ISSN 0041-8811
DEPÓSITO LEGAL pp 76-654

Revista de la Universidad del Zulia

Fundada en 1947
por el Dr. Jesús Enrique Lossada

Ciencias Sociales y Arte

Año 4 Nº 10
Septiembre - Diciembre 2013
Tercera Época
Maracaibo - Venezuela

Revista de la Universidad del Zulia 3ª época
Ciencias Sociales y Arte ///
Año 4 Nº 10, Septiembre-Diciembre 2013, 54 - 73
ISSN 0041-8811 ~ Depósito legal pp 76-654

La firma electrónica y los certificados electrónicos: mecanismos de seguridad del mensaje de datos

*Greily Villarreal**

Resumen

La importancia de las tecnologías de la información y comunicación (TIC), se deduce de múltiples actuaciones realizadas a través de medios electrónicos de transmisión y almacenamiento de datos, que van desde operaciones comerciales entre particulares, hasta procedimientos de contratación y/o trámites con el Estado; no obstante, nace la incertidumbre en quienes intervienen en un contrato electrónico, e inclusive a quienes acceden a portales web del gobierno, en cuanto a la seguridad, protección y eficacia jurídica de la información manejada. Por ello, el objetivo general de la presente investigación es determinar la existencia de mecanismos de seguridad de las transacciones electrónicas que permita remozar la confianza sobre este creciente modo de instrumentar las pretensiones de quienes acceden al uso de las TIC, para lo cual se realizó un estudio documental bibliográfico aplicando la hermenéutica jurídica, que permite evidenciar que el Estado ha desarrollado un conjunto de normas garantistas al uso de los medios electrónicos pero que sólo cuando se eduque a la sociedad y se creen las plataformas tecnológicas para asignar a

* Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia. greilyvillarrealvelasquez@gmail.com

RECIBIDO: 13-11-2013 /// ACEPTADO: 10-12-2013

cada ciudadano una firma electrónica con un certificado asociado, se podrá materializar el progreso tecnológico que en la legislación se vislumbra.

Palabras clave: Tecnologías de información y comunicación, documentos electrónicos, firma electrónica, certificados electrónicos, mecanismos de seguridad electrónicos.

The Electronic Signature and Electronic Certificates: Safety Mechanisms for Data Messages

Abstract

The importance of information and communication technologies (ICTs) can be deduced from multiple actions carried out through electronic means for data transmission and storage, which range from commercial operations between individuals to contracting procedures and/or procedures with the State. Nevertheless, uncertainty arises in those who intervene in an electronic contract and even those who access government web portals, as to the safety, protection and legal efficacy of the information being handled. The general aim of this research is to determine the existence of security mechanisms for electronic transactions that permit renewing confidence in this growing mode of orchestrating the claims of those who access use of ICTs. Therefore, a bibliographical documentary study applying legal hermeneutics was conducted. It shows that the State has developed a set of regulations to guarantee the use of electronic media. However, only when society is educated and technological platforms are created to assign an electronic signature with its associated certificate to every citizen will it be possible to bring into being the technological progress foreseen in the legislation.

Keywords: information and communication technologies, electronic documents, electronic signature, electronic certificates, electronic security mechanisms.

Introducción

Los documentos electrónicos, que hoy día sirven de vía, fundamento y eje de una cada vez mas creciente clase de actividades negociales, comunicacionales, intelectuales, contractuales y de toda índole de las que usa la sociedad contemporánea y que han pasado a ser por tanto, reconocidas y reguladas por las normas programáticas y especiales de los países, así como en Venezuela la Constitución Nacional de 1999 y la Ley de Mensajes de Datos y Firmas Electrónicas de 2001, abrazan la existencia y valor probatorio de esta clase de documentos, no pueden estar desprovistos de mecanismos de seguridad que garanticen en el usuario la seguridad jurídica de que las transacciones reflejadas en tales mensajes de datos, tienen la característica de integridad e inclusive la validez para soportar su pretensión en un eventual proceso administrativo o judicial en caso de controversias entre las partes.

En este sentido, la presente investigación ha tenido como objetivo general analizar la firma electrónica y el certificado electrónico concebido en la Ley de Mensaje de Datos y Firmas Electrónicas vigente, como mecanismos de seguridad de los mensajes de datos, que permitan a las partes tener la confianza para concertar transacciones electrónicas, e inclusive a un tercero que eventualmente deba dirimir una controversia cuyo documento fundante de la pretensión sea un documento electrónico, por lo que la valoración del mismo estaría supeditado a la presencia o no de los referidos mecanismos de seguridad.

