

PROGRAMA DE DERECHO E INFORMÁTICA

LECCIÓN OCHO

EL CERTIFICADO DIGITAL Y LA FIRMA ELECTRÓNICA

1. REGULACIÓN ACTUAL

La regulación en España de la firma electrónica se encuentra actualmente en la Ley 59/2003, de 19 de diciembre, de firma electrónica, modificada por última vez el 2 de octubre de 2016.

Pero lejos de lo que pudiera pensarse, nuestro país ya contaba con anterioridad al RD. 14/1999, de firma electrónica, con un entramado de normas legales y disposiciones de rango inferior a la ley que sostenían la validez y eficacia de la firma electrónica para determinados ámbitos.

Así, entre las leyes y normas con fuerza de la ley debe destacarse el artículo 45.5 de la Ley del Régimen Jurídico de la Administración del Estado y Procedimiento Administrativo Común, que ya en su redacción de 1992 establecía que los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de los originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos establecidos por esta y otras leyes.

La Ley del Mercado de Valores de 1988 regula las operaciones de Bolsa que se llevan a cabo mediante el Sistema de Interconexión Bursátil, integrado, como señala la propia Exposición de Motivos de la Ley, mediante una red informática. En esa línea debe encuadrarse el acuerdo de 11 de marzo de 1998 de la CNMV sobre implantación del CIFRA-DOC/CNMV (Sistema de intercambio de información a través de líneas telemáticas) (BOE de 27 de marzo de 1998).

La Ley 37/1992, de 28 de diciembre, sobre el IVA, permite, en su artículo 88-2, que las facturas puedan emitirse por vía telemática; posibilidad que ha sido más detallada en la Orden Ministerial de 22 de marzo de 1996.

También existe un conjunto de órdenes que regulan la declaración de IRPF para grandes empresas, PYMES y contribuyentes, disponibles *online* en <http://aeat.es>. Además, el procedimiento para la obtención e instalación de certificado con firma electrónica para hacer la declaración del IRPF puede obtenerse en <http://aeat.es/certfnmt.html>.

La Orden, de 19 de julio de 1999, por la que se aprueba el Registro de compraventa de bienes muebles a plazo, en su Disposición Adicional 6ª, autoriza a la DGRN para aprobar modelos en soporte informático o con firma electrónica, siempre que se garantice la identidad indubitada de los contratantes y la integridad e inalterabilidad del documento.

En el ámbito judicial también se ha admitido tanto la validez del documento electrónico como la eficacia del documento electrónico firmado electrónicamente.

Respecto de la validez del documento electrónico en el proceso, el artículo 230 LOPJ, dispone que, podrán utilizarse en el proceso cualesquiera medios técnicos de documentación y reproducción, siempre que ofrezcan las debidas garantías de autenticidad.

Y, por último y recién implantado, el RD 1065/2015, de 27 de noviembre que regula las comunicaciones electrónicas en la Administración de Justicia. Sistema LexNet, que, desde el 1 de enero de 2016, ha supuesto la comunicación electrónica de todos los profesionales del derecho, y los Juzgados, en los procedimientos judiciales iniciados a partir de esa fecha, lo que obliga a que todos los intervinientes en el proceso, siempre que sean profesionales, deban signar electrónicamente los documentos que presenten.

2. CONTENIDO Y ESTRUCTURA DE LA LEY DE FIRMA ELECTRÓNICA

Tal y como dispone el artículo 1. La Ley 59/2003 de Firma Electrónica regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación, sin que las disposiciones de la LFE alteren en modo alguno las normas relativas a la celebración, formalización, validez y eficacia de los contratos y cualesquiera otros actos jurídicos ni las relativas a los documentos en que unos y otros consten.

La Ley consta de 36 artículos agrupados en seis títulos, 10 disposiciones adicionales, con disposiciones transitorias, una disposición derogatoria y tres disposiciones finales.

El título I contiene los principios generales que delimitan los ámbitos subjetivo y objetivo de aplicación de la Ley, los efectos de la firma electrónica y el régimen de empleo ante las Administraciones públicas y de acceso a la actividad de prestación de servicios de certificación.

El régimen aplicable a los certificados electrónicos se contiene en el título II, que dedica su primer capítulo a determinar quiénes pueden ser sus titulares y a regular las vicisitudes que afectan a su vigencia. El capítulo II regula los certificados reconocidos y el tercero el documento nacional de identidad electrónico.

