EL TRATAMIENTO LEGAL DE LA FIRMA ELECTRÓNICA EN COLOMBIA Y EN EL DERECHO UNIFORME

Por Marco Pérez*

En esta breve ponencia deseo abordar algunos aspectos generales de las denominadas firmas electrónicas y en particular pretendo hacer algunas reflexiones sobre el alcance de las normas sobre firma y firma digital de la Ley 527 de 1999 y en el Decreto 1747 de 2001 [1].

En primer lugar voy a realizar una introducción a la importancia de la firma como elemento de seguridad en los mercados electrónicos, en segundo lugar abordaré la definición de firma electrónica, en tercer lugar estudiaré las diversas modalidades de firma electrónica que se pueden utilizar en entornos electrónicos a la luz de la legislación vigente en Colombia y finalmente presentaré algunas conclusiones sobre el tema tratado.

I. Introducción

Los sistemas de información en redes abiertas y cerradas están expuestos a innumerables riesgos y amenazas, unos y otras propias del entorno tecnológico en el cual operan dichos sistemas.

Los atributos de la información: su integridad, autenticidad y su confidencialidad se encuentran amenazados por incidentes informáticos como el espionaje y sabotaje informático, el acceso remoto no autorizado, los ataques con virus, la denegación del servicio o la interceptación de correos electrónicos.

Para proteger debidamente la información de las organizaciones, estos riesgos y amenazas se pueden minimizar usando sistemas de seguridad informática, como son los sistemas firewall, los sistemas antivirus, los sistemas de detección de intrusos o sistemas de autenticación como las firmas electrónicas.

El uso de firmas electrónicas es una de las formas de atenuar los riesgos y amenazas contra la información, en la medida que además de cumplir las funciones básicas de las

---

* Investigador de la Universidad Externado de Colombia. Esta ponencia fue presentada por el autor en el XVII Congreso Nacional de Derecho Comercial: "Derecho y Comercio Electrónico". organizado por el Colegio de Abogados de Medellín, Septiembre de 2001.

[1] Ley 527 de agosto 18 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones".

Decreto 1747 del 11 de septiembre de 2001. Por el cual se reglamenta parcialmente la ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales"

firmas manuscritas, sirven como restricción de acceso a los datos y a la información sensible de las organizaciones.

Cada método de firma electrónica ofrecerá menor o mayor confiabilidad de acuerdo con la capacidad técnica que posea para garantizar la presencia de los atributos de la información.

Dicha capacidad técnica determina en gran medida la confiabilidad de los métodos de autenticación; sin embargo desde mediados de los años noventa del siglo pasado y con el auge de Internet, se adoptaron en diversos países, leyes que definen criterios jurídicos mínimos para que una firma electrónica se acepte como válida y como equivalente a una firma manuscrita.

En la presente ponencia pretendemos revisar cómo las tecnologías de firma electrónica disponibles en el mercado, se ajustan a las exigencias señaladas en la Ley colombiana de firmas electrónicas y cuál es el nivel de confiabilidad técnica y jurídica que ofrecen dichas tecnologías para proteger los datos que se envían, reciben, trasmiten y conservan en entornos digitales.

II. La noción de firma electrónica

La firma manuscrita es el método más frecuente y habitual de expresar el consentimiento. La firma nos permite atribuir una declaración de voluntad o una declaración de ciencia a una persona determinada[2]. La firma en entornos físicos garantiza fundamentalmente el atributo de autenticidad de la información.

En el artículo 826 de nuestro Código de Comercio, se define firma como la expresión del nombre del suscriptor o de alguno de alguno de los elementos que la integren o de e un signo o símbolo empleado como medio de identificación personal.

Esta definición no coincide con el concepto de firma, que se asocia con los sistemas de autenticación que se utilizan escenarios digitales. Las definiciones tradicionales de firma, como la antes citada, hacen énfasis en la firma como resultado, porque la firma manuscrita vincula en su creación rasgos personales del firmante, que sirven para verificar la identidad del firmante, que acreditan que el firmante intervino en el acto de firma y que acepta el contenido del documento que suscribe.

Cuando existe duda sobre la identidad del firmante, la firma manuscrita una vez plasmada sobre el documento físico, puede ser cotejada con un patrón de firma establecido previamente que compendia los rasgos o trazos personales que el creador de la firma definió para crearla. Estas firmas son perennes, porque la seguridad que ofrecen esta vinculada con los trazos personalísimos que realiza el autor al suscribir cada documento[3].

[2] Madrid Parra Agustín, Seguridad, pago y entrega en el comercio electrónico, Revista de Derecho Mercantil, Madrid, Número 241, julio-septiembre de 2001, Pág. 1195.

[3] Madrid Parra Agustín, la identificación en el comercio electrónico, Revista de la Contratación Electrónica, Madrid, Número 15, abril 2001, 5-6.

