

Publicado en El Derecho, 8 de Octubre de 2002

UNA NUEVA CATEGORÍA DE INSTRUMENTO JURÍDICO: EL DOCUMENTO DIGITAL FIRMADO DIGITALMENTE- PARTE II

LA FIRMA DIGITAL

Por: Héctor Mario Chayer, Agustín Guido
Goldfeld y Damián Esteban Ventura¹

II La Firma Digital	2
II.1 La firma en los actos jurídicos.....	2
II.2 La firma en los documentos digitales.....	3
II.3 Algunos conceptos fundamentales	5
II.3.1 Clave privada, digesto seguro y clave pública	5
II.3.2 Las terceras partes confiables.....	7
II.3.3 El certificado digital	8
II.4 La firma digital en la Ley 25.506.	10
II.4.1 Presunción de autoría e integridad	13
II.4.2 Otras disposiciones.....	15

¹ Héctor Chayer es profesor de Filosofía y Ciencias de la Educación y abogado, con un Posgrado de especialización en Gestión de Sistemas y Tecnologías de la Información en la Empresa (Univ. Politécnica de Madrid – Cepade). Se desempeña como Profesor de Tecnología aplicada a la Justicia, y Administración y Gestión Judicial (UBA), y Director Académico de Fores – Foro de Estudios sobre la Administración de Justicia.

Agustín Goldfeld es abogado, Ayudante de Elementos de Derecho Civil (UBA) y Profesor de Derecho Civil I y Sucesiones (UNLZ), investigador de Fores, y se desempeña como Secretario Privado en el Juzgado Nacional de Primera Instancia en los Civil No 30.

Damián Ventura es abogado, Ayudante de Elementos de Derecho Civil (UBA) y Profesor de Derecho Civil I y Sucesiones (UNLZ), investigador de Fores, y se desempeña como Oficial en el Juzgado Nacional de Primera Instancia en los Civil No 30.

II La Firma Digital

II.1 La firma en los actos jurídicos

Una vez establecido el status jurídico de los documentos digitales, debe abordarse la segunda valla que parece obstaculizar la difusión de su uso en el tráfico jurídico. Se trata del requisito de la firma, regulado en principio en el Código Civil.

El artículo 1012 del Código Civil, luego de establecer que la firma es una condición esencial para la existencia de los instrumentos privados, señala que “...ella no puede ser reemplazada por signos ni por las iniciales de los nombres o apellidos”.

En materia testamentaria, el codificador dispuso en el artículo 3633 que “...cuando la ley exige la firma del mismo testador, debe ésta escribirse con todas las letras alfabéticas que componen su nombre y apellido. El testamento no se tendrá por firmado cuando sólo se ha suscrito el apellido, o con letras iniciales, nombres y apellidos, ni cuando en lugar de suscribir el apellido propio se ha puesto el de otra familia a la cual no pertenece el testador. Sin embargo, una firma irregular o incompleta se considerará suficiente cuando la persona estuviese acostumbrada a firmar de esa manera los actos públicos y privados”.

Luego, en la nota al artículo 3639 –refiriéndose al testamento ológrafo -, Vélez Sársfield destacó que “...la firma no es la simple escritura que una persona hace de su nombre o apellido: es el nombre escrito de una manera particular, según el modo habitual seguido por la persona en diversos actos sometidos a esta formalidad. Regularmente la firma lleva el apellido de la familia; pero esto no es de rigor si el hábito constante de la persona no era firmar de esta manera...”.

Según Julio César Rivera, “...la firma está constituida por trazos que constituyen el modo habitual que tiene una persona de escribir su nombre con la finalidad de manifestar la adhesión de su voluntad al texto a cuyo pie la pone...”². Sin embargo, no puede dejarse de lado que el desarrollo de las relaciones jurídicas, desde su inicio hasta su conclusión, debe regirse en todo momento por el principio de buena fe (artículo 1198 del Código Civil); ello ha de importar que aunque el trazo efectuado por alguno de los firmantes no sea el habitual, no pueda – por ese único motivo - desconocerlo, pues lo importante es que refleje la voluntad del sujeto.