El título II regula la actividad de prestación de servicios de certificación estableciendo las obligaciones a que están sujetos los prestadores –distinguiendo con nitidez las que solamente afectan a los que expiden certificados reconocidos-, y el régimen de responsabilidad aplicable.

El título IV establece los requisitos que deben reunir los dispositivos de verificación y creación de firma electrónica y el procedimiento que ha de seguirse para obtener sellos de calidad en la actividad de prestación de servicios de certificación.

Los títulos V y VI dedican su contenido, respectivamente, a fijar los regímenes de supervisión y sanción de los prestadores de servicios de certificación.

Por último, cierran el texto las disposiciones adicionales –que aluden a los regímenes especiales que resultan de aplicación preferente-, las disposiciones transitorias –que incorporan seguridad jurídica a la actividad desplegada al amparo de la normativa anterior-, la disposición derogatoria y las disposiciones finales relativas al fundamento constitucional, la habilitación para el desarrollo reglamentario y la entrada en vigor.

3. CONCEPTO JURÍDICO DE FIRMA ELECTRÓNICA EN LA LFE

El concepto jurídico de firma electrónica del Derecho español y comunitario es el de “conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante”, artículo 3, aunque la firma electrónica puede cumplir otras utilidades aparte, o al margen, de la identificación del sujeto firmante, especialmente en lo que refiere a garantizar la confidencialidad de las comunidades y la inalterabilidad de los documentos enviados a través de la red y firmados electrónicamente.

Así, por ejemplo, la firma del propio sujeto escaneada e incorporada a un documento electrónico es una firma electrónica e incluso la propia identificación del titular del documento al final del texto, y como tales han de ser tenida, si bien dicha firma, como ya he dicho con anterioridad, ofrece pocas garantías sobre la integridad e identidad del mensaje y, en definitiva contienen un elevado índice de inseguridad.

La firma electrónica más segura, desde un punto de vista técnico, es actualmente la llamada firma digital o de clave asimétrica. Es más, en muchas ocasiones se confunden las expresiones de firma digital y de firma electrónica, pero queda claro que la firma digital es una clase de firma electrónica, si bien no la única.

La firma digital consiste es una combinación de signos que forman una cadena lo suficientemente larga como para garantizar que sea imposible la existencia de una cadena igual y identificar así, de un modo fiable, a una persona con la autoría de un documento y la adhesión de ésta a su contenido.

A ello se añade dos elementos más: una clave privada y una clave pública, cuya finalidad es encriptar el documento electrónico al que se añade la firma como el documento en que se contiene la firma y que va unido al documento gracias a una función del correo electrónico.

Además, la firma electrónica suele estar en un documento electrónico expedido por una autoridad de certificación (que añade a dicho certificado su firma y otros datos que la ley especifica dependiendo del tipo de certificado), cuya finalidad primordial es certificar, bajo su responsabilidad, que determinada firma pertenece a una persona en concreto, pero que también disponen de la tecnología para crear y atribuir firma.

Pues bien, el artículo 3 LFE distingue entre “firma electrónica avanzada” y “firma electrónica reconocida”.

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.

Pero si la firma electrónica avanzada está basada en un certificado reconocido y es generada mediante un dispositivo seguro de creación de firma tendrá la consideración de “firma electrónica reconocida”, la cual tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel (artículo 3 LFE).

En definitiva, existe muchos tipos de firma y muchos modelos de utilizarla, todo ello con su debida y necesaria trascendencia jurídica, pero en el tipo de firma en el que está pensando la legislación es en la firma digital certificada a través de una entidad de certificación, de tal forma que ésta expide un documento (certificado) en el que consigna su propia firma digital, la cual puede confirmarse a través de otra entidad certificadora, y la firma digital del sujeto signatario junto con las claves pública y privada y el resto de requisitos que exija la legislación según el tipo de certificado. Dicho certificado, junto con la clave privada, quedan en manos del signatario, aconsejándose por razones de seguridad no guardar nunca el certificado en el disco duro del ordenador.

Quiero decir con ello, como luego se verá con más detenimiento, que si bien el concepto de firma electrónica, desde el punto de vista de jurídico es muy amplio, y en él tiene cabida desde la firma escaneada hasta la firma digital o de clave asimétrica y cualquier tipo de firma electrónica que se invente en el futuro, las distintas firmas electrónicas contenidas o no en distintas clases de certificados no pueden tener el mismo valor probatorio.

