La firma electrónica

Hermann Zubieta

Marco Llinás Volpe

Los mensajes de datos tiene y debe tener los mismos elementos y contenidos, tales como las fechas de emisión y recepción, los elementos básicos de una oferta donde interactúan todos los elementos reales, donde la ley sólo es la herramienta para desarrollar su aplicación, a través de sus presunciones y equivalencias.

La ley de comercio electrónico no pretendió introducir una tendencia del derecho basada en elementos novedosos quizá desaprovechando el momento y más bien desperdició la oportunidad de hacerlo, toda vez que se incorporaron los elementos técnicos propios del rigor del derecho. Sin embargo, lo que si hace la norma es arrastrar todos y cada uno de los requisitos, proporcionándoles una equivalencia funcional con los elementos tradicionales de larga data.

Ahora bien, lo anterior debe entenderse como la implementación de una herramienta. Como todo tránsito de sistema habrá que llenar aquellos vacíos mediante interpretación de la norma, toda vez que la norma en la cual se inspiró es de carácter general. Por tanto, existen aspectos particulares en los cuales habrá que ver cómo incorporarlos al ejercicio de la práctica. Tal es el caso de la certificación de los contenidos de los documentos firmados ante notario público que al tratarse mediante medios electrónicos no encuentra equivalencia funcional explícita.

Se pasará a continuación a revisar algunos aspectos característicos que trae la norma y especialmente el de equivalente funcional de la firma y firma digital, para mostrar como se puede reemplazar la firma manuscrita por mensajes de datos firmados, teniendo en cuenta algunos elementos técnicos que pueden ser cruciales.

I. Aspectos normativos

El comercio electrónico está basado en el intercambio de información mediante elementos electrónicos. La "ley modelo de comercio electrónico" de la Comisión de las Naciones Unidas para el Desarrollo Mercantil Internacional (CNUDMI), promulgada en 1996 con el fin de garantizar uniformidad en los conceptos y un desarrollo homogéneo de la normatividad en el comercio electrónico. Cada Estado ha adaptado la norma a su legislación nacional y en particular al campo de aplicación de la ley.

En Colombia la Ley 527 de 1999 regula el acceso y uso de los mensajes de datos, el comercio electrónico y las firmas digitales, así como de las entidades de certificación.

El tema de la equivalencia funcional tiene un enfoque más amplio bajo la legislación nacional que las que podemos encontrar en la legislación comparada. El legislador colombiano escogió que los documentos tradicionales o físicos tal y como se conocen hoy en la práctica tuvieran el mismo alcance que los datos de mensajes, lo que permite que se desarrolle con mayor libertad la utilización de los sistemas electrónicos dentro de una amplia gama de alternativas que la ley define y condiciona, pero sin restringir las aplicaciones tecnológicas.

Ahora bien, la Ley 527 de 1999 se aplica a todo tipo de información en forma de mensaje de datos. La excepción al principio general consiste en dos eventos. El primero se refiere a las obligaciones contraídas por el Colombia en virtud de Convenios o Tratados Internacionales y el segundo se refiere a las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

II. Mensajes de datos

El mensaje de datos, según la definición adoptada en la ley modelo de CNUDMI, es:

> Por 'mensaje de datos' se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax.

Esta definición abarca las comunicaciones verbales a través de una llamada telefónica que son producidas por elementos electrónicos. Igualmente el correo electrónico y los que aparecen en una página del WEB site. Además de representar la base del comercio electrónico estos mensajes de datos, son el fundamento de todas las actividades que involucran sistemas informáticos. De todos los mensajes de datos, hay algunos que tienen ciertas características que basados en la ley de los Estados, permiten hacer una equivalencia funcional entre éstos y los documentos escritos.

III. Mensaje de datos firmados

La equivalencia funcional de firma adoptada por CNUDMI en la ley modelo en su artículo 7.º, establece:

> 1. Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:
>
> a. Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y
>
> b. Si ese método *es tan fiable como sea apropiado* para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.
>
> 2. El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma (subrayado fuera del texto original).

