La firma digital

Algunas particularidades a observar para su implementación

Aníbal A. Pardini

La utilización de la tecnología en actos de la vida diaria y particularmente en el comercio, ha requerido algo tan simple, como complejo en las transacciones electrónicas: identificar a las partes y asegurar que el documento soporte permanezca inalterado; solo así podrá evitarse el repudio.

Como respuesta a esa necesidad, surge la firma digital, una herramienta cuya interpretación requiere algunos recaudos.

Este trabajo se orienta a quien deba asesorar sobre la incorporación de firma digital al negocio.

La firma digital el surgimiento [arriba]

Desde mediados de los 90, la impresionante masificación de la Tecnología de la Información y de las Comunicaciones, fue aprovechada (y también promovida) por el comercio, el cual adopto ribetes impensados. No solo se optimizó la del esquema tradicional, sino que se introdujeron drásticos cambios de esquemas de comercialización, que permitieron una redistribución de roles en el escenario del comercio. La adopción de la tecnología, conllevó una paulatina migración de soportes: de papel al documento electrónico.

Junto a la sofisticación técnica, transitaba el desconocimiento jurídico o repudio de operaciones cuya fuerza obligacional no había sido contemplada en las diferentes legislaciones, poniendo de manifiesto, a fuerza de fallos, los riesgos asociados a la implementación de canales electrónicos como vehículo transaccional.

Este cambio poco a poco fue mostrando que podría convertirse en el paso a un esquema más riesgoso desde el punto de vista legal (al desconocer el valor jurídico del soporte electrónico, que en el otro esquema, papel, se encontraba tasado), si no se adoptaban los ajustes necesarios para que el nuevo esquema ofreciera, por lo menos, las garantías que ostentaba el anterior. Esto no se lograría, hasta tanto uno no supiera que la persona con la cual contratábamos era quien decía ser y que el soporte de la transacción permaneciera inalterado.

En el esquema “papelizado” de comercio, además, existían numerosas formas de dar fe de dicho extremo a través de la intervención de 3ros quienes a través del poder con el que estaban investidos (funcionarios públicos, fedatarios, etc) podían asegurarlo. Pero en el caso del documento electrónico, no había forma de darle intervención a estos 3ros fedatarios, o 3ros de confianza. Si bien esta necesidad no fue exigida con la sola implementación de los esquemas de comercialización a través de tecnologías de información y comunicación (TIC), no es menos cierto que ello se debió a que estos esquemas funcionaban sobre la base de la costumbre y otros mecanismos que permitían evaluar la confianza del vendedor (calificaciones), como asimismo el monto de cada operación se encontraba en un límite en el cual, el comprador asumía el riesgo, o también, mediante la utilización de “pasarelas de

pago” que se valían de la identificación del plástico (por carácter transitivo), todos ellos insuficientes para evitar el repudio o rechazo del acto.

Cambio de paradigma [arriba]

Frente a este escenario incipiente, existía un mecanismo consolidado (jurídica y culturalmente) en el ámbito tangible, la firma hológrafa , que aseguraba tanto la autenticidad que establece que la persona firmante es quien dice ser, como el no repudio que establece que la persona firmante estuvo de acuerdo con el contenido del documento en el cual se insertó la firma. Por lo tanto, el documento físico firmado hológrafamente, aún hoy es considerado autentico, no repudiable[1] y por lo tanto es un elemento de prueba valido (él elemento por excelencia) en la mayoría de los sistemas legislativos.

Reconocida la necesidad de sortear el escollo que planteaba la tecnología (cuyo diseño se orientó desde su génesis a permitir la conexión, en detrimento de saber con quién se establecía dicha conexión) y teniendo en cuenta al elemento esencial de los actos jurídicos, cual es la manifestación de la voluntad cuya prueba más definitiva se logra través de la firma, es que surge esta herramienta técnico jurídica, la firma digital.

De esta manera, las transacciones que exigen la identificación de una de las partes, y precisan de la inalterabilidad del soporte que contiene la manifestación de una voluntad negocial, requieren de firma digital[2].

No basta tener certeza de quien tenemos en frente (pantalla mediante) sino también hace falta constatar (y poder acreditar en juicio) que ha dirigido (en el caso puntual y ante el acto que se invoca) su voluntad en un sentido u otro en un documento que, una vez confeccionado, debe mantenerse tal cual fue firmado, al menos, hasta que sea apreciado como prueba ante un juez.

La realidad en la cual vivimos, con esta doble dimensión (tangible e intangible[3]), requería que esta herramienta garantizara lo mismo que la firma hológrafa hacía en su dimensión: el no repudio.

Muchos esquemas de comercio electrónico han avanzado supliendo la identificación de las partes a través de la firma con, por ejemplo, las llamadas “pasarelas de pago”. Estas tienen por objeto viabilizar pagos de transacciones electrónicas, y lo cierto es que no alcanzan a ser una alternativa válida al no repudio, ya que si bien intentó “sustituirse” la manifestación de la voluntad negocial, con la identificación de las partes[4], el problema se planteó ante el desconocimiento de la operación[5]. Es en ese caso que se requiere, no de la acreditación del pago, sino de la determinación y atribución del contenido de la voluntad manifestada.

La firma digital surge como un elemento destinado a la dimensión virtual, superador de la firma hológrafa en cuanto a sus características, puesto que a los tradicionales atributos de autenticidad y no repudio, que tenía la manuscrita, se le agregó uno privativo de la firma digital : la integridad.

