

DE LA FIRMA AUTÓGRAFA A LA FIRMA DIGITAL: PERSPECTIVA VENEZOLANA

Dra. Gladys Rodríguez (*)

La Universidad del Zulia. Facultad de Ciencias Jurídicas y Políticas.

Instituto de Filosofía del Derecho “Dr. J.M. Delgado O”

E-mail gerodrigu@cantv.net

Introducción.-

Es frecuente en nuestra actual organización social la utilización de la firma en documentos tan dispares como pueden ser una simple nota, una carta un cheque o un contrato. Incluso personas con dificultad, de cualquier índole, para leer o escribir, aprenden a plasmar su firma en un documento. A veces, en último extremo, cuando alguien no puede estampar su firma, se recurre a la huella digital.

Desde un punto de vista jurídico, no se pone tanto el acento en definir qué sea una firma pero sí en cuanto cuáles son los efectos que de la misma se derivan. La firma se ha convertido en un hecho previo o dato fáctico del cual se parte. Con la salvedad de algunos supuestos especiales del registro de firmas en relación con fedatarios públicos, la firma manuscrita no se somete a control ni requisitos.

A menudo se oye hablar de “digital” o de “digitalizar” e incluso se mencionan estos términos con frecuencia; en la mayoría de los casos es probable que en esas ocasiones no se sepa exactamente a qué se refieren. El vocablo digital hace referencia a “dígito” o “número” y es la manera de representar información (de cualquier especie) numéricamente, en notación binaria, es decir, mediante ceros y unos. El *bit* es la partícula mínima de información . Digitalizar significa traducir señales de texto, imágenes, sonido o video a lenguaje binario o *bits*, que cuando se reproducen a gran velocidad, se obtiene una réplica, en apariencia, exacta a la original. La digitalización permite la comprensión y transmisión de gran cantidad de información a muy bajo costo, con alta fidelidad (debido a la posibilidad de corrección de errores que ésta permite) y a una gran velocidad. Los especialistas como Toffler, Naisbitt o Negroponte, sugieren un mundo distinto, desigual y cambiante a partir de la incorporación del concepto de digitalización y pronostican cambios fundamentales en la concepción de la sociedad (Negroponte, 1995)

En una versión casi neutra se ha dicho que “la tecnología digital es la llave de la culminación exitosa de la infraestructura de la información y también es la tecnología que reinventará la manera en que la gente vivirá, trabajará y se divertirá.. La digitalización consumará el casamiento de la televisión, las computadoras y el teléfono, haciendo posible la comunicación con cualquiera, en cualquier lugar y en cualquier momento” (Viviana, 2000: 74)

(*) Doctora en Derecho Magíster en Planificación y Gerencia de Ciencia y Tecnología. Abogada . Profesora Agregada de Informática Jurídica y Derecho Informático en la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia. Investigadora Responsable de Proyectos de investigación ante el Condes. Miembro de la Fundación Venezolana de Investigadores PPI Nivel I.

La noción digital, por su parte data de alrededor de 1860. Los primeros cables que transmitían los mensajes en clave Morse utilizando “puntos” y “rayas”, presentaban la dificultad de que la señal llegaba a destino debilitada y distorsionada, por lo que quien debía decodificar el mensaje se enfrentaba, muy a menudo a un grave problema. Como consecuencia de este inconveniente, en las líneas submarinas empezó a usarse un código denominado “*cable code*”. Este consistía en que el operador del cable debía manipular un interruptor que funcionaba como puente para posibilitar que el cable se conectara al polo negativo o al positivo de una batería, obteniendo así un punto o una raya respectivamente. Este sistema utilizó un principio similar al que actualmente utilizan las computadoras y las telecomunicaciones, es decir, una *convención binaria*. Por tal motivo el presente trabajo pretende exponer la evolución de la Firma, qué es una Firma y especialmente qué es una Firma Electrónica, cuáles son las funciones de una Firma, indicar cómo se crea una Firma Digital y cual es su validez a la luz del Decreto – Ley sobre Mensajes de Datos y Firmas Electrónicas Venezolana. Se partió de un estudio descriptivo y explicativo sobre la base de bibliografía nacional e internacional así como de la legislación nacional vigente.

1. Evolución de la Firma

El concepto histórico de firma, y, a la vez, el más amplio y genérico, ha sido el de cualquier rasgo hecho con la intención de expresar el consentimiento o la manifestación de voluntad vertida en el instrumento. Ahora bien, desde el punto de vista del derecho se le ha otorgado valor jurídico a las distintas representaciones de esa autenticación o confirmación de la identidad de la persona, de acuerdo con las sociedades y con los diversos momentos históricos.

Para el derecho, la firma tiene una importancia fundamental por razones históricas, se han utilizado los portadores tangibles de las manifestaciones humanas (por ejemplo los documentos) como medios para representar hechos de relevancia jurídica. Así la piedra el metal, el papiro y el papel, entre otros, han servido como medios para transmitir mensajes, y sus características físicas tangibles han sido fundamentales para los efectos del derecho

Pero en las últimas décadas el desarrollo de las nuevas tecnologías ha provocado una profunda transformación, cuando no una revolución, en los medios de comunicación y expresión de la voluntad y del conocimiento de las personas. Inicialmente, los computadores, utilizados como máquinas de escribir desarrolladas, facilitaron la emisión de documentos sobre los que luego se estampaba una firma. Actualmente, la intercomunicación de las computadoras posibilita no sólo la generación de documentos electrónicos, sino la transmisión de la información contenida en los mismos en tiempos mínimos, que permiten hablar, no ya de alta velocidad, sino de “tiempo real”, es decir, se accede a la “información distante justo al instante”. Se produce así el fenómeno que se ha dado en llamar “electronificación” o “digitalización” de las relaciones jurídicas (Illescas, 1997)

Las Firmas en el derecho venezolano posee algunos requisitos y se hayan diseminados a lo largo y ancho de la normativa vigente y para los fines de los objetivos propuestos se

debe determinar que es una firma, cuándo es necesaria y cuáles son sus funciones, en principio.