² Rivera, Julio César, op. cit., pág. 718/719.

Así lo ha sostenido Alberto G. Spota, para quien “...el requisito de habitualidad no cabe ser exigido cuando con él se pretenda lesionar la buena fe-creencia de la otra parte...”³. Este autor, además, fue un impulsor del criterio amplio –o lato- en materia de firma, incluyendo en ésta a la impresión digital: al respecto, sostuvo que ésta “... al pie de un documento escrito implica declaración de voluntad conforme con el contenido de tal escrito. Hay «firma» y hay conformidad, del mismo modo que cuando se «firma» en blanco, o cuando «firma» el ciego...”⁴.

Es decir que la firma, puesta al pie de un instrumento, cumple dos funciones principales: la primera, identificar al autor de la misma (imputación de autoría) y la segunda, dar cuenta de su conformidad con el contenido del acto (demostración de voluntad); pero, asimismo, permite vincular al documento con el signatario, adquiriendo así una función probatoria.

Es claro que la tradicional firma ológrafa no es útil a los fines de signar un documento digital, por no existir un soporte papel donde asentar el nombre escrito de una manera particular. Este es el vacío que debe ser llenado por sistemas técnicos que cumplan una función similar en los documentos digitales.

II.2 La firma en los documentos digitales

Como ya se ha visto, la firma es un requisito esencial tanto de los instrumentos privados como de los instrumentos públicos, y constituye el principal escollo para el avance de éstos en el ámbito de la celebración de los negocios jurídicos. La firma digital es un proceso técnico que proporciona la posibilidad de resolver este problema. La técnica jurídica más difundida a nivel internacional para lograr dichas funciones es la del criterio del “equivalente funcional”. A través de su utilización, la Ley Modelo sobre Comercio Electrónico⁵, en la conciencia de que los principales impedimentos para la difusión del comercio electrónico provienen de los requisitos legales que prescriben el empleo de la documentación tradicional en soporte papel, se propone ampliar el alcance

³ Spota, Alberto G., op. cit., pág. 702.

⁴ Spota, Alberto G., op. cit., pág. 699.

⁵ La Ley Modelo sobre Comercio Electrónico fue redactada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional procura facilitar a los Estados la modernización de su legislación. Una transcripción completa con el correspondiente análisis puede verse en Horacio Fernández Delpach, “Internet: su problemática jurídica”, Abeledo Perrot, Buenos Aires 2001.

de conceptos tales como “escrito”, “firma” y “original”. Este rol lo ha venido a cumplir en nuestro ordenamiento nacional la Ley 25.506 de Firma Digital

Se han descrito ya las funciones que la firma ológrafa cumple como medio de identificación del autor del documento y de reconocimiento de la voluntad por él expresada a través del contenido del instrumento.

Existen distintos métodos técnicos que, de una u otra forma, pretenden dar cumplimiento a los recaudos que deben satisfacerse para que los documentos digitales puedan adquirir la misma seguridad –y consecuente fuerza jurídica- que los documentos realizados en soporte papel.

Así, por ejemplo, es posible digitalizar la firma ológrafa por algún proceso, como podría ser el “escaneo”, para agregarla a un documento digital. Sin embargo, este sistema carece de seguridad en cuanto el archivo resultante del escaneo de la firma ológrafa resulta fácilmente duplicable y utilizable por terceros. Nada garantiza sobre la autoría del documento ni sobre la voluntad del presunto firmante.

Firma digital, en consecuencia, es un término que se reserva para aquellos mecanismos que, cumpliendo con los principios de la seguridad informática, satisfagan las mismas necesidades jurídicas que la firma manuscrita.

La Ley 25.506 de Firma Digital la define como el "... resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante encontrándose ésta bajo su absoluto control...", agregando que la firma digital "...debe ser susceptible de verificación por terceras partes tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma."

Posteriormente, en su artículo quinto, define a la firma electrónica como al "...conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital." Es una firma más “débil”, en tanto produce efectos jurídicos más limitados, como ya se verá⁶.

