unos a la propia firma al exigir capacidad del sistema o algoritmo utilizado para crear la firma, y para vincular ésta al firmante como para garantizar la ausencia de manipulaciones respecto de la propia firma, y también en relación con el documento en la que ésta se contiene, y otros al firmante al permitir su identificación y exigirle la custodia de los datos de creación de firma (clave privada).

Ahora bien, a diferencia de la anterior impugnación, el legislador para este supuesto remite a la aplicación del art. 326, apartado 2, de la LEC —relativo a la fuerza probatoria de los documentos privados—, establece los criterios a tener en cuenta en caso de impugnación de la autenticidad de un documento privado, estableciendo al efecto que cuando se impugne dicha autenticidad, el que lo haya presentado puede solicitar la confrontación pericial de letras o proponer cualquier otro medio de prueba útil y pertinente a este efecto. Por razones obvias, el cotejo de la firma electrónica avanzada resulta irrelevante, de ahí que desde la fórmula abierta y flexible en la proposición y práctica de la prueba que se propugna en el cita-

---

[81] Por su parte, el parágrafo 292.*a)* de la Ley de Enjuiciamiento Civil alemana, reformado por la Ley de 13 de junio de 2001, regula la prueba de la apariencia en caso de forma electrónica cualificada, y así establece que «*la apariencia de autenticidad de una declaración de voluntad presentada en formato electrónico deducida en base a la verificación según la Ley de firma, sólo podrá cuestionarse mediante hechos que justifiquen seriamente la duda de que la declaración ha sido formulada con la voluntad del titular del código de firma*». Este precepto sobre la base de la existencia de una firma electrónica cualificada señala que habrá una apariencia de autenticidad —teniendo presente el concepto de apariencia que se da en el Derecho alemán—, en relación con este tipo de firma, y aun en el caso de que se pueda cuestionar que el documento electrónico no ha sido firmado por el titular de la firma electrónica, no por ello se deja de partir de esta apariencia de autenticidad de la firma electrónica cualificada. En conexión con el parágrafo 126.*a)* del BGB, se cubre tanto el supuesto de inautenticidad formal, consecuencia de la inescindibilidad, característica esencial de la firma electrónica, como de los supuestos de inautenticidad formal —los supuestos de formación errónea del consentimiento—.

do precepto deba optarse por la presentación de otros medios de prueba adecuados que permitan demostrar la autenticidad de la firma que se cuestiona [82].

Si de la práctica de la prueba se desprende precisamente la autenticidad del documento, señala, asimismo el citado art. 326 de la LEC que se procederá de acuerdo con el art. 320.3 de la misma Ley, que impone las costas y gastos a cargo de quien ha formulado la impugnación, así como una multa de 20.000 a 100.000 pesetas, si la impugnación ha sido temeraria. Si, en cambio, de la prueba practicada no se puede deducir la autenticidad o no se ha propuesto prueba alguna, el tribunal lo valorará conforme a las reglas de la sana crítica.

Por otra parte, fuera de la norma del art. 3.8, pero en el seno de la misma LFE, en concreto en su Disposición Adicional décima, se añade un apartado 3 al art. 326 de la LEC con el siguiente tenor: *«cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica»*. Remisión lógica a lo establecido en el citado art. 3.8 para quien inicie el proceso en que se solicite o cuestione la eficacia de una firma, a los efectos de dotar de argumentos su demanda.

Evidentemente todo lo expuesto se entiende al margen de otras cuestiones, como la falta de plena capacidad de obrar del autor de la declaración de voluntad en el momento de emitirse la declaración de voluntad, que no se puede acreditar por el mero hecho de que el documento vaya firmado electrónicamente, con firma avanzada o reconocida, pero que podrá ser motivo igualmente de impugnación si consta la falta de aquélla.

En este contexto, para finalizar este apartado, debemos simplemente poner de manifiesto que pese a la dualidad en la impugnación de la firma por la que ha optado el legislador de la LFE, es posible que en la aplicación práctica del art. 3.8 permita que, si presentado como prueba una documento firmado mediante una firma electrónica reconocida, se pretenda impugnar dicha firma, sustentando que la misma no es tal, por no cumplir con los requisitos que exige la ley para ser considerada avanzada, no pueda acudirse a lo previsto en el mencionado art. 3.8 para la impugnación

---

[82] Para Andrés de la Oliva esta expresión razonable pero poco reveladora de la LEC, viene a indicar que se tratará, en todo caso, de una prueba pericial que debe valorarse probatoriamente conforme a las reglas de la sana crítica y, a su vez, el documento electrónico mismo sólo podrá valorarse según dichas reglas. Véase A. DE LA OLIVA SANTOS, «Consideraciones procesales sobre documentos electrónicos y firma electrónica», *Revista Crítica de Derecho Inmobiliario,* año LXXXI, núm. 687, enero-febrero de 2005, p. 128.

de la firma electrónica avanzada, aun tratándose de la impugnación de una firma electrónica reconocida [83].

Asimismo, aunque no lo señale la LFE, si se impugnara la autenticidad de una firma electrónica ordinaria, se procederá igual que en el caso de la firma electrónica avanzada, aplicando el procedimiento general de autenticidad de los documentos privados.

III. DOCUMENTOS ELECTRÓNICOS: CONCEPTO, CLASES Y FUERZA PROBATORIA

Una de las principales variaciones sufridas por el art. 3 durante la tramitación parlamentaria del Proyecto en el Senado, fue la incorporación, como ya expusimos, vía enmienda de nuevos apartados, en concreto del 5 al 8, destinados a ofrecer una regulación somera del documentos electrónico, sus clases y efectos, pasando a tener el art. 3 la rúbrica de «Firma electrónica y documentos firmados electrónicamente».

En el apartado 5 del art. 3 se define el documento electrónico como aquel «*redactado en soporte electrónico que incorpore datos que estén firmados electrónicamente*». Tal conceptuación constituye la base de admisión legislativa del documento electrónico, basada en el no rechazo del documento por el mero hecho de presentarse en forma electrónica, ya proclamada expresamente para los instrumentos públicos electrónicos en el art. 17 *bis*-1 de la Ley del Notariado cuando señala que «*los instrumentos públicos a que se refiere el artículo 17 de esta Ley no perderán su carácter por el solo hecho de estar redactados en soporte electrónico*».