2. De la Firma Manuscrita a la Firma Digital : Noción

Ya se ha mencionado en la evolución brevemente que puede entenderse por una firma. Por su parte la Real Academia Española la define como “el nombre y apellido o título de una persona que ésta pone con rúbrica al pie de un documento escrito de mano propia o ajena, para darle autenticidad, para expresar que se aprueba un contenido o para obligarse a lo que en el se dice”. No obstante, esta definición está restringida a las firmas manuscritas pero en la interacción social cotidiana, la realidad es otra pues, además de dichas firmas, se utilizan medias firmas, firmas marcando una “x”, firmas con sellos, firmas mecánicas o impresas, firmas con huellas digitales, firmas utilizando tecnologías biométricas modernas y firmas digitales, entre otras. (Avellán, 1999: 159)

En el caso de Venezuela, el legislador tuvo en mente las firmas manuscritas por lo cual la aceptación de otros tipos de firmas requirió la promulgación de una nueva legislación para otorgar validez a las firmas electrónicas y para establecer mayor certeza jurídica en cuanto a la validez de las mismas y esto igualmente ha ocurrido en otras latitudes.

En este sentido el Decreto – Ley sobre Mensajes de Datos y Firmas Electrónicas Venezolana se promulga el 28 de febrero de 2001 en el marco de la Ley Habilitante otorgada al Presidente de la República Bolivariana de Venezuela. Este Decreto – Ley fue un proyecto presentado por VenAmCham (Venezuelan American Chamber of Commerce) y la Cámara de Comercio Electrónico (CAVECOM). El Decreto – Ley reconoce en su artículo 1 eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico....., configurando esta disposición el objeto del Decreto- Ley. De igual manera, el referido Decreto – Ley define en su artículo 2 a la Firma Electrónica y establece. “ es toda información creada o utilizada por el signatario, asociada al mensaje de Datos, que permite atribuirle su autoría bajo el contexto en el cual ha sido empleado. En este sentido, la Ley de Firmas y Certificados Digitales Peruana es mucho más amplia en la definición cuando establece: “se entiende por firma electrónica cualquier símbolo basado en medios electrónicos, utilizado o adoptado por una de las partes con la intención precisa de vincularse o autenticar un documento (Ley No. 27269, Perú, artículo 1, primer aparte). Asimismo, el Decreto – Ley dispone en su artículo 18 qué es una Firma Certificada o Digital cuando establece: “la Firma electrónica, debidamente certificada por un Proveedor de Servicios de Certificación conforme a los establecido en este Decreto-Ley, se considerará que cumple con los requisitos señalados en el artículo 16”. Finalmente, la Firma Digital es un tipo de firma electrónica que se genera utilizando un mecanismo criptográfico que reduce el texto a un tamaño fijo (*message digest*) gracias a la aplicación de una función matemática denominada *hash* (1), y de la cual se hablará más adelante.

Ahora bien, la firma es necesaria porque ello implica el cumplimiento de los requisitos *ad solemnitatem* y los *ad probationem*. Estas categorías establecen, respectivamente, la distinción entre los requerimientos que son necesarios para la existencia o validez de un acto jurídico y aquellos que son necesarios para la admisibilidad o valoración de una prueba. Las limitaciones de espacio y la necesidad de darle prioridad al novedoso y complejo tema de las firmas electrónicas, sólo permiten señalar los aspectos legales básicos sin recurrir a las interesantes discusiones doctrinarias que existen en relación a los requisitos de firmas.

En este sentido, los requisitos *ad solemnitatem* se refieren a las formalidades que imponen las normas jurídicas para la existencia o validez de un acto jurídico. Estos requisitos se encuentran en instrumentos públicos y privados en todas las ramas del derecho (por ejemplo; el artículo 448 del Código Civil Venezolano impone el requisito de una firma cuando establece: “Las partidas del estado civil... deberá firmarlas el funcionario o la persona autorizada para el caso, y su Secretario, con asistencia de dos testigos...Deberán firmarlas también las partes...”

Los requisitos *ad probationem* son aquellos que se refieren a la admisibilidad y a la valoración de pruebas en juicio, un ejemplo lo encontramos el artículo 1387 del Código Civil Venezolano que establece : “No es admisible la prueba de testigos para probar la existencia de una convención celebrada con el fin de establecer una obligación o de extinguirla, cuando el valor del objeto exceda de dos mil bolívares”. Con esta norma se impone la necesidad de usar instrumentos privados o públicos para documentar y probar las obligaciones que excedan el monto.

Finalmente para concluir este aparte, es necesario verificar cuáles son los requisitos que la Firma debe poseer.

En los análisis técnicos jurídicos sobre las firmas electrónicas, el tema de las funciones de las firmas ha sido central pues los avances tecnológicos hasta los momentos no han logrado que la firma autógrafa u hológrafa pueda utilizarse en el medio electrónico. Aquello que tradicionalmente se ha entendido por firma autógrafa, pierde la capacidad para cumplir sus funciones en este medio. Si bien es posible crear una firma sobre un documento físico (no electrónico) y generar una imagen electrónica de la misma, es fácil que otra persona copie esa imagen electrónica y la coloque en cualquier documento electrónico, sin que el autor originario tenga la posibilidad de control sobre esto. Igualmente debido a la naturaleza de los documentos electrónicos, es muy fácil modificar su contenido sin que pueda detectarse alteración alguna.

