DOCUMENTO Y FIRMA DIGITAL: PARA ENTRAR EN TEMA (Versión 5.0, actualizada en febrero de 2013)

Dr. Jorge Oscar Rossi

Profesor Titular de la asignatura “Régimen Jurídico de los Consumidores y Usuarios”, Adjunto de “Contratos Civiles y Comerciales” y de “Obligaciones Civiles y Comerciales” en la Universidad Abierta Interamericana.

SUMARIO: Aclaración necesaria. 1. Palabras poco conocidas. 2. La vida en la Red. 3. Utilidad de la Firma Digital. 4. Tecnologías. 5. ¿Qué es una firma digital?6. La criptografía. 7. Tres conceptos clave. 8. Infraestructura de Firma Digital. 9. ¿Qué es un Criptosistema seguro? 10. La transmisión y el almacenamiento de los datos. 11. El impacto de la Ley de Firma Digital en el Derecho Privado. 12. La forma escrita: El instrumento privado. 13. Un nuevo concepto de Documento privado. 14. Diferencia entre firma digital y firma electrónica. 15. La Firma Digital y el Poder Judicial: Nación y Provincia de Buenos Aires. 16. Subasta electrónica y transferencia de inmuebles en la Provincia de Buenos Aires.

Aclaración necesaria

El presente trabajo, cuya mayor pretensión es que sirva a la comunidad jurídica para la comprensión de un tema que, día a día, gana en actualidad e importancia, le debe mucho a la Exposición de Motivos del Anteproyecto de Ley de Firma Digital que fuera redactado en 1999, a convocatoria del Ministerio de Justicia de la Nación , por los siguientes profesionales del Derecho y la Informática : Mauricio Devoto, Beatriz García, J. Andrés May, Pablo Palazzi, Patricia Prandini, Alejandro Román, Aldo Rosenberg, Pablo Tiscornia y Julio Tulián. La primera versión de este trabajo fue publicada el 19 de mayo de 2000 en www.diariojudicial.com.

1. Palabras poco conocidas

En esta materia, uno de los primeros problemas que debemos afrontar es el de una terminología novedosa y un tanto oscura, dada la formación que tenemos la mayoría de los abogados. Trataremos de poner en claro algunos conceptos.

Por empezar puede decirse que *un documento digital es una secuencia informática de bits (unos y ceros) que puede representar cualquier tipo de información (actos, hechos o datos), con independencia del soporte utilizado para almacenar o archivar dicha información.* Esta

representación de la información en base a **dígitos** implica en el ámbito informático una representación binaria, es decir por medio de unos y ceros.
Corresponde hablar de documento digital y no de documento electrónico, vocablo éste último que se utiliza erróneamente, a pesar de su popularidad. ¿Por qué?: Porque el procesamiento informático consiste en procesar dígitos binarios, no electrones.
Aunque es cierto que, cuando el documento digital se encuentra momentáneamente almacenado en la memoria volátil de una PC (memoria "RAM"), los dígitos de ese documento consisten de magnitudes eléctricas, también es cierto que cuando se encuentra almacenada en el disco duro de la PC , consiste en campos magnéticos (o, con mayor precisión, en imanes moleculares), cuando se encuentra perdurablemente almacenado en un CD-ROM consiste en agujeros perforados en la capa de aluminio del CD y, finalmente, cuando es transmitido por una fibra óptica de telecomunicaciones, consiste en fotones.
Lo que también es cierto es que en todas estas modalidades diferentes de almacenamiento y transmisión, el documento no pierde su cualidad numérica, es decir digital. Por eso, los especialistas consideran que conviene denominarlo como tal.
Uno de los problemas de los documentos digitales, por ejemplo una planilla de cálculos, un mail, un documento de Word, etc., **es que son fácilmente alterables**, es decir, que pueden ser modificados en su contenido. Otro inconveniente es el de la imposibilidad de conocer con certeza quién fue el autor de dichos documentos. Estos son dos obstáculos importantes a la hora de asignarle valor jurídico a la información digitalizada.

2. La vida en la Red

Es sabido que Internet reviste cada vez mayor importancia para la comunicación mundial, dado su carácter de red abierta de transmisión de datos. Esas redes permiten una comunicación interactiva entre interlocutores. Esto, entre otras cosas, permite nuevas posibilidades empresariales, creando herramientas que mejoran la productividad y reducen los costos, así como nuevas formas de llegar al cliente.
Surgen nuevas relaciones laborales, como el teletrabajo y los entornos virtuales compartidos.
Por otra parte, las administraciones públicas pueden usar la red en su gestión interna y en su interacción con empresas y ciudadanos. A su vez, el comercio electrónico brinda al país una excelente oportunidad para avanzar en su integración económica con las naciones del resto del mundo.

En nuestro país, el comercio electrónico es un hecho por todos conocido. Existen supermercados, aerolíneas, agentes bursátiles, cadenas de venta de electrodomésticos y bancos que ofrecen sus productos y servicios directamente por Internet.

Era necesario disponer de un entorno seguro en relación con la autenticación digital, vale decir, con la posibilidad de certificar tanto el contenido como la autoría del documento digital.

En la práctica existen diversos métodos para **firmar documentos digitalmente**. Algunos son muy sencillos (v. gr., insertar la imagen escaneada de una firma manuscrita en un documento creado con un procesador de texto), pero no permiten otorgarle validez jurídica a esa firma. Otros, más seguros, requieren la utilización de una tarjeta de coordenadas, como la que se utiliza en las operaciones de homebanking.

En Wikipedia se describe a la tarjeta de coordenadas como *"una herramienta de seguridad adicional al PIN o clave de seguridad bancaria requerida para realizar operaciones que impliquen movimiento de fondos o contratación de productos y servicios a través de servicios a distancia (banca electrónica o banca telefónica).*

Conforma un segundo factor de autenticación de la cuenta bancaria, pero a diferencia del PIN, que es fijo, es dinámica. Cuando una clave es dinámica es más difícil para los estafadores electrónicos (Phishing o correos fraudulentos) robar claves para hacer transferencias por Internet. Cada vez que lo intenten necesitarán una coordenada distinta, que es aleatoria y vence con cada sesión." [1]

Otros sistemas son muy avanzados, como la firma digital que utiliza la "criptografía de clave pública", que veremos más adelante.

Para tener validez jurídica, las firmas digitales deben permitir verificar tanto la **identidad** del autor de los datos (autenticación de autoría), como comprobar que dichos datos no han sufrido **alteración** desde que fueron firmados (autenticación de integridad).

3. Utilidad de la Firma Digital

Desde el sector público, a los gobiernos les interesa digitalizar la gestión de los Estados, permitiendo reemplazar los documentos y expedientes en papel por similares electrónicos, otorgándoles a estos valor legal y haciéndolos oponibles a terceros.