El tenor metodológico por medio del que fue posible materializar lo expuesto, fue el de una investigación de tipo analítica, el diseño bajo el cual se estructuró fue documental, utilizándose la técnica de la observación documental basado en la hermenéutica jurídica; así, dicho estudio se fundamentó en la revisión documental del cuerpo normativo nacional e internacional y de la doctrina patria y extranjera, conocimiento éste que fue operacionalizado a través de la elaboración de una matriz de análisis.

Con esta nueva forma de contratar se plantean controversias tales como la ausencia del soporte en papel y de la firma autógrafa y las dudas referidas a la seguridad y validez del documento emitido y contenido en un soporte electrónico, que quedan expresamente rebatidas con las consideraciones realizadas en el desarrollo del presente trabajo.

1. La firma electrónica

Carrascosa y otros (1991:50), exponen que la firma como signo distintivo y personal, reúne los siguientes elementos funcionales, aplicables también a las firmas electrónicas:

1. La identificación: La firma asegura la relación jurídica entre el acto firmado y la persona que lo ha firmado. Este elemento conduce al autor de la firma, y es un proceso pasivo por cuanto dicha función puede hacerse *a posteriori* o incluso sin el consentimiento del autor.
2. La autentificación: En contraposición a la anterior función, ésta consiste en un proceso activo según el cual el autor expresa su consentimiento sobre un acto jurídico. Es el acto que materializa el consentimiento en los actos jurídicos solemnes. Esto supone un vínculo material entre el escrito y la firma y un vínculo intelectual entre la firma y el texto del documento.

En consecuencia, firmar significa hacer propio el mensaje y manifestar la voluntad de apropiarse de los términos del escrito. Frente a la esencialidad de la firma en algunas declaraciones de voluntad, ésta no es determinante para la existencia y validez de la mayoría de las declaraciones negociales, en base al principio de libertad de forma de los contratos; no obstante, es necesaria para tener certidumbre acerca de la autoría de la declaración (función indicativa de la firma); del alcance del consentimiento contractual (función declarativa de la firma) y de la eventual prueba del contrato (función probatoria de la firma) (Flores, 2002:172).

Para definir a la firma electrónica, Rico (2005:198) señala que ésta "consiste en cualquier método o símbolo basado en medios electrónicos, utilizado o adoptado por una parte con la intención de vincularse o autenticar un documento, cumplido todas o algunas de las funciones características de una firma manuscrita".

En este sentido, la Ley de Mensajes de Datos y Firmas Electrónicas en el artículo 2, define a la Firma Electrónica como 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". La concepción anterior, obedece a un sentido amplio, sin limitarla por ejemplo, a la firma digital como se refirió *ut supra*, respecto al panorama latinoame-

ricano, lo cual evidencia el respeto al principio de neutralidad tecnológica presente en nuestro ordenamiento jurídico.

Asimismo, la Ley de Mensajes de Datos y Firmas Electrónicas vigente, consagra en el artículo 16 la validez y eficacia de la firma electrónica equiparándola a las funciones 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. A los efectos de este artículo, la Firma Electrónica podrá formar parte integrante del mensaje de datos, o estar inequívocamente asociada a éste; enviarse o no en un mismo acto.

No obstante, la firma electrónica que no cumpla con los requisitos señalados podrá constituir un elemento de convicción valorable conforme a las reglas de la sana crítica. La interpretación que exige la propia esencia de la firma es la de asumir la paternidad y alcance de las declaraciones inter-partes. En este sentido, Flores (2002) señala que a estos efectos no se opone el hecho de que estemos ante una firma de carácter electrónico, ni que la misma sea más o menos fiable técnicamente. De esta manera, se reconoce legalmente a la firma electrónica las funciones básicas atribuibles a la tradicional firma autógrafa o manuscrita y, por esta razón, es correcta la terminología "firma", que hasta ahora estaba restringida a la manuscrita.