⁶ Es por ello que la firma digital ha sido denominada, también, “firma electrónica avanzada” en España (Real Decreto Ley 14/1999, art. 2.a y b) En la misma línea, la ya citada ley chilena adopta como definiciones en su art. 2: “f) Firma electrónica: cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor; g) Firma electrónica avanzada: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría”.

II.3 Algunos conceptos fundamentales

II.3.1 Clave privada, digesto seguro y clave pública

En una apretada descripción técnica del proceso, se puede afirmar que la firma digital se vale de la criptografía asimétrica para generar dos claves matemáticamente complementarias, una “privada” (sólo conocida por el que firma el documento) y otra “pública” (que utilizan los terceros para verificar la firma digital), aunque por la irreversibilidad del proceso de generación de la segunda, no se puede obtener la clave privada por el hecho de conocer la pública.⁷ Son el resultado de hacer ciertas operaciones matemáticas sobre dos números primos cuya longitud es lo que otorga mayor seguridad al sistema, ya que resulta extremadamente difícil (prácticamente imposible) factorizar la clave pública para conocer la privada y poder utilizarla sustituyendo a su dueño.

Tanto en la creación de la firma digital como en su verificación se ejecuta el proceso llamado *hash function*. Este consiste en un algoritmo que, aplicando la clave privada a un documento digital determinado, crea un nuevo archivo denominado digesto seguro⁸, de una longitud fija, mucho menor que el mensaje original, pero substancialmente único.

El mensaje no se transforma necesariamente en confidencial, simplemente se le adosa al documento digital original la firma digital (digesto seguro + clave privada del firmante). Realizando el proceso inverso, el receptor verifica con la clave pública⁹ si esa firma digital fue creada con la respectiva clave privada (autenticación del suscriptor), y la coincidencia del digesto seguro que él obtiene con el digesto seguro transformado en firma digital durante el proceso de firma (autenticación del mensaje o integridad del documento digital).

Ahora bien, como se advierte, se habla de autenticar al emisor del documento, y no de asegurar la identidad del autor del mismo: es aquí, donde radica la principal falencia del sistema comparado con la firma ológrafa, ya que, aun cuando resulte

⁷ Además de para firmar, estas claves pueden usarse indistintamente para cifrar y descifrar un documento digital (aportándole así la característica de la confidencialidad: sólo quien tiene la clave puede acceder a la información que contiene), con la salvedad de que lo que encripta una puede ser descifrado solamente con la otra.

⁸ También llamado *hash result* o *hash value*.

⁹ Quien verifica accede a esta clave pública a través del certificado digital del firmante.

sumamente difícil sustraer el algoritmo de la firma digital para simular ser una persona, sigue siendo más probable que imitar perfectamente una firma en papel. Esta debilidad se suple a través de los deberes que la ley impone a los usuarios de este sistema, con estrictas responsabilidades sobre la guarda y control de la clave privada¹⁰, estableciendo por ejemplo la obligación de revocar un certificado digital asociado a claves “...ante cualquier circunstancia que pueda haber comprometido la privacidad de sus datos de creación de firma” (art. 25 d).

Este sistema de criptografía asimétrica o doble clave es el sistema de firma digital que la Ley 25.506 adopta sin nombrarlo y en el marco de una pretendida neutralidad tecnológica. Aunque en el cuerpo de la ley sólo se habla de datos de creación y de verificación de la firma digital, sin referencia alguna a la criptografía asimétrica, ni las claves privada y pública, el funcionamiento que describe se ajusta con precisión a este criptosistema asimétrico. Y en el Anexo que acompaña a la ley se define a los datos de creación de firma digital como “datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear su firma digital”; y a los datos de verificación de firma digital como “datos únicos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma digital, la integridad del documento digital y la identidad del firmante”.

Este sistema de doble clave aparece como el mejor a nivel técnico, tiene amplia divulgación en el ámbito internacional¹¹, y ya había sido adoptada por los antecedentes nacionales en la materia¹².