Desde el ámbito privado la utilidad de una Infraestructura de Firma Digital es inmensa. Veamos unos ejemplos:

[1] http://es.wikipedia.org/wiki/Tarjeta_de_coordenadas (consultado el 15/02/13)

1) Posibilitar la firma de formularios en sitios Web y de esta forma poder realizar trámites ante el Estado (vgr. AFIP [2]) por Internet.
2) Permitir el acceso seguro a Intranets, posibilitando el teletrabajo.
3) Permitir realizar transacciones administrativas, financieras y comerciales seguras por Internet.
4) **En el ámbito judicial**, las posibilidades son enormes:
a) Permitir realizar vía mail todas las notificaciones que deban hacerse a los domicilios constituidos en el proceso y, más aún, presentar los escritos de las partes.
b) Por esa vía, el juzgado podría enviar los oficios y/o testimonios a otros juzgados o a reparticiones estatales como los Registros de Estado Civil, de Propiedad Inmueble, Automotor, etc., y recibir las contestaciones.
c) Lo mismo con los oficios judiciales pidiendo informes a oficinas públicas o privadas, que se contestarían por la misma vía. Cualquier abogado puede apreciar el ahorro de tiempo, costos, esfuerzos y papeleo que eso implica.
5) Multiplicidad de contratos pueden formalizarse por este medio.

4. Tecnologías

La tecnología necesaria para otorgar validez legal a los documentos electrónicos ya existe.

Hoy día se pueden resolver fehacientemente las dos cuestiones fundamentales para la validez de estos documentos, de que hicimos referencia anteriormente:
1) Certificar quien es el autor de la información digital contenida en el documento (Requisito de Certeza).
2) Certificar que la información no fue modificada luego de ser firmada (Requisito de Integridad).

5. ¿Qué es una firma digital?

Restringiendo el término "firma digital", a aquellas que tienen aptitud para otorgar validez legal a los documentos digitales, podemos definirla como *el resultado de la aplicación de un procedimiento criptográfico extremadamente seguro a un documento digital, que permite garantizar su integridad.*
La validez legal de la firma digital ha sido reconocida en numerosos países, asimilándola a la firma ológrafa (España, Italia, Alemania, Francia, la mayoría de los estados de los EE.UU, etc.)

[2] Al respecto, ver http://www.afip.gob.ar/firmaDigital/ (consultado el 20/02/13)

En nuestro país, a fines del 2001 se sancionó la ley 25.506 (LFD), que regula el tema en forma integral. Esta ley es complementada por su decreto reglamentario, nº 2628/02. Estas dos normas introdujeron una de las más profundas reformas en el Derecho Privado Argentino, reforma que todavía no ha sido completamente vivenciada, porque sus efectos todavía no llegan a sentirse en el grueso de nuestra sociedad. Esta normativa trae una nueva conceptualización a un tema clásico del Derecho Civil como es el de la noción del documento privado, cuestión ligada a la de la forma de los actos jurídicos.

La LFD establece en su artículo 2º que *" Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto 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".*

6. La criptografía

La criptografía se define como *el arte de proteger la información*, tanto para proteger su privacidad como para proteger su integridad. El término criptografía proviene del griego cripto (oculto).

Para muchos especialistas, el mecanismo de firma digital debe ser criptográfico, pues si lo que se desea es proteger la información, o sea los dígitos, debe entrarse en ese campo.

También pueden utilizarse otros mecanismos en el proceso de firma digital, como por ejemplo, los mecanismos biométricos (vgr. Un sistema de lectura digital de huellas dactilares o del iris ocular), pero estos deben ir acompañados por el procedimiento criptográfico, para impedir que terceros accedan a la información.

Sin embargo, no todos los mecanismos criptográficos son considerados aceptables, al fin de otorgar valor jurídico a los documentos digitales.

Comparando al documento digital con aquel confeccionado en "soporte papel", vemos que la firma manuscrita tiene validez jurídica en nuestra sociedad y cultura pues se ha generado una costumbre que la considera aceptable para identificar al autor de un documento y, simultáneamente, asegurar la integridad del contenido de ese documento. Claro que para eso se deben cumplir las siguientes condiciones:

1. El documento debe escribirse con tinta indeleble y en soporte papel absorbente, tal que una enmienda o raspadura que altere la información escrita sea visible y evidente;
2. El documento debe poseer márgenes razonables que contengan los renglones escritos, por lo que cualquier escritura adicional sea visible y evidente;
3. La firma manuscrita se debe colocar delimitando la información escrita, tal que no sea posible agregar texto escrito excepto a continuación de la firma manuscrita;
4. El firmante debe utilizar siempre la misma o similar firma manuscrita para firmar los documentos de su autoría;
5. La firma manuscrita debe ser suficientemente compleja para que su falsificación no sea trivial,
6. Deben existir peritos caligráficos que puedan detectar las falsificaciones con un razonable grado de certeza.
La falla de cualquiera de los seis puntos especificados torna inseguro al mecanismo de firma manuscrita para documentos en soporte papel y permite así a su autor *repudiar* los documentos que le son atribuidos.

7. <u>Tres conceptos clave</u>

Integridad significa que la información no carece de ninguna de sus partes, que no ha sido modificada. La integridad es una cualidad imprescindible para otorgarle validez jurídica a la información. La firma digital detecta la integridad de la información que fuera firmada, en forma independiente al medio de su almacenamiento.

Inalterabilidad significa que la información no se puede alterar. Ya que, en realidad, la información siempre se puede alterar, este concepto no se refiere a la información en sí, sino a su medio de almacenamiento. La firma digital no impide que la información se altere, sino que detecta si ésta lo ha sido. Recordemos que la ley 25.506 dispone 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".*

Perdurabilidad significa que la información perdura en el tiempo y es una cualidad del medio de almacenamiento. La información que debe perdurar en el tiempo debe ser archivada en un medio perdurable. La inalterabilidad del medio de almacenamiento no guarda relación con la perdurabilidad de la información: Por ejemplo en la antigua informática, la "tarjeta perforada" de

cartón es un medio inalterable porque no es re-perforable, pero no demuestra buenas características de perdurabilidad pues es sensible a la humedad y a los roedores. Por el otro lado, el disco rígido de una computadora no es un medio inalterable de almacenamiento, pero demuestra excelentes características de perdurabilidad cuando opera como parte de un banco de discos, si la información se almacena con suficiente redundancia (es decir, si se hacen varias copias) y si los discos tienen un tiempo promedio entre fallas del orden de 350.000 horas (40 años).

Como se expuso en el análisis previo de la firma manuscrita, una de las cualidades esenciales para que la misma tenga validez jurídica es que no sea fácilmente falsificable por un tercero, es decir que existan garantías de que esa firma pueda ser creada sólo por una persona y no por otra.

En el ámbito informático y digital es posible reproducir cualquier información binaria, tal que la copia no es diferenciable de su original. Como ya se mencionó, esta es una de las razones por la que la firma manuscrita escaneada (digitalizada) no puede obtener validez jurídica.

El sistema debe poseer una condición que permita identificar al creador de una firma digital, teniendo en cuenta que cualquier cualidad manifiesta a simple vista puede ser fácilmente copiada y transferida de un documento a otro.

La condición buscada está disponible y consiste en el ***secreto no compartido***. El concepto en su esencia es muy simple: el creador de una firma digital posee un elemento que sólo él conoce y posee y que le permite crear firmas digitales tal que quién las verifica pueda establecer inequívocamente que al firmar, el creador de la firma digital necesariamente tuvo posesión de ese elemento, pero sin requerir que el creador de la firma digital tenga que divulgar ese secreto, con lo que dicho secreto dejaría de serlo.