Son, pues, verdaderos documentos que presentan una serie de características técnicas que los separan de los documentos cartáceos y que desde la propia regulación que ofrece la LFE ha de tratarse de documentos electrónicos que estén firmados con firma simple, con firma avanzada o con firma reconocida, dejando, en consecuencia, fuera de su ámbito de actuación a los documentos electrónicos no firmados.

Su naturaleza documental posibilita que al menos en principio le sean aplicables las diversas clasificaciones que vienen haciéndose de los documentos en general, sobre todo aquella que divide los documentos en públicos y privados, por razón de su autor y de sus diferentes efectos. En lógica

---

[83] En este mismo sentido véase G. GÁLLEGO HIGUERAS, «Comentarios a la reciente Ley 59/2003, de 19 de diciembre», *op. cit.,* p. 33.

consecuencia, el apartado 6 del art. 3 dispone que: «*El documento electrónico será soporte:*

1. *De documentos públicos* que son aquellos *"firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos en la ley en cada caso"*» [art. 3.6.*a)*].

Supone la consagración de la admisibilidad del documento público electrónico y pone fin, en consecuencia, a la discusión abierta sobre si era o no posible su existencia[84]. A la definición normativa de documentos públicos, se añade la ya conocida clasificación, en atención a su autor, en judiciales, notariales y administrativos, a los que podemos añadir los registrales, como los del Registro Civil, o los autorizados por los Registradores de la Propiedad y Mercantiles.

Ahora bien, esta conceptuación de documento público electrónico, como tal documento público, supone asimismo tener presente el concepto que con referencia a este último hace el art. 1.216 del Código Civil y está implícito en la enumeración del art. 317 de la LEC.

Así, el citado art. 1.216 dispone que «*son documentos públicos los autorizados por un Notario o empleado público competente, con las solemnidades requeridas por la Ley*». Por tanto, para la existencia de un documento público es necesario: 1) la condición de funcionario público de su autor. A estos efectos, la LEC 1/2000 requiere que los funcionarios públicos que expidan documentos públicos «*estén facultados para dar fe*» (art. 317.5.º y 6.º), y la LFE exige, en los términos expuestos, que los funcionarios autores del documentos «*tengan legalmente atribuida la facultad de dar fe pública*»; 2) la competencia para tal documentos del funcionario público, o que actúe «*en el ámbito de sus competencias*», como dice la LFE, y 3) el cum-

---

[84] Plaza Penadés reclamaba la posibilidad de que los documentos públicos pudieran adoptar la forma de documentos electrónicos. Al efecto señalaba que «nada impide que un documento electrónico pueda revestir el carácter de público si es emitido por un notario o empleado público competente, con las solemnidades requeridas por la Ley, cuando desempeña su función legal de fedatario o funcionario público». Véase J. PLAZA PENADÉS, «Eficacia de la firma electrónica en los Registros de la Propiedad y Mercantil», en *Revista Crítica de Derecho Inmobiliario,* núm. 667, 2001, p. 2038.

Sin embargo, con un criterio más restrictivo a la admisibilidad de los documentos públicos electrónicos, se pronunciaba la Instrucción de la Dirección General de Registros y del Notariado de 19 de octubre de 2000 (*BOE,* núm. 269, de 9 de noviembre de 2000), que venía a limitar el uso de la firma por los fedatarios públicos a la remisión de comunicaciones prevista en los arts. 175 y 249 del Reglamento Notarial.

plimiento por el funcionario de los requisitos o solemnidades que en cada caso exigen las leyes.

De los documentos públicos electrónicos judiciales, la LEC 1/2000 se refiere en numerosas ocasiones a la utilización de medios electrónicos en el proceso civil (arts. 135.5, 147, 162, 384 y 326.3). De los documentos públicos electrónicos administrativos, la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dedica el art. 45 —no modificado por la Ley 4/1999, de 26 de noviembre— a esta materia y admite una amplia utilización de las técnicas electrónicas por la Administración. En esta línea, la LFE ratifica lo dispuesto en la Ley de Régimen Jurídico tanto en el mencionado art. 3.6.*a)* como en el art. 4 de la misma LFE. Y, de los documentos públicos electrónicos notariales, la Ley de Acompañamiento 24/2001 y la actual Ley 24/2005 de impulso a la productividad. A estos últimos documentos dedicaremos un apartado; de ahí que remitamos al estudio particularizado que de los mismos hagamos en el apartado que dediquemos a tal fin [85].

---

[85] En el ámbito de Derecho comparado, en *Alemania* no se admite el documento público electrónico, pues no se ha aprovechado la aprobación de la Ley de adaptación de las formalidades de Derecho privado, para reformar los parágrafos 128 y 129 del BGB. En *Italia,* el Decreto de 28 de diciembre de 2000 se ocupa, como ya hacía el Reglamento de 1997, de referirse a la posibilidad de autenticación de la firma digital por un oficial público, en general un notario, en el art. 24.1, 2 y 4 del citado Decreto. Así, dispone: «*1. Si ha per riconosciuta, ai sensi dell'art. 2.703 del codice civile, la firma digitale, la cui apposizione è autenticata dal notario o da altro pubblico ufficiale autorizzato. 2. L'autenticazione della firma digitale consiste nell'attestazione, da parte del pubblico ufficiale, che la firma digitale è stata aposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto responde alla volontà della parte e non è in contrasto con l'ordinamento giuridico ai sensi dell'art. 28, primo comma, n. 1 della legge 6 febbraio 1913, n. 89*» («Se ha reconocido, en el sentido del art. 2.703 del Código Civil, la firma digital, cuya fijación es autenticada por el notario u otro oficial público, que la firma digital ha sido puesta en presencia del titular, previa comprobación de su identidad personal, de la validez de la clave utilizada y del hecho que el documento suscrito responde a la voluntad de la parte y no es contrario al ordenamiento jurídico en el sentido del art. 28, apartado 1, de la Ley de 6 de febrero de 1913».)

Y en el Decreto Legislativo 10/2002, de 23 de enero, de reforma del Decreto de 2000 citado, se desconoce el documento público electrónico.