En vista de estas circunstancias, desde finales de los años setenta, se han buscado alternativas para reproducir en el medio electrónico las funciones de la firma y con ello lograr un “equivalente funcional”entre la firma manuscrita y la firma electrónica . Sin embargo, esto no ha sido ni fácil ni uniforme pues las funciones que cumple una firma suelen ser muy variadas dependiendo de las circunstancias. Siguiendo a la Real Academia Española antes referida, son tres las posibles funciones:

- ? Autenticidad
- ? Aprobación del Contenido
- ? Sujeción a las obligaciones contenidas en el documento.

Estas funciones están limitadas pues pueden no darse en ciertas circunstancias en las cuales se usen firmas. Si consideramos por ejemplo, la segunda de éstas, pudiera imaginarse el caso en que una firma no se coloque con el objeto de aprobar el contenido de un documento sino para dejar constancia de que se leyó el mismo. Por tanto, resulta conveniente utilizar un concepto más amplio como los siguientes:

- ? Ayuda en la Identificación del autor (Autenticidad)
- ? Ayuda en la demostración de la intención del autor
- ? Ayuda en asegurar la integridad de la información firmada (Integridad)

Y en el caso de la firma digital se añaden las funciones de Seguridad o Confidencialidad y No Repudio.

A continuación se explicarán estas funciones brevemente con el objeto de que sirvan como punto de referencia en la descripción de las diversas tecnologías usadas para realizar firmas electrónicas

? Ayuda en la Identificación del autor (Autenticidad)

La primera y la más obvia de las funciones de la firma es la identificación del autor de la misma por medio de la asociación de la firma con la persona específica:

- a) sea por el nombre que se lee en la firma (en el caso de las firmas legibles)
- b) por motivos de estilo (comparando a simple vista o por expertos grafotécnicos con ejemplares de firmas previas)
- c) por acuerdos entre el autor y las personas que verifican la firma (por ejemplo, las iniciales del autor en un documento en una oficina)

En la firma manuscrita, el mecanismo de seguridad que permite asociar la misma con una persona determinada se basa en el supuesto de que esa persona es la única que puede producirla de una manera específica así como en otros mecanismos establecidos por la ley para casos específicos (ejemplo testigos). En el caso de haber dudas al respecto, un experto grafotécnico podrá realizar la comparación de la firma en cuestión con ejemplares anteriores o producida para el caso por el presunto autor. Dentro de esta función de la identidad o autenticidad, hay que considerar un factor adicional que se manifiesta tanto en el medio físico como en el electrónico, que es el uso de la firma para otorgar acceso a un espacio determinado. Es frecuente, por ejemplo que al entrar en algún lugar se exija la presentación de alguna tarjeta de identidad u otros certificados o constancias que usualmente contienen una foto, la firma, el nombre, posición etc. de la persona . En el medio electrónico, estas dos funciones de la identificación (es decir la asociación entre un documento y una persona y para otorgar acceso a un sitio físico o electrónico) se tienden a amalgamar puesto que en lugar de presentar una tarjeta de identidad a un portero, ésta se pasa por un lector magnético que determina si la persona tiene o no autoridad para ingresar. Dependiendo del nivel de seguridad establecido, pudiera requerirse al portador de la tarjeta de identidad (magnética o inteligente) que introduzca su clave, es decir que produzca su firma electrónica. El lector magnético verificaría dicha clave asociándola con la información contenida en la tarjeta misma o en una base de datos central, mediante la cual se asocia la misma con una persona específica. Lo que se quiere ilustrar con estos ejemplos es que en el medio electrónico, la distinción conceptual entre un medio de identificación y un medio de firma tienden a converger y esto puede resultar en que la firma electrónica tenga usos más diversos que la firma en el medio físico.(Avellán, 1999)

En definitiva, en Internet es prácticamente imposible verificar quien ha escrito la firma que presenta. Mientras que con la firma digital al receptor le basta comprobar si el certificado digital en donde está contenida la firma está en vigor y si ha sido incluido en el directorio de certificados revocados o suspendidos. Una vez comprobados ambos extremos, utiliza la clave pública del remitente para comprobar que la firma digital de éste es auténtica, todo ello confiere una ventaja a la Firma digital (Font, 2000)

? Ayuda en la demostración de la intención del autor

Esta es una función que pudiera ser subjetiva u objetiva según el documento de que se trate. En aquellos documentos en los cuales la ley otorga un significado específico a la firma (por ejemplo letras de cambio), generalmente no hay dudas con respecto a la intención del firmante y por ello puede decirse que la intención del autor está objetivada. Pero pensemos, por ejemplo, en el caso de un contrato redactado en una oficina y firmado en el encabezado por el gerente de dicha oficina ¿ Se trata de una aceptación de los términos del contrato, de la aprobación de la redacción para que se proceda a la impresión definitiva del mismo o de algún otro significado específico que

se le haya dado en esa oficina? Las variaciones son infinitas pero los mecanismos existentes funcionan debido a las costumbres, los convencionalismos, en el contexto en que se colocan las firmas y otros aspectos que han permitido cierta estabilidad y seguridad en cuanto a la intención.

En el medio electrónico, la intención del autor es más difícil de comprender puesto que aún no existen prácticas generalizadas o costumbres con respecto a las tecnologías que se están utilizando para firmar electrónicamente ni con respecto los contextos de dicho medio. Sin embargo el Decreto –Ley sobre Mensajes de Datos y Firmas Electrónicas Venezolano establece en su artículo 6 lo siguiente: “ Cuando para determinados actos o negocios jurídicos la ley exija la firma autógrafa, ese requisito quedará satisfecho en relación con un mensaje de datos al tener asociado una Firma Electrónica”. Ello significa que existe una equivalencia funcional entre la firma manuscrita y la firma electrónica a la luz de la legislación nacional vigente.