Un documento firmado digitalmente[6] puede evidenciar mediante el procedimiento de verificación, si dicho documento ha sufrido alteraciones o cambios, posteriores a la firma, garantizándose así que el documento ha

mantenido su integridad. En esto hay que establecer una diferencia, la firma digital no asegura la “inalterabilidad” del documento electrónico firmado digitalmente pero si asegura su integridad. Parece un juego de palabras? Bien, los documentos electrónicos firmados digitalmente pueden ser alterados, pero dicha alteración será evidenciada posteriormente mediante un procedimiento de verificación, y por ende no llegarán a ser íntegros; en cambio los documentos físicos pueden sufrir alteraciones del contenido posteriores a la firma, y las mismas quedaran sujetas a pericias, mas no a una simple verificación.

En este esquema, con carencias que provenían tanto de la tecnología que comunicaba, como del propio documento electrónico que se generaba como resultado, surge como respuesta la firma digital.

Recepción normativa [arriba]

La tendencia reguladora (desde finales de los 90) de la materia, ha encontrado un denominador común, estructural[7] y de técnica[8] sustentado en cuatro conceptos fundamentales: firma electrónica o digital, documento electrónico, certificados digitales y prestadores de servicio de certificación.

Hay normativa diseñada para ser tomada como guía (Ley modelo de UNCITRAL, Directiva Europea[9]) y otras que han sido naturalmente adoptadas (ley de UTAH). Los ordenamientos jurídicos de América Latina, han seguido los estándares de la Ley Modelo de Naciones Unidas[10] y de la ley de Utah, recogiendo de la primera los principios de no discriminación y de equivalencia funcional para los conceptos tradicionales de “escrito”, “firma” y “original”. Esto ha dado un marco de cierta homogeneidad dentro de la diversidad normativa, y también ha permitido con una relativa facilidad la celebración de acuerdos (privados) de reconocimiento reciproco de certificados digitales, lo que permite su uso transfronterizo.

Estas legislaciones, han incorporado o reconocido herramientas que tienen diferente alcance y denominación: firmas electrónicas (simples), firmas digitales y/o electrónicas avanzadas, certificadas o calificadas según la denominación adoptada por cada país.

En general, se parte de la concepción de la firma electrónica como género y de la digital o de la electrónica avanzada como una especie. La diferencia, suele residir en que la firma digital o electrónica avanzada, utiliza de manera prevalente una tecnología más robusta en términos de seguridad[11], un tercero de confianza para su emisión[12] y un procedimiento más riguroso de identificación del titular del certificado de firma digital , lo que se traduce en ventajas jurídicas (aseguran la confiabilidad y apropiabilidad)[13].

Al destacar el contraste entre ambas, se ha sostenido que “la diferencia entre una firma digital y/o electrónica avanzada, certificada o calificada y una firma electrónica simple es que la primera tiene mayor fuerza probatoria, pues no será necesario determinar su confiabilidad y apropiabilidad, gozando de esa presunción, no solo por la tecnología utilizada, sino porque exige la intervención de un prestador de servicios de certificación o entidad de certificación digital, quien compromete su responsabilidad en la identificación inequívoca de una persona en medios electrónicos.”

Es importante distinguirlas, puesto que a cada categoría se adscribe un régimen legal especifico, con presunciones y cargas probatorias diferentes. En nuestra legislación, se ha traducido en dotar a la firma digital de presunciones (autoría Art 7° e integridad Art 8°, Ley 25.506) invirtiendo la carga de la prueba, en el caso de la firma electrónica "Art 5° En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez."

Previo a la sanción de Código Civil y Comercial, algunas interpretaciones habían propiciado cierta confusión sobre la validez y alcance de la firma electrónica respecto de la digital, tal vez por no reparar en la particularidad de cada esquema, o simplemente en el Artículo 1 de la ley[14] que establece un ámbito de aplicación condicionado a la existencia de un certificado digital[15] del cual emana la firma a clasificar y por lo tanto, a la pertenencia o no a una infraestructura[16] que dota de determinados elementos de seguridad que se traducen en ventajas jurídicas.

Dicho de otro modo, según la misma ley, las firmas sean electrónicas (por no satisfacer los requisitos de validez del Art 9°) o digitales deberán ser emitidas mediante certificados digitales (Art 13° y 14°), con lo cual, un pin de un banco, o un usuario de un sistema, no deberían ser considerados firma electrónica a los efectos de esta ley.

Esta es una posición restringida, pero proviene del análisis sistémico de la ley, a diferencia de gran parte de la doctrina argentina, que ha partido de la comparación de los Artículos 5° y 2°, más no la remisión al Art. 9°, que siempre refiere a la existencia de un certificado. Es previsible que la doctrina extranjera arribe a otras conclusiones, puesto que sus esquemas legales son más laxos en algún sentido, al referirse a la firma electrónica, más precisamente.

Hay otras razones que han tratado de ser encontradas en regulaciones posteriores (Decreto 2628/02[17]) que intentan justificar la inclusión de firmas fuera de los certificados (algún inciso, entiendo, avanza por sobre la ley tornándose inconstitucional, lo que tampoco es raro en materia de tecnología[18]).

Esta discusión quedó zanjada con el Art 288 que establece "La firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde. Debe consistir en el nombre del firmante o en un signo.

En los instrumentos generados por medios electrónicos, el requisito de la firma de una persona queda satisfecho si se utiliza una firma digital, que asegure indubitablemente la autoría e integridad del instrumento. "

Esquema de firma digital [arriba]

Es importante repasar como es el funcionamiento del sistema, para comprender algunos "porque".

Básicamente está quien necesita firmar, quien necesita verificar la firma, un tercero de confianza que otorga certificados para firmar, y alguien que controle el sistema.