En *Francia* es donde se ha reconocido y consagrado el acto auténtico electrónico, así en el art. 1.316-4 del *Code Civil,* apartado 1, *in fine,* se establece que la firma necesaria para la perfección de un acto jurídico, cuando es puesta por un oficial público, confiere autenticidad al acto *(«Quand elle est apposée par un officier public, elle confère l'authenticitè à cet acte»)*. Y la Ley núm. 445, de 29 de febrero de 2000, dirigida a la adaptación del derecho de prueba a las tecnologías de la información y relativa a la firma electrónica, ha añadido un nuevo párrafo al art. 1.317 del *Code Civil*, en el que tras definir el acto auténtico como «*aquel acto que es aprobado por un oficial público, teniendo la competencia para ello en el lugar donde es redactado el acto y con las solemnidades requeridas»,* dispone que puede ser confecciona-

2. *De «documentos expedidos y firmados electrónicamente por funcionarios y empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica»* [art. 3.6.*b)*].

La LEC se refiere a estos documentos —a los que la Ley de Acompañamiento 24/2001 denomina «oficiales» [art. 109.1.*c)*] o tradicionalmente simples documentos administrativos—, al regular en el art. 319.2 *«la fuerza probatoria de los documentos administrativos no comprendidos en los números 5 y 6 del artículo 317 a los que las leyes otorguen el carácter de públicos»*. Son, por tanto, los expedidos por funcionarios sin fe pública, por lo que no se les puede calificar de públicos, aunque, como dice el citado art. 317, una ley concreta les califique como tales.

Ahora bien, de impugnarse la autenticidad de una firma electrónica reconocida de estos documentos firmados por funcionarios y empleados públicos en el ejercicio de sus funciones, como de hacerlo respecto de la autenticidad de la firma electrónica reconocida de un fedatario (Notario u otro fedatario público) en un documento público —como manifestación de su dación de fe—, exige en ambos casos que se lleve a cabo la comprobación prevista en el art. 3.8 de la LFE en los términos vistos, pues esta firma es tan impugnable como cualquier otra en que no interviene fedatario o funcionario [86].

De documentos privados

De nuevo, ante el silencio del Código Civil, es la LEC la que conceptúa estos documentos, si bien lo hace desde una perspectiva negativa, al disponer en su art. 324 que «*se considera documentos privados, a efectos de prueba en el proceso, aquellos que no se hallen en ninguno de los casos del artículo 317*». Esto es, son documentos privados electrónicos todos los que no son documentos públicos, estén firmados con firma electrónica simple, con

---

do en soporte electrónico *(«L'acte authentique est celui qui a été reçu par officiers publics ayant le droit d'instrumenter dans le lieu où l'acte a été rédigé, et avec les solemnités requises.*

Il peut éter dressé su support électronique s'il est établi et conservé dans des conditions fixées par décret en Coseil d'État»).

[86] Véase A. DE LA OLIVA, «Consideraciones procesales sobre documentos electrónicos...», *op. cit.,* p. 127, quien añade que «*nada hay en esta Ley ni en ninguna otra que permita concluir que el documento con firma electrónica reconocida hace prueba plena si de la comprobación sólo se desprende que, en general, el «prestador de servicios de certificación» actúa conforme a la LFE*».

firma electrónica avanzada o firma electrónica reconocida; pues, como expusimos, la LFE deja fuera a los documentos electrónicos no firmados.

Ahora bien, el que se trate de documento privado firmado con firma electrónica reconocida, no supone, como se deja traslucir por algunos autores, que estos documentos, por las especiales características técnicas que ofrece dicha firma electrónica reconocida, tendrían o deberían tener los mismos efectos procedimentales que corresponde a un documento público, una suerte de nueva categoría *cuasi* pública de esos documentos privados electrónicos con esa firma específica [87]. Pues tal planteamiento no podría aceptarse de partida, entre otras razones porque cualquiera que sea el soporte en que manifieste el documento para que sea considerado público y se le dote de ese valor jurídico reforzado que el ordenamiento otorga en atención a esa específica naturaleza resulta necesaria la intervención de un funcionario con fe pública. Al respecto, acertadamente establece García Mas que «el que exista una firma electrónica reconocida no altera la categoría o modalidad documental, ya que ésta se rige por las normas sustantivas y lo que ocurre es que en este caso existirá una equivalencia funcional entre la firma manuscrita y la firma electrónica, pero en ningún caso que el documento en ese soporte electrónico sea denominado de una o de otra forma» [88].

Finalmente, la LFE tras la definición y fijación de los tipos de documentos alude al valor y eficacia jurídica de los mismos, estableciendo al efecto en el apartado 7 del art. 3 que dependerá esencialmente del tipo de documento que sea y de la legislación que asimismo le sea aplicable [89].

1. Eficacia probatoria del documento firmado electrónicamente

Como ya referimos cuando hablamos de la novedad que constituía el apartado 8 del art. 3 de la LFE respecto de la regulación contenida en el RDL 14/1999, dejamos para un estudio posterior el análisis de la eficacia probatoria del documento firmado electrónicamente, por parecernos la

---

[87] Fco. J. GARCÍA MAS, *Comercio y firma electrónicos, op. cit.,* p. 62.

[88] Fco. J. GARCÍA MAS, *Comercio y firma electrónicos, op. cit.,* p. 64; del mismo autor, «El documento público electrónico», *op. cit.,* pp. 134-135, quien, asimismo, puntualiza que «*de otra manera se desfigura y destruye nuestro sistema de seguridad jurídica, acercándolo de modo absoluto al sistema anglosajón. Es la actuación del funcionario público la que dota de valor documental público al documento por él confeccionado*».

[89] En este mismo sentido, se expresa el art. 3.2 del Decreto portugués núm. 290-D/99.

ubicación más adecuada para su tratamiento ésta en que se analizan los documentos electrónicos.

Señala el art. 3.8 que *«el soporte en el que se hallen los datos firmado electrónicamente será admisible como prueba documental en juicio».* Admisible, pues, como «prueba» en juicio y, más en concreto, como «prueba documental» en el proceso. Tal regulación es, en todo caso, continuación del criterio adoptado por el art. 24.2 de la Ley 34/2002, de servicios de la sociedad de la información, siguiendo al art. 17 *bis* de la Ley del Notariado, introducido por la Ley de Acompañamiento 24/2001, reguladora del «documento público electrónico» o «instrumento público electrónico», esto es, del documento público notarial electrónico. Ahora bien, este vínculo existente entre el art. 3.8 de la LFE y el art. 24 de la LSSI, que resulta indiscutible, lo será sólo para aquellos casos —por lo demás, muy frecuentes en la práctica— en los que el documento electrónico aportado como prueba tenga causa en un contrato electrónico y contenga una firma electrónica.