Este mecanismo existe y en el ámbito de la criptografía se denomina **criptografía asimétrica o criptografía de clave pública**. La criptografía asimétrica utiliza dos claves diferentes pero íntimamente relacionadas, tal que lo que encripta una clave sólo puede ser desencriptado por la correspondiente otra clave, y no por una clave ajena a ese par. El mecanismo matemático utilizado asegura además que conociendo la clave pública no se tiene información alguna sobre la correspondiente clave privada. Este mecanismo contrasta con la más tradicional criptografía simétrica que utiliza una misma clave para encriptar y para desencriptar un texto, por lo que el destinatario del texto para poder leerlo necesariamente debe conocer la clave secreta utilizada para encriptar ese texto con lo que esa clave secreta pierde tal cualidad. Por ello la criptografía

simétrica solo sirve para otorgarle privacidad a la información pero no como tecnología de firma digital.

En la criptografía asimétrica, **la clave de creación de la firma digital** se denomina **clave privada** y es mantenida secreta por el firmante, mientras que **la clave de verificación de la firma digital** se denomina **clave pública** y se da a conocer. Las firmas digitales creadas por el firmante utilizando su clave privada son verificadas por el destinatario del documento con la correspondiente clave pública. **El hecho de que una firma digital sea verificable por medio de una cierta clave pública implica necesariamente que esa firma fue creada por la correspondiente clave privada que, por definición, el firmante siempre mantuvo secreta y nunca divulgó.**

Es esencial para su validez jurídica que el mecanismo de firma digital contemple la utilización de un secreto no compartido por el creador de una firma digital, pues este secreto no compartido es lo único que impide que un tercero falsifique su firma. Esta seguridad de no falsificación es intrínseca a cualquier mecanismo de firma.

El algoritmo de clave asimétrica más popular por un amplio margen es el denominado RSA en honor a sus inventores Ronald Rivest, Adi Shamir y Leonard Adleman que lo desarrollaron en el Massachussetts Institute of Technology de los EE.UU. en 1977. La criptografía asimétrica RSA tiene disponibles, por ejemplo, múltiples implementaciones en los navegadores y servidores más populares y gratuitos del Internet, con una base establecida de usuarios de decenas de millones en los diferentes países del mundo. [3]

El requisito de implementar la firma digital únicamente mediante la criptografía asimétrica tampoco es restrictivo ni tecnológica ni comercialmente, pues la criptografía asimétrica no es una tecnología ni un algoritmo especial y propietario, sino meramente una definición que abarca a todo y cualquier algoritmo criptográfico que utilice una clave diferente para encriptar que para desencriptar, de los cuales existen por lo menos una treintena de algoritmos diferentes utilizables.

8. Infraestructura de Firma Digital

El sistema de Firma Digital necesita, para su funcionamiento, de una infraestructura que la haga posible. Una Infraestructura de Firma Digital *es un conjunto de hardware, software, bases de datos, redes, procedimientos y obligaciones legales*, que permite que las personas físicas y

[3] Para los interesados en profundizar el tema y ver como la criptografía asimétrica RSA sirve tanto para encriptar información como para autenticar (firmar) la autoría e inalterabilidad de la misma, recomendamos esta dirección: http://es.wikipedia.org/wiki/RSA (consultada 15/02/13)

jurídicas se identifiquen entre sí al realizar transacciones o intercambiar documentos electrónicos.

En una Infraestructura de Firma Digital tendremos un **Ente Licenciante**, que es el órgano administrativo encargado de otorgar las licencias a los certificadores de clave pública y de supervisar su actividad. Actualmente, el decreto 1028/2003 encomendó tal función a la Oficina Nacional de Tecnologías de Información de la **SUBSECRETARÍA DE LA GESTION PÚBLICA de la JEFATURA DE GABINETE DE MINISTROS.**

A su vez, también estará el **certificador de clave publica licenciado** será una persona jurídica de carácter público o privado, cuya función consiste en otorgar los certificados digitales (conf. art 26 LFD).

Concretamente, el art. 17 de la LFD dispone que *"Se entiende por certificador licenciado a toda persona de existencia ideal, registro público de contratos u 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".

Al respecto, **la Decisión Administrativa 6/2007** aprobó los requisitos para el licenciamiento de certificadores , para Políticas de Certificación, los contenidos Mínimos de la Política de Privacidad, el perfil Mínimo de Certificados y Listas de Certificados Revocados, entre otras.

El art. 10 de la nueva norma dispone que *"La actividad de los certificadores licenciados se realizará con arreglo a los principios de objetividad, transparencia y no discriminación " y el 12 establece que toda la documentación solicitada en el proceso de licenciamiento "será considerada confidencial".*

Por otra parte, está previsto que también existan certificados digitales emitidos por certificadores **no licenciados** por el llamado Ente Administrador de Firma Digital. Estos certificados digitales emitidos por certificadores no licenciados serán válidos para producir los efectos jurídicos que la ley otorga a la firma **electrónica** (conf. art. 2º Decreto 2628/02). Dicho de otra manera, no valen para hacer una firma digital. Ya veremos la diferencia entre ambos tipos de firma.

Por último, en la base de la Infraestructura de Firma Digital están los **titulares de los certificados digitales**, que serán los usuarios del sistema.

De la definición de firma digital que ensaya el art. 2º de la LFD , se desprende que los **titulares de los certificados digitales** deben poseer *una " información de exclusivo conocimiento"*. Con

esta "información de exclusivo conocimiento", el titular podrá firmar digitalmente y precisamente, el hecho de que él sea el único que conozca estos datos, es lo que garantiza la autoría de la firma.

El sistema utilizado internacionalmente para lograr un tipo de firma digital que garantice la autoría, integridad a inalterabilidad del documento es el conocido como de *criptografía asimétrica de clave privada y pública*. Si bien la LFD no adopta expresamente este sistema, dejando esa decisión al Poder Ejecutivo, la*" información de exclusivo conocimiento"* que menciona en su art. 2º se corresponde perfectamente con el concepto de clave privada.

Como dijimos, el sistema de Infraestructura de Firma Digital dispone de un certificado digital y de dos tipos de claves:

Certificado de clave pública: es un documento digital firmado digitalmente por un certificador de clave pública, que asocia una clave pública con su titular durante el período de vigencia del certificado.

Clave pública: es aquella que se utiliza para verificar una firma digital, en un criptosistema asimétrico seguro.

Clave privada: es aquella que se utiliza para firmar digitalmente, mediante un dispositivo de creación de firma digital, en un criptosistema asimétrico seguro.

9. ¿Qué es un Criptosistema seguro?

Un criptosistema es seguro si no es posible acceder a la información encriptada o crear una firma digital sin poseer previamente la correspondiente clave secreta (clave privada).

Por ejemplo, un criptosistema es seguro si, utilizando todas las computadoras disponibles, no es computacionalmente factible probar todas las claves diferentes posibles hasta hallar la clave secreta que corresponde.

Con esto se evita un ataque a un criptosistema denominado "de fuerza bruta". Este ataque es análogo a probar todas las combinaciones posibles de un candado numérico de bicicleta hasta dar con la combinación correcta. La resistencia al ataque de fuerza bruta de un criptosistema utilizado para firma digital debe poder medirse en miles o millones de años.