¹⁰ Un aporte a futuro puede hacerlo la biometría, que permite la autenticación del sujeto por el reconocimiento de ciertas características físicas o biológicas del mismo, como ser su voz, la lectura de las huellas digitales o del iris, etc.. La información biométrica, si bien es única, no es secreta: algunos de estos aspectos de la persona pueden ser fácilmente capturados por terceros, como la voz por medio de una grabación o las huellas dactilares –por ejemplo- de un vaso. Por eso, parece recomendable la integración de este mecanismo con el de criptografía de clave pública.

¹¹ En los Estados Unidos prácticamente todos los Estados han implementado una legislación sobre firma digital; la mayoría se ha basado en la Ley del Estado de Utah sobre la Firma Digital (Utah Digital Signature Act), que comenzó a regir el 1 de mayo de 1995.

¹² En tal sentido, se pueden mencionar la Resolución N° 45/97 de la Secretaría de la Función Pública, que autorizó el empleo en el ámbito de la Administración Pública Nacional de la tecnología para la utilización del documento electrónico y la firma digital; la Resolución N° 293/97 de la Superintendencia de AFJP y el Decreto N° 427/98 del Poder Ejecutivo Nacional, que autorizó el empleo de la firma digital en la instrumentación de los actos internos del Sector Público Nacional que no produzcan efectos jurídicos individuales en forma directa. Este último la define como el “resultado de una transformación de un documento digital empleando un criptosistema asimétrico y un digesto seguro, de forma tal que una persona pueda determinar con certeza: 1.- Si la transformación se llevó a cabo usando la clave privada que corresponde a la clave pública del firmante, lo que impide su repudio; 2.- Si el documento digital ha sido modificado desde que se efectuó la transformación, lo que garantiza su integridad. La conjunción de los dos requisitos anteriores garantiza su no repudio y su integridad”. Esta enumeración la completan la Resolución N° 194/98 SFP, la Resolución N° 212/98 SFP, el Art. 61 de la Ley 25.237 de Presupuesto Administración Pública Nacional del año 2000, DA N° 102/00, y el Decreto 673/01 de la Secretaría para la Modernización del Estado.

Habitualmente, la clave privada es conservada en el disco rígido de la computadora de su titular, y es administrada por los navegadores de Internet o "browsers" (como el *Internet Explorer* o *Netscape Navigator*); pero también puede residir en una tarjeta inteligente, llamada "smartcard". El uso de estas tarjetas tienen ciertas ventajas respecto a la utilización de claves privadas residentes en las computadoras. Estas poseen un chip, que en algunos casos es un simple dispositivo de almacenamiento y en otros es un microprocesador, en cuyo interior está almacenada la clave privada. Pareciera que la portabilidad de la tarjeta facilita la guarda por su titular y ayuda a evitar un uso ilegítimo, en comparación con el archivo que está alojado en una máquina. De alguna manera, brinda a su titular la misma seguridad que llevar en el bolsillo su tarjeta de crédito o las llaves de su hogar. En ambos casos (sea que la clave privada esté almacenada en una PC o en una tarjeta), su uso siempre puede ser protegido con un código o PIN ("personal identification number"). Otra diferencia es que los certificados sin tarjeta son 'exportables', se pueden transferir a otra máquina, mientras los de tarjeta son incopiables. Para concluir con esta comparación, resulta más fácil para el usuario percibir que ha perdido una tarjeta que detectar una intrusión en el sistema informático que haya resultado en la copia del certificado almacenado (si bien esto último es fácilmente detectable cuando se ha implementado una solución de seguridad informática); en cualquier caso, la pérdida del control exclusivo sobre la clave privada debe conducir a su titular a revocar el certificado digital ante la autoridad certificante.

II.3.2 Las terceras partes confiables

Para el funcionamiento de este sistema de criptografía de clave pública, es necesaria la existencia de terceras partes o *trusted third parties*, quienes van a certificar acerca de la existencia, vigencia y estado de la clave pública del firmante. Según el art. 17 de la Ley 25.506 puede ser una "persona de existencia ideal, registro público de contratos o un organismo público que expide certificados, presta otros servicios en relación con la firma digital y cuenta con una licencia para ello, otorgada por el ente licenciante. La actividad de los certificadores licenciados no pertenecientes al sector público se prestará en régimen de competencia. El arancel de los servicios prestados por los certificadores licenciados será establecido libremente por éstos". El artículo

siguiente autoriza a las entidades que tienen el control de la matrícula de servicios profesionales a constituirse en certificadores en lo referido a esa función¹³.