Eso sí, toda firma electrónica por simple que sea, y aún no certificada, debe tener eficacia jurídica, si bien los trámites conducentes a comprobar su veracidad serán más gravosos que los de “*la firma electrónica reconocida*”.

4. EFECTOS JURÍDICOS DE LA FIRMA ELECTRÓNICA

El artículo 3 LFE, tan extenso como asistemático, se asienta en dos preceptos clave. De un lado el punto noveno del artículo 3 LFE, que señala que no se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica. De otro lado, el apartado 4º de dicho precepto, según el cual, 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.

Además de la doble eficacia, la Ley parte de la existencia de un vínculo o nexo entre la firma electrónica y el documento electrónico con los datos en él contenido, pues el precepto dice literalmente que la “firma (electrónica reconocida), tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita”. Por tanto, los efectos de la firma lo son respecto de los contenidos del documento electrónico al que está unida la firma.

Pero qué valor o eficacia tiene el documento electrónico firmado.

El artículo 3 LFE, como hemos visto, distingue entre documentos electrónicos firmados con firma reconocida y el resto de documentos que contiene otro tipo de firma electrónica o digital.

Al documento firmado con firma reconocida la Ley le otorga la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica.

Mientras que al documento firmado electrónicamente, pero con una firma que no sea avanzada y basada en un certificado reconocido, no se le negarán efectos jurídicos ni será excluido como prueba en juicio, por el mero hecho de presentarse en forma electrónica (artículo 3-2), sin que la norma especifique cuál sea su eficacia.

Ello se debe a que la existencia de múltiples clases de firmas electrónicas con distintos niveles o grados de seguridad no permiten adoptar una solución uniforme y única, sino que se deberá estar a cada caso en concreto, y la eficacia dependerá de la mayor o menor seguridad o fiabilidad de la firma respecto de la identidad de las personas e integridad y no repudio de los datos contenidos en el documento.

Así, cualquier documento, por el solo hecho de estar firmado electrónicamente, no tiene por qué negársele eficacia o inadmitirse como prueba en juicio, pero deberán probarse los extremos relativos a la identidad, integridad, autenticación y no repudio.

Sólo el documento firmado electrónicamente mediante firma electrónica reconocida cumple los requisitos de identidad, integridad, autenticación y no repudio, y por ello la eficacia de sus datos y su admisión como prueba en juicio se produce sin necesidad de adversar los extremos controvertidos de la integridad del documento, salvo que se plantee una controversia sobre los mismos y se consiga probar la falta de identidad o integridad del documento.

La diferencia, por tanto, entre el documento electrónico firmado con firma electrónica reconocida, respecto de los documentos firmados con otro tipo de firmas menos seguras, es que los extremos de autoría, integridad, confidencialidad y no repudio se presumen existentes, salvo prueba en contrario, y siempre con una responsabilidad de estos extremos por parte del titular de la firma o de la entidad certificadora (artículo 14 LFE), no siendo necesaria su prueba, que se presumen, lo que determina la carga de probar que la autoría e integridad del documento aparente no se corresponde con la realidad fáctica a quien invoque tales circunstancias.

5. RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Cuando ha intervenido una entidad de certificación bien expidiendo firma, bien certificando titulares y claves de firma, la eficacia de la firma electrónica se ve reforzada mediante un sistema especial de responsabilidad, y que tiene un tratamiento peculiar y distinto del resto de prestadores de servicios de la información e intermediarios, cuya responsabilidad se regula en la Directiva 31/2000/CE de comercio electrónico.

Así, el artículo 22 LFE, dispone que, los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que les impone esta Ley. La responsabilidad del prestador de servicios de certificación regulada en esta Ley será exigible conforme a las normas generales sobre la culpa contractual (art. 1101 y ss. CC) o extracontractual (arts. 1902 y concordantes del CC), según proceda, si bien, tanto en el ámbito de la responsabilidad contractual como el de la responsabilidad extracontractual, corresponderá al prestador de servicios de certificación demostrar que actuó con la diligencia profesional que le es exigible.