? Ayuda en asegurar la integridad de la información firmada (Integridad)

Otra función de la firma es contribuir a que la información en el documento firmado no sea alterada después de que la firma haya sido colocada, aunque no es una función exclusiva de la firma, pues las limitaciones físicas del papel u otro objeto físico, ayudan en tal sentido, la firma ayuda al ser colocada al pie del texto.

En el medio electrónico, las tecnologías de firmas electrónicas basadas en la criptografía ha convertido a la firma en el método más confiable para determinar si un documento electrónico ha sido modificado desde que la firma en cuestión fue realizada. Primeramente, vale indicar que el Decreto – Ley al que hemos hecho referencia anteriormente, considera en su artículo 7 lo siguiente: “ Cuando la ley requiera que la información sea presentada o conservada en su forma original, ese requisito quedará satisfecho con relación a un mensaje de datos si se ha conservado su integridad.... A tales efectos, se considerará que un Mensaje de Datos permanece íntegro, si se mantiene inalterable desde que se generó, salvo algún cambio de forma propio del proceso de comunicación, archivo o presentación”. Y es que en un entorno tan vasto y potencialmente hostil como Internet, es muy difícil para el receptor de un documento advertir si éste ha sido manipulado, mientras que al incorporar el *hash* cualquier manipulación sería evidente de forma inmediata.

En este sentido deben aclararse algunos conceptos, por ejemplo criptografía, la criptografía es una rama de la criptología que consiste en mantener mensajes secretos, mientras que la criptología es la rama de las matemáticas compuesta por la criptografía y el criptoanálisis. El criptoanálisis es la rama de la criptología que consiste en transgredir los sistemas criptográficos a fin de leer los mensajes secretos.

Por otra parte, en relación a la función hash, es necesario aclarar que los esquemas de firma digital suelen ser muy lentos en su transmisión y, en ocasiones, la longitud de la firma suele ser similar o mayor al mensaje mismo; por ende, en la práctica se utiliza la función *hash* antes de firmar un mensaje. Esta función consiste en aplicar a un mensaje de longitud variable, una representación de longitud fija del propio mensaje, que se denomina valor *hash* (este valor es siempre mucho menor que el mensaje , por ejemplo, un mensaje de 1 megabyte de longitud, puede reducirse a 64 o 128 bits de longitud). (Viviana , 2000)

Bajo este contexto de seguridad algunos autores consideran con razón que el documento o mensaje encriptado se transforma en un documento que ninguna otra persona pudo

haber generado y además, que la firma digital es más segura que la ológrafa, puesto que además de asegurar que el mensaje fue realmente generado por quien lo envía, garantiza que ninguna parte de él ha sido modificada.

Pero además se debe garantizar que quien recibe el mensaje es la persona que el emisor desea lo lea, ello implica seguridad y al mismo tiempo se busca garantizar que no se pueda negar la autoría de un mensaje enviado, así como no poder rechazar que un mensaje ha sido recibido, lo cual implica un No rechazo o No Repudio.

De lo anterior que la Firma Digital requiera lo siguiente:

- a) Estar vinculada al signatario de manera única
- b) Permitir la identificación del signatario
- c) Haber sido creada por medios que el signatario pueda mantener bajo su exclusivo control
- d) Estar vinculada a los datos relacionados de modo que se detecte cualquier modificación ulterior de los mismos.

Requisitos que además de contenerlos la doctrina también el legislador patrio los incorporó en el Decreto – Ley en su artículo 16.

Tales consideraciones ponen de manifiesto que estos métodos aportan la confiabilidad necesaria como para ser utilizados en el tráfico jurídico. Sin embargo, se debe resaltar que el proceso tecnológico de firmar digitalmente instrumentos no es suficiente por sí sólo, pues para que pueda cumplir adecuadamente con su objetivo requiere de un contexto determinado, usualmente denominado Infraestructura de clave pública o infraestructura de firma digital o Criptografía Asimétrica.

3. Las Firmas Digitales: Criptografía

Hoy existen métodos criptográficos modernos, desarrollados a partir de la II Guerra Mundial, cuando empiezan a aparecer los primeros computadores, y son conocidos como: Los Sistemas Criptográficos Simétricos (2) y Los Sistemas Criptográficos Asimétricos (3).

De los dos sistemas antes mencionados, el Sistema Criptográfico Asimétrico o de Clave Pública ha resultado más beneficioso para garantizar el cumplimiento de los requisitos legales y superar la desventaja del Sistema de Criptografía Simétrico, según el cual, al tenerse acceso a la clave secreta se puede descifrar el mensaje.

¿ Cómo funciona entonces la Criptografía Asimétrica para enviar un mensaje cifrado?

Paso 1.

El emisor da a conocer a todos los usuarios (receptores) con quienes comparte información su clave pública. Lo mismo hace el receptor.

Paso 2

Cuando el emisor quiere enviar un mensaje al receptor, y quiere que éste solamente sea visto por el receptor, el emisor deberá cifrar el mensaje, haciendo uso de la clave pública del receptor, mediante un programa que obtiene en forma gratuita en Internet.

Paso 3

El mensaje cifrado es enviado por medios no seguros. E-mail, correo postal, fax, etc.

Paso 4

El receptor recibe el mensaje y la única forma de descifrarlo, es haciendo uso de su clave privada.