Las firmas manuscritas, son hoy la herramienta fundamental para imprimirle confianza y seguridad al tráfico jurídico, sin embargo en la medida que el uso y circulación de la información digital se ha venido generalizando, han irrumpido en las relaciones jurídicas, las llamadas firmas electrónicas, las cuales son también herramientas de confianza, pero con características diferentes, porque se utilizan en redes de comunicaciones cerradas o abiertas como puede ser una red EDI o la red Internet [4] .

Las denominadas firmas electrónicas, poseen elementos que no son los mismos de la noción tradicional de firma, porque en un entorno electrónico, entre otras circunstancias, el original de un documento no se puede distinguir de una copia, ni lleva una firma manuscrita y no reposa sobre un papel[5].

Las firmas electrónicas son métodos matemáticos, numéricos o lógicos, son un conjunto de instrucciones que sirven fundamentalmente para identificar a una persona que se comunica a distancia utilizando dispositivos o equipos informáticos para crear, procesar, enviar, recibir o almacenar su información en forma de mensajes de datos y usando redes de comunicación para trasmitirla[6].

Los métodos de firma electrónica, además de imputar o atribuir de forma confiable un mensaje de datos a una persona determinada, sirven como mecanismo de ingreso o acceso a sistemas de información. Como se mencionó antes, estos métodos pueden ser más o menos seguros de acuerdo con la capacidad técnica que posean para garantizar y verificar la presencia de los atributos de la información a la cual se vincula el método: autenticidad, integridad y confidencialidad.

La confiabilidad técnica de un método de firma electrónica puede estar dada por la eficiencia para lograr su cometido, por el alcance de la tecnología seleccionada para identificar al usuario de un sistema de información o para autenticar los mensajes de datos a los cuales se vincula, por la diligencia y cuidado que tenga el usuario en su utilización o por la confiabilidad de dicha tecnología en relación con el propósito de la comunicación. Algunos métodos de firma electrónica deben ser modificados o cambiados con el paso del tiempo, porque pueden quedar expuestos al conocimiento de personas diferentes a su titular o porque el estado de la técnica permite romper su seguridad o vulnerar su confiabilidad.

Los métodos de firma electrónica de uso más común en redes de comunicación, basan su confiabilidad y desempeño técnico, en los siguientes criterios[7]:

---

[4] " Firmas electrónicas son los medios técnicos disponibles en el mercado o que se estén desarrollando, para que algunas o todas las funciones identificadas como características de las firmas manuscritas se puedan cumplir en un entorno electrónico" . Guía para la Incorporación al Derecho Interno de la Ley Modelo de la Comisión de las Naciones Unidas sobre Firma Electrónica. Documento A/CN/ .9 / 493 - 17 de mayo de 2001. Párrafo 30. pág 22.

[5] Guía para la Incorporación al Derecho Interno de la Ley Modelo de la Comisión de las Naciones Unidas sobre Firma Electrónica. Documento A/CN/ .9 / 493 - 17 de mayo de 2001. Párrafo 30. pág 22.

[6] Biddle Bradford, Legislating Market Winners: Digital Signature Laws and Electronic Commerce Market Places, San Diego Law Review, Vol 34, 1997, pág 1225.

[7] Baker Stewart A. – Hurst Paul R. - The Limits of Trust , Criptography, Goverments and Electronic Commerce, Kluwer Law International, 1998, pág 1 – 8.

Criterio	Método
Algo que usted sabe o conoce	Password o clave personal
Algo que usted tiene o posee	Clave privada de un método de firma digital, incorporada en un dispositivo físico - tarjeta con banda magnética o con un microchip-.
Algo que usted es	Dispositivo de identificación biométrico: disposición de los rasgos de la huella digital, de los vasos sanguíneos del iris del ojo, de las líneas de la palma de la mano, de la estructura ósea del rostro o del timbre de la voz.

Como conclusión preliminar, resulta relevante afirmar que las tecnologías o métodos de firma electrónica, poseen características diferentes y su uso responde a los diversos niveles de seguridad de la información que se requieran o necesiten en cada organización o espacio negocial. Si la seguridad exigida es superior, el método de firma será más complejo o se utilizarán métodos diversos que coexisten unos con otros y que aplican los criterios de confiabilidad citados antes.

III. La validez de las firmas electrónicas

La Ley Modelo de Comercio Electrónico (1996), de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional CNUDMI- en adelante LMCE -, sirvió de texto guía principal para la elaboración de la Ley 527 de 1999. Esta Ley Modelo se basa entre otros, en el principio del equivalente funcional, el cual consiste en determinar si las funciones de un requisito de forma consignado sobre papel, se pueden cumplir con técnicas o métodos asociadas con el denominado comercio electrónico[8].

En particular en cuanto a la definición de firma electrónica, nuestra ley acoge el texto del artículo 7o de la LMCE[9], que desarrolla el principio de equivalencia funcional de los métodos de firma electrónica, cuando cumplen las funciones que se atribuyen a una firma manuscrita en las comunicaciones consignadas sobre papel.