Uno podría pensar que al aumentar la velocidad de las computadoras, se debilita la seguridad de la criptografía, dado que aumenta la probabilidad de éxito de un ataque de fuerza bruta. Sin embargo, sucede lo contrario. El aumento de velocidad de las computadoras hace factible utilizar claves más largas, lo cual aumenta exponencialmente el grado de dificultad del ataque de fuerza bruta, aún utilizando las computadoras más veloces. En efecto, el aumento de

velocidad de las computadoras aumenta la brecha entre la longitud de claves que es factible utilizar y los algoritmos criptográficos que se pueden quebrar.
El ataque de fuerza bruta no es el único ataque posible. Un criptosistema también puede ser quebrado si el problema de solución difícil sobre el cual se basa deja de serlo. Por ejemplo el más popular criptosistema asimétrico, denominado RSA, se basa en la dificultad del factoreo de grandes números. El ataque de fuerza bruta al criptosistema RSA no será exitoso mientras el factoreo de números de cientos de dígitos de longitud continúe siendo computacionalmente no factible.
Es importante destacar que para que un mecanismo de firma digital sea confiable, no solo debe ser seguro el criptosistema utilizado, sino que también debe ser segura la implementación de dicho criptosistema en software o hardware. Por ejemplo, la implementación maligna de un mecanismo de firma digital en un programa de computadora podría capturar la clave secreta de firma y guardarla subrepticiamente en un archivo.
Finalmente, vale destacar que la confiabilidad de un mecanismo de firma digital también depende del grado de conciencia de las personas que lo utilizan. Aunque se base en un criptosistema seguro y en una implementación segura, un mecanismo de firma digital deja de ser confiable si las personas comparten sus claves secretas de firma entre sí, por ejemplo el jefe con su secretaria cuando éste parte de vacaciones.
Por ello la confiabilidad de un mecanismo de firma digital depende de los eslabones del criptosistema, su implementación y su utilización que, conjuntamente, forman una cadena cuyo grado de confiabilidad está dado por la resistencia de su eslabón más débil.
Por otro lado, es importante destacar que la firma manuscrita tampoco es perfecta o infalible, puesto que es decididamente posible en ciertos casos alterar de forma indetectable el contenido de un documento en soporte papel o falsificar una firma manuscrita.
Según los especialistas, es técnicamente posible sintonizar un láser para que se corresponda con el color de una tinta, tal que al accionar el láser, la tinta literalmente se vaporiza y se levanta del papel sin dejar rastro detectable alguno.
Sin embargo, las aludidas imperfecciones de los mecanismos de firma manuscrita en documentos en soporte papel no impiden los actos jurídicos, ni gubernamentales ni comerciales que se basan en ella, ni que la firma manuscrita figure como requisito en las leyes y reglamentos de nuestro país o de otros.

10. La transmisión y el almacenamiento de los datos

Es importante destacar que la firma digital está ligada íntimamente al documento digital que la origina y que junto a ese documento y el certificado de clave pública correspondiente permiten en conjunto y de manera autosuficiente verificar la integridad del documento y la identidad del creador de la firma.
Como se puede observar, la cuestión de la transmisión de la información en general, y de un documento digital en particular, no forma parte alguna del mecanismo de firma digital y de la validez jurídica del documento digital firmado.
A título ejemplificativo, una persona puede crear un documento digital y su respectiva firma digital en una PC para que luego ese documento y su firma permanezcan en esa PC, o para ser copiados a un disquete, o para ser enviados por correo electrónico a cualquier lugar del mundo, sin que se vea afectada de manera alguna la capacidad de esa firma digital de verificar la integridad de ese documento y de establecer la identidad de su creador, preservando así la validez jurídica del mismo.

11. <u>El impacto de la Ley de Firma Digital en el Derecho Privado</u>

Como expresáramos, la normativa en estudio trae una nueva conceptualización a un tema clásico del Derecho Civil como es el de la noción del documento privado, cuestión ligada a la de la forma de los actos jurídicos.
Precisamente, la forma de los contratos, es decir, la manera en que estos se exteriorizan en el mundo jurídico, resulta de fundamental importancia para la prueba (actos formales ad probationem) o para la propia existencia (actos formales ad solemnitatem) del acto jurídico.
Hasta ahora, básicamente nos manejábamos con las disposiciones del Código Civil en la materia.
Por empezar, el art. 973 del Código consagra el principio de libertad de formas, al establecer que *"Cuando por este Código, o por las leyes especiales no se designe forma para algún acto jurídico, los interesados pueden usar de las formas que juzgaren convenientes"*, principio aplicable a los contratos por la remisión que hace el art. 1182, (*" Lo dispuesto en cuanto a las formas de los actos jurídicos debe observarse en los contratos"*).
A su vez, el art. 1145 nos dice que el consentimiento, elemento fundamental de los contratos, puede exteriorizarse expresamente *("verbalmente, por escrito, o por signos inequívocos")* o de manera tácita *(resultante de hechos o de actos que lo presupongan, o que autoricen a presumirlo)*
Sin embargo, esta libertad en materia de forma encuentra dos límites muy importantes:

1) Aquellos contratos que requieren una forma impuesta por la ley, como condición para su existencia y/o validez (actos formales ad solemnitatem), como, por ejemplo, la donación de inmuebles, que por imperio del art. 1810 del C. Civil debe ser hecha por instrumento público, "bajo pena de nulidad".
2) Aquellos contratos que requieren una forma impuesta por la ley, como condición para su prueba, (actos formales ad probationem). Al respecto, el art. 1193 establece que *" Los contratos que tengan por objeto una cantidad de más de diez mil pesos, deben hacerse por escrito y no pueden ser probados por testigos"*. Esta disposición, en la práctica, hace que todos los contratos sean formales ab probationem, dado que los diez mil pesos que se mencionan datan de la década del sesenta, época en que el artículo mencionado fue reformado por la ley 17.711. Con los sucesivos cambios monetarios originados por la inflación que azotó a la República Argentina , este monto es irrisorio hoy en día. Por su parte, el Código de Comercio, contiene una disposición similar, aplicable a la prueba de los contratos comerciales, en su artículo 209, bien que el monto mencionado allí es de "doscientos pesos fuertes"...del siglo XIX. Ahora bien, este rigor en materia probatoria, que parece exigir indefectiblemente la celebración por escrito del contrato al efecto de su demostración en juicio, se ve considerablemente atenuado por las excepciones que aparecen y se explican en los arts. 1191 y 1192 del C. Civil, esto es: a) la existencia de principio de prueba por escrito (*"Cualquier documento público o privado que emane del adversario, de su causante o de parte interesada en el asunto, o que tendría interés si viviera y que haga verosímil el hecho litigioso"*.), b) principio de ejecución (*"Cuando una de las partes hubiese recibido alguna prestación y se negase a cumplir el contrato"*) y c) imposibilidad de obtener o de presentar la prueba designada por la ley (*"Cuando la obligación hubiese sido contraída por incidentes imprevistos en que hubiese sido imposible formarla por escrito"*, como es el caso del llamado *"deposito necesario"*)
Si se dan cualquiera de estas situaciones, se admitirán todos los medios de prueba, tales como testigos, indicios coincidentes o presunciones legales.