Nuestro sistema de firma digital es jerárquico[19] por lo que depende del Estado[20] quien controla el sistema en su actuación como autoridad de aplicación del régimen y como Autoridad Certificante Raíz (Autoridad Certificante

administrada por el ente licenciante), constituyendo la única instalación de su tipo y revistiendo la mayor jerarquía de la Infraestructura de Firma digital de la REPUBLICA ARGENTINA.

Asimismo, del régimen participan tanto el sector público, como el privado, en régimen de libre concurrencia.

Una vez aprobados los requisitos de licenciamiento, el ente licenciante emite certificados digitales a las Autoridades Certificantes de los certificadores licenciados[21] para que estos puedan otorgar certificados digitales[22], con los cuales se firman digitalmente los documentos electrónicos o digitales[23].

En este esquema, la Autoridad Certificante Raíz firma un certificado a un certificador licenciado, quien a su vez firma con ese certificado, firma un certificado digital a un suscriptor, quien a su vez puede firmar un documento digital. Pues bien, quien reciba dicho documento, o un tercero, podrán verificar esta cadena de firmas, en lo que se denomina "cadena de confianza", recorriendo, cual línea de endosos, las diversas autorizaciones en jerarquía, hasta llegar al punto de inicio: la Autoridad Certificante Raíz.

La ley que establece este sistema (Ley 25.506), fue reglamentada por el Decreto 2628/02. La decisión administrativa 6/07 aprobó los procedimientos técnicos que permitían implementar el sistema de licenciamiento, es decir, establecía los requisitos que debían satisfacer quienes quisieran ser certificadores licenciados, habiendo sido derogada por la Dec. Adm. 927/14 que además de aggiornar el régimen, introduce conceptos de mucha importancia[24].

La DA 927/14, amplía la noción de "infraestructura de firma digital" es decir el ecosistema donde debe darse el ciclo de vida (otorgamiento, renovación, revocación ya que en nuestra legislación no se prevé la "suspensión") de los certificados digitales mediante los cuales se obtienen las firma previstas en la ley: la digital si cumple con los requisitos del Art 9, o la electrónica si no los cumple (Art 5) pero siempre, para ser consideradas tales, debe estar dentro de esta infraestructura, así dispone

"Art. 14. — Componen la Infraestructura de Firma digital de la REPUBLICA ARGENTINA:

a) El ente licenciante y su Autoridad Certificante Raíz,

b) Los certificadores licenciados, incluyendo sus autoridades certificantes y sus autoridades de registro, según los servicios que presten,

c) Las autoridades de sello de tiempo,

d) Las autoridades de competencia,

e) Los suscriptores de los certificados y

f) Los terceros usuarios, según lo dispuesto en el Anexo I del Decreto Nº 2628 del 19 de diciembre de 2002 y su modificatorio. "

Esto completa la idea del esquema de firma digital.

AUTORIDAD DE REGISTRO Y DE CERTIFICACION

Esta DA 927/14 establece de manera expresa, dos actividades[25] que hacen al iter de la generación de un certificado. Un certificador licenciado, emite certificados digitales (los comercializa), para ello realiza dos tareas (identificar y emitir certificados) que encuentran reflejo en la organización interna que adoptan.

Estos son los llamados "terceros de confianza" quienes brindan seguridad al sistema, al intervenir en el proceso de identificación y generación del certificado digital, garantizando mediante su accionar conforme a procedimientos reglados y contenidos en su política de certificación, que el suscriptor es el único que conoce su clave privada al momento de serle otorgada la firma. Esto separa a la firma digital y la electrónica, de otros métodos de autenticación (que algunos autores asimilan a la firma electrónica) en el cual solo intervienen dos partes: quien otorga el método y quien es usuario. Es este esquema, quien predispone el sistema tiene un permiso superior, que así como le permite "blanquear" la clave, también le permite conocerla, y suplantar la identidad del usuario, si quisiera. Esto, mediante la intervención del tercero de confianza no ocurre.

Para la identificación cuentan con la llamada Autoridad de Registro[26], que no es sino la encargada de la identificación y autenticación del solicitante, verificando tanto su identidad como la documentación que respalda los atributos invocados (por ejemplo la representación legal que invoca respecto de una persona jurídica).

Es importantísimo destacar que la presencia física del solicitante ante el certificador licenciado o sus autoridades de registro, es considerada una "condición ineludible" para el cumplimiento de los trámites necesarios para la emisión del correspondiente certificado digital[27].

Esto halla sentido en que es el último contacto del solicitante con lo que será constitutivo de su "identidad digital" y n puede ser suplido por la intervención de un escribano, tal como dice la normativa citada.

Finalizado dicho proceso de identificación, se requiere la firma de los instrumentos que le garantizan al solicitante una adecuada explicación sobre el alcance de sus derechos y obligaciones respecto del certificado digital que adquiere, cuestión que debe ser realizada a través de un consentimiento libre, expreso e informado del solicitante. Dicho documento (acuerdo de suscriptor) debe estar publicado en el sitio web del certificador licenciado, y formando parte de la política, no puede modificarse, sino a través de un procedimiento administrativo por ante la autoridad de aplicación. En dicho consentimiento, además, debe constar la confirmación por parte del solicitante, de que la información a incluir en el certificado es correcta[28].

La Autoridad de Registro, comunica a la Autoridad de Certificación (ambas del certificador licenciado o autorizadas por este) que debe emitir el certificado digital para el solicitante, desde ahora titular, de acuerdo a la información recabada.

Cabe aclarar que la Autoridad de registro puede estar en una sede, delegada por el Certificador Licenciado, o funcionar de manera móvil[29], siempre previa autorización del ente licenciante.