En todo caso, con la novedad que aporta el citado art. 3.8 de la LFE se llena la omisión del RDL 14/1999 y de la Directiva, pues en ambos simplemente se ordenaba la admisibilidad de la firma electrónica como prueba en juicio, pero sin determinar de qué tipo de medio probatorio se trataba [90]; y, asimismo, se modifica el criterio contrario a la naturaleza documental de tal medio de prueba contenido en la LEC. Así, en el texto originario de esta LEC 1/2000, los documentos electrónicos son medios de prueba, pues, como disponía el art. 299.2, *«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 permitan 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»*; pero no son «documentos»

[90] Por su parte, en esta línea, el art. 10 del Decreto 445/2000 señala que: «*1. Il documento informatico ha l'efficacia probatoria prevista dall'articolo 2.712 del codice civile, riguardo ai fatti ed alle cose rappresentate. 2. Il documento informatico, sottoscritto con firma elettronica, soddifa il requisito legale della forma scritta. Sul plano probatorio il documento stesso è liberamente valutabile, tenuto conto delle sue caratteristiche oggettive di qualità e sicurezza. Esso inoltre soddisfa l'obbligo previsto dagli artt. 2.214 e seguenti del codice civile e da ogni altra analoga disposizione legislativa o regolamentare*» («El documento informático tiene la eficacia probatoria prevista en el art. 2.712 (relativo a las reproducciones mecánicas), en consideración a los hechos y a la cosa representada. 2. El documento informático, suscrito con firma electrónica, satisface el requisito legal de la forma escrita. Sobre el plano probatorio el documento mismo es libremente valorable, teniendo en cuenta sus características objetivas, de calidad y seguridad. Esto, además, satisface la obligación prevista en los arts. 2.214 y siguientes del Código Civil y a toda otra análoga disposición legislativa o reglamentaria».)

ni públicos ni privados al no estar incluidos en los números 2 y 3 del art. 299.1. Por tanto, aunque constituyen medios de prueba procesal, para la LEC se trata de medios distintos de los documentos públicos y privados. Se enumeran y regulan de forma separada y con criterios diferentes respecto de estos últimos, no sólo en lo que se refiere al modo de su producción en juicio (art. 384.1 y 2), sino respecto a su fuerza probatoria, puesto que los documentos públicos y privados tienen eficacia de prueba legal (arts. 319 y 326), mientras que los documentos electrónicos se valorarán por el tribunal *«conforme a las reglas de la sana crítica aplicables a aquéllos según su naturaleza»* (art. 384.3). Y ello, a pesar de la existencia del art. 812, donde se hace referencia a los documentos, cualquiera que sea su forma y clase o soporte físico en que se encuentren, para acudir al proceso monitorio.

Con la LFE al añadir al art. 326 de la LEC un apartado 3, en el que se contiene una remisión expresa al art. 3 de la LFE, en los términos ya vistos, se introduce en la Ley adjetiva un criterio favorable a la consideración de documentos, a los documentos electrónicos.

Por tanto, el soporte en que se hallen los datos electrónicamente será admisible como prueba documental en juicio, rigiéndose por las normas procesales probatorias de los documentos públicos o privados, según se trate, efectivamente, de un documento de una u otra clase.

No obstante, esta regla general, para García Mas opera únicamente «en los casos en que los datos estuviesen firmados con firma electrónica reconocida a efectos del principio ya visto, de equivalencia funcional y del pleno reconocimiento del mismo valor y eficacia a la firma electrónica reconocida y a la manuscrita. Dejando para las otras firmas el principio que estaba en la Ley de Enjuiciamiento Civil, reconduciéndose a las reglas de valoración de la sana crítica»[91].

Aun no estando exenta de razón, lo cierto es que la ley se refiere a los documentos firmados electrónicamente como verdaderos documentos, sin marcar diferencias en atención a la clase de firma, sino a la naturaleza del documento (público o privado), a los efectos de su aportación como prueba documental en juicio.

---

[91] Fco. J. GARCÍA MAS, *Comercio y firma electrónicos, op. cit.,* p. 68.

IV. FIRMA ELECTRÓNICA Y FEDATARIOS PÚBLICOS

En el art. 1 del RDL 14/1999 referido al ámbito de aplicación de la norma, en su párrafo final se contenía una previsión novedosa en torno a la firma electrónica en la actividad de los fedatarios públicos (notarios) con el siguiente contenido: «*Las normas sobre la prestación de servicios de certificación de firma electrónica que recoge este Real Decreto-Ley no sustituyen ni modifican las que regulan las funciones que corresponden realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación.*»

Esta cláusula de salvaguarda de la función notarial y registral respecto de la actividad desarrollada por los prestadores de servicios de certificación en la firma de documentos se mantiene en el proyecto de ley de firma electrónica remitido por el Gobierno a las Cortes Generales, si bien, no ya en el texto articulado, sino en una Disposición Adicional primera con el título «Fe pública y uso de la firma electrónica por Notarios y Registradores de la Propiedad, Mercantiles y de Bienes Muebles», que amplía su contenido al referirse no sólo a la legislación específica reguladora de la incorporación de técnicas electrónica, informáticas y telemáticas al campo de la seguridad jurídica preventiva, sino también a la función de prestadores de servicios de certificación del Consejo General del Notariado y del Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles. No obstante, este contenido varía durante la tramitación parlamentaria del citado Proyecto en el Senado, vía enmienda [92]; afectando dicha variación tanto al título como al contenido. Así, en la redacción definitiva de la LFE se generaliza la cláusula de salvaguarda, no centrándose específicamente en la función notarial y registral, sino alcanzando a todos «los funcionarios que tengan legalmente la facultad de dar fe», de ahí que se opte en el título del encabezamiento por la «Fe pública y el uso de la firma electrónica»;

---

[92] Se presenta la enmienda número 287 por el Grupo Parlamentario Popular en el Senado. *BOCG,* Senado, núm. 158, Serie II, 21 de octubre de 2003, p. 112. Incorporándose al texto del Proyecto en el Dictamen de la Comisión de 21 de noviembre de 2003. La *justificación* normativa se basa, si se quiere que la firma electrónica sea útil y operativa, en la necesidad de reconocer eficacia probatoria a los documentos firmados electrónicamente, públicos y privados, consecuencia de atribuir al soporte material firmado electrónicamente la cualidad de documentos, y todo ello con la finalidad de potenciar la sociedad de la información mediante el rápido establecimiento de un marco jurídico para la utilización de una herramienta que aporta confianza en la realización del comercio electrónico en redes abiertas, como es el caso de Internet.

asimismo, se evita en el contenido del texto, hacer expresamente una remisión a la regulación específica sobre la aplicación de las técnicas informáticas al ámbito notarial representado por la ya mencionada Ley de Acompañamiento 24/2001, como hacer mención, igualmente, de la actuación de los órganos colegiados notariales y registrales como prestadores de servicios de certificación [93].