12. <u>La forma escrita: El instrumento privado</u>

Tradicionalmente, se dice que instrumento privado es todo escrito que da constancia de un hecho u acto con consecuencias jurídicas, que ha sido firmado por particulares sin intervención de un funcionario público competente y que no tiene otro requisito que la firma.
Estrictamente, este concepto así expresado puede hacernos perder de vista la muy necesaria distinción entre el documento, el soporte del documento y lo documentado. Así el documento es la representación que exterioriza el hecho o acto jurídico documentado*. El documento no es*

el contrato, sino su representación, por dar un ejemplo. El soporte, a su vez, será el medio físico que contenga al documento

En la época de Vélez Sarsfield, y hasta no hace demasiado tiempo, el soporte de los documentos era, generalmente, el papel. Dicho de otra manera, el hecho o acto jurídico documentado debía escribirse en un papel. Para ser absolutamente precisos, el documento privado debía contenerse o "soportarse" o "almacenarse" en una superficie apta para ser escrita en un lenguaje humano, que contenga dicha escritura, acompañada de una o más firmas. Académicamente hablando, un testamento ológrafo puede hacerse en una tablilla de madera, aunque el "soporte papel" era el común en los documentos privados.

Lo que caracteriza al documento privado es que cumple el requisito de la firma.

Como dijimos, la firma manuscrita tiene validez jurídica en nuestra sociedad y cultura pues se ha generado una costumbre que la considera aceptable para identificar al autor de un documento y, simultáneamente, asegurar la integridad del contenido de ese documento, siempre que se den las condiciones de las que habláramos en el punto 6.

13. <u>Un nuevo concepto de Documento privado</u>

Pero el documento digital no es un "escrito" , sino un cúmulo de información almacenada en un soporte adecuado, representación en forma informática o electrónica de actos, hechos o datos jurídicamente relevantes.

Expresado de otra manera, tal como dijimos al inicio de este trabajo, un documento digital es ***una secuencia informática de bits (unos y ceros) que puede representar cualquier tipo de información (actos, hechos o datos), con independencia del soporte utilizado para almacenar o archivar dicha información.*** Esta representación de la información en base a **dígitos** implica en el ámbito informático una representación binaria, es decir por medio de unos y ceros.

Precisamente, el artículo 6º de la LFD dice que *"Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura".*

Atención con esto: " *Un documento digital también satisface el requerimiento de escritura"*, simplemente quiere decir que el acto este puesto por escrito, **pero no que esté firmado.** El *requisito de firma* es ***distinto*** al **requisito de escritura** y solo se alcanza en esta materia con la firma digital o con la firma electrónica, aunque en este último caso, como veremos, corresponde a quien quiere valerse de la firma acreditar su validez.

Al respecto, el artículo 1012 del Código Civil establece que la firma de las partes es una **condición esencial** para la existencia de todo acto bajo forma privada.

Una última aclaración en esta materia: un documento digital puede consistir en texto (v gr. un archivo *.txt), imágenes fijas (v gr. un archivo *.gif), imágenes en movimiento (v gr. un archivo *.mg), o audio (v gr. un archivo *.wav).

Una definición de documento privado que incluya tanto a los documentos digitales como a los "clásicos" en soporte papel podría ser la siguiente: *Documento privado es la representación que exterioriza un acto o hecho, siempre que resulte inteligible para una persona común, aunque para ello se requiera la intervención de medios técnicos, con total independencia del soporte en que conste y debiendo contener un mecanismo de firma por el que se pueda verificar con un aceptable grado de seguridad su autoría, inalterabilidad e integridad.*

Esta definición propuesta está inspirada en el texto de los artículos 263 a 266 del Proyecto de Código Civil y Comercial de 1998.

Unas palabras respecto de esta definición:

Cuando una persona lee las distintas cláusulas de un contrato que aparecen escritas en un papel, no necesita más que saber leer y tener buena vista, por así decirlo. No pasa lo mismo con los documentos digitales. Como ya dijimos, estos son representaciones digitales, es decir, ***una secuencia informática de bits (unos y ceros).*** Para que resulte inteligible para una persona común, para que esta pueda leer el documento digital, (si consiste en texto), o verlo (si se trata de imágenes), o escucharlo (puede ser un audio), es necesario utilizar, por ejemplo, una PC. Es por ello que, cuando advertimos que el documento privado debe ser *inteligible para una persona común,* hicimos la salvedad de que *para ello se requiera la intervención de medios técnicos.*

De esta manera, podemos sintetizar un aspecto de la cuestión, concluyendo que en la actualidad, en nuestro Derecho, un documento digital firmado digitalmente es un documento privado en igualdad de condiciones con aquellos realizados en soporte papel.

Por último, añadimos que el Proyecto de Código Civil y Comercial Unificado de 2012, actualmente en tratamiento en el Poder Legislativo, expresa en su art. 288 que "...*En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza un método que asegure razonablemente la autoría e inalterabilidad del instrumento."* El párrafo transcripto es prácticamente idéntico al que figura en el art. *266* el Proyecto de Código Civil y Comercial de 1998:

"...En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza un método para identificarla; y ese método asegura razonablemente la autoría e inalterabilidad del instrumento." [4]

14. <u>Diferencia entre "firma digital" y "firma electrónica"</u>[5]

Según el art. 3º de la LFD **,** *la firma **digital** tiene los mismos efectos jurídicos que la firma manuscrita.* Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.

En cambio, para la LFD , (art. 5º), la firma **electrónica** es el 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.** Una de las principales diferencias practicas con la firma digital se da en materia probatoria, pues **se invierte la carga de la prueba**, dado que, en caso de ser desconocida la firma electrónica, **corresponde a quien la invoca acreditar su validez**.

Por otra parte, no se aplican las disposiciones de la LFD a:

a) Las disposiciones por causa de muerte;

b) Los actos jurídicos del derecho de familia;

c) Los actos personalísimos en general;

d) Los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.

Como vemos, una de las ventajas de la firma digital por sobre la firma electrónica es que se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma y que, si dicha verificación es positiva, que ese documento digital no ha sido modificado desde el momento de su firma. Esas son las presunciones de autoría e integridad que establecen los artículos 7 y 8 de la LFD.

Finalmente, para que una firma digital sea válida deben cumplirse los siguientes requisitos, (art. 9º LFD):

---

[4] Proyecto de Código Civil unificado con el Código de Comercio y sus fundamentos - 1998 (Comisión creada por Dto. 685/95) http://infoleg.mecon.gov.ar/codigos/proycodciv-1998.doc

[5] Utilizamos la terminología de la LFD, sin perjuicio de nuestra opinión, expresada más arriba, de lo incorrecto de utilizar la palabra "electrónica" en este tema. En nuestra opinión, en lugar de firma digital y firma electrónica, debería distinguirse en firma digital certificada y firma digital no certificada, respectivamente.

* 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 según el procedimiento de verificación correspondiente;
* Que dicho certificado haya sido emitido o reconocido, por un certificador licenciado.