Así, aunque se pueda hablar de firma en todos los casos, porque la distinta configuración técnica de la firma electrónica de la manuscrita no altera la función primordial de la misma, la cual es identificar al autor de las respectivas declaraciones negociales y determinar el alcance de éstas últimas (aceptación, comunicaciones, mensajes de datos, etc.), el diferente grado de "fiabilidad tecnológica" en los métodos de elaboración de la firma electrónica determinan la distinción entre un concepto amplio y general de firma electrónica, representado por la denominada firma electrónica, firma electrónica simple, y un concepto estricto, restringido a las firma electrónica avanzada o firma electrónica refrendada o firma electrónica segura, de acuerdo con los distintos preceptos reguladores de la firma electrónica.

En este orden de ideas, Rico (2005) apunta que todas las firmas electrónicas independientemente del procedimiento utilizado para generarlas, gozan de reconocimiento legal y son admisibles como medios de prueba en juicio, tal como lo dispone el ordenamiento jurídico venezolano. El legislador venezolano en su intento de no favorecer una tecnología sobre otra, enuncia de manera general las condiciones de equiparación, insistiendo en las garantías mínimas de seguridad que debe ofrecer todo documento electrónico y quizás con mayor compromiso en el comercio en redes abiertas, a saber: el no repudio, la confidencialidad, la autenticidad y la integridad del mensaje.

En España, "la Ley 59 de 2003, atribuye a la firma electrónica reconocida el mismo valor jurídico de la firma manuscrita, entendiendo que este instrumento atribuye autenticidad al documento electrónico, por lo tanto se admite como medio de prueba en juicio". Sin embargo, comenta Rico (2005) que en el Derecho Europeo son más específicas las condiciones necesarias para que opere la equiparación entre la firma electrónica y la firma manuscrita en comparación a la legislación venezolana. Tales requisitos se encuentran tanto en la Directiva comunitaria como en la Ley 59 de 2003, los cuales se agrupan en dos categorías:

1. Los certificados que contienen el par de claves: Referido a la noción de certificado como requisito necesario para otorgar valor jurídico a la firma electrónica; el cual será desarrollado en los puntos siguientes como un mecanismo de seguridad en la contratación electrónica.
2. El dispositivo de creación de firma: En Europa, para que la firma electrónica tenga los mismos efectos de las firmas manuscritas, se exige además de la expedición del certificado correspondiente, la utilización de un dispositivo seguro de creación de firma. Este requisito no se encuentra previsto en forma expresa en el Derecho venezolano; no obstante, en un futuro debe preverse el mecanismo técnico que avale el producto de firma electrónica, cuyo funcionamiento debe ser certificado por el prestador de servicios de certificación.

No obstante, Arias (1999), enseña que la firma electrónica de documentos es una realidad, que con múltiples garantías y procedimientos lógicos de control, ofrece la misma o mayor fiabilidad que la manuscrita y, además, parece ser el camino más expedito para concordar la realidad de las relaciones comerciales o mercantiles, que se apoyan en gran parte en la herramienta informática con el mundo del Derecho.

1.1. Modalidades de firma electrónica

La firma electrónica se identifica con la denominada firma digital (basada en criptografía de clave pública), firma electrónica avanzada o firma electrónica reconocida, ésta última relacionada con una especie de sello digital, modalidades éstas que permitirán al receptor constatar el origen del mensaje y comprobar que no ha sido alterado en su transmisión (Rico, 2005).

Así, la firma digital es definida por La Ley 527 de 1999, del ordenamiento jurídico colombiano, en el artículo 2, bajo los siguientes términos:

> "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 clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación".

Expone Zubieta (2005:78) que "la firma digital es un valor numérico que se adhiere al mensaje de datos, por lo tanto, no cambia el texto original del mensaje, sólo le agrega información relativa a la autoría o respecto de la aceptación de su contenido". De lo anterior se puede colegir, que un documento firmado digitalmente no oculta su contenido, característica también de los documentos físicos tradicionales firmados de forma manuscrita, puesto que puede existir un documento firmado en el cual no se reconozca la firma ni el autor de la misma, pero cuyo contenido sea legible. Esta modalidad constituye un tipo de firma electrónica.