No obstante, pese a la generalidad en los términos de la actual Disposición Adicional primera, nos vamos a centrar en este apartado a la función notarial y registral, en los términos en que se pronuncia la Ley 24/2001, y su modificación por la también mencionada Ley 24/2005, de 18 de noviembre, de Impulso a la productividad.

En la citada Ley 24/2001, en concreto en la sección 8.ª, de «Incorporación de técnicas electrónicas, informáticas y telemáticas a la seguridad preventiva» (arts. 106-115), se implanta la regulación de la normativa del uso de la firma electrónica de los notarios, y registradores para facilitar el traslado de documentos y la práctica de comunicaciones y notificaciones entre los fedatarios públicos, los Registros Públicos y los Órganos Administrativos y Judiciales, aunque estos últimos ya tengan regulación específica (art. 106).

Para ello, los notarios y registradores tendrán que disponer obligatoriamente de sistemas telemáticos, para la emisión, comunicación y recepción de información, y de una manera inmediata, con independencia de otros sistemas que aparezcan en un futuro en virtud de avances tecnológicos. Deberán disponer de una dirección de correo electrónico, que será asignada por el propio Consejo General del Notariado y el Colegio de Registradores, respectivamente (art. 107 y Disposición Transitoria vigésima). El uso de la firma electrónica tendrá un ámbito específico de actuación, centrado en la remisión de documentos públicos notariales, partes, declaraciones, y autoliquidaciones tributarias, solicitudes o certificaciones por vía electrónica por parte de un notario o registrador de la propiedad dirigidas a otro notario o registrador, a las Administraciones Públicas, o a cualquier órgano jurisdiccional, y siempre por razón de su oficio. Por el mismo medio

---

[93] Disposición Adicional primera. *Fe pública y uso de la firma electrónica.* «*1. Lo dispuesto en esta ley no sustituye ni modifica las normas que regulan las funciones que corresponden a los funcionarios que tengan legalmente la facultad de dar fe en documentos en los que se refiere el ámbito de sus competencias siempre que actúen con los requisitos exigidos en la ley.*

2. En el ámbito de la documentación electrónica, corresponderá a las entidades prestadoras de servicios de certificación acreditar la existencia de los servicios prestados en el ejercicio de su actividad de certificación electrónica, a solicitud del usuario, o de una autoridad judicial o administrativa.»

seguro, podrá remitirse copias electrónicas simples a las entidades y personas interesadas cuando su identidad e interés legítimo le conste al notario; de la misma forma podrán remitirse por los registradores de la propiedad y mercantiles notas simples informativas. La firma electrónica avanzada también podrá ser empleada por notarios y registradores para el envío de documentos e informaciones a los particulares con el valor, efectos y requisitos que se determinen reglamentariamente (art. 110).

Aunque se trate de una normativa especial, en lo referente al uso de la firma electrónica deberá respetar la normativa general representada en la actual LFE, sin perjuicio de las especialidades y peculiaridades derivadas del ejercicio de la función notarial y registral. Así, el art. 108 que lleva por rúbrica «Adecuación a los principios rectores de la firma electrónica», señala que la prestación de servicios de certificación se hará de conformidad, ahora, con la Ley 59/2003, a efectos de expedir certificados electrónicos, mediante los que se vinculen unos datos de verificación de firma, a la identidad, cualidad profesional, situación administrativa de los notarios y registradores de la propiedad, mercantiles y de bienes muebles en activo, así como la plaza de destino asignada. Y atendiendo al régimen especial de la firma electrónica de notarios y registradores, deberá tener la firma electrónica el carácter de avanzada y habrá de cumplir los requisitos que se establecen en al art. 109 de la Ley 24/2001.

Una aplicación fundamental de esta firma electrónica notarial será la posibilidad de presentar por vía telemática, en los Registros de la Propiedad y Mercantiles, los documentos susceptibles de calificación y de inscripción, tanto en el Registro de la Propiedad como en el Mercantil. También podrá testimoniar en soporte papel, bajo su fe, las notificaciones o comunicaciones que por medios electrónicos reciba de otros notarios, de los registradores de la propiedad o mercantiles o de órganos de la Administración estatal, autonómica, judicial, etc., e incluso podrá almacenar dichas notificaciones en soporte informático. Y, asimismo, como una aplicación más, la legitimación notarial de firmas, en documentos privados o la presentación electrónica de éstos en el Registro u oficina pública, debiendo tener lugar bajo la firma electrónica avanzada de un notario en activo tal presentación electrónica.

Por otra parte, la Disposición Adicional vigesimasexta y la Disposición Transitoria vigesimoprimera de la Ley 24/2001 referidos a la actuación de los órganos colegiados como prestadores de servicios de certificación, disponen que en el plazo máximo de seis meses desde la entrada en vigor de esta Ley el Consejo General del Notariado y el Colegio de Registradores de

la Propiedad y Mercantiles de España deberán constituirse en prestadores de servicios de certificación, pudiendo celebrar a estos efectos los oportunos convenios y, de otro lado, que en el plazo máximo de nueve meses, también desde la entrada en vigor de la citada Ley, los notarios y registradores deberán obtener del prestador de servicios de certificación su firma electrónica avanzada. A tal efecto, el 19 de mayo de 2002 se firmó el Convenio de colaboración entre el Consejo General del Notariado y la Fábrica de Moneda y Timbre-Real Casa de la Moneda. Lo que permite la intervención de los notarios y registradores en relación con la utilización de la firma electrónica y certificados, con la consiguiente mayor seguridad y fiabilidad que tales instrumentos van a reportar en los documentos firmados electrónicamente.

Y en la Disposición Transitoria decimonovena se regula la obligación de trasladar el contenido de los asientos de los registros de la propiedad y mercantiles a soporte informático en el plazo de un año desde la entrada en vigor de la Ley.