[8] " La Ley Modelo no pretende definir un equivalente informático para todo tipo de documentos de papel, sino que trata de determinar la función básica de cada uno de los requisitos de forma de la documentación sobre papel, con miras a determinar los criterios que, de ser cumplidos por un mensaje de datos, permitirían la atribución a ese mensaje de un reconocimiento legal equivalente al de un documento de papel que haya de desempeñar idéntica función. Cabe señalar que en los artículos 6 a 8 de la Ley Modelo se ha seguido el criterio del equivalente funcional respecto de las nociones de "escrito", "firma" y "original", pero no respecto de otras nociones jurídicas que en esa Ley se regulan.". Párrafo 18. Guía para la Incorporación al Derecho Interno de la Ley Modelo de la Comisión de las Naciones Unidas sobre Comercio Electrónico. Nueva York, 1999. pág 22.

[9] " 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.
3) Lo dispuesto en el presente artículo no será aplicable a: [...]." . Artículo 7 - Firma. Ley Modelo de la Comisión de las Naciones Unidas sobre Comercio Electrónico. Nueva York, 1999. pág 6.

El artículo 7o de la Ley 527 de 1999, que corresponde al artículo 7 de la LMCE, ofrece una solución general, que establece los requisitos mínimos que de ser observados por un mensaje de datos[10], lo acreditan como un documento firmado. Esta norma es de carácter imperativo y no puede ser modificada por acuerdo entre las partes.

Como la solución jurídica del artículo 7o de la Ley 527, es general y neutra, se abrió el espectro de las tecnologías o métodos de firma, que se pueden utilizar como equivalentes de la firma manuscrita. Nuestra Ley, a diferencia de otras legislaciones, no relaciona o define los estándares técnicos de los diversos métodos de firma electrónica, que se consideren válidos o confiables.

Revisemos con más detenimiento el artículo 7o de la Ley 527 de 1999. Esta norma expresa que todo requisito de firma manuscrita que esté establecido en cualquier norma vigente[11] – constitucional, legal, reglamentaria, etc- se podrá observar válidamente con un método de firma electrónica, que cumpla con los siguientes requisitos mínimos:

1) Debe permitir *identificar* al iniciador de un mensaje de datos

2) Debe servir *para indicar que el contenido cuenta con su aprobación*.

3) Debe ser confiable y apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Esta disposición permite que los requisitos de firma, que están presentes en el ordenamiento colombiano en normas de nivel nacional, departamental o municipal sean cumplidos con métodos de firma electrónica, siempre y cuando se observen los requisitos antes expresados y no resulta aplicable a requisitos de autenticidad complejos, como la presencia de firmas autenticadas, firmas certificadas o el uso de sellos.

El artículo 7o de la ley 527, consagra una categoría jurídica- no una categoría técnica - que al desarrollar el principio de equivalencia funcional, persigue que los jueces o árbitros, apliquen los requisitos de la ley caso por caso sin restringir el uso de nuevas tecnologías de firma. Para cada tecnología de firma, el juez o el árbitro hará una adecuación de la misma, frente a los requisitos del artículo 7o de la Ley 527 de 1999. Cuando se utilicen métodos de firma electrónica y no exista un requisito legal de autenticidad, que deba ser observado obligatoriamente por las partes, el artículo 7o, tendrá función orientadora tanto para las partes como para el juez o el árbitro.

---

[10] Ley 527 de 1999. Artículo 2°. Definiciones. Para los efectos de la presente ley se entenderá por:

a) Mensaje de Datos. La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax;

[11] La sentencia 831 del año 2001, de la Corte Constitucional es el primer precedente judicial en Colombia, que aplica a un requisito de forma particular establecido en nuestro ordenamiento jurídico, el principio de equivalencia funcional de los artículos 6, 7 y 8 de la Ley 527 de 1999. La Corte señalo en su decisión que conforme al artículo 6 de la Ley 527 de 1999, los jueces pueden utilizar validamente mensajes de datos como equivalentes a un documento en papel, para proferir un mandamiento escrito, que ordene el arresto, la prisión o el registro del domicilio de una persona determinada (artículo 28 de la Constitución Nacional).

Establece el artículo 7o que las funciones de firma, que se deben cumplir con el método de autenticación utilizado, son dos: 1) identificar al iniciador del mensaje y 2) Permitir indicar que el contenido cuenta con su aprobación.

Estas dos funciones, son las funciones básicas de una firma manuscrita. La pregunta que nos debemos hacer es si los métodos de firma enunciados en la sección II. del presente documento, cumplen con dichas funciones y si observan los requisitos mínimos establecidos en la norma en estudio.

a) Métodos de firma basados en el criterio " algo que usted sabe"

Los métodos de firma, como los passwords o las claves personales, están basados en el criterio " algo que usted sabe " y permiten en principio solo identificar al originador del mensaje. Revisemos si pueden cumplir las funciones de firma señaladas en el artículo 7º de Ley 527 de 1999.