Por su parte, la firma electrónica avanzada, adoptada en el ordenamiento jurídico español, es definida en la Ley 59 de 2003, en el artículo 3.2, como la firma que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que quien suscribe puede mantener bajo su exclusivo control. Y finalmente, la firma electrónica reconocida, también adoptada en el ordenamiento jurídico español, es definida en la citada Ley en el artículo 3.3, como una especie de firma electrónica avanzada, basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de fir-

ma. Así para el legislador español, es la firma electrónica reconocida la que equivale en términos legales, a la firma manuscrita.

La distinción de los términos de firma electrónica avanzada o firma electrónica reconocida, adoptados por el legislador español, la marca el principio de neutralidad tecnológica. En corolario, dentro de la categoría genérica de firma electrónica, se encuentra la firma digital, firma electrónica avanzada y firma electrónica reconocida, las cuales se diferencian por el sistema utilizado para la generación de las mismas y en el valor jurídico atribuido; por ejemplo, si se trata se una firma electrónica simple, es porque ésta utiliza cualquier procedimiento electrónico, como los sistemas criptográficos simétricos; y de tratarse de una firma digital o electrónica avanzada, el método utilizado es la criptografía asimétrica o de clave pública, la cual es equiparable legalmente a la firma manuscrita.

Igualmente, como expone Flores (2002:183) "esa fiabilidad tecnológica, se proyecta jurídicamente en su inalterabilidad, de manera similar a lo que acontece en el ámbito de las firmas manuscritas". Todos los aspectos antes tratados, se involucran bajo el régimen de seguridad que proporcionan al documento electrónico, una serie de mecanismos que han sido diseñados en función de asegurar, aún a pesar de la inmaterialidad característica de esta clase de documentos, su validez dentro del proceso probatorio. La inmaterialidad a la que se aduce, viene a significar una condición genérica que involucra la prescindencia, de la inmediación física ordinaria que priva para la formación de los documentos públicos y de los privados tradicionales; y que imponen cuando menos la concurrencia de las partes, de una con otra o de ambas separadamente, pero sí en presencia del funcionario que rendirá fe del contenido de los mismos, en caso de ser públicos.

En virtud de que para la formación del documento electrónico se prescinde de la presencia física, entendida bajo los términos anteriores, se hace alusión a una inmaterialidad, que no obedece a la constancia concreta o no del documento en alguna forma tangible, pues en puridad de conceptos, ambas serían perceptibles a los sentidos, y luego, materiales de acuerdo a su particular naturaleza. La inmaterialidad quiere significar entonces la no inmediación de quienes se involucran con ocasión del documento electrónico, que su constancia sea igualmente electrónica y, que deben prevalerse entonces de los mecanismos de seguridad que le garan-

ticen, aún a pesar de su abstracción, el verdadero valor que como medio de prueba éste pueda representar.

Igual que acontece de ordinario, para la documentación tradicional (documentos públicos o privados), la firma viene a representar el vínculo más directo de la autoría con el contenido suscrito dentro del documento electrónico; pues tal cual la rúbrica que opera de la irrepetible mecánica de la escritura humana, la electrónica cuenta también con este carácter de originalidad, que posibilita el hecho de vincular a un único sujeto con la signatura bajo la cual queda entendida su identificación en el documento.

En el entendido del documento electrónico, la firma no debe ser comprendida bajo el mismo modo de percepción que comúnmente asume, y que cultural y jurídicamente aparece ligada a una representación gráfica de posible comprensión, o de mera simbología, que no representa más que el significante de la identidad de algún individuo. Comúnmente la firma manuscrita, y a diferencia de lo que acontece con la electrónica, suele valerse del empleo de otros medios de identificación, que actuando de modo conjunto permiten vincular verdaderamente al autor con el documento, tal como sería la expresión de la cédula de identidad e incluso de las huellas digitales.

En este sentido, la firma electrónica, prescinde de varias de las características propias de la rúbrica común, primeramente actúa como un mensaje de datos en sí misma, ligada a otro mensaje más amplio, que es propiamente la información transmitida. Puesto que la firma transporta un conocimiento detallado acerca de la identidad del autor del documento, o de quien rinde validación sobre el mismo, no amerita sino de la expresión de aquel código que va a significar la unión de todos los datos de identidad necesarios al reconocimiento de la persona con la que se vincula.