Finalmente, además de lo indicado anteriormente, en el art. 115 de la citada Ley 24/2001, se modifica la Ley del Notariado de 28 de mayo de 1862, introduciendo un nuevo art. 17 *bis*, en el que se define el documento público notarial electrónico, disponiendo que este documento debe reunir las características esenciales de autorización por el notario, cualquiera que sea su soporte, es decir, tanto en soporte papel como en el electrónico, y que por estar en soporte electrónico, no perderá su carácter de instrumento público. Su contenido se presume, por tanto, veraz e íntegro de acuerdo con lo dispuesto en esta Ley y en otras. No obstante, las copias autorizadas de las matrices que podrán expedirse y remitirse electrónicamente, con firma electrónica avanzada, por el notario autorizante de la matriz o por quien le sustituya legalmente, sólo podrán expedirse para su remisión a otro notario o a un registrador o a cualquier órgano de las Administraciones públicas o jurisdiccional, siempre en el ámbito de su respectiva competencia y por razón de su oficio. Si esas copias autorizadas electrónicas, se trasladan a soporte papel, para que conserven su autenticidad y garantía notarial, es necesario que dicho traslado lo realice el notario al que se le hubiese enviado, el cual signará, firmará y rubricará el documento haciendo constar su carácter y procedencia. Por razones de seguridad y ante el problema de la ruptura del par de claves o de la reproducción sin control de esas copias autorizadas, no podrán remitirse éstas a los particulares, pero sí las copias simples electrónicas siempre que le conste feha-

cientemente al Notario, la identidad e interés legítimo de cualquier interesado que las solicite.

Ahora bien, esta Ley 24/2001, como hemos indicado, ha sido modificada por la Ley 24/2005, en cuya sección 2.ª, «Impulso a la utilización de medios telemáticos por parte de los usuarios de los servicios registrales y notariales», en su artículo vigesimoséptimo de «Impulso a la tramitación telemática» se modifica: 1) El art. 106 de la Ley 24/2001, disponiendo que la presente sección tiene por objeto, por una parte, la atribución y uso de la firma electrónica reconocida por parte de los notarios y registradores. Referencia a este tipo de firma que no se contenía, sin embargo, en la anterior regulación del art. 106, y, por otra, a los sistemas de emisión, transmisión, comunicación y recepción de información entre notarios y registradores, así como el resto de los documentos que de conformidad con lo dispuesto en su legislación específica puedan ser objeto de inscripción. 2) Se modifica el art. 107 en relación a la implantación obligatoria de sistemas telemáticos, se añade respecto a la regulación anterior que el Colegio de Registradores de la Propiedad y Mercantiles de España y el Consejo General del Notariado dispondrán de redes privadas telemáticas que deberán garantizar una interconexión segura por los procedimientos exclusivos cuyos parámetros y características técnicas sean gestionados por las respectivas organizaciones corporativas. 3) Se modifica también el contenido del art. 108 sobre la adecuación a los principios rectores de la firma electrónica, donde se especifica, a diferencia de la regulación anterior —que hacía referencia al RDL 14/1999—, que la prestación de servicios de certificación se hará de conformidad con lo dispuesto en la Ley 59/2003, a los efectos de expedir certificados electrónicos mediante los que se vinculen unos datos de verificación de firma a la identidad, cualidad profesional, situación administrativa de los notarios y registradores de la propiedad, mercantiles y de bienes muebles en activo, así como la plaza de destino asignada. Los notarios y registradores deberán disponer para la adecuada prestación de sus funciones públicas de firma electrónica reconocida. Dicha firma electrónica reconocida deberá obtenerse de un prestador de servicio de certificación que cumpla los requisitos del art. 20 de la LFE. El Colegio de Registradores y el Consejo General del Notariado a través de sus medios correspondientes deberá garantizar a los prestadores de servicios de certificación que lo soliciten, incluidas las respectivas organizaciones corporativas, la condición de registrador o notario en activo al tiempo de la firma de la calificación o comunicación notificada o del instrumento público remitido, la vigencia, revocación y suspensión del certificado elec-

trónico, mediante el mantenimiento de un directorio actualizado de certificados debidamente protegido, así como un servicio de consulta permanente, rápido y seguro. Asimismo, dichas organizaciones corporativas deberán aplicar el mecanismos de sellado del tiempo en cuanto envío y recepción de información se practique, en los términos que reglamentariamente se disponga. Y 4) Se modifica el art. 109, y especifica que el régimen especial de la firma electrónica de notarios y registradores deberá estar amparada por un certificado reconocido emitido por un prestador de servicios de certificación de conformidad con lo dispuesto en la LFE.

Tanto en una y otra normativa, se destaca la intervención de los notarios y registradores en relación con la utilización de la firma electrónica, en concreto, en la modalidad de reconocida, y los certificados emitidos por los mismos, con la importante contribución a la seguridad y fiabilidad que la citada intervención dota a los documentos electrónicos firmados electrónicamente, tanto en las relaciones de ambos cuerpos notariales entre sí, como en su relación entre particulares, y la importante condición de prestadores de servicios de certificación que corresponde tanto al Consejo General del Notariado como al Colegio de Registradores de la Propiedad, Mercantiles y de Bienes Muebles.

V. FIRMANTE

El art. 6 de la LFE bajo el título de «Concepto de certificado electrónico y de firmante», establece en su apartado primero la definición de elemento objetivo del sistema, el propio certificado y, en su apartado segundo, la del elemento subjetivo, representada en la noción de firmante como *«la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en nombre de una persona física o jurídica a la que representa»*. Se trata del titular del par de claves que utiliza las mismas formalmente a efectos de firma, y a quien, en principio, se le atribuye la autoría de los mensajes firmados con aquéllas. Es el solicitante, titular o suscriptor del certificado vinculado a los elementos de firma.

Ahora bien, desde los términos de la definición expuesta, ajustándose cuanto menos al espíritu de la legislación comunitaria[94] —y, a diferencia

[94] Art. 2.3 de la Directiva define firmante como «*la persona que está en posesión de un dispositivo de creación de firma y que actúa en su propio nombre o en el de la entidad o persona física o jurídica a la que representa*».

del art. 2, apartado *c),* del RDL 14/1999, que únicamente consideraba como signatario a la «persona física»— la LFE admite como titular del certificado y firmante, tanto a la persona física como a la persona jurídica.

Respecto a la persona física firmante, no se exigirá otros requisitos en el tráfico electrónico, que los que tendrían lugar en el ámbito de la contratación tradicional. Así, la plena capacidad de obrar en la actuación de aquélla.