Hasta el dictado de la Decisión Administrativa 6/2007, como no se había reglamentado el otorgamiento y revocación de las licencias a los certificadores que así lo soliciten, no podían existir certificadores licenciados y por eso, no existían certificados de firma digital. Solo existían, en la terminología de la LFD , certificados de firma electrónica. De ahí la trascendencia de esta norma.

Actualmente existen solo **cuatro certificadores licenciados (Fuente: https://www.acraiz.gob.ar/?page_id=51 (15/02/13)** :

* Administración Federal de Ingresos Públicos (AFIP)
* Administración Nacional de la Seguridad Social (ANSeS)
* Oficina Nacional de Tecnologías de Información (ONTI)
* ENCODE S.A., hasta el momento, único certificador privado licenciado, (http://www.encodeac.com.ar/)

15. La Firma Digital y el Poder Judicial: Nación y Provincia de Buenos Aires

La ley nacional 26.685 (BO 07/07/11) autorizó *"la utilización de **expedientes electrónicos, documentos electrónicos, firmas electrónicas, firmas digitales**, **comunicaciones electrónicas y domicilios electrónicos constituidos,** en todos los procesos judiciales y administrativos que se tramitan ante el Poder Judicial de la Nación, con idéntica eficacia jurídica y valor probatorio que sus equivalentes convencionales"*, facultando a la Corte Suprema de Justicia de la Nación y el Consejo de la Magistratura de la Nación, de manera conjunta, para que reglamenten su utilización y dispongan su "gradual implementación" (conf. arts. 1° y 2°)

Ya en el año 2007 la Corte Suprema de Justicia de la Nación creó la Comisión Nacional de Gestión Judicial, encabezada el presidente del Máximo Tribunal, Ricardo Lorenzetti, e integrada por jueces de todo el país.

La Comisión es la dependencia encargada de delinear políticas estratégicas y planes operativos que, mediante la incorporación de nuevas tecnologías y criterios de gestión, impulsan el rediseño de la organización del Poder Judicial. [6]

Por ejemplo, ya existe un sistema de comunicaciones online con el Registro Nacional de las Personas.
En el marco del mismo, los tribunales pueden acceder de forma electrónica a la información relacionada con la búsqueda de datos de personas físicas en el marco de una causa judicial, como por ejemplo la fecha de nacimiento, datos filiatorios y domicilio, a través de una plantilla disponible en el correo electrónico institucional de los juzgados, obteniendo respuesta inmediata a lo requerido.
Los tribunales que lo utilizan son: Cámara Nacional en lo Criminal y Correccional Federal, Cámara Nacional de Apelaciones en lo Civil, Cámara Nacional en lo Criminal y Correccional, Cámara Nacional Electoral, Cámara Nacional de Apelaciones en lo Comercial, Cámara Federal de Casación Penal, tres juzgados del fuero Nacional del Trabajo, Cámara Federal de Apelaciones de San Martín, Cámara Federal de Apelaciones de General Roca, Cámara Federal de Apelaciones de Tucumán, Cámara Federal de Apelaciones de Corrientes, la Cámara Federal de Apelaciones de Mar del Plata y la Cámara Federal de La Plata. [7]

Por su parte, a nivel provincial, los Poderes Judiciales de Santa Fe[8], Chubut [9], Rio Negro [10] y San Luis [11], entre otros, están implementando su Infraestructura de Firma Digital.

En cuanto a la provincia de Buenos Aires, esta adhirió, mediante la sanción de la Ley N ° 13.666, a la LFD.
En la actualidad, el decreto 305/12 (BO Nº 26856 14/6/12) designó a la Secretaría General de la Gobernación como Autoridad de Aplicación de la Ley Nº 13.666.

---

[6] En http://www.pjn.gov.ar/ pueden consultarse los servicios disponibles por "vía electrónica", los que, según el fuero de que se trate, consisten en la posibilidad de presentar Demandas, confeccionar poderes o realizar notificaciones electrónicas

[7] Ver http://www.cij.gov.ar/nota-10728-Se-extiende-el-uso-de-sistema-de-intercambio-electronico-de-informacion-en-causas-judiciales.html (consultado el 26/02/13)

[8] Ver http://www.justiciasantafe.gov.ar/portal/index.php/esl/Informacion-General/Firma-Digital (consultado el 25/02/13).

[9] Ver http://www.juschubut.gov.ar/index.php/firma-digital (consultado el 25/02/13).

[10] Ver http://www.jusrionegro.gov.ar/inicio/manualesFD/index.php (consultado el 25/02/13).

[11] Ver http://www.justiciasanluis.gov.ar/gxpsites/hgxpp001.aspx?3,50,177,O,S,0,MNU;E;23;5;MNU;, (consultado el 25/02/13).

Por otra parte, la ley provincial 14.142, publicada en el suplemento del Boletín Oficial el 26 de julio de 2010 incorpora "*el uso del correo electrónico como medio de notificación para litigantes y auxiliares de la justicia"* y delega su reglamentación en la Suprema Corte de Justicia (art. 8º). A su turno, por el Acuerdo N° 3540, del 30 de marzo de 2011, la Suprema Corte de Justicia de la Provincia de Buenos Aires aprobó el "Reglamento para la notificación por medios electrónicos".
Para redactarlo, el Máximo Tribunal bonaerense se basó en una experiencia previa: La prueba piloto de notificaciones electrónicas, que fue puesta en marcha por el Acuerdo N° 3399 del 5 de noviembre de 2008.
Así, en los considerandos del nuevo Acuerdo, destaca la Suprema Corte que *"el sistema diseñado como prueba y que por la presente se dispone extender progresivamente con carácter obligatorio,* ***se apoya en la creación de un sitio web seguro****, en el que los textos de los proveídos a notificar* ***se firman digitalmente****, quedando en condiciones de ser accedidos por las partes. De este modo, se garantiza la* ***seguridad del acto de anoticiamiento, con el uso de la firma digital*** *por parte de funcionarios, partes y auxiliares de justicia."* (la negrita es nuestra)

Volviendo a la ley 14.142, la misma modifica los artículos 40, 143, 144, 148 e introduce el 143 bis en el Código Procesal Civil y Comercial de la Provincia de Buenos Aires. Además, modifica el artículo 16 de la Ley 11653 (procedimiento ante los tribunales laborales) y dispone que el sistema de notificación por correo electrónico será también de aplicación *"a los procesos previstos en la Ley de Concurso y Quiebras, Ley Nº 24522 y sus modificatorias"* (art. 7º).

a) "DOMICILIO ELECTRONICO"
En cuanto a la reforma del Código Procesal Civil y Comercial de la Provincia , se establece que en el primer escrito que presente, o audiencia a que concurra, si es ésta la primera diligencia en que interviene, toda persona que litigue por su propio derecho o en representación de tercero, deberá constituir domicilio dentro del perímetro de la ciudad que sea asiento del respectivo juzgado o tribunal, **juntamente con una casilla de correo electrónico, que será la asignada oficialmente al letrado que lo asista, donde se le cursarán las notificaciones por cédula que no requieran soporte papel y la intervención del Oficial Notificador** (conf. art. 1º ley 14.142).