Estos actores del sistema, llamados entonces “certificadores licenciados” por la ley¹⁴, se encargan del registro, administración y publicidad de las claves públicas, como así también de los datos identificatorios de los titulares de éstas. Para ello emiten un certificado de clave pública o certificado digital o identificador digital. Es un archivo digital con la información mencionada, firmado digitalmente por el certificador con su propia clave privada. En otras palabras, esta autoridad de certificación acredita la relación existente entre una clave pública determinada y los datos de su propietario, mediando entre el mundo digital y el mundo físico.

La herramienta utilizada es llamada en la Ley 25.506 “certificado digital”. A su vez, el certificador licenciado debe poder firmar digitalmente, para lo cual debe contar con un certificado de clave pública. Los certificadores licenciados reciben este certificado de un “ente licenciante”¹⁵ madre, organismo que además les brinda la licencia necesaria para prestar sus servicios.

Las funciones y obligaciones de los certificadores licenciados se encuentran normados en detalle en los artículos 19º y 21º respectivamente.

II.3.3 El certificado digital

Pero veamos qué es un certificado digital. Es un documento digital firmado digitalmente, en el que un certificador licenciado da fe de la titularidad de un determinado sujeto respecto de una clave pública. Constituye una especie de “DNI” digital.

¹³ Esto constituye una interesante alternativa para estas instituciones, en particular los Colegios que agrupan a los abogados, en su caso, en pro de procurar brindar servicios crecientes, en cantidad y calidad, a sus matriculados, así como defender y ampliar los espacios de actuación profesional. Para la abogacía, esto implica muchas veces la reacción frente a avances injustificados de otras profesiones, o de profesionales de otros países, sobre el campo que la ley específicamente asigna al abogado argentino, y también actuar proactivamente, ocupando espacios hoy vacantes. Uno de estos ámbitos, en parte incipientemente explotado desde el exterior o desde otras profesiones, es el ciberespacio. Preparar la infraestructura técnica y operativa para que los abogados actúen en el campo de la comunicación electrónica con valor legal se inscribe claramente en esta dirección. Para ello, parece conducente avanzar creando los medios para que los abogados intervengan profesionalmente utilizando en plenitud las potencialidades de las nuevas tecnologías de la información.

¹⁴ Se aborda su definición, funciones, obligaciones y cese en el Capítulo III, arts. 17 a 23.

¹⁵ Resulta por lo menos curioso que la Ley 25.506 haya omitido considerarlo por separado, aunque lo menciona en doce artículos; posiblemente se trate de una omisión involuntaria en el proyecto finalmente aprobado.

Es un archivo que contiene determinados datos: básicamente, la clave pública, su fecha de vencimiento, el nombre y los datos del titular, y eventualmente puede incluir alguna otra información.

Pueden distinguirse, en la perspectiva de los usuarios de este sistema, los Certificados de Correo electrónico (que se obtienen mediante un procedimiento que sólo verifica la existencia de una determinada dirección de correo electrónico) y los Certificados de identificación personal (que incluyen algún procedimiento de verificación de la identidad del requirente del certificado)¹⁶.

Como ya se dijo, este certificado debe estar firmado digitalmente por un certificador licenciado, que es el único que tiene la facultad de manifestar que una clave pública pertenece a una persona y no a otra. Y tiene como principal finalidad dar cumplimiento al requisito de "no repudio" del documento firmado. Es decir, que al dar fe de la relación existente entre un sujeto y su clave pública, la autoría de un documento firmado con la clave privada correspondiente se atribuye a ese sujeto.