Cualquier persona que intercepte el mensaje, leerá una gran cantidad de símbolos alfanuméricos y la única forma de descifrarlo será con la clave privada del receptor, ni siquiera con su clave pública.

Ahora ¿Cómo funciona un sistema criptográfico asimétrico para asegurar la autenticidad de un documento?

Supongan que el emisor del mensaje, sospecha que hay personas que se hacen pasar por él y están enviando documentos con su nombre.

Paso 1

El emisor envía el documento al receptor y lo cifra con su clave privada, que solamente él conoce .

Paso 2

Cuando el receptor recibe el documento, solamente lo puede descifrar con la clave pública del emisor.

Si el documento es descifrado, entonces se puede decir que proviene de quien dice provenir.

Y, finalmente, ¿Qué ocurre si el mensaje que quería enviarse era confidencial?

En el caso anterior, cualquier persona con la clave pública del emisor, podía comprobar que el documento es auténtico, pero el documento queda expuesto a cualquiera que tenga la clave pública del emisor.

Entonces para que el mensaje además de autentico, sea confidencial se deberá:

Paso 1

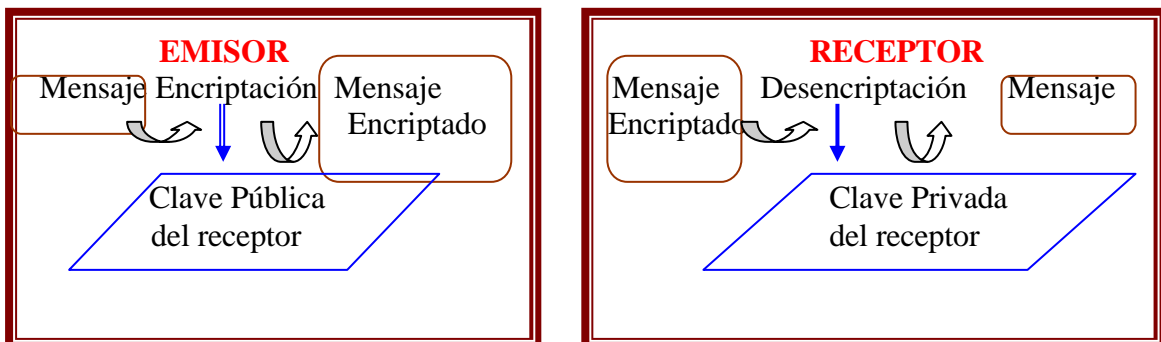
El emisor cifra su mensaje con su clave privada, lo cual permite que sólo sea descifrado por su clave pública y

Paso 2

Luego el emisor vuelve a cifrar el mensaje ya cifrado, con la clave pública del receptor.

Paso 3

El receptor descifra el mensaje solamente con su clave privada y lo autentica con la clave pública del emisor.



Fuente RSA Security Inc.

No obstante, los beneficios de la criptografía asimétrica se ha determinado que los algoritmos (4) de encriptación asimétrica son cien (100) veces más lentos que los algoritmos de encriptación simétrica. Por ello, los algoritmos actuales encriptan el mensaje mediante claves simétricas y envían la propia clave simétrica dentro del mensaje pero encriptada según algoritmos de clave asimétricas. (Rodríguez, 2001)

Así de la criptografía llegamos a la Firma Digital.

3.1. ¿Qué es una Firma Digital?

Las firmas digitales son utilizadas para verificar la integridad y autenticidad de un mensaje. Esto último también se puede lograr utilizando algoritmos criptográficos convencionales. La firma digital garantiza además la no repudiabilidad de un mensaje y por lo tanto tiene el mismo valor legal que una firma holográfica tradicional (en los países que poseen una ley de firma digital). En la República Bolivariana de Venezuela, por Decreto – Ley de febrero de 2001, se otorga ese status a dicha técnica para garantizar la seguridad, autenticidad, integridad y no repudio a los mensajes tele transmitidos por vía electrónica. Incluso se dictó también el Decreto Presidencial de Ley de Registro Público y del Notariado Gaceta Oficial No. 5.556, de fecha 13 de noviembre del año 2000, cuyos artículos reconocen la eficacia y valor jurídico de los medios electrónicos, por ejemplo en su artículo 4 establece: “Todos los soportes físicos del sistema registral y notarial actual se digitalizarán y se transferirán progresivamente a las bases de datos correspondientes.

El proceso registral y notarial podrá ser llevado a cabo íntegramente a partir de un documento electrónico”

Asimismo, el artículo 5 habla sobre la Firma electrónica y dispone lo siguiente “ La firma electrónica de los Registradores y Notarios tendrá la misma validez y eficacia probatoria que la ley otorga a la Firma autógrafa”. Lo cual evidencia nuevamente la equivalencia funcional existente.

Las firmas digitales son generadas utilizando un algoritmo de clave pública. Para ello se encripta con la clave privada del emisor un hash del mensaje a firmar. Cualquier persona puede verificar la validez de la firma digital del mensaje utilizando la clave pública del emisor del mensaje.

Cabe señalar que la participación masiva de tráfico de información, requiere la presencia de una Autoridad Certificante (CA) de reconocido prestigio, que garantice el origen de cada clave pública activa en el sistema, encargándose de difundir aquellas que queden fuera de servicio, lo que se conoce como lista de revocación. En el caso de Venezuela tenemos la Superintendencia de Proveedores de Servicios de Certificación Electrónica.

La firma digital está basada en la utilización de la criptografía de clave pública, es decir, en algoritmos matemáticos que operan a través del juego de un par de claves, privada y pública, las que se encuentran íntimamente vinculadas.