Estos métodos se utilizan como mecanismo de acceso a los servicios en línea dirigidos a los consumidores. Los servicios de banca personal en la red Internet, el usuario se autentica ante el banco virtual, utilizando su nombre de usuario y su clave de acceso secreta, antes de iniciar la sesión de consulta o realizar la transacción. Las sucursales financieras ubicadas en esta red publica, suelen ofrecer adicionalmente al usuario un canal de comunicación seguro, en el cual los datos de la transacción viajan encriptados, para impedir que su confidencialidad sea vulnerada y que sean conocidos por personas no autorizadas.

Respecto de lo dispuesto en el artículo 7º, este método podría ser considerado firma, porque el usuario de un servicio de banca en línea, además de identificarse con su nombre de usuario y clave personal, aceptó previamente el carácter vinculante de su uso y su confiabilidad. Dicha aceptación la manifestó al suscribir el contrato de cuenta de ahorros o cuenta corriente y al aceptar los términos del acuerdo de comunicación que regula la utilización del canal Internet. Los acuerdos de comunicación generalmente se perfeccionan por escrito o a través de la utilización de un mecanismo de aceptación en línea - click wrap agreement-. En su texto se establece que las transacciones realizadas en línea por el usuario son válidas y que el usuario será responsable por todas las operaciones adelantadas con su clave de acceso, inclusive las transacciones llevadas a cabo por personas no autorizadas.

Los métodos basados en el criterio " algo que usted sabe" , sirven primordialmente para autenticar sesiones de comunicación en línea, más que para autenticar o firmar mensajes de datos particulares. El usuario una vez agotado el proceso de autenticación y que se le permite ingresar al sistema de información del banco, puede desistir de realizar consultas o transacciones, a pesar de haber utilizado el método de firma convenido.

En conclusión, estos métodos son un mecanismo de acceso a sistemas de información que funcionalmente se pueden asimilar en determinados casos a una firma.

De otro lado y conforme a lo dispuesto en el literal b del artículo 7º , el método de firma debe ser confiable y apropiado para el propósito por el cual el mensaje fue generado o comunicado.

Para analizar este punto regresemos al ejemplo de la banca personal en Internet. El método es confiable si el banco puede verificar en sus bases de datos, que el usuario al utilizar su clave personal es quien dice ser, si la información relativa a cada transacción se transmite de forma confidencial y si es posible verificar la integridad de la información relativa a las operaciones que adelanta el usuario

En este caso la confiabilidad del método, la encontraríamos en las condiciones de seguridad que ofrece la plataforma tecnológica del banco, pero también en el carácter privado y secreto del password o clave personal creada por el usuario para acceder a los servicios del banco en Internet.

En cuanto a lo apropiado del método según el propósito de la comunicación[12], los bancos suelen ofrecer mayores niveles de seguridad en la medida en que la transacción virtual, sea de mayor cuantía o entidad. Por ejemplo en el caso de operaciones en línea con empresas o personas jurídicas, algunos bancos utilizan sistemas de autenticación robusta, que además de claves personales de acceso al sistema, utilizan certificados digitales emitidos por el mismo banco a cada cliente corporativo y que le permite al mismo banco, con la clave pública del cliente verificar su identidad, verificar la autenticidad de los mensajes de datos que el cliente firme con su clave privada y constatar la integridad de los mensajes recibidos.

b) Métodos de firma basados en "algo que usted es"

Como mencionamos antes los dispositivos de autenticación biométrica, validan la identidad de las personas a partir de características biológicas únicas. Estas tecnologías son novedosas en Colombia, pero su aceptación en países desarrollados crece día tras día[13].

[12] " Para determinar si el método seleccionado con arreglo al párrafo 1) del artículo 7 de la LMCE, es apropiado, pueden tenerse en cuenta, entre otros, los siguientes factores jurídicos, técnicos y comerciales: 1) la perfección técnica del equipo utilizado por cada una de las partes; 2) la naturaleza de su actividad comercial; 3) la frecuencia de sus relaciones comerciales; 4) el tipo y la magnitud de la operación; 5) la función de los requisitos de firma con arreglo a la norma legal o reglamentaria aplicable; 6) la capacidad de los sistemas de comunicación; 7) la observancia de los procedimientos de autenticación establecidos por intermediarios; 8) la gama de procedimientos de autenticación que ofrecen los intermediarios; 9) la observancia de los usos y prácticas comerciales; 10) la existencia de mecanismos de aseguramiento contra el riesgo de mensajes no autorizados; 11) la importancia y el valor de la información contenida en el mensaje de datos; 12) la disponibilidad de otros métodos de identificación y el costo de su aplicación; 13) el grado de aceptación o no aceptación del método de identificación en la industria o esfera pertinente, tanto en el momento cuando se acordó el método como cuando se comunicó el mensaje de datos; y 14) cualquier otro factor pertinente.". Párrafo 58. Guía para la Incorporación al Derecho Interno de la Ley Modelo de la Comisión de las Naciones Unidas sobre Comercio Electrónico. ONU. Nueva York, 1999. pág 41.