Un proceso típico por el cual se obtiene un certificado digital puede describirse así:

- ⇒ Un solicitante ingresa al sitio web del certificador licenciado, efectúa el requerimiento del certificado e ingresa sus datos personales.
- ⇒ En su propia PC, genera su par de claves (la clave pública y la clave privada) y envía su clave pública al certificador licenciado.¹⁷
- ⇒ Recibe entonces un código de identificación para su pedido.
 - ⊗ Si se trata de un certificado de identificación personal, un operador debe convocar al requirente para concurrir personalmente, verificar la información enviada, validar la identidad del suscriptor y aprobar la emisión del certificado.
 - ⊗ Si es un certificado de correo electrónico, se envía a la dirección de correo denunciada por el solicitante un mensaje, que debe ser respondido por el solicitante.
- ⇒ En cualquiera de los dos casos, recién entonces (validada la identidad o la existencia del correo electrónico, según el caso), un documento digital es firmado digitalmente por un "Oficial Certificador" y se envía al solicitante, que pasa a tener así un certificado digital.

¹⁶ También existen los certificados para servidores, que cumplen una función diferente dentro del sistema de certificación.

¹⁷ Es de hacer notar que la clave privada nunca sale de su poder.

II.4 La firma digital en la Ley 25.506.

El 23 de diciembre de 2001 entró en vigencia la Ley 25.506, de Firma Digital, que consta de 53 artículos distribuidos a lo largo de diez capítulos.

El artículo segundo de la ley, como ya se expresó, define a la **firma digital** como “...el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su exclusivo control. La firma digital debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma”, dejando en manos de la Autoridad de Aplicación la fijación de los procedimientos de la misma y su verificación, con el requisito de que los mismos deben estar en consonancia con estándares internacionalmente vigentes.

El artículo quinto, por su parte, se refiere a la **firma electrónica**, entendiendo por tal “...al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital...”. Dada esta definición por comparación con la firma digital, ambas serán tratadas en lo sucesivo conjuntamente, con las puntualizaciones del caso.

Es necesario, pues, determinar cuáles son los requisitos legales establecidos para que una firma sea considerada digital.

1.- En primer lugar, es indispensable la existencia de un documento digital, susceptible de ser firmado. Es definido por el artículo 6º como “..la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo...”.

2.- Dispone también la ley que a dicho documento digital se le aplique un procedimiento matemático que requiera información de exclusivo conocimiento del firmante. Este recaudo legal lo cumple el sistema de criptografía asimétrica, ya

que la denominada clave privada no necesita (ni debe) salir nunca de la esfera de control exclusiva de su titular.

3.- Exige también que la firma digital sea susceptible de verificación por “terceras partes”, las que no son otras que los certificadores licenciados a los que se refiere el Capítulo III (artículos 17 a 23). Son terceros no vinculados al negocio jurídico en que se originó el documento digital firmado digitalmente.

Conforme lo dispone el artículo 17, el certificador licenciado es quien expide el certificado digital, que debe contener, como mínimo, los siguientes datos (artículo 14): identificar indubitablemente al titular de la firma digital y al certificador licenciado que lo emite, indicando su período de vigencia y los datos que permitan su identificación única; ser susceptible de verificación respecto de su estado de revocación; diferenciar claramente la información verificada de la no verificada incluidas en el certificado; contemplar la información necesaria para la verificación de la firma; e identificar la política de certificación bajo la cual se emitió.

Este certificado es un documento digital firmado digitalmente por el certificador licenciado, que asocia una clave pública a su titular durante su período de vigencia, pues únicamente dentro de dicho período es válido el certificado (artículo 15, primer párrafo).

4.- La verificación efectuada debe permitir la identificación del autor del documento digital firmado digitalmente (artículo 2º).

Para poder emitir un certificado digital, el certificador licenciado debe asegurarse la identificación del titular: es por ello que deberá revocarlo cuando determinara que la información en virtud de la cual emitió el certificado digital era

falsa o cuando los procedimientos de emisión o verificación dejaran de ser seguros (artículo 19, inciso e, puntos 2 y 3).

5.- La verificación efectuada debe permitir detectar cualquier alteración del documento digital posterior a su firma (artículo 2º), brindando así una garantía de integridad de la información que los documentos en soporte papel no poseen. Como ya se ha descripto, el procedimiento del digesto seguro garantiza, en la tecnología criptográfica de clave pública, que cualquier modificación del documento con posterioridad a su firma será detectada de modo automático en el proceso de verificación del digesto seguro.