Toda persona que quiera “firmar” digitalmente información para su posterior transmisión debe generar su propio par de claves. La bondad de la criptografía de clave pública radica en que no se necesita compartir a clave: la clave privada queda en poder del usuario y es la utilizada para “firmar”. Sólo la clave pública se publicita y es utilizada para verificar la firma.

La firma digital no se asemeja en nada a la firma tradicional. Por ello, es conveniente determinar ¿ Cómo se crea o realiza la Firma Digital?.

3.2. Formación de la Firma Digital

El proceso de creación de par de claves lo realiza un *software* especial: en general, la clave privada queda almacenada en el *hardware* del usuario y se activa por medio de una contraseña, aunque también puede ser almacenada en otros dispositivos como una tarjeta inteligente.

Las claves no son otra cosa que una combinación de letras y números, es decir, un conjunto de *bits* que a su vez constituyen un conjunto de ceros y unos.

La creación de una Firma Digital implica combinar los caracteres que conforman la clave privada del usuario con los caracteres del documento o información al que se le quiere adosar la “firma”. Este nuevo conjunto de caracteres obtenidos a partir de la mezcla de los caracteres del documento/información con los de la clave privada, es lo que constituye la firma digital. En dicha mezcla quedan comprendidos todos los caracteres que conforman el documento, incluso los espacios en blanco, de forma tal que cada combinación (clave privada más documento, es decir, firma) es única para cada documento. Como se advierte, también es muy importante la longitud de la clave. Entre los algoritmos más utilizados para esta creación se encuentra el RSA ⁽⁴⁾.

Una vez obtenida la “firma”, el suscriptor/emisor la transmite conjuntamente con el documento. Asimismo, transmite su clave pública para ser utilizada en el proceso de verificación.

3.3. Validez de la Firma Digital

Ahora, ¿Cómo se comprueba a validez de la Firma Digital?

El destinatario recibe el documento con la firma digital y la clave pública del suscriptor. Procede entonces a iniciar el proceso de verificación de la firma digital adosada al documento recibido. Aplica la clave pública del suscriptor a la firma digital. Como resultado de este proceso se obtiene una serie de caracteres que son comparados con los que conforman el documento transmitido. Si los caracteres coinciden, la “firma” es válida, ya garantiza que fue aplicada por el titular de la clave privada que se corresponde con la clave pública utilizada para la verificación y que el documento no ha sido alterado.

En suma, cada clave efectúa una transformación unívoca sobre los datos y es función inversa de la otra, por lo que una clave sólo puede descifrar lo que su par encriptó y a la inversa, es decir que la clave puede ser utilizada en ambas direcciones. Por tanto, podemos afirmar que si un usuario puede descifrar un mensaje con la clave pública de una persona, sólo ésta última pudo haber usado su clave privada inicialmente para encriptarlo. Cabe señalar que todo este proceso se realiza automáticamente y en pocos segundos.

En este sentido el Legislador Patrio consagró una serie de requisitos para dar validez y Eficacia probatoria a la firma, así lo consagra en el artículo 16 que establece:

Artículo 16

La Firma Electrónica que permita vincular al signatario con el mensaje de Datos y atribuir la autoría de éste, tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. A tal efecto, salvo que las partes dispongan otra cosa, la Firma Electrónica deberá llenar los siguientes aspectos:

1. Garantizar que los datos utilizados para su generación puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad.

2. Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento
3. No alterar la integridad del Mensaje de Datos.

Incluso establece el mismo Decreto – Ley que en caso de no poseer los requisitos antes mencionados y por tanto aunque no se le atribuye el valor referido, sin embargo, podrá constituir un elemento de convicción valorable conforme a las reglas de la sana crítica.

3.4. Sobre Digital

Los sobres digitales son utilizados para resolver el problema de distribución de claves cuando se usan algoritmos simétricos. Los sobres digitales son generados utilizando un algoritmo de clave pública. Para ello se encripta una clave de sesión con la clave pública del destinatario del mensaje. Solo el destinatario podrá abrir el sobre y recuperar la clave de sesión necesaria para desencriptar el mensaje encriptado. Existen empresas que implementa sobres digitales combinando cualquier algoritmo simétrico con RSA (2), como la Firmas Digitales SRL Soluciones Criptográficas (FDCrypt), una empresa argentina asociada a Verisign Inc, empresa líder en el mercado mundial de certificados digitales. (www.FdCript.com.ar)

4. Técnicas para Firmar Electrónicamente

Al considerar las Firmas Electrónica lógicamente se observa que ésta es el género y la Firma Digital es la especie. Es así que existen diferentes categorías de tecnologías para firmar electrónicamente, a saber:

Basadas en “algo que se sabe”, esta categoría está conformada por los medios que basan la firma electrónica en información que la persona sepa, por ejemplo si se llama por teléfono al banco donde se tiene una cuenta para solicitar cualquier servicio (balance, transferencia, consulta de saldo, etc), se le pedirá “algo que ella sabe”, su número de cuenta y una clave, con lo cual queda verificada la identidad.

Basadas en “algo se tiene”, los medios utilizados en esta categoría determinan la identidad de la persona con base en objetos tangibles que la persona posee. Por ejemplo en el caso de los cajeros automáticos de los bancos la posibilidad de retirar dinero de una cuenta requiere la presentación de una tarjeta magnética o inteligente y además pulsar una clave. Aquí se ha logrado cumplir las funciones de identidad, integridad e intención.

Finalmente las basadas en “algo que se es”, esta categoría establece la identidad de una persona basado en algo que la persona es físicamente o algo que sea capaz de producir de manera exclusiva o, que al menos, sea difícil de reproducir. Por ejemplo las huellas dactilares, otros ejemplos: el rostro, la voz, los iris de los ojos, el patrón de venas de la muñeca y la firma digital generada sobre una tabla digitalizadora y programa de computación combinada con operaciones criptográficas y que ha sido considerada por los tecnólogos como la más viable hasta los momentos para su uso a gran escala.