La responsabilidad, en principio, se configura como contractual en el caso de incumplimiento de las obligaciones legales o contractuales establecidas entre la Autoridad de Certificación y el titular de la firma y siempre que tenga su base en la contraversión de aquello a lo que las partes se habían obligado, mientras que la responsabilidad de la entidad de certificación frente a terceros será en principio extracontractual; si bien en la práctica resulta en ocasiones difícil discernir el carácter contractual o extracontractual de la responsabilidad, que se en todo caso atenuado por la doctrina de la “unidad de culpas”.

Por supuesto, aunque es obvio, el sistema de protección y de seguridad del tráfico económico a través de redes mediante documentos con firma electrónica basado en certificados expedidos por entidades de certificación se refuerza con la protección penal y con la responsabilidad civil derivada del delito en los casos de falsificaciones y estafas cometidas mediante la manipulación de firmas electrónicas.

Se observa claramente que la responsabilidad civil de las entidades se asienta primordialmente sobre la idea de responsabilidad subjetiva, esto es basada en la culpa o negligencia, si bien hay una inversión legal de la carga de la prueba, no siendo necesario que el usuario pruebe la negligencia de la entidad de certificación, ya que ésta se presume *iuris tantum*. Es, por tanto, al prestador de servicios a quien corresponde demostrar que actuó con la debida diligencia para conseguir su exoneración.

Además, los prestadores de servicios de certificación asumirán toda la responsabilidad frente a tercero por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.

Junto a ese régimen general, el artículo 22 prevé dos supuestos específicos en los que responderá la entidad de certificación. El primero deriva del incumplimiento las obligaciones señaladas en los párrafos b) al d) del artículo 12 de la Ley cuando garantice un certificado electrónico expedido por un prestador de servicios de certificación establecido en un Estado no perteneciente al Espacio Económico Europeo, siendo responsable por los daños y perjuicios causados por el uso de dicho certificado. El segundo deriva de los daños que se causen al firmante o a tercero de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico.

El artículo 22 termina señalando, en su apartado quinto, que la regulación contenida en esta Ley sobre la Responsabilidad del Prestador de Servicios de Certificación se entiende sin perjuicio de lo establecido en la legislación sobre cláusulas abusivas en contratos celebrados

con consumidores. Este es un precepto que está en plena sintonía con lo dispuesto en la Directiva sobre firma electrónica, por lo que dejaría sin efecto las cláusulas exoneratorias de responsabilidad para la entidad de certificación que contravengan el régimen de responsabilidad previsto en la LFE.

Es, en, el artículo 23, donde se regulan las limitaciones de responsabilidad de los prestadores de servicios de certificación.

Así, el prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, si el firmante incurre en alguno de los siguientes supuestos:

- a) No haber proporcionado al prestador de servicios de certificación información veraz, completa y exacta sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación.
- b) La falta de comunicación sin demora al prestador de servicios de certificación de cualquier modificación de las circunstancias reflejadas en el certificado electrónico.
- c) Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
- d) No solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma.
- e) Utilizar los datos de creación de firma cuando haya expirado el período de validez del certificado electrónico o el prestador de servicio de certificación le notifique la extinción o suspensión de su vigencia.
- f) Superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por el prestador de servicios de certificación.

Si el firmante fuese una persona jurídica, el solicitante del certificado electrónico asumirá todas estas obligaciones.

Además, en el caso de los certificados electrónicos que recojan un poder de representación del firmante, tanto éste como la persona o entidad representa, cuando ésta tenga conocimiento de la existencia del certificado, están obligados a solicitar la revocación o suspensión de la vigencia del certificado en los términos previstos en esta Ley.

De otra parte, en el apartado cuarto del artículo 23 se dispone que el prestador de servicios de certificación tampoco será responsable por los daños y perjuicios ocasionados al firmante o a terceros de buena fe si el destinatario de los documentos firmados electrónicamente actúa de

forma negligente. Se entenderá, en particular, que el destinatario actúa de forma negligente en los siguientes casos:

- a) Cuando no compruebe y tenga en cuenta las restricciones que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.
- b) Cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado publicada en el servicio de consulta sobre la vigencia de los certificados o cuando no verifique la firma electrónica.

Asimismo, el prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe por la inexactitud de los datos que consten en el certificado electrónico, si éstos le han sido acreditados mediante documento público. En caso de que dichos datos deban figurar inscritos en un registro público, el prestador de servicios de certificación deberá comprobarlos en el citado registro en el momento inmediato anterior a la expedición del certificado, pudiendo emplear, en su caso, medios telemáticos.