Las cuestiones anteriores que atienden a la vinculación, o al nexo que existe entre la identificación del sujeto emisor del documento electrónico, y la expresión concreta de la firma, vendría a representar uno de los caracteres esenciales e insuperables para que la rúbrica electrónica rinda su necesario valor. El nexo entre la individualización de la persona natural o jurídica, y el mensaje de datos que se implícita en la firma, debe ser de tal característica de inequívoca identidad, que no surja duda alguna acerca de la autoría del emisor, cuando se evidencie la percepción del conjunto alfanumérico que es la firma electrónica.

Las anteriores exigencias de plena conexidad, entre la firma electrónica y la individualización de su sujeto titular, en nada obstan al hecho, de que pueda una persona poseer más de una firma electrónica. Lo que sí es preciso, en razón de la naturaleza de mecanismos de seguridad que esta representa, es que cada una indefectiblemente dirija sin duda a la identificación de la persona emisora del documento electrónico. En lo anterior, se muestra un claro avance de la firma electrónica, sobre la rúbrica común, en el sentido de que para todos los actos que ameriten la suscripción, la persona utiliza la misma simbología de la firma, no pudiendo cambiar ésta ni aún por error en el trazo, dado que tal variación induce incluso a la invalidación del documento; no así sucede en la firma electrónica, donde el vínculo entre el código alfanumérico y la persona a la que pertenece, se mantiene inalterable, por no depender en nada de la acción física humana, sino de una intelectual que se limita a la recordación de una clave.

En este orden de ideas, la variedad de firmas electrónicas se patentiza en el plano venezolano, en todos aquellos trámites que bajo el empleo de las Tecnologías de Información y Comunicación (TIC), ameritan por parte de quien las emplea, del uso de una clave de identificación que funge como firma electrónica en sentido genérico, por más que para ésta no hubiere actuado algún sistema de certificación. Estas firmas, que pudieran llamarse comunes, en virtud del índice de su empleo para gran cantidad de actividades cotidianas, se asimilan a aquellas que en otros países (especialmente en Europa), se conocen como Firmas Electrónicas Avanzadas. Así entonces, y haciendo como ya se dijera, símil con las distinciones europeas que existen para las firmas electrónicas, la firma avanzada representaría en Venezuela, aquel mecanismo de seguridad cuya protección se basa en el hecho de que quien la emplea, ha tenido también autoría en la misma; de allí que sea presumiblemente quien la conozca de modo exclusivo y eventualmente pueda introducir a ella cualquier especie de cambio, bastando que modifique la clave que la representa.

Situación distinta acontece con aquellas firmas electrónicas que vienen representadas por claves otorgadas por instituciones, servicios u otras personas, o que se vinculan y representan directamente en los datos que proporcionan el soporte electrónico del que derivan; tal sería el caso de este último supuesto, el número de telefonía móvil que aparece ligado como firma, a los mensajes de texto que se envían o reciben a través de és-

tos. Lo mismo acontece con los documentos electrónicos que se transmiten vía fax. Los supuestos anteriores serían los que podrían identificarse con la Firma Electrónica Simple, adoptada por el ordenamiento jurídico español.

Dentro de las modalidades en las que la firma avanzada puede manifestarse, necesita mención aparte, el caso del correo electrónico, en atención al cual es necesario mencionar que el "e-mail" puede tener firma o no; en caso de contenerla la misma será de naturaleza electrónica y particularmente certificada por un prestador de servicios de certificación debidamente autorizado, caso en el cual sería firma electrónica reconocida, entendida ésta como aquella que proporciona el mayor índice de seguridad esperable de dicho mecanismo. Este tipo de firma electrónica se basa, en la emisión de un certificado electrónico, sobre la firma avanzada que hubiere creado el titular; es decir, que se amerita necesariamente de la voluntad de la persona para la formación de la firma a certificar, no siendo susceptibles de tal procedimiento, las firmas digitales o simples.

En corolario, en Venezuela para que la firma electrónica tenga efectos jurídicos de firma autógrafa, se requiere la concurrencia de los siguientes requisitos: a) que los datos utilizados para su generación se puedan producir una sola vez; b) ofrecer seguridad suficiente, de que la firma no pueda ser falsificada; c) no alterar la integridad del mensaje de datos, ello de conformidad con el artículo 16 de la Ley de Mensaje de Datos y Firmas Electrónicas. Sin embargo, en caso de no cumplir con todos esos requisitos, puede constituir un elemento de convicción valorable (un indicio), según el artículo 17 *ejusdem*.