Tratándose de persona jurídica, constituye una de las principales novedades de la Ley, tal como se establece en su Exposición de Motivos [95], frente al mundo tradicional en soporte papel, su condición de firmante y la posibilidad de expedir certificados a nombre de aquélla. Novedad que viene, además, consagrada expresamente en el art. 7 de la LFE, rubricado «Certificados de personas jurídicas», y confirmada en otros preceptos de la misma Ley, como el art. 11.2.*e),* dedicado a la identificación del firmante de certificados reconocidos.

1. Firma electrónica de la persona jurídica

Como hemos constatado, constituye una novedad sin precedentes en el Derecho español [96] la regulación contenida en el art. 7, al introducir en nuestro Derecho la figura de los certificados de personas jurídicas, que tienen la particularidad de ser emitidos a favor de las mismas, de tal manera que la firma que certifican no es la del representante de la persona jurídica, sino la de la propia persona jurídica en sí. Ésta como tal tiene una firma digital propia e independiente de las personas que las representan [97].

Por su parte, el art. 2 («Definiciones») de la Ley Modelo para las firmas electrónicas UNCITRAL igualmente señala que «*para los fines de la presente Ley...:* d) *Por "firmante" se entenderá la persona que posee los datos de creación de firma y que actúa en nombre propio o de la persona a la que representa».*

Asimismo, la Ley de Firma Digital de Utah (Título I, sección 103, «Definiciones», sección 21) conceptúa persona: «*Persona física o jurídica capaz de firmar un documento sea legalmente o como cuestión de hecho.*» Y el art. 2.5 de la Ley belga de 2001 «*Titulaire de certificat: une personne physique ou morale à laquelle un prestataire de service de certification a délivré un certificat*» (titular del certificado: persona física o moral a la que un prestador de servicios de certificación entrega un certificado).

[95] Apartado III de la Exposición de Motivos de la LFE.

[96] El RDL 14/1999 únicamente admitía, como excepción a la regla general del art. 2.*c),* y a efectos de cumplimiento de las obligaciones tributarias, la expedición de certificados a favor de personas jurídicas (art. 5.3).

[97] En el art. 11.2.*e)* señala que se incluirán en los certificados reconocidos, al menos, los siguientes datos: «e) *La identificación del firmante... y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.*»

La justificación para tal medida parece residir en la idea de ser conveniente que determinados actos del tráfico sean asumidos directamente por la persona jurídica y no de la persona física representante de la misma, con el objeto de facilitar la contratación de todo tipo de servicios y realización de trámites [98].

Ahora bien, aunque la persona jurídica tenga una firma propia, resulta necesario que la solicitud de tal firma se lleve a cabo por los representantes legítimos de la entidad, persona física, cuya identidad debe constar en el certificado expedido como responsable de la misma; pues, como es lógico, la persona jurídica sólo puede actuar a través de las personas físicas que la representan. Sobre tal base, el apartado 1 del citado art. 7 dispone que *«podrán solicitar certificados electrónicos de personas jurídicas, sus administradores, representantes legales y voluntarios con poder bastante a estos efectos».* Se establece una legitimación restrictiva, una habilitación específica, pues han de ser representantes de la persona jurídica, bien en la modalidad de representantes orgánicos de las sociedades mercantiles (administradores), o en la de representantes legales o voluntarios, siempre con poder suficiente a tales efectos. Estos representantes/solicitantes de certificados de la persona jurídica serán normalmente persona física, aunque nada impide que lo sea también una persona jurídica en condición de administrador de otra, si bien en este caso igualmente habrá de designarse a una persona física *«como representante suyo para el ejercicio de las funciones propias del cargo»* (art. 143 RRM para las Sociedades Anónimas).

Por otra parte, en este mismo apartado, en línea precisamente con lo expuesto, se dispone que *«los certificados electrónicos de personas jurídicas no podrán afectar al régimen de representación orgánico o voluntario regulado por la legislación civil o mercantil aplicable a cada persona jurídica».* En nuestro tráfico jurídico, las personas jurídicas quedan vinculadas por la firma de una persona física con facultades de representación que actúa en nombre de la persona jurídica representada, quedando siempre clara la identidad del firmante y la representación que ostenta, a los efectos de poder analizar si efectivamente tiene poder suficiente para obligar a la persona jurídica.

---

[98] Véanse A. VILCHES TRASSIERRA, «Las personas jurídicas y la firma electrónica en la Ley 59/2003», en *Revista Aranzadi de Derecho y Nuevas Tecnologías,* año 2004-3, núm. 6, p. 56; R. RUBIO VELÁZQUEZ y C. RODRÍGUEZ SAU, «I Parte. Aspectos legales», en *La firma electrónica*, *op. cit.,* p. 89.

Para ambos supuestos, el art. 11.4 de la LFE dispone que «*si los certificados reconocidos admiten una relación de representación, incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente, y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado 2 del artículo 13*». Y, además, se hace recaer sobre tal persona física representante, la responsabilidad del cumplimiento de los deberes de diligencia inherentes a la condición de firmante tanto si él es firmante, como si lo es la persona jurídica. De forma que, si en los certificados de persona jurídica debe constar la identidad del firmante —el documento o la inscripción en la que se basa tal representación—, y como tal representante es responsable del uso del certificado y del cumplimiento de todas las obligaciones inherentes a la condición de firmante, ¿cuál es entonces la diferencia con el certificado del representante *stricto sensu*? Parece que la misma reside, además de en la determinación de la condición de firmante, no del representante, sino de la persona jurídica, en la detallada regulación establecida por el legislador, con la exigencia de que actúe, según dispone, el apartado III de la Exposición de Motivos de la LFE, «*como resortes de seguridad jurídica, con los que se trata de conjugar el dinamismo que debe presidir el uso de los certificados en el tráfico (...), para evitar que puedan nacer obligaciones incontrolables frente a terceros debido a un uso inadecuado de los datos de creación de firma*».

Lo que viene a exigir el establecimiento de una serie de restricciones que afectan, aparte y en los términos vistos a quienes se encuentran legitimados para solicitar un certificado de persona jurídica, al uso y custodia de la firma electrónica, y al ámbito material de eficacia de la misma.