Finalmente, la exención de responsabilidad frente a terceros obliga al prestador de servicios de certificación a probar que actuó en todo caso con la debida diligencia”.

Otra fuente de responsabilidad, tanto civil como administrativa, es la derivada del artículo 17 LFE, que sujeta el tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad a lo dispuesto a lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y disposiciones dictadas en su desarrollo (especialmente en árido terreno de la cesión inconsentida de datos personales).

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

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

Por último, los prestadores de servicios de certificación que hayan consignado un seudónimo en el certificado, a solicitud del signatario, están especialmente obligados a constatar su verdadera identidad y conservar la documentación que la acredite. Dichos prestadores de servicios estarán obligados a revelar la identidad de los titulares de certificados cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previsto en la legislación de protección de datos y sin perjuicio de lo que, en la legislación específica en materia tributaria, de defensa de la competencia y de seguridad pública, se disponga sobre la identificación de las personas.

6. LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN

Los sujetos que hacen posible el empleo de la firma electrónica son los denominados prestadores de servicios de certificación. Para ello expiden certificados electrónicos, que son documentos electrónicos que relacionan las herramientas de firma electrónica en poder de cada usuario con su identidad personal, dándole así a conocer en el ámbito telemático como firmante.

Así, según el artículo 2 LFE, dicha Ley se aplicará a los prestadores de servicios de certificación establecidos en España y a los servicios de certificación que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

Se denomina prestador de servicios de certificación la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

Se entenderá que un prestador de servicios de certificación está establecido en España cuando su residencia o domicilio social se halle en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.

Se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en él, de forma continuada o habitual, de instalaciones o lugares de trabajo en los que realice toda o parte de su actividad.

Se presumirá que un prestador de servicios de certificación está establecido en España cuando dicho prestador o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.

Pero la mera utilización de medios tecnológicos situados en España para la prestación o el acceso al servicio no implicará, por sí sola, el establecimiento del prestador en España.

Pues bien, el artículo 5 LFE dispone que la prestación de servicios de certificación no está sujeta a autorización previa y se realizará en régimen de libre competencia. No podrán establecerse restricciones para los servicios de certificación que procedan de otro Estado miembro del Espacio Económico Europeo. Los órganos de defensa de la competencia velarán por el mantenimiento de condiciones de competencia efectiva en la prestación de servicios de certificación al público mediante el ejercicio de las funciones que tengan legalmente atribuidas.

De otra parte, la prestación al público de servicios de certificación por las Administraciones públicas, sus organismos públicos o las entidades dependientes o vinculadas a las mismas se realizarán con arreglo a los principios de objetividad, transparencia y no discriminación.

Además, la Ley obliga a los prestadores de servicios de certificación a efectuar una tutela y gestión permanente de los certificados electrónicos que expiden. Los detalles de esta gestión deben recogerse en la llamada declaración de prácticas de certificación, donde se especifican las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados electrónicos. Además, estos prestadores están obligados a mantener accesible un servicio de consulta sobre el estado de vigencia de los certificados en el que debe indicarse de manera actualizada si éstos están vigentes o si su vigencia ha sido suspendida o extinguida.

Por otra parte, la Ley contiene las garantías que deben ser cumplidas por los dispositivos de creación de firma para que puedan ser considerados como dispositivos seguros y conformar así una firma electrónica reconocida.

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.

Adicionalmente, la Ley establece un marco de obligaciones aplicables a los prestadores de servicios de certificación, en función de si éstos emiten certificados reconocidos o no, y determina su régimen de responsabilidad, teniendo en cuenta los deberes de diligencia que incumben a los firmantes y a los terceros destinatarios de documentos firmados electrónicamente.

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. Así, se favorece la autorregulación de la industria, de manera que sea ésta quien diseñe y gestione, de acuerdo con sus propias necesidades, sistemas voluntarios de acreditación destinados a mejorar los niveles técnicos y de calidad en la prestación de servicios de certificación. El nuevo régimen nace desde el convencimiento de que los sellos de calidad son un instrumento eficaz para convencer a los usuarios de las ventajas de los productos y servicios de certificación electrónica, resultando imprescindible facilitar y agilizar la obtención de estos símbolos externos para quienes los ofrecen al público. Si bien se recogen fielmente en la Ley los conceptos de “acreditación” de prestadores de servicios de certificación y de “conformidad” de los dispositivos seguros de creación de firma electrónica contenidos en la Directiva, la terminología se ha adaptado a la más comúnmente empleada y conocida recogida en la Ley 21/1992, de 16 de julio, de Industria.