Por su parte, el "Reglamento para la notificación por medios electrónicos" (en adelante, RNME), dispone en su art. 3º que *"…toda persona que litigue por su propio derecho o en representación de tercero,* ***deberá constituir domicilio electrónico en el casillero virtual que le será asignado al letrado que la asista o represente en la base de datos del sitio WEB de notificaciones****, contando con* ***certificado de firma digital que avalará la autenticidad e intangibilidad de la operatoria.*** *Si fuese asistida o representada por varios profesionales del derecho, deberá precisar cuál de los casilleros virtuales asignados a estos será su domicilio electrónico."* (la negrita es nuestra)

b) MEDIOS DE NOTIFICACION ALTERNATIVOS A LA CÉDULA

Además, en los casos donde el Código Procesal Civil y Comercial establezca la notificación por cédula, ella también podrá realizarse por los siguientes medios:

"1) ***Correo electrónico oficial****.*

2) Acta Notarial.

3) Telegrama Colacionado con copia certificada y aviso de entrega.

4) Carta Documento con aviso de entrega.

Se tendrá por cumplimentada la entrega de copias si se transcribe su contenido.

En caso que ello resulte imposible o inconveniente las copias quedarán a disposición del notificado en el Juzgado, lo que así se le hará saber.

Se tomará como fecha de notificación el día de labrada el acta o entrega del telegrama o carta documento, salvo que hubiera quedado pendiente el retiro de copias, en cuyo caso se computará el día de nota inmediato posterior.

Esta última fecha se tomará en cuenta en los supuestos que la notificación fuera por medio de correo electrónico, independientemente que se transcriba o no el contenido de las copias en traslado."(conf. art. 2º ley 14.142).

De todas maneras, el correo electrónico **no podrá utilizarse** para notificar el *traslado de la demanda, de la reconvención y de los documentos que se acompañen con sus contestaciones, la citación de personas extrañas al proceso y las sentencias definitivas y las interlocutorias con fuerza de tales, con excepción de las que resuelvan negligencias en la producción de la prueba*. (conf. art. 2º ley 14.142).

Por su parte, el juzgado o tribunal deberá realizar **de oficio**, por medio de **correo electrónico** o por cédula las resoluciones que *declaran la cuestión de puro derecho, la que ordena la apertura a prueba, las que se dictan entre el llamamiento para la sentencia y ésta, las que se dicten como consecuencia de un acto procesal realizado con anterioridad al plazo que la ley*

señala para su cumplimiento, la providencia que cita a audiencia preliminar y la que provee a la prueba ofrecida. (conf. art. 2º ley 14.142).

Por su parte, el RNME establece en su art. 1º que *"Siempre que esté disponible el uso de la notificación electrónica, no se podrá utilizar la notificación en formato papel, salvo que existieren razones fundadas en contrario."*

c) PROCEDIMIENTO LABORAL

Además, se sustituye el artículo 16 de la Ley 11653, el que quedará redactado de la siguiente forma:

"Artículo 16: Las providencias quedarán notificadas por ministerio de la ley, los días martes y viernes o el siguiente hábil si alguno de ello no lo fuere, sin necesidad de nota, certificado u otra diligencia.

Se notificarán personalmente o por cédula:

a) El traslado de la demanda, de la reconvención y de sus contestaciones.

b) La audiencia a que se refiere el artículo 29.

c) La declaración de rebeldía.

d La citación al acto previsto en el artículo 25.

e) La providencia que declare la cuestión de puro derecho y los traslados a que se refiere el artículo 32, último párrafo.

f) El auto de apertura y recepción de prueba, el de designación de la audiencia de vista de la causa, las cargas procesales que se impongan a las partes y, en su caso, los traslados para alegar por escrito.

g) El traslado de los informes y dictámenes periciales, de los autos que ordenen intimaciones y medidas para mejor proveer.

h) La sentencia definitiva, juntamente con la liquidación a que se refiere el artículo 48.

i) La providencia de "autos" contemplada en el artículo 57 inciso b).

j) La denegatoria de los recursos extraordinarios.

k) Las que hacen saber medidas cautelares, o su modificación o levantamiento.

l) Las resoluciones en los incidentes, las interlocutorias con carácter de definitivas y aquellas otras providencias que, en su caso, se indique expresamente.

Cuando así se lo disponga podrá notificarse por carta documento, por telegrama, por acta notarial o por correo electrónico.

Se tendrá por cumplimentada la entrega de copias si se transcribe su contenido.

En caso que ello resulte imposible o inconveniente, las copias quedarán a disposición del notificado en el Tribunal, lo que así se la hará saber.
Se tomará como fecha de notificación el día de labrada el acta o entrega del telegrama o carta documento, salvo que hubiera quedado pendiente el retiro de copias, en cuyo casos se computará el día de nota inmediato posterior.
Esta última fecha se tomará en cuenta en los supuestos que la notificación fuera por medio electrónico, independientemente que se transcriba o no el contenido de las copias en traslado*."* (la negrita es nuestra)

d) NOTIFICACIÓN POR CORREO ELECTRÓNICO Y LEY DE FIRMA DIGITAL

El art. 143 bis, incorporado al Código Procesal Civil y Comercial de la Provincia de Buenos Aires por la nueva ley, establece:
"Artículo 143 bis: Notificación por correo electrónico. El ***letrado patrocinante o apoderado de la parte que tenga interés en la notificación, el síndico, tutor o curador "ad litem", en su caso, enviará las notificaciones utilizando el sistema de correo electrónico habilitado al efecto por el Poder Judicial, conforme determine la reglamentación****.*
La ***oficina de notificaciones*** *encargada de la base de datos del sistema de comunicaciones electrónicas del Poder Judicial* ***emitirá avisos de fecha de emisión y de recepción a las casillas de correo electrónico de las partes y del Tribunal o Juzgado****.*
El envío de un correo electrónico importará la notificación *de la parte que lo emita."* (la negrita es nuestra)
La ley no lo menciona expresamente, ni era necesario hacerlo, pero el antecedente normativo del sistema de notificaciones judiciales por correo electrónico **es la LFD**.
El RNME dispone en su art. 4º que *"El abogado, el juez o los funcionarios habilitados confeccionarán la cédula y la signarán con tecnología de firma digital.*
Si la cédula fuera confeccionada por el abogado, la misma quedará por 24 horas a disposición del órgano jurisdiccional para ser remitida al servidor del Poder Judicial. Si fuera confeccionada por el juez o el funcionario habilitado, será remitida directamente a dicho servidor*.*
En todos los casos el sistema registrará:
a) la ***fecha y hora en que el documento ingrese al mismo*** *y quede disponible para el destinatario de la notificación;*
b) la ***fecha y hora en las que el destinatario accedió*** *al servidor del Poder Judicial para notificarse;*

*c) la **fecha y hora en las que el destinatario descargó** dicha notificación;*
*d) si la cédula fuera suscripta por el abogado, el sistema también registrará la **fecha en la que la cédula hubiera quedado a disposición del órgano jurisdiccional** para ser remitida al servidor.*
*El funcionario **imprimirá una constancia para ser agregada al expediente, certificando fecha y hora de ingreso al sistema registrada en el servidor."*** (la negrita es nuestra)

Momento en que opera la notificación: Según el art. 5º del RNME, *"La notificación se tendrá por cumplida **el día martes o viernes inmediato posterior** -o el siguiente día hábil si alguno de ellos fuera feriado- **a aquél en el que la cédula hubiere quedado disponible para su destinatario** en el sitio web aludido en el artículo 3o."* (la negrita es nuestra)
De acuerdo al artículo 6º del RNME los funcionarios judiciales intervinientes en el proceso de notificación contarán con certificado digital, que será otorgado por la autoridad certificante del Poder Judicial. En cuanto a las partes y abogados intervinientes, el mismo artículo establece que **estas podrán aportar un certificado digital propio**.
En ese sentido, el artículo siguiente precisa que "*Los Colegios Profesionales **podrán brindar a sus matriculados el servicio de firma digital,** obteniendo de las autoridades pertinentes la habilitación respectiva para actuar como certificadores licenciados (artículo 18, Ley 25.506)."* (la negrita es nuestra). Veremos que, con posterioridad, por un convenio celebrado entre la Suprema Corte bonaerense y el Colegio de Abogados de la Provincia de Buenos Aires se acordó que **los Colegios Departamentales cumplirán funciones de Autoridad de Registro de Firma Digital,** reservándose la Suprema Corte la función de "certificador licenciado".

