# *La firma digital y las "apostilles"**

**Por Marcela A. Labrouve**

## 1. Introducción

Generalmente, el nacimiento de una rama jurídica surge a consecuencia de los cambios sociales que se ven reflejados en las soluciones normativas con el transcurso de los años. Pero, en el caso del derecho informático no hubo ese transcurrir del tiempo, el cambio fue brusco y en poco tiempo, como consecuencia del impacto de la informática en la sociedad.

En cuanto a la comunicación se ha vislumbrado un nuevo mercado: el comercio electrónico, explotando la capacidad del contacto sin necesidad del traslado físico de cosas ni de personas; y desde el punto de vista del almacenamiento de la información podemos afirmar que hemos pasado del soporte papel al documento electrónico, como soporte que contiene la información.

### a) Documento electrónico

Tradicionalmente, el documento se ha entendido como un cuerpo físico que contiene información susceptible de ser percibida por los sentidos. Sin embargo, hoy nos tenemos que separar un poco de la "materialidad" del soporte para darle cabida al *revolucionario documento electrónico*.

En los soportes electrónicos, al igual que los cartulares, se recogen los pensamientos, locuciones o hechos del ser humano, incorporándolos en su contenido, tendiente a representar la realidad de los hechos.

Además, su contenido es también escrito, pero dicha escritura –por sus particularidades tecnológicas– no puede ser leída por el hombre sin la ayuda de un decodificador que normalmente es una computadora.

Que el documento sea electrónico, no obstante que su configuración o elaboración está circunscrita a métodos tecnológicos cuyo contenido pudiera concentrase o almacenarse para su resguardo en dispositivos distintos al común del papel, no desvirtúa su composición documental como tal, pues es allí en donde se concentra la posibilidad tangible de trasladar, objetivizar y lograr la inmediatez de su contenido, independientemente de las funciones prácticas de su creación y las formas de su utilización.

Técnicamente, el documento electrónico es un conjunto de impulsos eléctricos que contienen información y que recayendo en un soporte susceptible de almacenarlo (CD, disquete, disco rígido de una computadora, etc.), una vez sometidos a un proceso determinado (a través del computador), permiten su decodificación al lenguaje natural a través de una pantalla o una impresora.

* Bibliografía recomendada.

Pero un documento electrónico es fácilmente alterable, además, no puede determinarse quien fue su autor, por lo tanto son documentos digitales que por sí solos no son aptos para ser utilizados en circuitos administrativos no repudiables.

Un *e-mail*, por ejemplo, se divide en "paquetes" diferentes que luego se vuelven a unir cuando llegan al destinatario. En ese proceso el documento puede ser alterado.

Por esto, tenemos que hablar de la seguridad, y respecto de ello encontramos varios problemas a superar:

*1*) la identidad del autor de la información;

*2*) la integridad de la información;

*3*) la fiabilidad del soporte digital;

*4*) la inalterabilidad;

*5*) la perdurabilidad;

*6*) la privacidad, y

*7*) la confidencialidad de la información transmitida y almacenada.

Para superar los problemas de seguridad se crearon diferentes mecanismos de autenticación.

**b) Mecanismos de autenticación**

Es aquel medio técnico específico que nos permite identificar con seguridad determinada cosa o persona.

Dentro de estos mecanismos de autenticación –en el medio que nos ocupa– encontramos como género las *firmas electrónicas*, que son cualquier tipo de sistema, por ejemplo, las firmas escaneadas, o los métodos biométricos (como el iris y las huellas digitales) las cuales pueden estar limitadas por ciertos parámetros; y como una especie de éstas encontramos a la *firma digital*, que se basa fundamentalmente en la criptografía asimétrica, como método de codificación.

Una firma digital es un bloque de caracteres que acompaña a un documento (o fichero) acreditando quién es su autor (autenticación e identificación) y que no ha existido ninguna manipulación de los datos con posterioridad a su envío (integridad).

Para firmar un documento digital, su autor utiliza su propia clave secreta (sistema de criptografía asimétrica), a la que sólo él tiene acceso, lo que impide que pueda después negar su autoría (no revocación o no repudio). De esta forma, el autor queda vinculado al documento de la firma.

Por último, la validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

En la criptografía asimétrica, la clave de encriptado se denomina "clave privada" y es mantenida secreta por el firmante, mientras que la clave de desencriptado 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 (manuscrita, digital).

Entonces, el sistema de la firma digital garantiza el no repudio del documento digital, permite detectar cualquier alteración e identificar fehacientemente al autor por medio de un sistema criptográfico extremadamente seguro.

### c) Infraestructura de firma digital

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

Ahora bien, para poder firmar digitalmente se necesitan un par de claves, que son individuales y se obtienen utilizando un programa en la computadora.

Este par de claves son dos números relacionados entre sí, de más de 500 cifras cada uno, que se generan por única vez. Una de ellas pasa a ser pública y la otra se mantiene privada. Sería como un rompecabezas de dos piezas.