[13] De acuerdo con cifras de la firma International Biometric Group - www.biometricgroup.com- , el uso de métodos de autenticación biométrica en sistemas de información, han tenido en el año 2001 la siguiente demanda a nivel mundial:

Tecnología Biométrica	Participación en el mercado
Escáneres de Huellas digitales	44%
Sistemas del reconocimiento del rostro	14%
Escáneres de geometría de la mano	13%
Sistemas de autenticación de voz	10%
Sistemas de escaneado de iris	8%

Estos métodos de autenticación biométrica han desplazo el uso de passwords y claves personales, para proteger el acceso a las redes de las empresas y a la información digital altamente sensible de las organizaciones; porque los passwords y claves personales son fácilmente expuestos, extraviados o inapropiadamente compartidos. Además no hay necesidad de realizar reposición de tarjetas de acceso perdidas o nueva asignación de contraseñas olvidadas, ya que las características corporales no cambian, no se modifican, extravían, ni se pueden prestar o ceder.[14]

En lo referente a la utilización de estos mecanismos como método valido de firma, a la luz de lo dispuesto en el artículo 7 de la Ley 527 de 1999, el análisis es similar al que realizamos para los métodos de firma basados en el criterio anterior : " algo que usted sabe" .

Estos métodos sirven en particular para identificar a la persona, pero también podrían servir para vincular al originador con el contenido del mensaje, si existe por ejemplo una relación jurídica precedente – contrato laboral - en virtud de la cual el usuario del dispositivo biométrico tiene acceso exclusivo y restringido a sistemas de información - Intranet o red corporativa - y puede realizar actividades que lo vinculan contractualmente.

Respecto de la exigencia de confiabilidad del método de firma basado en un dispositivo biométrico y establecida en el literal a) del artículo 7º de la Ley 527, ésta se verificará de acuerdo a la capacidad de esta tecnología de garantizar los atributos de la información. En la práctica estos métodos ofrecerán mayor o menor nivel de confiabilidad de acuerdo con el uso que se haga de ellos y si complementan otras tecnologías de seguridad como el uso de certificados de firma digital[15].

En lo atinente al requisito previsto en el artículo 7º , referente a que el método de firma, además de confiable, sea apropiado para los fines por los cuales se generó o comunicó el mensaje, en el caso de dispositivos biométricos éstos serán apropiados de acuerdo con la importancia de la comunicación o transacción. En la medida que la transacción revista mayor importancia, estas tecnologías se utilizarán en concurrencia con otras tecnologías de seguridad que permitan verificar la presencia de cada uno de los atributos de la información que se envía y recibe.

c) Métodos de firma basados en el criterio "algo que usted tiene o posee".

El tercer criterio de confiabilidad de los métodos de firma electrónica: es el criterio que basa su confiabilidad "en algo que usted tiene o posee". Las llamadas firmas numéricas o digitales son las que se ajustan a este criterio.

---

[14] www.biometricgroup.com

[15] " Ciertas técnicas de firma se basarían en la autenticación mediante un dispositivo biométrico basado en las firmas manuscritas. Con ese dispositivo el firmante firmaría de forma manual utilizando un lápiz especial en una pantalla de computadora o en un bloc numérico. La firma manuscrita seria luego analizada por la computadora y almacenada como un conjunto de valores numéricos que se podrían agregar a un mensaje de datos y que el receptor podría recuperar en pantalla para autenticar la firma . Este sistema de autenticación exigiría el análisis de muestras de firmas manuscritas y su almacenamiento utilizando el dispositivo biométrico." Guía para la Incorporación al Derecho Interno de la Ley Modelo de la Comisión de las Naciones Unidas sobre Firma Electrónica. Documento A/CN/ .9 / 493 - 17 de mayo de 2001. Párrafo 33. pág 23.

Las firmas digitales son métodos de firma electrónica, basados en algoritmos de encriptación asimétrica y que utilizan llaves o claves públicas y privadas en el proceso de creación y verificación de las firmas. Esta tecnología de firma, también se denomina criptografía de clave pública [16].

Nuestra Ley de Comercio Electrónico, les da un tratamiento preferencial a las firmas digitales, en los artículos 2º y 28º , definiéndolas en el primero y en el segundo estableciendo sus efectos y sus atributos de validez.

La consagración legal de estas firmas como una modalidad de firma electrónica, se ha generalizado en muchos países, en la medida que ofrecen un mayor nivel de confianza para garantizar la presencia de los atributos de la información: autenticidad, integridad y confidencialidad y no repudio [16].