La actividad del Oficial de Registro de una Autoridad de registro, puede ser sustituida por la intervención de un escribano? Mi respuesta es que no, basada en el Art 34 de la misma decisión administrativa que establece que "La presencia física del solicitante ante el certificador licenciado o sus autoridades de registro, será condición ineludible para el cumplimiento de los trámites necesarios para la emisión del correspondiente certificado digital. "y esto no puede ser dispensado.

El fundamento es sencillo: la actividad de identificación y validación de atributos, debe ceñirse a un procedimiento (que forma parte de la política única de certificación) que puede ser diferente al que realice el escribano, a quien no se le puede imponer, por ejemplo, el deber de satisfacer el consentimiento informado que es una carga impuesta al certificador licenciado.

EL PROCEDIMIENTO DE FIRMADO. EL PROCEDIMIENTO DE VERIFICACION

¿Como se valida una firma digital?

Imaginemos que recibimos un documento electrónico y necesitamos validar la firma contenida en él. Como se procede? "el sistema permite validar la integridad del contenido a través de una operación que funciona básicamente de la siguiente manera:

i. Al efectuarse un procedimiento de firma digital o electrónica avanzada, certificada o calificada, el usuario procede a firmar dando una clave única que está bajo su control lo que le permite acceder al medio de almacenamiento de su firma (USB criptográfica, una tarjeta inteligente o en un medio lógico en su computador).

ii. Seguidamente, el sistema realiza un procedimiento de cifrado del contenido generando un resultado matemático único por documento compuesto por todos los caracteres del mismo, independientemente del número de páginas.

iii. Al intentarse hacer una modificación -por mínima que sea, como por ejemplo, cambiar una minúscula por una mayúscula-, en el proceso de verificación, el sistema revalida el resultado matemático, de detectarse un cambio de carácter, el resultado matemático no será el mismo y advertirá su alteración, por lo que la firma será invalidada.

iv. Si, por el contrario, el documento electrónico firmado se mantuvo inalterado, el proceso de verificación notificará el éxito y corresponderá a un documento totalmente íntegro que nunca podrá ser cuestionado por la contraparte. [30]

Es oportuno recalcar que tal como un pez muta a pescado según se encuentre en el agua o fuera de ella, la firma digital pierde su esencia y características cuando se imprime el documento electrónico que la contiene, ya que el mismo tiene la fuerza probatoria de un papel impreso, sin firma.

La firma digital sustituye a la holografa? [arriba]

Muchos ensayos doctrinarios, basados en la lectura de la ley y de doctrina extranjera, así lo sostienen.

Es correcto pensar en firma digital como en una alternativa a la firma hológrafa para los casos permitidos por la ley 25.506, el C.C. y C y con ese límite.

No es correcto pretender aplicar el régimen de la firma hológrafa al de la digital, y si bien se intenta habitualmente esta operación, entiendo que se corre un riesgo: tratar de asignarle a aquella (digital) todas las características de esta (hológrafa), o pretender que la firma digital tenga respuestas para todos los interrogantes que plantea la firma hológrafa.

En mi opinión no han de asimilarse como sinónimos, por muchísimas razones[31] que exceden este trabajo, pero me permito citar una de tantas: la exposición de motivos de la ley, así lo confirma:

“Una última referencia cabe realizarse. No estamos reglamentando un reemplazo de la firma manuscrita de nuestro Código Civil. Si pensáramos que es así nos equivocamos.”

“Nuestra integración al comercio electrónico global -ya hemos dicho- requiere que sean adoptados instrumentos técnicos y legales con reconocimiento casi universal. Casi todos los países utilizan el término "firma", pero se trata de echar mano a un vocablo y no a un concepto literal.

Menos que menos si se trata del concepto de firma ológrafa. Alemania utiliza para la certificación digital el término "sello" con la idea de evitar confusiones. Por eso, la "firma digital " no debe ser limitada a pensarse como reemplazo de la manuscrita. Hemos explicado que sus efectos son diferentes tanto como los principios en que se asienta.”[32]

Dicho esto, cabe agregar que la “equiparación” entre ambas lo es solo en cuanto a su funcionalidad, y acotada al ámbito que le reservan, tanto el C.C.y C.[33] como la misma ley de firma digital [34], no a los regímenes establecidos para su uso.

Entre los motivos que pueden llevar a confusión, se encuentra:

1- La ley Modelo de la UNCITRAL incorpora el concepto de equivalencia funcional. El sentido de este tratado no fue anular a la firma hológrafa, ni al papel, sino crear un espacio para el desarrollo de estas alternativas. Es cierto que el tiempo puede llevar a que lo preponderante sea el uso de la firma digital, pero mientras tanto hay respuestas que el derecho tiene que dar en un marco de seguridad jurídica, y existen normas para hacerlo, con lo cual serán los criterios para su aplicación los que deban pulirse.

2- Que la firma hológrafa ha sido quien ocupara el papel preponderante en el modo en que se perfeccionaban los contratos, aunque no el único (algunos contratos se perfeccionan sin firma - transporte, remate).

Prefiero entender que la firma digital brinda un sistema alternativo, originado por una necesidad del tráfico comercial, que recibido legalmente, viene a ser una herramienta con características que pueden asimilarla a la firma hológrafa y sustituirla en algunos casos, mas no tienden a cumplir el mismo rol, ya que algunas

cuestiones, tanto contextuales (papel, Art 4 ley 25.506) como conceptuales (testamento), no permiten dicha sustitución.