En este contexto, sobre la base que la persona jurídica, en tanto que ficción jurídica inmaterial, no puede manejar directamente los elementos inmateriales que permiten firmar electrónicamente, el legislador atribuye la custodia y el uso de los elementos de firma a una persona física, que como solicitante ha de tener una legitimación especial para actuar; de ahí que el apartado 2 del art. 7 disponga expresamente que «*la custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico*». Ahora bien, y eso es lo chocante —si partimos de la exigencia de seguridad jurídica que se demanda en torno a la firma electrónica, basada en el secreto de la clave privada—, que se permita el uso material de los elementos de firma, también a terceras personas, tal como se infiere expresamente de la Exposición de Motivos de

la Ley e implícitamente del propio texto articulado. Desde tal perspectiva, los sujetos habilitados para suscribir documentos con la firma electrónica de una persona jurídica no serán únicamente los representantes legales legitimados para ello, sino, además, todo un conjunto de personas que conforman el círculo de confianza en torno al solicitante del certificado, pues éste es en última instancia el responsable del mal uso que se haga del certificado. Se rompe con la exigencia claramente expuesta en líneas precedentes, en la que se impone al titular del certificado/firmante el deber de guardar secreto de los datos de creación de firma. Este riesgo que supone el permitir la existencia de múltiples personas con capacidad real para vincular a una persona jurídica mediante una única firma electrónica, que se nos antoja inaceptable y criticable [99], sin embargo, se encuentra en cierta forma limitado, no sólo por el hecho de la responsabilidad en la custodia que asume el solicitante, ante usos indebidos de la firma, con la consiguiente prudencia en la cesión a cualquier tercero del uso de la firma, sino también porque la operatividad de la cesión en el uso de los certificados queda circunscrita a un ámbito material específico.

Precisamente, a este ámbito material se refiere el apartado 3 del citado art. 7 al señalar que «*los datos de creación de firma sólo podrán ser utilizados cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario*». Dicho giro o tráfico ordinario se define en la Exposición de Motivos al indicarse que en éste «*se comprenden las transacciones efectuadas mediata o inmediatamente para la realización del núcleo de la actividad de la entidad y las actividades de gestión o administrativas necesarias para el desarrollo de la misma, como la contratación de suministros tangibles e intangibles o de servicios auxiliares*». Tal giro o tráfico viene a coincidir con el objeto social inscrito de la sociedad. Ahora bien, la elección de esta limitación general al uso de la firma electrónica responde a la experiencia de la actuación común en el comercio tradicional de los factores y mandatarios verbales que vinculan con sus actos a aquellos a los que representan y que no cuentan con unas atribuciones formalizadas en documento público (arts. 281 y ss. del Código de Comercio) [100].

---

[99] De la misma opinión G. GÁLLEGO HIGUERAS, «Comentarios a la reciente Ley 59/2003...», *op. cit.,* p. 36; A. VILCHES TRASSIERRA, «Las personas jurídicas y la firma electrónica en la Ley 59/2003...», *op. cit*., p. 58.

[100] G. GÁLLEGO HIGUERAS, «Comentarios a la reciente Ley 59/2003...», *op. cit*., p. 37.

Junto a este límite general, el art. 7.3 permite, asimismo, a las personas jurídicas «*imponer límites adicionales, por razón de la cuantía o de la materia, para el uso de dichos datos que, en todo caso, deberán figurar en el certificado electrónico*». Por tanto, la actuación del solicitante, como de cualquier otra persona física vinculada a la persona jurídica, se encuentra condicionada por un doble límite, y aunque en cierta forma disminuye el riesgo potencial descrito en torno al uso de la firma de persona jurídica, sin embargo, viene a introducir cierta confusión, pues aquellos actos que excedan del giro o tráfico ordinario tendrán un tratamiento diferente según que el certificado haya sido utilizado por el administrador como representante de la sociedad, valiéndose de un certificado de persona física; que cuando este mismo administrador usa un certificado de persona jurídica: en el primer caso, la actuación del administrador vinculará a la sociedad; no así en el segundo supuesto, salvo que se demuestre que el acto lo fue en beneficio de aquélla. Realmente, la única posibilidad para resolver esta duplicidad de consecuencia es pensar que el legislador cuando se refiere al certificado de persona jurídica lo hace en referencia a aquellos actos del giro o tráfico más ordinario de la actividad de la persona jurídica, de actuación automatizada desde una máquina o servidor [101].

Finalmente, sobre la base de los límites al uso de la firma electrónica de persona jurídica, el apartado 4 del citado art. 7 señala que «*se entenderán hechos por la persona jurídica los actos o contratos en los que su firma se hubiera empleado dentro de los límites previstos en el apartado anterior. Si la firma se utiliza trasgrediendo los límites mencionados, la persona jurídica quedará vinculada frente a terceros sólo si los asume como propios, o se hubiesen celebrado en su interés. En caso contrario, los efectos de dichos actos recaerán sobre la persona física responsable de la custodia de los datos de creación de firma, quien podrá repetir, en su caso, contra quien los hubiera utilizado*». Se impone la responsabilidad de custodia sobre los datos al solicitante, a la par que responde éste ante el tercero por el mal uso del certificado de persona jurídica. El hecho de no asumir en este caso la persona jurídica los actos como propios, o no haberse celebrado los mismos en su interés, y que los efectos gravosos de dichos actos recaigan sobre el solici-

---

[101] A. VILCHES TRASSIERRA, «Las personas jurídicas y la firma electrónica», *op. cit.,* pp. 60-61, quien en esta línea hace referencia «a los denominados por la doctrina "certificados de servidor", es decir, aquellos certificados de firma electrónica instalados en un ordenador al que los usuarios se conectan remotamente y sirve para garantizar la seguridad y autenticidad de la comunicación, así como la de todos los documentos o archivos que salgan al exterior a través del mismo».

tante de un certificado de firma electrónica de persona jurídica, determinará, tal como expusimos, cierta prudencia y control por parte del solicitante a la hora de ceder el uso de los datos de creación de la firma de la persona jurídica. Esta responsabilidad del solicitante por usos indebidos, como las limitaciones indiciadas, contribuyen en cierta forma a aceptar el contenido de la LFE para el supuesto de cesión del uso y revelación de la clave privada a terceros; pero, a la vez, suponen una barrera para el triunfo de estos certificados. En todo caso, la Ley reconoce al solicitante el derecho a repetir contra aquella otra persona vinculada a la persona jurídica que en el uso de la firma hubiera trasgredido los límites mencionados.