Aunado a las consideraciones previas, la firma electrónica proporciona cuatro manifestaciones fundamentales de seguridad, que se desprenden como implicación directa de sus propias características, y que son: en primer lugar la autenticidad, siendo ésta la garantía que permite identificar sin lugar a dudas al autor del mensaje de datos que se encuentra suscrito; en segundo lugar la integridad, condición que refiere a la imposible manipulación del contenido del documento electrónico, una vez que éste ha sido suscrito electrónicamente y haber sido enviado; en tercer lugar se tiene la seguridad de confidencialidad que trae consigo la firma electrónica, en virtud de que el mensaje de datos y la información que éste proporciona, solo puede ser conocida por quien suscribe electrónicamente y por

quien es el destinatario del documento electrónico; finalmente, el no repudio es la condición que se une a la firma electrónica, en cuanto a que quien ha suscrito no puede luego negar ni su autoría, ni el contenido del documento electrónico.

El Estado venezolano con la promulgación de la Ley de Mensaje de Datos y Firmas Electrónicas dio un paso para impulsar esta materia; no obstante, se evidencia de la praxis el abandono a tal disposición, por cuanto se tiene por ejemplo un artículo publicado por la Agencia Bolivariana de Noticia que data de fecha 02 de junio de 2007, en el cual se informaba que para el año 2009 se preveía en Venezuela el uso de firmas electrónicas asociadas a las cédulas de identidad; sin embargo, actualmente continúa en desarrollo por el actual Servicio Autónomo de Identificación, Migración y Extranjería (SAIME) y la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE). Se afirmaba que el referido documento permitiría además de la identificación, realizar transacciones y acceder a servicios del Gobierno, desde firmar documentos en Notarías, pagar impuestos, registrarse en el Consejo Nacional Electoral, entre otros, pero no se ha materializado.

2. Certificados electrónicos

2.1. Función de los certificados electrónicos

En la Ley de Mensajes de Datos y Firmas Electrónicas se define a los certificados electrónicos de la siguiente manera: "Artículo 2. A los efectos del presente Decreto-Ley, se entenderá por: (…) Certificado Electrónico: Mensaje de Datos proporcionado por un Proveedor de Servicios de Certificación que le atribuye certeza y validez a la Firma Electrónica". El cual debe ser entendido concatenadamente con el artículo 38 *ejusdem,* que plantea la función principal de los certificados electrónicos, cual es garantizar la autoría de la firma electrónica que certifica así como la integridad del mensaje de datos.

Igualmente, la citada Ley regula en el artículo 43 los aspectos que deben contener los certificados electrónicos y se observa que en tales requisitos, el legislador venezolano obvia la mención de la firma electrónica del PSC que emite el certificado, a efectos de comprobar su autenticidad, lo cual resulta indispensable para vincular jurídicamente los documentos

electrónicos con su emisor. En este mismo orden de ideas, el Reglamento Parcial de la citada Ley, establece en el artículo 32, que el contenido de los certificados electrónicos no se limita a lo anterior, pero hace la siguiente salvedad, a saber: "Los Certificados Electrónicos emitidos por los Proveedores de Servicios de Certificación Electrónica, podrán incluir información adicional a la requerida en el artículo 43 del Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas, siempre y cuando ésta no dificulte o impida su lectura o el reconocimiento de dichos certificados por terceros".

En este sentido, un sistema de certificación electrónica permite, por una parte, acreditar la autenticidad de las partes intervinientes en una transacción de este tipo; y por la otra, permite conocer la hora y fecha del envío de un documento electrónico, circunstancia por demás importante para determinar el momento de la formación del contrato, de una notificación electrónica, de una contestación de alguna demanda, o del nacimiento de las obligaciones de las partes, entre otras situaciones de relevancia jurídica.

Enseña Rico (2005:223) que:

> "Dentro de los componentes básicos de un sistema de certificación electrónica encontramos tres elementos: (1) el uso de la firma electrónica, (2) la presencia de un tercero de confianza –el prestador de servicios de certificación, comúnmente conocido por las siglas PSC– y (3) la emisión de un documento que respalde esa firma; el certificado electrónico".

Por su parte, Font (2000:73) expone que "un certificado digital es una credencial electrónica emitida y firmada (digitalmente) por una Autoridad de Certificación. El certificado digital contiene la clave pública de una determinada persona o identidad a la que queda vinculada".