Las exclusiones previstas en el Art 4° de la ley 25.506, si se quiere, refuerzan esta idea. En esto pienso distinto que Lorenzetti (lo que a él seguramente no le quita el sueño) que los motivos por los cuales se plantean estas respondan a que "la firma digital tiene su campo principal de utilidad en las relaciones comerciales entre empresas, y por ello el legislador excluye de su aplicación[35]" a determinados actos. En mi parecer, responde a que la firma hológrafa tiene una asociación intrínseca con el firmante, nadie puede "compartir" su firma con otra persona. En el caso de la firma digital, mientras la clave privada se encuentre bajo el absoluto control del firmante (Art 4°información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control) y hasta tanto se haya solicitado a la autoridad de registro la revocación por tal motivo, los efectos jurídicos del acto otorgado le son atribuibles. Podría interpretarse, que a diferencia de otras legislaciones que han incluido el término "posesión" y "privada", abren la puerta para la referencia al absoluto control puede incluir a sistemas[36] o a otras personas diferentes al firmante, quien podría otorgar un acto cuyos efectos le serían atribuibles al titular del certificado[37]. Ese sería el motivo por el cual, la categoría de actos contemplados en el Art 4° tienen que ver con lo más íntimo de una persona y por ende quedan excluidos.

Firma digital, firma electronica, metodos de autenticacion [arriba]

Así como dato, información y conocimiento (cada uno de ellos con un régimen jurídico diferente) suelen ser utilizados como sinónimos, puede plantearse una confusión al referirnos sin cuidado a firma digital, electrónica o un método de autenticación, también con regímenes jurídicos diferentes.

La construcción del concepto de firma digital se realiza a partir de la satisfacción de requisitos técnicos y jurídicos. No pueden existir unos sin los otros. Es más, puede disponerse de tecnología más sofisticada que la requerida por el Estado para la firma digital, y si no se complementa con el requisito jurídico no estamos en presencia de firma digital [38]

Entender esto es muy importante, porque la construcción de este concepto conlleva a que sea interpretado no solo desde la lectura de la ley, sino desde la comprensión de esquemas técnicos de funcionamiento que a su vez determinan una realidad sobre la cual funciona la firma digital. Esta realidad puede presentar características que condicionan su posibilidad de ser aplicada y por ejemplo, pueden relegar el uso de firma digital o de firma hológrafa por su incompatibilidad con el ámbito. Contrario sensu, pretender una aplicación de plano del régimen que regula a la firma hológrafa, a la firma digital, sería un grave error (aunque muchos autores han caído en la tentación) ya que las realidades para las cuales están diseñados ambos regímenes no son iguales[39]. Piense solamente en esto: en el ámbito digital no hay originales y copias de un documento firmado digitalmente. Son tantos originales como copias se hagan de él. Esto impide, por ejemplo, que algunos regímenes (títulos de crédito) sean de incompatible aplicación.

Para diferenciar a la digital de la electrónica, hay que partir de nuestra ley. La misma ley presupone la existencia de un certificado digital[40] válido[41] para firmar. Si la firma emitida mediante dicho certificado, satisface los requisitos previstos en el Art 9°, es decir "a) Haber sido creada durante el período de vigencia del certificado digital válido del firmante; b) Ser debidamente verificada

por la referencia a los datos de verificación de firma digital indicados en dicho certificado según el procedimiento de verificación correspondiente; c) Que dicho certificado haya sido emitido o reconocido, según el artículo 16 de la presente, por un certificador licenciado"., será firma digital y gozará de las presunciones previstas en los Arts. 7°[42] y 8°[43], caso contrario será electrónica.

Todo lo que se "firme" prescindiendo de un certificado digital, será un método de autenticación[44] de un usuario (no necesariamente una persona) frente a un sistema. Puede darse sin la necesidad de satisfacer algún estándar tecnológico determinado, y sobre un esquema predisponente-usuario. (Sin la intervención de terceros).

Este mecanismo por existir por fuera de una infraestructura determinada (la IFDRA precisamente), carece de la posibilidad de que le sea aplicado el régimen previsto por la Ley 25.506, debiendo buscarse la regulación de sus efectos, en el C.C.C. (Art 287 precisamente) ó en los acuerdos que hayan celebrado las partes para asignarles trascendencia jurídica[45].

Hay una tesis interpretativa para diferenciar la firma digital de la electrónica, que se basa en partir del concepto de firma electrónica previsto en el art 5to de la ley 25.506.

Es interesante repasar el argumento que nos acerca un verdadero maestro del derecho como lo es Eduardo Molina Quiroga. El trabajo[46] se refiere al valor de los documentos electrónicos, y lo interesante es repasar cual es el argumento que utiliza tanto para clasificarlos, como para asignarles valor probatorio. "Luego de la sanción de la ley 25.506, podemos distinguir tres clases de documentos electrónicos: a) los que tiene firma digital , cuyos requisitos de validez establece el art. 9º de dicha norma, y en la actualidad son de difícil aplicación(al momento del artículo, no habían certificadores licenciados privados); b) los que tienen firma electrónica, que está definida en el art. 5º de la ley 25.506 y c) los que carecen de cualquiera de estos elementos, y que llamaremos mensajes no firmados, especie compuesta por todos aquellos mensajes de correo electrónico que se envíen sin utilizar métodos de protección de datos.

Aquí se plantea el problema respecto a su equivalencia funcional y su eficacia jurídica. En general, los autores coinciden en que la validez probatoria del correo no firmado es bastante pobre, debido básicamente a dos cuestionamientos: por una parte, que no cuenta con las medidas de seguridad de la firma digital, que aseguran la autenticidad, la integridad, la autoría y el no repudio. Por otro lado, se afirma que estando a disposición el mecanismo de la firma digital –o, llegado al caso, electrónica– no corresponde otorgar eficacia al documento digital que no contenga ninguna de ambas.