Estas claves que genera el programa son hechas por medio de un algoritmo, entendido éste como un conjunto de pasos matemáticos que se han de seguir para resolver un problema. En este caso el problema a resolver es el “mensaje” contenido en el documento electrónico.

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 éstos valor legal y haciéndolos oponibles a terceros.

Desde el ámbito privado la utilidad de una infraestructura de firma digital es inmensa.

### d) 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 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.

En cuanto a la firma digital se deben tener en cuenta tres conceptos básicos:

1) *Integridad*. Se refiere a 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.

2) *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.

3) *Perdurabilidad*. 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. El disco rígido de una computadora no es un medio inalterable de almacenamiento, pero demuestra excelentes características de perdurabilidad 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).

## 2. Las apostillas

La *apostille* es un documento o certificado anexo al documento original notarizado o al documento que se encuentre certificado (copia certificada).

En el caso de documentos notarizados, mediante la *apostille* se verifica que la persona que lo ha notarizado se encuentra autorizada para hacerlo en el momento de la notariarización.

En el caso de documentos o instrumentos registrados o asentados por dependencias gubernamentales, certificados por las mismas, con la *apostille* se verifica que la persona que expidió el documento es o era funcionario designado en el Estado del que se trate, facultado para expedir la certificación.

La República Argentina es Estado signatario de la Convención para la Supresión de Legalizaciones de Documentos Públicos Extranjeros, firmado en La Haya el 5 de octubre de 1961, desde su ratificación por ley 23.458, que se refiere específicamente a las *apostilles*.

### a) Documentos públicos

En el marco de la Convención citada se consideran “documentos públicos”[1] –susceptibles de apostillado– a los siguientes:

[1] Art. 1° de la Convención para la Supresión de Legalizaciones de Documentos Públicos Extranjeros, La Haya, 1961.

*1*) Los documentos emitidos por una autoridad o un funcionario perteneciente a un tribunal del Estado, incluso los extendidos por un fiscal de justicia (sentencias judiciales, laudos arbitrales, oficios, exhortos, mandamientos, etc.).

*2*) Los documentos administrativos (partidas de nacimiento, actas de defunción, actas de matrimonio, etc.).

*3*) Las actas notariales (escrituras traslativas de dominio, testamentos, actas, poderes, etc.).

*4*) Las certificaciones oficiales en documentos firmados por personas privadas, tal como la certificación del registro de un documento o de una fecha determinada y la autenticación de firmas en documentos de carácter privado (contratos en general, certificados laborales, escolares, etc.).

No obstante, la Convención especifica que no será aplicada "a los documentos extendidos por funcionarios diplomáticos o consulares" ni "a los documentos administrativos relacionados directamente con una operación comercial o aduanera".

La legalización a la que se refiere la Convención "sólo consistirá en la formalidad por la cual los funcionarios diplomáticos o consulares del país en cuyo territorio deba ser presentado el documento, certifican la autenticidad de la firma, el carácter con que actuó el signatario del documento y, de corresponder, la identidad del sello o timbre que lleva el documento"[2].

De acuerdo al art. 5° "la acotación deberá dar fe de la autenticidad de la firma, del carácter con que el signatario haya actuado y de corresponder, de la identidad del sello o el timbre que lleva el documento".

Asimismo, cada Estado contratante designará a aquellas autoridades con competencia para efectuar las acotaciones previstas por la Convención, notificando tal designación y toda modificación a la autoridad prevista por el mencionado instrumento internacional[3], las cuales deberán llevar un registro *ad hoc* en el que volcarán los datos necesarios de las acotaciones que realicen.

## 3. Aplicación de la firma digital al procedimiento de "apostilles"

Este trabajo no busca de ningún modo la derogación del procedimiento de *apostilles* previsto por la Convención de La Haya de 1961, sino la adecuación del mentado documento internacional a la realidad social y jurídica de la actualidad.

En la nueva era digital, donde ya son un hecho, por ejemplo, los cibertribunales virtuales –en el cual cotidianamente se realizan innumerables contratos y transacciones comerciales vía Internet– viene a quedar obsoleto el trámite internacional de las *apostilles* como hasta ahora se ha desarrollado.

La propuesta concreta, que por este medio venimos a plantear, busca adaptar el marco legal instaurado internacionalmente a las nuevas tecnologías e incluir como medio de certificación –de aquellos documentos (que para este tipo de certificación deberán ser "digitales") susceptibles de apostillado– a la firma digital, como mecanismo de autenticación válido y jurídicamente ya aceptado.

[2] Art. 2° de la Convención.
[3] Art. 6° de la Convención.

Resulta obvio que en ciertos documentos, en los que por su forma extrínseca necesaria (p.ej., los formularios 08 para la transmisión de dominio de los automotores), será de aplicación imposible la firma digital –al menos por ahora y mientras se mantengan dichas exigencias– como mecanismo de autenticación; pero en cambio, hay otros documentos en los que podemos vislumbrar su capacidad para ser susceptibles de certificación digital utilizando como medio a la firma digital.