Por su parte, las legislaciones europeas han definido al certificado electrónico de la siguiente manera: en primer lugar, España en la Ley 59/2003 de 19 de diciembre sobre firma electrónica, lo define en el artículo 6, así: "Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad".

Por su parte, en la legislación francesa, en el Decreto Nº 2001-272 del 30 de marzo de 2001, es definida esta institución como: "*Article 1: Au*

sens du présent décret, on entend par: 9. Certificat Électronique: un document sous forme électronique attestant du lien entre les dones de vérification de signatura électronique et un signataire" (Artículo 1: En el sentido del presente decreto, entendemos por: 9. Certificado Electrónico: un documento bajo forma electrónica que atestigua del vínculo entre los dones de comprobación de la firma electrónica y un signatario).

En este mismo sentido, España en la Ley 59/2003, de 19 de diciembre sobre firma electrónica, define al certificado electrónico en el artículo 6, del modo siguiente: "Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad". Asimismo, la Unión Europea en la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica, define en el artículo 2 a los certificados electrónicos de la siguiente manera: "A los efectos de la presente directiva se entenderá por: 9) Certificado: la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de ésta".

El carácter que se repite en las definiciones aportadas sobre certificado electrónico, deviene de su primordial función: vincular una clave pública con un determinado titular. Así se tiene que la principal función del certificado electrónico es asociar la identidad de una persona determinada a una clave pública concreta (e indirectamente a una clave privada). Entonces, los usos de los certificados electrónicos, se puede enumerar de la siguiente manera: 1) autenticar si quien remite el mensaje de datos al que se adjunta el certificado es efectivamente quien dice ser, lo que se conoce como garantía de autoría; y 2) proporcionar al receptor del certificado la clave pública del remitente que le permita desencriptar el texto del mensaje de datos, lo que se conoce como garantía de integridad. Por tanto, para que el certificado electrónico cumpla con la finalidad que se ha destinado será necesaria la intervención del Proveedor del Servicio de Certificación (PSC).

A las entidades encargadas de otorgar tales certificados electrónicos le son consideradas como las terceras partes de confianza (*Trusted Third Parties*) que son aquellas entidades que merecen la confianza de otros actores en un escenario de seguridad donde no existe confianza directa en-

tre las partes involucradas en una cierta transacción. Es por tanto necesaria, una infraestructura de clave pública para cerrar el círculo de confianza, proporcionando una asociación fehaciente del conocimiento de la clave pública a una entidad jurídica, lo que le permite la verificación del mensaje y su imputación a una determinada persona.

La previsión de la certificación como mecanismo de seguridad para el documento electrónico, se encuentra contemplado en la Ley de Mensajes de Datos y Firmas Electrónicas, siendo la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE) el órgano encargado por parte del Estado, de la designación de aquellos institutos u organismos que concretamente certificarán las firmas electrónicas que sean susceptibles de la adquisición de tal seguridad. Es preciso señalar que actualmente tal proceso de "revestimiento de seguridad sobre las firmas electrónicas", no se está produciendo en efecto, en virtud de que la Superintendencia antes referida, se encuentra en proceso de análisis, revisión e implementación para la fecha.

En este mismo sentido, y en el plano supuesto del inicio del proceso de certificación de las firmas electrónicas, se encuentra el organismo público que aún no se encuentra plenamente operativo, denominado Fundación Instituto de Ingeniería para Investigación y Desarrollo Tecnológico, órgano adscrito al Ministerio del Poder Popular de Ciencia y Tecnología, y como institución privada, el proveedor de certificados PROCERT C.A.

2.2. Certificados Electrónicos. Categorización.

La Ley de Mensajes de Datos y Firmas Electrónicas, no alude a las diversas categorías de certificados que se emiten en la práctica. Por lo tanto, se tomará lo contemplado en la Directiva sobre Firma Electrónica, la Ley 59/2003, la cual distingue una categoría especial de certificados que ofrece mayores niveles de seguridad a los usuarios, a los que denomina "certificados reconocidos". De acuerdo con lo estipulado del artículo 11.1 *ejusdem*, los certificados reconocidos son certificados electrónicos expedidos por un PSC, que cumple los requisitos establecidos en la Ley en cuanto la comprobación de la identidad y demás circunstancias de los solicitantes, a la fiabilidad y las garantías de los servicios de certificación que presten (Rico, 2005:240).