En síntesis, los cinco requisitos legales en la Argentina, para poder afirmar que se trata de una firma digital que funciona para los documentos digitales como el “equivalente funcional” de la firma ológrafa en los documentos en soporte papel, son:

- Que exista un documento digital a ser firmado
- Que el procedimiento matemático de firma requiera información de exclusivo conocimiento del firmante.
- Que la firma digital sea susceptible de verificación por terceros
- Que el proceso de verificación permita la identificación del autor del documento digital firmado digitalmente.
- Que el proceso de verificación permita detectar cualquier alteración del documento digital posterior a su firma.

En caso de faltar alguno de ellos, no se estará en presencia de un documento digital firmado digitalmente, lo que no impide que, si se trata de un conjunto de datos electrónicos utilizados por el signatario como medio de identificación aplicados a un documento digital, se considere que existe un documento digital firmado *electrónicamente*.

Como es fácil de advertir, la firma digital detenta mayores seguridades que la electrónica, y es por ello que la ley les atribuye distinta virtualidad jurídica.

El artículo 3° de la Ley 25.506 asimila la firma digital a la firma ológrafa, estableciendo que “cuando la ley requiera una firma manuscrita, esa exigencia también quedará satisfecha por una firma digital”, agregando que “este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia”.

La aclaración efectuada en la última parte de la norma resulta superflua e innecesaria, toda vez que la ley requiere de la firma de las partes únicamente cuando atribuye efectos jurídicos a la misma, o a su ausencia; si ninguna de estas circunstancias prevé consecuencias jurídicas significa que la firma o su ausencia resultan indiferentes al ordenamiento jurídico, por lo que la aplicabilidad o no de este principio deviene abstracto.

II.4.1 Presunción de autoría e integridad

Pero además de considerar la ley que la firma digital cumple la exigencia de la firma manuscrita, establece ciertas presunciones que derivan de la definición misma que brinda en el artículo 2°: las presunciones de autoría y de integridad.

En efecto, el artículo 7° de la Ley 25.506 dispone, regulando acerca de la primera de las presunciones mencionadas –también denominada por la doctrina como “garantía de no repudio”- que “se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma”; por su parte, el artículo 8°, en orden a la presunción de integridad, estatuye que “si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma”¹⁸.

Es fácil advertir que los documentos digitales firmados *digitalmente* no sólo satisfacen el requisito de la firma ológrafa, sino que existen además fuertes presunciones *iuris tantum* con relación a la autoría del documento y a su integridad, que superan lo previsto para la firma manuscrita en el Código Civil.

¹⁸ En línea con la crítica ya expresada al Proyecto de Código Civil de 1998 cuando el mismo habla imprecisamente de “asegurar la inalterabilidad del documento”, aquí también el legislador podría haber optado con más rigor por una redacción que apuntara a la no modificación del *contenido* del documento digital.

El documento firmado *electrónicamente*, por el contrario, no crea presunción alguna acerca de su autoría, y “en caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez” (art. 5°).

En un artículo confuso, que merece algunas aclaraciones, la ley agrega que “los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, el valor probatorio como tales, según los procedimientos que determine la reglamentación” (art. 11°). Este artículo permite cumplir con el requisito del “doble ejemplar” cuando existen convenciones bilaterales.

La primera observación es relativa al término “documento electrónico”, que se utiliza por única vez en todo el texto de la ley, y que a nuestro juicio constituye un error de técnica legislativa, que debe leerse como “documento digital”¹⁹.

Nada se dice, ni en este lugar ni en el resto del articulado, respecto del valor del documento firmado *electrónicamente*, sino que simplemente determina la inversión de la carga de la prueba de la autoría en el ya transcrito artículo 5°. Sin embargo, el artículo 11°, al referirse exclusivamente a los documentos electrónicos o reproducidos en formato digital que sean firmados *digitalmente*, parecería quitarle al documento digital firmado *electrónicamente* la posibilidad de dar cumplimiento al requisito del doble ejemplar establecido en el Código Civil, limitando así su potencialidad como instrumento privado en los actos perfectamente bilaterales. Difícilmente sería esto sostenible, dada la aptitud de los documentos digitales para su reproducción; y con seguridad la interpretación jurisprudencial, que ha sido habitualmente amplia respecto a la exigencia del doble ejemplar, extenderá a los documentos digitales firmados *electrónicamente* e idénticos entre sí, la posibilidad de satisfacer la exigencia del doble ejemplar en los casos que la ley así lo pide.