Esta definición da la posibilidad de utilizar *cualquier método* que permita identificar el iniciador de un mensaje de datos y no está atada directamente a la generación de la firma a través de un método de clave pública*. Sin embargo, queda pendiente la determinación de cuándo un método es tan fiable cómo apropiado para un fin determinado. Podríamos entender que un método *es tan fiable como sea apropiado* en términos que garantice su integridad en términos razonables de seguridad y fidelidad.

El correo electrónico comúnmente permite identificar al iniciador del mensaje del mismo. Así un simple correo electrónico indica de quién proviene. ¿Pero que tan confiable es este método? Pero, ¿acaso podremos conocer si tiene la aprobación del suscriptor?

* Este método se fundamenta en la teoría de clave pública como sistema de cifrado, basado en el uso de una clave privada y una pública.

Seguramente para una transacción financiera es muy inseguro, pero para establecer un simple requerimiento a una entidad pública puede ser que sea suficiente. Teniendo en cuenta que es posible hacer un cierto rastreo de los correos y que la suplantación es un delito, este puede ser un mecanismo adecuado para aceptar derechos de petición y además considerarlos firmados.

IV. Firma digital

Muchas de las regulaciones introducen el término de firma digital como una especie del género de firma o firma electrónica, relacionándola directamente con el método de clave pública.

La firma digital según el artículo 2.º literal c de la Ley 527 de 1999 señala:

> c. Firma Digital. Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la *clave del iniciador* y al texto del mensaje, permite determinar que este valor se ha obtenido exclusivamente con la *clave del iniciador* y que el mensaje inicial no ha sido modificado después de efectuada la transformación (subrayado del texto original).

El artículo 28 de la Ley 527 de 1999 le otorga equivalencia a la firma manuscrita a la firma digital:

> Artículo 28. Atributos jurídicos de una firma digital. Cuando una firma digital haya sido fijada en un mensaje de datos se presume que el suscriptor de aquella tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.
>
> Parágrafo. El uso de una firma digital tendrá la misma fuerza y efectos que el uso de una firma manuscrita, si aquélla incorpora los siguientes atributos:
>
> 1. Es única a la persona que la usa.
> 2. Es susceptible de ser verificada.
> 3. Está bajo el control exclusivo de la persona que la usa.
> 4. Está ligada a la información o mensaje, de tal manera que si éstos son cambiados, la firma digital es invalidada.
> 5. Está conforme a las reglamentaciones adoptadas por el Gobierno Nacional".

La técnica de firma digital basada en clave pública utiliza una clave para generar la firma y otra para verificarla. La clave de verificación es llamada *clave pública* con la cual cualquier persona puede verificarla. La clave para generar la firma es llamada *clave privada*, y sólo el iniciador de la firma puede generarla.

La dificultad de derivar la clave privada a partir de la clave pública es el factor que ofrece confianza a los usuarios de los sistemas de firma digital. Esto implica que si se conoce la clave pública, en la práctica, un tercero no podrá obtener la clave privada, con el fin de evitar la suplantación.

La firma digital es un valor numérico que se adhiere al mensaje de datos. No cambia el texto original del mensaje, sólo le agrega información propia de la firma. Así, un documento firmado digitalmente no oculta su contenido. Similar cosa sucede con los documentos físicos que son manuscritos ya que se puede recibir un documento firmado en el cual no se reconozca la firma ni el autor de la misma, pero el contenido del documento en sí es totalmente legible. No obstante, se puede aplicar un método adicional que permite cifrar el documento.

Por último, la firma digital es generada a partir del mensaje de datos y la clave privada. Por tanto, hay una dependencia entre documento y firma. Lo cual en general indicaría que si por alguna razón existen dos documentos distintos firmados con la misma clave privada, su firma digital será distinta.

V. Independencia del iniciador de la firma digital

En la firma digital es posible generar una firma verificable sin la presencia de una persona que lo avale y está basado en la existencia de un modelo de confianza que garantiza que solo el dueño de la clave privada esté en capacidad de generar la firma digital.