La Ley 527 de 1999, en su artículo 2[17], define la firma digital. Esta definición integra los elementos técnicos de la firma digital, basada en tecnología de criptografía de clave pública, veamos:

Se define la firma digital como un valor númerico, que se crea con la clave privada del firmante. Para crear firmas digitales se utiliza un programa de computador basado en un procedimiento matemático denominado algoritmo de creación de firmas. La firma digital cambia de un documento a otro en la medida en que los datos de la clave privada se mezclan con los datos de cada documento que sea firmado con la misma clave privada. Para cada documento firmado se crea una nueva firma digital. Lo que no cambia es la clave privada.

El procedimiento de verificación de la autenticidad de las firmas, es un programa de computador basado en un procedimiento matemático que se denomina algoritmo de verificación de firmas. A través de este procedimiento se verifica que el documento fue firmado con la clave privada del firmante (autenticidad) y que la información del documento se conserva completa e inalterada (integridad).

---

[16] " La tecnología de criptografía de clave pública consiste en generar dos números través de un programa de computo, matemáticamente relacionados, a los que se les denomina llaves. Una llave es un número de gran tamaño, que se puede conceptualizar como un mensaje digital, como un archivo binario o como una cadena de bits o bytes. Las llaves tienen características matemáticas. Su generación es siempre en parejas y están relacionadas de tal forma que si dos llaves públicas son diferentes, entonces las correspondientes llaves privadas son diferentes y viceversa. En otras palabras si dos sujetos tienen llaves públicas diferentes, entonces sus llaves privadas son diferentes. La idea es la de que cada individuo genere un par de claves: pública y privada. El individuo debe mantener en secreto su clave privada, mientras que la llave pública la puede dar a conocer a otros individuos. El procedimiento de firmado consiste en que mediante un programa de computo, un sujeto alimenta un documento a firmar y su llave privada (que solo el conoce) . El programa produce como resultado un mensaje digital (la firma digital) . Juntos el documento y la firma constituyen el documento firmado. El proceso de autenticación consiste en que mediante un programa de computo se alimenta el documento firmado y la llave pública del supuesto firmante. El programa indica si el documento es autentico o no es autentico." Mendívil Ignacio, ABC de los documentos electrónicos seguros, www.acertia.com , México, 1999, pág 3.

[17] Ley 527 de 1999. " Artículo 2. (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".

El artículo 28[18] de la Ley 527, establece expresamente las funciones y los atributos jurídicos de la firma digital.

Señala la norma, que se presume que cuando una firma digital haya sido fijada en un mensaje de datos, el suscriptor del mensaje, tenía la intención de acreditar ese mensaje de datos y de ser vinculado con el contenido del mismo.

Esta presunción es de carácter legal y admite prueba en contrario. Sin embargo quien pretenda beneficiarse de la presunción, deberá observar los requisitos del parágrafo del mismo artículo 28.

En este parágrafo, se establece expresamente que la firma digital será equivalente a la firma digital, si está última, 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.

Estos atributos de validez, son concurrentes y reiteran los elementos técnicos y de funcionamiento de este tipo de tecnología. Es importante señalar que la norma no es precisa en cuanto al atributo del numeral 3, por cuanto la firma digital no está bajo control exclusivo de la persona que la usa; lo que se encuentra bajo poder exclusivo del suscriptor o firmante, es la clave privada.

El artículo 28 de la Ley 527, fue reglamentado por el artículo 15 del Decreto 1747 de 2000.[19]

---

[18] Ley 527 de 1999. 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.

19 Decreto 1747 de 2000. Artículo 15. USO DEL CERTIFICADO DIGITAL. Cuando quiera que un suscriptor firme digitalmente un mensaje de datos con su clave privada, y la respalde mediante un certificado digital, se darán por satisfechos los atributos exigidos para una firma digital en el parágrafo del artículo 28 de la ley 527 de 1999, sí:

1. El certificado fue emitido por una entidad de certificación abierta autorizada para ello por la Superintendencia de Industria y Comercio.

De la lectura de esta norma reglamentaria, podemos advertir que los atributos legales de la firma digital deben ser concurrentes para beneficiarse de la presunción de validez del artículo 28. El Decreto 1747 en su artículo 15, creó las denominadas firmas digitales certificadas, que son las creadas y verificadas con la tecnología de criptografía de clave pública y que adicionalmente están respaldadas en certificados digitales emitidos por entidades de certificación autorizadas.

Es importante precisar que si la información que se pretende hacer valer judicialmente consta un mensaje de datos firmado digitalmente y dicha firma se respalda en un certificado digital, no se requiere que el interesado, pruebe la presencia de los atributos del parágrafo del artículo 28, basta con que allegue con la demanda, el mensaje de datos firmado, el certificado digital vigente, la resolución emitida por la Superintendencia de Industria y Comercio, que autoriza las actividades de la entidad de certificación que emitió el certificado y el contrato entre la entidad de certificación y el suscriptor que acredite expresamente los usos para los cuales se podía utilizar el certificado[20].