Finalmente, debe criticarse la delegación que se hace en la reglamentación a cargo del Poder Ejecutivo Nacional, pues si la misma se refiere al valor probatorio, excede las facultades reglamentarias que le confiere el artículo 99 de la Constitución Nacional; en efecto, el valor probatorio sólo puede ser establecido mediante los códigos de fondo o – en su caso- por los códigos procesales. En el primer caso corresponderá al Congreso de

¹⁹ En este caso, parece hablar de los documentos creados en formato digital directamente, por oposición a documentos en formato digital que reproducen documentos que originalmente constaban en otro soporte (sic) aunque en el texto no se menciona ningún tipo de soporte, haciendo gala de una imprecisión notable que merece una futura corrección.

la Nación determinarlo, y en el segundo a las provincias, pero nunca al P.E.N. Y no se advierte qué otra reglamentación podría efectuarse con relación a este artículo.

II.4.2 Otras disposiciones

Para que la firma digital aplicada a un documento sea válida, el artículo 9º indica que se deben cumplir con determinados requisitos: haber sido creada durante el período de vigencia del certificado digital válido del firmante, ser debidamente verificada por la referencia a los datos de verificación de firma digital indicados en dicho certificado y que éste haya sido emitido o reconocido según lo normado en la propia ley.

La ley establece también que “la exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción” (art. 12º).

Este precepto permite sostener que los documentos digitales firmados digitalmente podrán cumplir en un futuro cercano las funciones de los instrumentos públicos: pero además en lo inmediato puede suceder tal situación. Nada impediría, por ejemplo, que las copias de los documentos otorgados en los Registros –un acta de nacimiento, matrimonio o defunción- sean archivadas mediante un documento digital firmado digitalmente, pasando a ser, por tanto, instrumentos públicos (artículo 979, inciso 10º, del Código Civil).

En el Capítulo IV se legisla respecto de los derechos y obligaciones de los titulares de un certificado digital, encontrándose entre los primeros el derecho a ser informado por el certificador licenciante y, previo a la emisión del certificado digital, sobre las condiciones del mismo, características y efectos de este sistema. Tiene, entre otros, el derecho de que el certificador emplee los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por él, y a ser informado sobre ello.

Ahora bien, en el artículo 37 la ley dispone que las relaciones entre el certificador licenciado y el titular del certificado se rigen por el contrato que celebren entre ellos; no obstante, hubiera sido pertinente que la ley fijara un sistema de responsabilidad objetiva para el caso de que aquél generara daños derivados del incumplimiento de su obligación

de emplear los medios técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el titular.

Entre las obligaciones a cargo del titular del certificado digital, la más importante es la que le impone el deber de mantener el control exclusivo de sus datos de creación de firma digital, no compartirlos e impedir su divulgación. El incumplimiento de esta obligación le impedirá eximirse del deber de reparar los daños que cause, en aplicación del principio conforme el cual *nemo propiam turpitudinem allegans est auditor*.

En su Capítulo V, la ley instaura un sistema de Auditoría tanto para el Ente Licenciante como para los Certificadores Licenciados y crea también la Comisión Asesora para la Infraestructura de Firma Digital - cuyas funciones e integración están previstas en el capítulo VIII- en el ámbito jurisdiccional de la Autoridad de Aplicación, la que cae en cabeza de la Jefatura de Gabinete de Ministros, determinando sus funciones y obligaciones en el Capítulo VI. Finalmente, el sistema de responsabilidad estatuido por la ley está regulado en el Capítulo IX y en el Capítulo X se prevén las sanciones para los incumplimientos de las obligaciones establecidas por la misma. Más allá de la importancia que revisten estas cuestiones, su tratamiento quedará para otra oportunidad.