Por ejemplo, las contrataciones *on line*, las sentencias y laudos arbitrales dictados por los cibertribunales anteriormente citados y porqué no –si nos adelantamos un poco en el tiempo– los exhortos, los oficios y hasta las sentencias dictadas por los magistrados de los juzgados, tribunales, cámaras y cortes (que hoy podemos consultar desde la sede de tribunales por medio de una computadora) en un futuro no muy lejano van a llevar inserta la correspondiente firma digital del o de los autores de las mismas y habrán pasado del soporte papel al soporte digital sin que por ello pierdan su fuerza ejecutoria y su legalidad.

**a) Implementación**

De acuerdo a las disposiciones del Ministerio de Relaciones Exteriores Comercio Internacional y Culto de nuestra República, en general el trámite usual de *apostille* es el siguiente:

*1*) Solicitar ante quien corresponda el documento público o privado a legalizarse por medio del procedimiento de apostillas.

*2*) Autentificar la firma original de dichos documentos ante un notario público (cabe aclarar que en el caso de los notarios, en cumplimiento de lo dispuesto por el Convenio firmado el 2/7/97 por el Ministerio de Relaciones Exteriores, Comercio Internacional y Culto y los colegios notariales de la República Argentina cada colegio de escribanos sólo legaliza los documentos notariales firmados por escribanos de su demarcación) o bien, ante la autoridad administrativa que corresponda, según el caso.

*3*) Enviar dichos documentos a la Secretaría de Estado solicitando la apostilla (*apostille of the hague*) en una carta donde se especificará el destino final del documento.

La implementación de las *apostilles* utilizando como medio de certificación y autenticación a la firma digital se desarrollaría de la siguiente forma:

*1*) Se solicitaría ante quien corresponda o se obtendría por medios propios (en caso de instrumentos privados) el "documento electrónico" a legalizarse "firmado digitalmente".

*2*) Se verificaría la autoría de la firma digital por medio del "certificado digital" emitido por autoridad certificante licenciada (de los cuales al respecto cabe recordar las presunciones de autoría e integridad). Si la firma digital correspondiera a un funcionario de la Administración pública, será la Subsecretaría de la Función Pública la encargada de emitir el certificado de firma digital que avale la firma antedicha. Si la firma digital correspondiere a un funcionario del Poder Judicial, será la respectiva Corte de Justicia de cada Estado provincial la encargada de emitir el certificado digital que avale dicha firma. Si la firma digital correspondiere a personas (físicas o jurídicas de carácter privado) la certificación se complementará con la firma digital de un

notario, encontrándose, la firma de este último, certificada por el correspondiente certificado de firma digital que emitirá al efecto, por ejemplo, el colegio de escribanos respectivo, quien a su vez será quien firme digitalmente en último término. Se cumpliría de esta manera con el recaudo de lo que denominamos "*apostille* digital".

*3*) Finalmente, el "documento electrónico", firmado digitalmente y con la firma certificada por medio de la "*apostille* digital" podrá ser presentado en formato digital (*smart card*, disquete o CD) o enviado por *e-mail* ante quien deba presentarse.

## 4. Conclusiones

Para concluir, creemos necesario que el Ministerio de Relaciones Exteriores, Comercio Internacional y Culto propicie una reforma ampliatoria a la Convención de La Haya del 5 de octubre de 1961, a los efectos de que se incluya a la firma digital como un nuevo medio de llevar a cabo el trámite de *apostilles*.

La reforma ampliatoria que proponemos es la siguiente:

Agregar como inc. *e* del art. 1° el siguiente texto: "*Los documentos digitales firmados digitalmente por las personas, entes y/o autoridades autorizadas por cada Estado*".

Incorporar como último párrafo del art. 4° el siguiente: "*En el caso de tratarse de un documento digital firmado digitalmente, la acotación prevista en el artículo 3, párrafo primero, deberá hacerse por medio de la firma digital de la persona autorizada inserta en el mismo documento digital, debiendo adjuntar al mismo la clave pública y el certificado digital correspondientes*".

Incorporar como último párrafo del art. 5° el siguiente: "*En el caso de tratarse de un documento digital firmado digitalmente, con el solo hecho de ser recibido y haber sido decodificado por el destinatario con la clave pública correspondiente y teniendo el certificado digital del emisor en vigencia, se presumirá la autenticidad de la de la firma y el documento*".

Incorporar como último párrafo del art. 6° el siguiente: "*Al momento de la aprobación de esta reforma, cada Estado designará las personas, entes y/o autoridades autorizadas a certificar por medio de firma digital respecto de los cuales remitirá al Ministerio de Asuntos Extranjeros de los Países Bajos, 'vía e-mail', las claves públicas y las copias de los certificados digitales que avalen dichas firmas digitales*".

Incorporar como último párrafo del art. 7° el siguiente: "*En el caso de los documentos digitales firmados digitalmente, cada una de las personas, entes y/o autoridades designadas de acuerdo con el artículo 6, deberá hacer al menos una copia 'back up' de los documentos digitales que acote*".

Y por último, incorporar como nuevo artículo el siguiente: "*Los Estados signatarios podrán hacer reserva respecto de las modificaciones introducidas en cuanto a los documentos digitales firmados digitalmente*".