Recordemos que en un sistema de Infraestructura de Firma Digital, como venimos diciendo, se emiten certificados digitales. Justamente, como decíamos supra, los certificados son otorgados por los "certificadores licenciados". Como también dijimos, cada certificado dispone dos tipos de claves:
Clave pública: es aquella que se utiliza para verificar una firma digital, en un criptosistema asimétrico seguro.
Clave privada: es aquella que se utiliza para firmar digitalmente, mediante un dispositivo de creación de firma digital, en un criptosistema asimétrico seguro.

En este sentido, el 30 de Agosto de 2012, la Suprema Corte bonaerense celebró un convenio con el Colegio de Abogados de la Provincia de Buenos Aires (COLPROBA), que tiene por objeto regular la instrumentación y los mecanismos operativos para la constitución por parte del COLPROBA como Autoridad de Registro de Firma Digital y del Máximo Tribunal bonaerense en su calidad de Organismo Certificador Licenciado. Como puede observarse, por este convenio, los Colegios Departamentales cumplirán funciones de Autoridad de Registro de Firma Digital, reservándose la Suprema Corte la función de "certificador licenciado". En una Infraestructura de Firma Digital, la Autoridad de Registro tiene a su cargo las funciones de validación de la identidad y otros datos de los suscriptores de certificados. Dichas funciones son delegadas por el certificador licenciado.

Imaginemos como funcionará el sistema cuando se encuentre completamente implementado: Por ejemplo, el letrado de la actora, matriculado en el Colegio de Abogados de Morón, cuando notifique a la demandada por correo electrónico, debe firmarlo digitalmente, utilizando su clave privada.

Dicho letrado tiene un certificado de firma digital, otorgado por la Suprema Corte de la Provincia. La identidad y su condición de matriculado fueron validadas por el Colegio de Abogados de Morón, en su calidad de "Autoridad de Registro de Firma Digital". El certificado de firma digital, como ya expresáramos, cuenta con una clave privada, que solo conoce el letrado, y una clave pública, es decir, una clave a la que puede acceder cualquiera. Por su parte, el letrado de la demandada, al recibir la notificación, verificará la autenticidad de la misma utilizando dicha clave pública.

16. Subasta electrónica y transferencia de inmuebles en la Provincia de Buenos Aires

La ley 14238, publicada en el Boletín Oficial del 25 de enero de 2011, sustituyó varios artículos del Código Procesal Civil y Comercial provincial, e incorporó la "subasta electrónica", a través de Internet, en reemplazo de la subasta tradicional.

La nueva norma modificó los artículos 558, 559, 562, 563, 575, 578, 581 y 585 del Código Procesal Civil y Comercial, que integran el capítulo titulado "CUMPLIMIENTO DELA SENTENCIA DE REMATE".

Con la reforma, el nuevo artículo 562 del Código Procesal Civil y Comercial provincial define a la "subasta electrónica" como un ***"proceso interactivo de búsqueda de precio, mediante la***

***puja simultánea entre distintos postores, realizada a través de Internet**, mediante un programa automatizado revestido de **adecuadas condiciones de seguridad**, cuya información se transmite y procesa por medios electrónicos de comunicación, en las condiciones que fije, que deberán indicarse en los edictos y, en su caso, en la propaganda."* (la negrita y el subrayado es nuestro).

El mismo artículo aclara que la subasta se hará en forma "electrónica", cualquiera sea la naturaleza de los bienes a subastar. **Además, se deroga el art. 576, referido al "lugar" del remate.**

En definitiva, se reemplaza el tradicional remate, donde los que desean participar deben concurrir al lugar donde se desarrolla la subasta, por un mecanismo de subasta por internet.

La Suprema Corte de Justicia de la Provincia de Buenos Aires **reglamentará la subasta prevista en el art. 562, estando autorizada a delegar en las Cámaras de Apelaciones la implementación del sistema**. *"**Habilitará una página web** con características de seguridad apropiadas y funcionalidad adecuada a la realización de la subasta electrónica, la que podrá ser utilizada en todos los Departamentos Judiciales. **También establecerá los criterios y procedimientos para que el público en general pueda inscribirse en un registro de postores, que estará abierto de forma permanente, garantizando la seriedad y eficacia de la subasta, así como la sencillez y economía de recursos.**"* (conf. art. nuevo art. 562 CPCCPB, la negrita es nuestra)

Obviamente, uno de los objetivos de la reforma es dar una mayor transparencia a las subastas judiciales y "abrir" las mismas al público en general, buscando evitar la formación de "ligas" de compradores.

El artículo 562 también establece que "*Se podrá exigir el empleo de firma electrónica o de **firma digital** **para validar las ofertas realizadas** y/o **para la suscripción del boleto de compraventa.**"* (la negrita y el subrayado es nuestro)

¿Cuándo debía comenzar el nuevo régimen?

El artículo 3º de la ley 14238 dispone que

*"La presente Ley entrará en vigencia a los **180 días a partir de su publicación**. En ese plazo la Suprema Corte de Justicia de la Provincia de Buenos Aires reglamentará e implementará el procedimiento de subasta electrónica, el cual será aplicable a todas las subastas ordenadas con posterioridad a ese plazo. **Mientras tanto las subastas judiciales se realizarán mediante el anterior sistema**."* (la negrita es nuestra)

Reiteramos que la ley fue publicada en el Boletín Oficial del 25 de enero de 2011.

Por último, en materia inmobiliaria, el 6 de agosto de 2012 la Suprema Corte bonaerense firmó un convenio junto al Colegio de Escribanos y el Registro de la Propiedad para implementar la firma digital entre estas entidades[12]. El objetivo es implementar un sistema por el cual los notarios puedan realizar sus presentaciones (vgr. solicitud de certificados, inscripciones, etc.) obtener las respuestas del Registro (vgr. emisión de certificados, constancias de inscripción, etc.) por vía digital.

****

[12] Ver http://www.scba.gov.ar/institucional/nota.asp?expre=Convenio%20con%20el%20Colegio%20de%20Escribanos%20y%20el%20Registro%20de%20la%20Propiedad%20sobre%20firma%20electr%F3nica (consultado 25/02/13)