Es así que en el Estado de Utah en Estados Unidos de Norteamérica se dispone, desde mayo de 1995, de la primera Ley de Firma Digital en el mundo. Esta ley le otorga seguridad jurídica a los documentos electrónicos o digitales firmados únicamente por medio de la criptografía de clave pública. No admite ni contempla técnicas alternativas (Rengifo, 2000)

5.- La Firma Digital en la Práctica

Las Firmas electrónicas se afianzan como una tecnología segura, formal y legal en la mayoría de países a nivel mundial. Y aun cuando existen diferentes tratamientos es uno de los medios más seguros.

Desde África hasta América, en los cinco continentes, los países han encontrado en la aplicación de la firma electrónica la solución para simplificar trámites administrativos, gestiones y transacciones que pueden realizarse por medios electrónicos con seguridad; una vez que se identifica a los actores de modo inequívoco y se garantiza la integridad de los mensajes enviados o recibidos.

Las firmas electrónicas para emplearse con fines de identificación requieren la certificación de pertenencia. Es decir, una entidad independiente tiene que garantizar que una firma electrónica pertenece a una persona y asumir la responsabilidad por ésta garantía o certificación. Esta actividad es la que realizarán las entidades de certificación y que CONATEL puede bien encargarse de regular y estarán bajo la supervisión de la Superintendencia de Proveedores de Certificación Electrónica como lo indica el Decreto – Ley venezolano en su Capítulo V el artículo 22 .

La prioridad del Gobierno debería ser impulsar, motivar y facilitar el uso de las tecnologías de firma electrónica, convirtiéndose en el principal usuario de las mismas. Para esto, existe una necesidad, demostrada, en varios procesos que se están llevando adelante como Aduanas, Compras Públicas, Gobierno Electrónico, entre otros.

Ésta, como todas las decisiones de un gobierno, es una decisión política y en este caso incluso será de oportunidad política.

Generalmente el servicio que prestan en la práctica estas empresas con la utilización de Firmas Digitales comprende:

- ▶ Resguardo de la información empresarial y personal
Tecnología de avanzada (top throughput)
- ▶ Ajuste a normas criptográficas internacionales ANSI / ISO / NIST-FIPS / CCITT X. 509/PKCS RSA Data Sec.
- ▶ Resguardo de la información empresarial y personal
Tecnología de avanzada (top throughput)
- ▶ Asesoramiento y soporte total posventa con personal residente en el país. Call Center y Hot-Line (24 Hs. x 365 días) para clientes que lo requieran.
- ▶ Documentación completa y cursos de capacitación para programadores usuarios (On-post training), en la medida e intensidad que cada cliente requiera.

El tema de la Firma Electrónica en la realidad es un tema de vital importancia para el desarrollo del comercio-e y para la estabilidad de Internet como plataforma de intercambio de información segura y confiable.

Al texto legal venezolano de homologan los efectos de la firma manuscrita a la firma electrónica y se establecen los requisitos mínimos que confieren seguridad e integridad a los mensajes de datos y a la firma electrónica y aquellos que debe tener un certificado electrónico, que contiene información legitimada por un ente certificador que vincula a

una persona natural o jurídica confirmando su identidad. Con la nueva ley se adopta un marco normativo que avala los desarrollos tecnológicos sobre seguridad, los países con legislaciones más recientes sobre el tema han optado, al igual que Venezuela por proyectos simples, tecnológicamente neutros (artículo 1 último aparte) y dinámicos. (Hacker, 2001) Capaces estos métodos de permitir un desarrollo en el escenario actual.

Conclusiones

El uso de la firma se generaliza como medio de atribución de la autoría de una obra, que puede ser de muy variada naturaleza, desde una obra de arte (una pintura) a un contrato (una compraventa) En nuestro ordenamiento jurídico se observó cómo en ocasiones no se requiere la firma en forma explícita, pues se exige el consentimiento más no la firma. Sin embargo, la práctica ha hecho que la firma sea el medio más frecuente y habitual de expresar el consentimiento. Las nuevas tecnologías han surgido y ello ha permitido que ingreso a sistemas abiertos de comunicación como Internet con gran incertidumbre, para ello debe comprenderse que la seguridad que brindan los medios electrónicos es tanta o más que la conseguida por medio del papel. A la seguridad se suma la mayor eficiencia en términos generales, pero con esto no se pretende ignorar la posibilidad de fallas y consecuencias funestas, derivadas de la dependencia de los computadores.

Pero la seguridad técnica no lo es todo, con la firma electrónica se puede garantizar la integridad de un mensaje electrónico y su autoría, con las diferentes funciones algorítmicas complejas se puede determinar el origen y momento de generación o transmisión del mismo. Pero el paso decisivo para el uso de esta tecnología depende de la confianza que se genere en los posibles usuarios. Illescas Ortiz señala con acierto que la confianza descansa no sólo en la seguridad que ofrezca la técnica, sino también en la seguridad jurídica (2001). Con el Decreto – ley , al igual que la ley Colombiana (Decreto 527 de diciembre de 1999) y la Ley Modelo Uncitral (Comisión de Naciones Unidas para el Derecho Mercantil Internacional) sobre Firmas Electrónicas, se tiene una regulación sobre las firmas electrónicas contenida en tres artículos fundamentales (Ley Sobre mensajes de Datos y Firmas Electrónicas Venezolana artículos 16 al 19). Además de definir la firma electrónica y establecer su validez, la ley establece el servicio de proveedores de certificación de firmas y la superintendencia de Proveedores de Servicio de Certificación .