Respecto a la equivalencia funcional, el correo simple ha sido asimilado tanto a un instrumento particular no firmado, cuanto a la correspondencia epistolar."

Al referirse al valor probatorio de los correos electrónicos "Algunos autores consideran que el correo electrónico simple, tal como lo hemos conceptuado al decir que se trata de aquel enviado sin tomar ninguna medida de seguridad adicional a las establecidas por el propio sistema de correo electrónico (es decir, el nombre de usuario y contraseña), no consiste en una tercera categoría distinta

del documento con firma digital y del documento con firma electrónica, si no antes bien se identifica plenamente con este último.

Para sostener esta tesitura, se parte de la base de que el art. 5 de la ley 25.506 define a la firma electrónica como 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". De allí que cuando se utiliza un mecanismo de autenticación distinto al previsto por ley para la firma digital, no importa cuál sea, nos hallamos frente a una firma electrónica. Y el correo electrónico simple funciona bajo el sistema de nombre de usuario y contraseña, con lo cual entraría en la categoría de documento con firma electrónica. Siendo así, será equivalente per se a un instrumento privado, siempre que el juez admita el razonamiento efectuado.

Estimamos que una recta interpretación de la ley de firma digital permite entender que la firma electrónica a la que se refiere consiste en la utilización de una técnica de protección que, sin ser la de la firma digital, asegure razonablemente la autenticidad e integridad del mensaje; como así también la aplicación de la firma digital cuando se carezca de alguno de sus requisitos. No parece que ninguno de ambos casos se presente en el correo electrónico simple en sí mismo, ya que aún aceptando que el mecanismo de usuario y contraseña pueda asegurar la autoría del mensaje, el hecho de no contar con ningún método de seguridad en la elaboración y emisión del mensaje que sea verificable impide asegurar que el contenido del documento no ha sido modificado luego de su emisión. Desde otro punto de vista, la aceptación sin más de la tesis mencionada, parecería identificarse con la simple presentación de una impresión, con los problemas que esto trae aparejado y que han sido brevemente expuestos arriba.

Por ello, los mismos autores sostienen que "de nada sirve que un e-mail sea confirmado desde el punto de vista sustancial como poseedor de validación como prueba en juicio al haber sido constatada su autenticidad, si dicho correo no pudo ser debidamente adquirido por el proceso mediante su adecuada prueba por conducto de los medios probatorios correspondientes. O, siguiendo un razonamiento lógico, el juzgador nunca llegará a analizar la autenticidad de un e-mail si no fue, previamente, debidamente probado en juicio. Además de la validación de la copia impresa, es necesario aportar al juez información respecto de los mecanismos de almacenamiento y conservación utilizados". De esta forma, se estaría acudiendo a una prueba compleja o combinada, utilizando elementos diversos para generar la convicción del juzgador. "

La firma digital está tomando día a día más protagonismo en la vida diaria, en breve comenzaran a parecer conflictos que van a requerir la utilización fluida de conceptos solidos sobre la materia.

La ley de firma digital, tiene una particularidad, es muy explícita. Tal vez por ello este trabajo se orientó a sugerir elementos que permitan alimentar al sentido crítico que se debe disponer al momento de leer la ley.

Notas [arriba]

[1] El repudio generalmente va asociado a la carga de la prueba, es decir, quien alega la autenticidad, una vez desconocida en juicio debe correr con la prueba de la misma. En el sistema de firma digital, como se verá, esta carga se invierte debiendo quien niega la validez de la firma, correr con la prueba de tal aseveración
[2] Esta denominación varía según el país de que se trate pudiendo ser: firma digital o electrónica avanzada, certificada o calificada.
[3] Prefiero utilizar esta concepción unicista, a la usual contraposición de "mundo virtual y mundo real", puesto que real es el mundo en el cual vivimos y hacemos negocios, ya sea en la dimensión tangible (papel) como intangible (documentos electrónicos).
[4] Mejor dicho, valerse de la identificación de las partes (o de una de ellas) realizada por la tarjeta de crédito mediante la cual se efectúa el pago, para sustituir una manifestación de voluntad.
[5] Un ejemplo para traer a colación es del ámbito laboral, el pago de haberes por medios electrónicos. Una cuestión es "acreditar el pago", lo que puede hacerse con el comprobante de la transferencia bancaria, ahora bien, ello no suple la puesta a disposición de la "liquidación del haber", ya que pueden cuestionarse los rubros que la componen. Llevado al absurdo, acreditar el pago de más cantidad de sueldo, no eximiría la conformidad con la "liquidación" ya que por ejemplo, algunos rubros pueden ser no remunerativos.
[6] Básicamente el proceso de firma funciona de la siguiente manera: El firmante proporciona a un sistema, información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control (art 2, ley 25506). Seguidamente, el sistema ejecuta un procedimiento matemático que contiene tres términos: una clave pública, el contenido del documento reducido a números binarios, y la clave privada del firmante (punto anterior) lo que genera un resultado matemático único por documento. Si se modifica el documento (por mínimo que sea) esto impacta en uno de los términos que intervienen en el procedimiento matemático, alterando su resultado y evidenciando la alteración. Si, el documento electrónico firmado no se alteró, en el proceso de verificación se evidenciara tal coincidencia, la que se traducirá en la integridad del documento, que no podrá ser repudiado.
[7] Casi todas tratan firma, documento, certificados y prestadores e infraestructura.
[8] Estableciendo principios mínimos y delegando a las autoridades la reglamentación que permite menor obsolescencia legislativa, frente al avance tecnológico, como asimismo la utilización de lenguaje tecnológicamente neutro.
[9] Directiva 1999/93/CE del Parlamento Europeo y del Consejo del 13 de diciembre de 1999
[10] ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU). Ley Modelo sobre comercio electrónico de la Comisión de la Naciones Unidas para el derecho mercantil internacional (CNUDMI – UNCITRAL) 1996 – 2005. "Principio de no discriminación (Art. 5). No se privará de efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensajes de datos electrónicos y no en soporte de papel." Criterio de "equivalencia funcional" (Arts. 6, 7 y 8) Determinando qué función básica cumplen los requisitos formales de la documentación en soporte de papel, cumplidos los mismos por un mensaje de datos se le podrá atribuir un reconocimiento legal equivalente.
[11] Tecnología de clave púbica asimétrica en nuestro caso.
[12] En nuestro caso un certificador licenciado, que puede provenir del ámbito público como privado mediante su licenciamiento.
[13] Fundamentos de la firma digital y su estado del arte en América Latina y el