Dado que la prestación de servicios de certificación no está sujeta a autorización previa, resulta importante destacar que la Ley refuerza las capacidades de inspección y control del Ministerio de Ciencia y Tecnología, señalando que este departamento podrá ser asistido de entidades independientes y técnicamente cualificadas para efectuar las labores de supervisión y control sobre los prestadores de servicios de certificación.

Finalmente, conviene tener presente lo dispuesto en el artículo 20, donde se señala las obligaciones de los prestadores de servicios de certificación que expida certificados reconocidos, pues además de las obligaciones generales previstas en la Ley, los prestadores de servicios de certificación que expidan certificados reconocidos deberán cumplir las siguientes obligaciones:

- a) Demostrar la fiabilidad necesaria para prestar servicios de certificación.
- b) Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.
- c) Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica.
- d) Utilizar sistemas y producto 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 sirven de soporte.
- e) Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante.
- f) Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.
- g) Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

Además, los prestadores de servicios de certificación que expidan certificados reconocidos deberán constituir un seguro de responsabilidad civil por importe de al menos 3.000.000 de euros para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan (rebajándose así los 6.000.000 euros que se exigían en el RDLFE de 1999). Dicha garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea al menos de 3.000.000 de euros.

7. RÉGIMEN JURÍDICO DE LOS CERTIFICADOS

Según el artículo 6 LFE, 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.

Además, según el artículo 11 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.

Los certificados reconocidos incluirán, al menos, los siguientes datos:

- a) La indicación de que se expiden como tales.
- b) El código identificativo único del certificado.
- c) La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
- d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
- e) La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.
- f) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.
- g) El comienzo y el fin del período de validez del certificado.
- h) Los límites de uso del certificado, si se establecen.
- i) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite y 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. Pues bien, según el artículo 12ª, antes de la expedición de un certificado reconocido, los prestadores de servicios de certificación deberán cumplir las siguientes obligaciones:

- a) Comprobar la identidad y circunstancias personales de los solicitantes e certificados con arreglo a lo dispuesto en el artículo siguiente.
- b) Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido.
- c) Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.
- d) Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación.

Respecto de la comprobación de la identidad y otras circunstancias personales de los solicitantes de un certificado reconocido, el artículo 13 LFE dispone que la identificación de la persona física que solicite un certificado reconocido exigirá su personación ante los encargados de verificarla y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en derecho. Podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado reconocido ha sido legitimada en presencia notarial.

El régimen de personación en la solicitud de certificados que se expidan previa identificación del solicitante ante las Administraciones públicas se regirá por lo establecido en la normativa administrativa.

En el caso de certificados reconocidos de personas jurídicas, los prestadores de servicios de certificación comprobarán, además, los datos relativos a la constitución y personalidad jurídica y a la extensión y vigencia de las facultades de representación del solicitante, bien mediante consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, bien mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente, cuando aquéllos no sean de inscripción obligatoria.

Cuando el certificado reconocido contenga otras circunstancias personales o atributos del solicitante, como su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, éstas deberán comprobarse mediante los documentos oficiales que las acrediten, de conformidad con su normativa específica.

Los prestadores de servicios de certificación podrán realizar las actuaciones de comprobación previstas en este artículo por sí o por medio de otras personas físicas o jurídicas, públicas o privadas, siendo responsable, en todo caso, el prestador de servicios de certificación.

De todos modos, cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya al prestador de servicios de certificación en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados en este artículo y el período de tiempo transcurrido desde la identificación es menor de cinco años, o cuando para solicitar un certificado se utilice como vigente para cuya expedición se hubiera identificado al firmante en la forma prescrita en este artículo y le conste al prestador de servicios de certificación que el período de tiempo transcurrido desde la identificación es menor de cinco años. Se podrá omitir los trámites de comprobación de identidad.