La inquietud que surge, es si las firmas digitales que no cuenten con el respaldo de un certificado digital se entenderán como no validas a la luz del artículo en mención.

Si la firma digital del mensaje de datos no cuenta con el respaldo de un certificado digital, el interesado debe probar la presencia de los atributos del artículo 28, para que dicha firma se entienda equivalente a una firma manuscrita. Los artículos 7º y 28 de la Ley 527 de 1999, que definen firma y firma digital además de ser imperativos, sirven de orientación cuando el derecho interno deje totalmente a discreción de las partes la autenticación de los mensajes de datos.

Adicionalmente si dicha firma digital no certificada, se utiliza para cumplir un requisito de forma establecido en la ley, el interesado deberá acreditar la presencia de los requisitos del artículo 7º de la Ley 527 de 1999, que ya fueron citados antes. Sin embargo es importante mencionar que la confiabilidad de una firma digital, se acredita probando los atributos de la firma establecidos en el artículo 28.

En este punto de la ponencia, es imperioso comentar acerca de la validez de las firmas digitales respaldadas por certificados emitidos por una entidad de certificación extranjera y no autorizada para operar conforme a la legislación colombiana.

Nuestra Ley 527 de 1999, en su artículo 43[21], exige que los certificados extranjeros sean validados por una entidad de certificación colombiana, sin embargo por la dinámica

---

2. Dicha firma se puede verificar con la clave pública que se encuentra en el certificado con relación a firmas digitales, emitido por la entidad de certificación.

3. La firma fue emitida dentro del tiempo de validez del certificado, sin que éste haya sido revocado.

4. El mensaje de datos firmado se encuentra dentro de los usos aceptados en la DPC, de acuerdo al tipo de certificado.

[20] Parra Quijano Jairo, Manual de Derecho Probatorio, Ediciones Librería el Profesional, Bogotá, 2002, Pág. 481.

[21] Ley 527 de 1999.- Artículo 43. *Certificaciones recíprocas*. Los certificados de firmas digitales emitidos por entidades de certificación extranjeras, podrán ser reconocidos en los mismos términos y condiciones exigidos en la ley para la emisión de certificados por parte de las entidades de certificación nacionales, siempre y

del comercio electrónico en Internet, es posible que algunas empresas vengan usando firmas avaladas en certificados extranjeros cuyo emisor no ha sido autorizado para operar en Colombia, como entidad de certificación.

En concepto 02026239 del año 2002, la oficina jurídica de Superintendencia de Industria y Comercio, en respuesta a un derecho de petición elevado por el autor de esta ponencia, expreso que las firmas digitales avaladas por certificados extranjeros se entenderían validas a la luz de los artículos 7º y 28 de la Ley 527 de 1999, porque estas disposiciones no establecen como requisito de validez de los métodos de firma electrónica, la presencia de un certificado digital o el respaldo de una entidad de certificación autorizada.

Otro aspecto acerca de la validez de las firmas digitales en Colombia, que genera interrogantes, fue la diferenciación que hizo el artículo 1 del Decreto 1747 de 2000, entre entidades de certificación cerradas y abiertas [22].

La Superintendencia de Industria y Comercio SIC en el concepto antes mencionado, señaló que la razón fundamental que tuvo el Gobierno Nacional, para diferenciar entre entidades de certificación abiertas y cerradas, fue el hecho de que las entidades de certificación cerradas no están destinadas para prestar servicios al público.

Las entidades de certificación cuando operan en redes cerradas, también son un agente de confianza o de seguridad jurídica. Son un tercero confiable en el entorno cerrado, que es a la vez parte en la comunicación y ente certificante de las firmas digitales que se usan en esa red. Generalmente los servicios de entidad de certificación cerrada los utilizan empresas que negocian o transan entre si, de forma no presencial a través de canales dedicados como redes virtuales privadas o que proveen servicios a través de Internet a usuarios específicos - Banca o gobierno en línea -.

El artículo 4 del decreto 1747 de 2000, señala adicionalmente que:

" ..... Los certificados emitidos por las entidades de certificación cerradas deberán indicar expresamente que sólo podrán ser usados entre la entidad emisora y el suscriptor. Las entidades deberán informar al suscriptor de manera clara y expresa, previa expedición de los certificados, que éstos no cumplen los requisitos del artículo 15 del presente decreto" .

Esta norma, establece de forma equivocada, que los certificados digitales emitidos por las entidades de certificación cerradas poseen menor valor que los emitidos por

---

cuando tales certificados sean reconocidos por una entidad de certificación autorizada que garantice en la misma forma que lo hace con sus propios certificados, la regularidad de los detalles del certificado, así como su validez y vigencia.