Caribe, SELA, SP/Di N° 7-12.
[14] ARTICULO 1º — Objeto. Se reconoce el empleo de la firma electrónica y de la firma digital y su eficacia jurídica en las condiciones que establece la presente ley.
[15] Articulo 13 y 14 Ley 25506.
[16] ARTICULO 26. — Infraestructura de Firma Digital. Los certificados digitales regulados por esta ley deben ser emitidos o reconocidos, según lo establecido por el artículo 16, por un certificador licenciado.
[17] En los casos contemplados por los artículos 3°, 4° y 5° de la Ley N° 25.506 podrán utilizarse los siguientes sistemas de comprobación de autoría e integridad:
a) Firma electrónica,
b) Firma electrónica basada en certificados digitales emitidos por certificadores no licenciados en el marco de la presente reglamentación, (Inciso sustituido por art. 5° del Decreto N° 724/2006, B.O. 13/6/2006)
c) Firma digital basada en certificados digitales emitidos por certificadores licenciados en el marco de la presente reglamentación,
d) Firma digital basada en certificados digitales emitidos por certificadores extranjeros que hayan sido reconocidos en los siguientes casos:
1. En virtud de la existencia de acuerdos de reciprocidad entre la República Argentina y el país de origen del certificador extranjero.
2. Por un certificador licenciado en el país en el marco de la presente reglamentación y validado por la Autoridad de Aplicación.
[18] En oportunidad del dictado del acuerdo reglamentario 1363, el TSJ de Córdoba estableció la adopción del expediente electrónico, el cual "Se conformará con documentos electrónicos y/o digitales firmados digitalmente por magistrados y funcionarios del Poder Judicial (Acuerdo Reglamentario No 882, Serie "A" del 17/5/07 y Resolución N° 1, dictada por el Presidente de la Sala Civil y Comercial del Tribunal Superior de Justicia el 15/04/2013), documentos electrónicos y/o digitales firmados electrónicamente por abogados del foro local y documentos digitalizados de terceros incorporados por el Juzgado o por los abogados bajo las pautas técnicas especificadas en el Anexo. Los documentos digitales que los abogados incorporen al expediente digital para formular sus peticiones ante el Juzgado, se considerarán firmados electrónicamente mediante la utilización del usuario y clave de identificación personal suministrados por el Tribunal Superior de Justicia"
[19] A diferencia de los sistemas basados en la confianza de entidades de renombre (utilizados en USA, por ejemplo)
[20] ARTICULO 29. — Autoridad de Aplicación. La autoridad de aplicación de la presente ley será la Jefatura de Gabinete de Ministros
[21] ARTICULO 17. — Del certificador licenciado. 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.
[22] ARTICULO 13. — Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.
[23] ARTICULO 6º — Documento digital. 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.
[24] DA 927/2014, cambia el sistema de licenciamiento por política, por el de política única, con lo cual un certificado de firma digital sirve para firmar