Notas

(1) HASH: Los algoritmos de hashing (también llamados fingerprint, checksum o digesto de mensaje) permiten verificar que un mensaje no ha sido modificado. Dado un mensaje de tamaño arbitrario, producen una salida de tamaño fijo. Este tipo de funciones se conocen como funciones sin inversa debido a que es muy fácil calcular un hash para un mensaje, pero muy difícil encontrar un mensaje que produzca un valor particular de hash. Dado que la cardinalidad del espacio de todos los mensajes posibles es mucho mayor que el número de combinaciones distintas para un tamaño determinado de hash, necesariamente existen diversos mensajes que producen el mismo resultado, aunque es computacionalmente imposible encontrarlos.

Los algoritmos de hashing implementados en FDCrypt son MD4, MD5, SHA, SHA-1, RIPEMD-128 y RIPEMD-160, todos ellos cumpliendo rigurosamente con las normas internacionales vigentes

(2) Criptografía Simétrica: Sistema de cifrado basado en claves privadas, tanto el que envía el mensaje como el que lo recibe, conocen y utilizan la misma clave secreta tanto para encriptar el mensaje como para desencriptarlo.

(3) Criptografía Asimétrica: Son los sistemas creados en 1976 en la Universidad de Standford, Estados Unidos, se basan en la utilización de dos claves diferentes por cada usuario: la clave pública y la clave privada. Ambas claves, aun cuando son completamente diferentes, trabajan a dúo para encriptar y desencriptar mensajes. El mensaje se encripta con clave privada y se desencripta con clave pública y viceversa.

(4) Algoritmo: es una lista de instrucciones que realiza una descripción paso a paso y precisa de un proceso, que está garantizado que resuelve cualquier problema que pertenezca a un tipo determinado y que termina después de que se ha llevado a cabo un numero finitos de pasos.

Bibliografía

Avellán, J (1999) “ Las Firmas Electrónicas y la Seguridad de la Comunicaciones en Línea” En **Comercio Electrónico las fronteras de la Ley**. Compilador Lorenzo La Carrero. Editorial Cámara Venezolana de Comercio Electrónico . p 143-152.

Firmas Digitales SRL Soluciones Criptográficas (2002) Firmas Digitales En: www.FdCript.com.ar

Font, A (2000) **seguridad y Certificación en el Comercio Electrónico**. Editorial Biblioteca Fundación retevision 165 p.

Hacker, U (2001) “ Firma con Ley” En : wwwl@red.com Consultada el mes de mayo de 2002.

Illescas, R (1997) “ El transporte terrestre de mercancías: internacionalización y electronificación” . Madrid. p129 .

Madrid , A (2001) “ Aspectos jurídicos de la identificación en el comercio electrónico” En: **Derecho del Comercio Electrónico** Compiladores Illescas, r y Ramos, I . editorial La Ley- Actualidad, S.a. p 185-247.

Negroponte N (1995) Ser Digital, Atlántida p 21 y siguientes.

Rengifo, E (2000) “ Comercio Electrónico. Docuemto Electrónico y Seguridad Jurídica. En: **Comercio Electrónico Memorias**. Editorial Universidad Externado de Colombia p 9-52.

Rodríguez, G (2001) “ El Comercio ElectrónicoAlgunas consideraciones de seguridad. En **Revista de Derecho** . No. 16. Vol. I Barranquilla p142-158.

Rodner, J (2001) "El negocio jurídico electrónico en Venezuela". En **La Regulación del Comercio Electrónico en Venezuela**. Editorial Biblioteca de la Academia de Ciencias Políticas y Sociales. Serie No. 16. Caracas. P 19-85

Viviana , A (2000) **Comercio Electrónico y derecho**. Editorial Astrea. Buenos Aires. 443 p.

Legislación

Decreto – Ley Sobre Mensajes de Datos y Formas Electrónicas Gaceta Oficial No. 37.148 del 28 de febrero de 2001.

Código Civil Venezolano Reforma de 19983.

Código de Comercio Venezolano.

DE LA FIRMA AUTÓGRAFA A LA FIRMA DIGITAL: PERSPECTIVA VENEZOLANA

Resumen

Uno de las consecuencias de una red abierta como Internet son los problemas de seguridad y confidencialidad. Este trabajo se propone exponer la evolución de la Firma, definir lo qué es una Firma y especialmente qué es una Firma Electrónica, cuáles son las funciones de una Firma, indicar cómo se crea una Firma Digital y cual es su validez a la luz del Decreto – Ley sobre Mensajes de Datos y Firmas Electrónicas Venezolana.

Se partió de un estudio exploratorio – descriptivo y se concluye que la firma electrónica posee la misma eficacia y validez, que la firma manuscrita y así lo establece el Decreto-Ley

Palabras Claves: Internet, Firma Digital, Decreto – Ley Sobre Mensajes de Datos y Firmas Electrónicas, Eficacia y Validez

SINCE THE HANDWRITING TOWARDS THE DIGITAL SIGNATURE: VENEZUELAN PERSPECTIVE

Abstract.

One of the consequences of an open network as Internet, are the problems of security and confidentiality. This paper intends to show the evolution of the Digital Signature, to define what the signature and specialty digital signature is, its functions, to show how to do a digital signature and which is its efficacy and valid in the new Venezuelan Electronic Signature and Dates Message Law.

This paper starts from an exploratory – descriptive study and concludes that the Digital Signature has the same efficacy and valid that the hand writing signature and this is established in the Law.

Keys Words : Internet, Digital Signature, Venezuelan Electronic Signature and Dates Message Law, Efficacy and Valid.