Por otra parte, todo certificado tiene una vigencia limitada que se justifica por motivos técnicos, ya que un certificado no puede estar vigente más allá del tiempo en que un tercero puede descifrar la clave privada y hacer uso de la firma electrónica ajena. En ese sentido, el artículo 8 LFE, apartado segundo, dispone que 1 período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma y que en el caso de los certificados reconocidos este período no podrá ser superior a cuatro años

Además, según el artículo 8, apartado primero, son causas de extinción de la vigencia de un certificado electrónico:

- a) Expiración del período de validez que figura en el certificado.
- b) Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.
- c) Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.
- d) Resolución judicial o administrativa que lo ordene.
- e) Fallecimiento o extinción de la personalidad jurídica del firmante; fallecimiento, o extinción de la personalidad jurídica del representado; incapacidad sobrevenida, total o parcial, del firmante o de su representado; terminación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.
- f) Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.
- g) Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.
- h) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

La extinción de la vigencia de un certificado electrónico surtirá efectos frente a terceros, en los supuestos de expiración de su período de validez, desde que se produzca esta circunstancia y, en los demás casos, desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

De igual modo, el artículo 9 dispone que los prestadores de servicios de certificación suspenderán, la vigencia de los certificados electrónicos expedidos si concurre alguna de las siguientes causas:

- a) Solicitud del firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.
- b) Resolución judicial o administrativa que lo ordene.
- c) La existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados contempladas en los párrafos c) y g) del artículo 8.1.
- d) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

La suspensión de la vigencia de un certificado electrónico surtirá efectos desde que se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

En caso de extinción o suspensión de la vigencia de certificados electrónicos, el prestador de servicios de certificación hará constar inmediatamente de manera clara e indubitada, la extinción o suspensión de la vigencia de los certificados electrónicos en el servicio de consulta sobre la vigencia de los certificados en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes de la extinción o suspensión de su vigencia. Además, el prestador de servicios de certificación informará al firmante acerca de esta circunstancia de manera previa o simultánea a la extinción o suspensión de la vigencia del certificado electrónico, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto. En los casos de suspensión, indicará, además, su duración máxima, extinguiéndose la vigencia del certificado si transcurrido dicho plazo no se hubiera levantado la suspensión.

Eso sí, la extinción o suspensión de la vigencia de un certificado electrónico no tendrá efectos retroactivos y se mantendrá accesible en el servicio de consulta sobre la vigencia de los certificados al menos hasta la fecha en que hubiera finalizado su período inicial de validez.

Finalmente, el artículo 14 prevé la equivalencia internacional de certificados reconocidos, en el sentido de que los certificados electrónicos que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro del Espacio Económico Europeo expidan al público como certificados reconocidos de acuerdo con la legislación aplicable en dicho Estado se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumpla alguna de las siguientes condiciones:

- a) Que el prestador de servicios de certificación reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos y haya sido certificado conforme a un sistema voluntario de certificación establecido en un Estado miembro del Espacio Económico Europeo.
- b) Que el certificado esté garantizado por un prestador de servicio de certificación establecido en el Espacio Económico Europeo que cumpla los requisitos

establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos.

- c) Que el certificado o el prestador de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

8. EL DNI ELECTRÓNICO

También ha de destacarse la regulación que la Ley contiene respecto del documento nacional de identidad electrónico, que se erige en un certificado electrónico reconocido llamado a generalizar el uso de instrumentos seguros de comunicación electrónica capaces de conferir la misma integridad y autenticidad que la que actualmente rodea las comunicaciones a través de medios físicos.

Así, el artículo 15 dispone que el documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.

Además, la Ley impone a todas las personas físicas o jurídicas, públicas o privadas, la obligación o el deber de reconocer la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

En cuanto a los requisitos y características del documento nacional de identidad electrónico, el artículo 16 LFE se limita a señalar que los órganos competentes del Ministerio del Interior para la expedición del documento nacional de identidad electrónico cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios de certificación que expidan certificados reconocidos con excepción de la relativa a la constitución de la garantía de los 3.000.000 de Euros a la que se refiere el apartado 2 del artículo 20, así como que la Administración General del Estado empleará, en la medida de lo posible, sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el documento nacional de identidad electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados.

Como puede observarse, la Ley se limita a fijar el marco normativo básico del nuevo DNI electrónico poniendo de manifiesto sus dos notas más características –acredita la identidad de su titular en cualquier procedimiento administrativo y permite la firma electrónica de documentos- remitiéndose a la normativa específica en cuanto a las particularidades de su régimen jurídico.