cualquier tipo de documento (con las excepciones del CCC y del Art 4° de la ley 25.506) y además se reconocen servicios relacionados con la Firma Digital. Art. 12. — Los certificados digitales emitidos por certificadores licenciados, en el marco de la Infraestructura de Firma Digital de la REPUBLICA ARGENTINA, podrán ser utilizados por sus titulares para firmar digitalmente cualquier documento o transacción, pudiendo ser empleados para cualquier uso o aplicación, como así también para autenticación o cifrado. Art 10. — Para la prestación de otros servicios en relación con la firma digital se utilizarán:
a) Certificados de aplicaciones, definidos como aquellos que tienen la finalidad de identificar a la aplicación o servicio que firma documentos digitales o registros en forma automática mediante un sistema informático programado a tal fin.
Los certificados digitales que permitan identificar en forma fehaciente en internet o cualquier otra red informática, a los servidores que establezcan conexiones seguras, son también certificados de aplicaciones.
b) Sellos de tiempo, siendo éstos los que indican fecha y hora cierta, asignadas a un documento o registro electrónico.
c) Sellos de competencia, definidos como aquellos que acreditan competencias o roles, relaciones laborales o cualquier otro atributo de su titular.
[25] Las funciones son más y están previstas tanto en la ley como en el Dec 2628/02 y completados por la DA 927/14.
[26] Art. 33. — Las autoridades de registro son las entidades facultadas por los certificadores licenciados para cumplir las funciones establecidas en el artículo 35 del Decreto Nº 2628/02, bajo la responsabilidad de dichos certificadores licenciados.
[27] Art. 34. — La presencia física del solicitante ante el certificador licenciado o sus autoridades de registro, será condición ineludible para el cumplimiento de los trámites necesarios para la emisión del correspondiente certificado digital.
[28] DA 927/14. Art. 26. — Para la emisión de certificados, los certificadores licenciados y/o sus autoridades de registro, deberán contar con el consentimiento libre, expreso e informado del solicitante, el que deberá constar por escrito.
En este consentimiento debe constar la confirmación por parte del solicitante, de que la información a incluir en el certificado es correcta. El certificador licenciado no podrá llevar a cabo publicación alguna de los certificados que hubiere emitido sin previa autorización de su correspondiente titular, sin perjuicio de lo dispuesto en el artículo 19, inciso f) de la Ley Nº 25.506.
[29] Art. 37. — Las autoridades de registro podrán desarrollar su actividad en puestos móviles, previa autorización del ente licenciante solicitada por el certificador licenciado, encontrándose también alcanzadas por las auditorías mencionadas en el artículo 35 y debiendo cumplir la normativa aplicable a la materia.
El certificador podrá solicitar autorización para funcionar bajo esa modalidad para una o varias de sus autoridades de registro o bien podrá requerirla para una autoridad de registro que funcionará exclusivamente bajo esa modalidad.
[30] Fundamentos de la firma digital y su estado del arte en América Latina y el Caribe, SELA, Secretaría Permanente del SELA, Caracas, Venezuela Mayo de 2012 SP/Di N° 7-12
[31] Hay condiciones de ámbito (electrónico) soporte, y modo de relacionamiento que determinan un escenario diferente.
[32] Dictamen de la Comisión Cámara Revisora: Cámara de Senadores, Orden del día: 1033/2001
[33] Código Civil y Comercial, ARTÍCULO 288.- Firma. La firma prueba la autoría de la declaración de voluntad expresada en el texto al cual corresponde. Debe consistir en el nombre del firmante o en un signo.
En los instrumentos generados por medios electrónicos, el requisito de la firma de

una persona queda satisfecho si se utiliza una firma digital, que asegure indubitablemente la autoría e integridad del instrumento.
[34] 25.506, ARTICULO 3º — Del requerimiento de firma. Cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia.
ARTICULO 4º — Exclusiones. Las disposiciones de esta ley no son aplicables:
a) A las disposiciones por causa de muerte;
b) A los actos jurídicos del derecho de familia;
c) A los actos personalísimos en general;
d) A 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.
[35] Comercio Electrónico, Ricardo L. Lorenzetti, Abeledo Perrot, Pag 83
[36] Actualmente mediante certificados de aplicación, también puede programarse a un sistema para que firme digitalmente de manera automática.
[37]http://www.lynch-abogados.com.ar/Publicaciones/IT_TIC/DigSignature/FirmDig2002-7Ene02.pdf. "Información de exclusivo conocimiento del firmante: aquí la ley incorpora conceptos equívocos para lo que debe ser una clara definición conceptual, más propios de recomendaciones que de la naturaleza de un instituto. Requiere información que en la generalidad de los casos supone que sólo pertenece a la esfera del exclusivo conocimiento de quien quiere firmar. ¿Significa esto acaso que si la información no es 'del exclusivo conocimiento del firmante' no hay firma digital? Creo que no es así y sólo debe ser susceptible de conocimiento exclusivo, pero el que lo comparta no le quita ese carácter. Encontrándose ésta bajo su absoluto control: aquí cabe la misma observación del anterior; esto es una recomendación, pero no integra la definición. Debe ser de su conocimiento exclusivo y estar 'bajo su absoluto control'. Esto supone tener en todo momento la posibilidad de su utilización, sin depender de terceras personas, pero el que el firmante resuelva compartirlo, nuevamente no quita el carácter de firma digital"
[38] Tal como ocurre con los certificadores extranjeros que no han sido reconocidos en nuestro país. (Art 16 Ley 25.506)
[39] Antecedentes similares existieron cuando se quiso asimilar el régimen de la correspondencia epistolar al email (por ejemplo en el caso del periodista Jorge Lanata, previo al dictado de la ley 26.388).
[40] ARTICULO 13. — Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.
[41] ARTICULO 14. — Requisitos de validez de los certificados digitales. Los certificados digitales para ser válidos deben:
a) Ser emitidos por un certificador licenciado por el ente licenciante;
b) Responder a formatos estándares reconocidos internacionalmente, fijados por la autoridad de aplicación, y contener, como mínimo, los datos que permitan:
1. Identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única;
2. Ser susceptible de verificación respecto de su estado de revocación;
3. Diferenciar claramente la información verificada de la no verificada incluidas en el certificado;
4. Contemplar la información necesaria para la verificación de la firma;
5. Identificar la política de certificación bajo la cual fue emitido
[42] ARTICULO 7º — Presunción de autoría. Se presume, salvo prueba en contrario, que toda firma digital pertenece al titular del certificado digital que permite la

verificación de dicha firma.
[43] ARTICULO 8º — Presunción de integridad. 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
[44] Operación que permite identificar a un usuario (no necesariamente vinculado a una persona identificada) ante un sistema de información.
[45] En esta categoría es muy amplia; pueden incluirse a los contratos de EDI (transferencia electrónica de datos) y a los bancarios (cajeros automáticos y home banking) que precisan de un instrumento jurídico celebrado de manera previa, que defina el alcance, definiciones técnicas (se entenderá por firmante, etc) le otorgue trascendencia jurídica y le reconozca entidad al sistema, como también aquellos con una validación simple a través de la remisión de un mail, que otorguen el acceso a un sistema.
[46] Eficacia probatoria de los correos y comunicaciones electrónicas,

© Copyright: Universidad Austral