No obstante, la equivalencia funcional no trata el tema del aval notarial. Por tanto, en caso de ser requerido tal formalidad se puede adherir el aval notarial al documento digital. Éste deberá ser una firma digital o bien una firma electrónica.

VI. Vulnerabilidad de documentos físicos

La firma manuscrita se genera de forma independiente del documento firmado. Esto trae consecuencia tales como la posibilidad de alternación del documento final. Por ello se suele colocar las iniciales en cada hoja para asegurar que no se altere una vez firmado.

Este método primitivo es a todas luces vulnerable. Sin embargo, más allá llevaría a que se colocara papel adhesivo sobre los documentos, pero en caso de ser el texto voluminoso éste método sería engorroso. Lo anterior muestra la fragilidad de la seguridad involucrada en el tema de documento escrito en papel en materia sobre de falsificaciones.

Con la firma digital esto no sucede por estar integrada con el documento. Cualquier cambio en el texto inhabilitaría la firma, mostrándola inválida en el momento de la verificación.

El nivel de seguridad de la firma digital está dado por los métodos utilizados para la generación de la clave y de la firma digital. Recordemos que hay algunos métodos que ofrecen más seguridad que otros.

VII. Seguridad

El fundamento de la seguridad de una firma digital consiste en la dificultad de derivar la clave privada a partir de clave pública. No obstante, subsiste la posibilidad que un sistema de información pruebe con todas las posibles combinaciones de claves (dado que son simples números), hasta dar con la solución. Sistema que se conoce con el nombre de fuerza bruta.

En el momento que un tercero logre derivar la clave privada de una persona, puede generar firmas de forma fraudulenta. Por tanto, se pierde la capacidad de identificar al iniciador del mensaje. Es así como cualquier firma generada con esa clave privada deja de tener validez.

En efecto, la vigencia de un documento firmado digitalmente está determinada por la fecha de creación de las claves privada y pública y la probabilidad de derivar la clave privada a partir de su clave pública en la fecha de vigencia del documento.

La vigencia de los documentos firmados digitalmente es otorgada por la fecha de creación de las claves, y no, la fecha de la firma del documento. Esta característica tiene especial relevancia al momento de analizar la firma de un documento digital de larga vida. Es así como una firma válida generada hoy, puede no ser válida en 10 o 15 años, puesto que el algoritmo o el tamaño de las claves utilizado podrían quedar obsoletos.

Los métodos matemáticos y las longitudes de las claves hacen cada vez más difícil el proceso de derivación a "fuerza bruta". Igualmente existe la posibilidad de refrendar las firmas digitales de los mensajes de datos, agregándoles al mensaje de datos cuya firma esté perdiendo actualidad, una nueva firma con los estándares vigentes, quedando así estancado el período en el que se realizó la primera firma.

* * *

Así las cosas, las firmas certificadoras (Resol. 26930 del 26 de octubre de 2000) tendrán que tener en cuentas todas las vicisitudes técnicas mencionadas. Pero sobre todo deberán garantizar la certeza sobre la legitimidad de los documentos y deberán implementar audaces mecanismos para agilizar los trámites sin que se vea afectados la integridad de los mismos. Aunque parece ser que los límites son de orden técnico consideramos que a este respecto la normatividad deberá abarcar la exigencia de la nueva realidad cibernética

Bibliografía

Ley Modelo de CUNDMI sobre las firmas electrónicas.

Ley 527 de 1999, República de Colombia.

Decreto 1747 de 2000, República de Colombia.

Resolución 26930 del 26 de octubre de 2000, Superintendencia de Industria y Comercio, República de Colombia.

SMEDINGHOFF, Thomas J. Certification Authority "Liability analysis". Amercian Bankers Association. 1998. Information Technology and Electronic Commerce (ITEC) Law Department.

The essential Role of Trusted Tirad Parties in Electronic Commerce. A. Michael Froomkin. 75 Oregon L. Rev. 49 (1996).

UK Government Policy on Encryption. Yaman Akdeniz. Web Journal of Currrent Legal Issues in association with Blackstone Press Ltd.