9. LA FIRMA ELECTRÓNICA DE LAS PERSONAS JURÍDICAS

Concluiré esta revisión de los aspectos más destacados de la Ley 59/2013 con un tema que merece un tratamiento singular, como es el establecimiento en la Ley del régimen aplicable a la actuación de personas jurídicas como firmantes, a efectos de integrar a estas entidades en el tráfico telemático (artículo 7 LFE). Se va así más allá del Real Decreto-Ley de 1999, que sólo permitía a las personas jurídicas ser titulares de certificados electrónicos en el ámbito de la gestión de los tributos. Precisamente, la enorme expansión que han tenido estos certificados en dicho ámbito en los últimos años, sin que ellos hayan representado aumento alguno de la litigiosidad ni de inseguridad jurídica en las transacciones, aconsejan la generalización de la titularidad de certificados por personas morales.

En todo caso, los certificados electrónicos de personas jurídicas no alteran la legislación civil y mercantil en cuanto a la figura del representante orgánico o voluntario y no sustituyen a los certificados electrónicos que se expidan a personas físicas en los que se reflejen dichas relaciones de representación.

Como resortes de seguridad jurídica, la Ley exige, por un lado, una especial legitimación para que las personas jurídicas soliciten la expedición de certificados; por otro lado, obliga a los solicitantes a responsabilizarse de la custodia de los datos de creación de firma electrónica asociados a dichos certificados, todo ello sin perjuicio de que puedan ser utilizados por otras personas físicas vinculadas a la entidad. Por último, de cara a terceros, limita el uso de estos certificados a los actos que integren la relación entre la persona jurídica y las Administraciones públicas y a las cosas o servicios que constituyen el giro o tráfico ordinario de la entidad, sin perjuicio de los posibles límites cuantitativos o cualitativos que puedan añadirse. Se trata de conjugar el dinamismo que debe presidir el uso de estos certificados en el tráfico con las necesarias dosis de prudencia y seguridad para evitar que puedan nacer obligaciones incontrolables frente a terceros debido a un uso inadecuado de los datos de creación de firma. El equilibrio entre uno y otro principio se ha establecido sobre las cosas y servicios que constituyen el giro o tráfico ordinario de la empresa de modo paralelo a cómo nuestro más que centenario Código de Comercio regula la vinculación frente a terceros de los actos de comercio realizados por el factor del establecimiento.

Adicionalmente, se añade un régimen especial para la expedición de certificados electrónicos a entidades sin personalidad jurídica a las que se refiere el artículo 33 de la Ley General Tributaria, a los solos efectos de su utilización en el ámbito tributario, en los términos que establezca el Ministerio de Hacienda.

Sin embargo, el régimen jurídico de firma electrónica de las personas jurídicas responsabilidad del uso indebido de la firma electrónica a la persona física que la solicitó y a quien se le concedió y, además, si dicha persona física deja de formar parte de la persona jurídica obliga a tomar las medidas de pertinentes, que avocarán, por criterios de seguridad, a la extinción del certificado.

Quizá, con la firma electrónica de las personas jurídicas, se ha querido llevar al mundo comercial una realidad que ha funcionado con eficacia en las relaciones entre las personas jurídicas y la Administración (por ejemplo, como ocurre con el pago del impuesto de sociedades), pero el problema estriba, en mi opinión, en el carácter más dinámico que tiene la

representación de las personas jurídicas en el tráfico y la posibilidad de revocación o cese de tal representación, y, en ese sentido, creo que no se justifica la existencia de este certificado de firma electrónica a favor de personas jurídicas y que se debía de haber optado por el mismo sistema de actuación que se emplea fuera de línea, en el que los representantes (personas físicas) de la persona jurídica puedan actuar en su nombre, máxime si se tiene en cuenta que el desarrollo tecnológico experimentado en los Registros Españoles permite solucionar la cuestión de la representación de las personas jurídicas de forma sencilla, segura y eficaz, ya que con una conexión telemática en línea (es decir, en tiempo real) con el Registro Mercantil permite comprobar con total fiabilidad la realidad y vigencia de la representación. Será la práctica, en definitiva, la que ponga de manifiesto el acierto y la utilidad de la firma electrónica de las personas jurídicas.