[22] Decreto 1747 de 2000.- Artículo 1 . DEFINICIONES. Para efectos del presente decreto se entenderá por:

1. ENTIDAD DE CERTIFICACIÓN CERRADA: Entidad que ofrece servicios propios de las entidades de certificación sólo para el intercambio de mensajes entre la entidad y el suscriptor, sin exigir remuneración por ello.

2. ENTIDAD DE CERTIFICACIÓN ABIERTA: La que ofrece servicios propios de las entidades de certificación, tales que:

   a. Su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor; o

b. Recibe remuneración por éstos

entidades de certificación abiertas, a pesar de que ellos pueden ofrecer los mismos niveles de confiabilidad técnica y jurídica. La tecnología de emisión de los certificados y de creación y verificación de las firmas que usa la entidad de certificación cerrada se basa en algoritmos de encripción asimétrica, que es la misma tecnología de seguridad que utiliza la entidad de certificación abierta.

Conforme a esta norma del Decreto 1747, una firma digital amparada en un certificado emitido por una entidad de certificación cerrada, no goza de forma automática del beneficio de la presunción legal del artículo 28 y quién pretenda hacer valer en juicio, un documento firmado con dicha firma, deberá probar primero la presencia de los atributos que establece el parágrafo de este artículo.

El artículo 4º resulta restrictivo del principio de autonomía de la voluntad y le niega efectos jurídicos a un método de firma que es confiable. En otros términos va en contravía de los principios minimalista, de neutralidad tecnológica y no discriminación que sustentan la normativa de la Ley 527 de 1999 [23].

El principio minimalista expresa que los estados nacionales que adopten los principios de la LMCE, no deben crear normas que establezcan requisitos adicionales para las firmas electrónicas frente a los requisitos de forma relativos a documentos en papel [24].

Sobre este último aspecto de esta ponencia, me parece pertinente citar el mandato expreso del texto de la Directiva Europea de Firma Electrónica[25], en su considerando 16, que señala que los Estados miembros de la Unión, no se deben negar efectos jurídicos a las firmas electrónicas utilizadas en sistemas cerrados.

Esta directiva tiene un ámbito de aplicación diferente a una ley nacional, como nuestra Ley 527 de 1999, sin embargo reconoce expresamente un principio que también sustenta a nuestra ley y al desarrollo del comercio electrónico en Internet. Es el principio de la autonomía de la voluntad de las partes para definir métodos que se ajusten a su necesidades particulares. Dice la directiva en el mencionado considerando que ha de respetarse la libertad de las partes para concertar de común acuerdo las condiciones en que aceptarán las firmas electrónicas y no se debe privar a las firmas electrónicas utilizadas en sistemas cerrados de eficacia jurídica ni de su carácter de prueba en los procedimientos judiciales.

IV. Conclusiones

---

[23] Ley 527 de 1999.- Artículo 5°. *Reconocimiento jurídico de los mensajes de datos.* No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos. (principio de no discriminación)

[24] **"**..... Debe considerarse que las reglas enunciadas en el capítulo II expresan el "mínimo aceptable" en materia de requisitos de forma para el comercio electrónico, por lo que deberán ser tenidas por imperativas, salvo que en ellas mismas se disponga lo contrario. El hecho de que esos requisitos de forma deban ser considerados como el "mínimo aceptable" no debe, sin embargo, ser entendido como una invitación a establecer requisitos más estrictos que los enunciados en la Ley Modelo." Párrafo 21. Guía para la Incorporación al Derecho Interno de la Ley Modelo de la Comisión de las Naciones Unidas sobre Comercio Electrónico. Nueva York, 1999.

[25] Directiva 1999/93/CE del Parlamento Euopeo y del Conejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica.

Como conclusión de esta ponencia, presento algunas consideraciones finales acerca del tratamiento legal de las firmas electrónicas en Colombia:

a) El Gobierno Nacional debe revisar las normas del decreto 1747 de 2000, referentes a los efectos jurídicos de los certificados emitidos por entidades de certificación cerradas y eliminar las restricciones jurídicas que no consulten la dinámica del comercio electrónico en Internet.

b) Se deben utilizar los principios y normas de la Ley 527 de 1999, para estudiar posibles reformas legales a los requisitos de autenticidad de carácter complejo, como los establecidos en el Estatuto Notarial o en Código Civil y que representan un obstáculo para el desarrollo del comercio electrónico en Internet.

c) Como parte de la agenda de conectividad que lidera el Ministerio de Comunicaciones y la Presidencia de la República, se debe establecer un programa de capacitación de jueces y árbitros, sobre los aspectos técnicos y jurídicos relativos a la validez y valoración probatoria de los mensajes de datos y las firmas electrónicas.

d) Las empresas que estén migrando sus datos e información a entornos electrónicos, deben revisar oportunamente: las funciones, la confiabilidad y el propósito de las tecnologías de firma que utilizan en redes cerradas y abiertas y verificar si su alcance se ajusta a lo dispuesto en las normas de la Ley 527 de 1999 sobre validez de los mensajes de datos y las firmas electrónicas.