Apunta Rico (2005:240) que de acuerdo con el contenido de los certificados y las distintas funciones para la cual se expiden, podemos distinguir las siguientes categorías:

- Los certificados de identidad, cuya función principal se concreta en vincular al usuario del certificado con un par de claves determinado.
- Los certificados de atributos, denominados también "certificados de autorización o potestad". Estos certificados acreditan otro tipo de atributos del usuario como puede ser su vinculación a una determinada entidad o los poderes de representación en una sociedad.
- Los certificados transaccionales, los cuales dejan constancia de que algún hecho o formalidad ocurrió en presencia de un tercero. Estos certificados facilitan el cumplimiento de formalidades o solemnidades en entornos electrónicos. Ç
- Los certificados de tiempo, los cuales permiten dar fe que un documento existía en un momento determinado, acreditando el día y la hora en que el documento fue firmado electrónicamente o el momento de su envío.

Entonces, aún cuando en la legislación venezolana no se hace distinción expresa de diversas categorías de certificados electrónicos, es clara la Ley especial de la materia, y el reglamento parcial que la desarrolla, al establecer los requisitos mínimos que deben contener tales documentos de manera que puedan cumplir a cabalidad la función de seguridad y certeza jurídica al cual están llamados a otorgar a los mensajes de datos que ellos avalen.

2.3. Proveedores de Servicios de Certificación (PSC).

La credibilidad y seguridad del sistema se hace descansar en la intervención de un prestador de servicios de certificación o autoridad de certificación. Estos organismos, son terceros de confianza con una función que tiene trascendencia pública por su contenido, de comprobar identidades, certificar cifras, o guarismos y la pertenencia de estas a personas concretas con sus características y prestar otros servicios de seguridad, que incluyen aspectos técnicos, jurídicos y administrativos.

Los PSC son personas físicas o jurídicas, de naturaleza pública o privada, que asumen diversas funciones relacionadas con la firma electrónica, destacándose entre ellas, la certificación de la identidad del firmante me-

diante su vinculación a un par de claves determinadas, función que se cumple a través de la emisión de los certificados electrónicos. Se propugna, entonces, la implementación de los sistemas de certificación electrónica, con incorporación en la infraestructura de claves públicas de una tercera persona, de un tercero ajeno a la negociación; es decir, el Proveedor de Servicios de Certificación (PSC), cuya función es la de garantizar la identidad de las partes (del emisor y del receptor), lo que asegura la autenticidad del mensaje de datos transmitido electrónicamente; la inalterabilidad del contenido del mensaje de datos; la fecha de emisión y de recepción, si es el caso, del mensaje de datos contentivo de la voluntad contractual de las partes, entre otros.

El elemento relativo a la naturaleza del proveedor de servicios atiende a las características tecnológicas de los distintos servicios que prestan aquellas empresas, que sirven a la comunicación de documentos electrónicos (mensajes de datos). Debe entenderse por tales caracteres, aquellos que se vinculan con la posibilidad de establecer comunicaciones en áreas determinadas del espacio geográfico, nacional o trasnacional, así como a las especificidades del servicio o a la versatilidad del mismo.

La naturaleza del proveedor de servicios, determina la susceptibilidad de un documento electrónico, para ser comunicado entre distintos tipos de soporte, pues, el servicio permite tal posibilidad, como sería el caso de algunos servidores públicos de Internet, desde cuyos portales pueden remitirse correos electrónicos a teléfonos móviles, o aquellas empresas de telefonía celular, cuya plataforma tecnológica posibilita la producción y remisión de mensajes de texto, que pueden ser recibidos en soportes electrónicos portátiles o fijos, pero manifestados en procesadores de información (computadoras).

Conclusiones

La contratación electrónica representa una nueva forma de expresar la voluntad de las partes, producto del desarrollo de la tecnología, en búsqueda de facilitar la transmisión de mensajes y agilizar las transacciones jurídicas comerciales. Así, las actividades contractuales que operan por vía electrónica, no sólo cubren lo atinente al comercio (en lo que quedaría comprometido un interés económico o negocial), sino que además con mayor frecuencia se llevan a cabo por esta vía, diligencias, operaciones y

conductas en general que comprometen derechos sustanciales de la persona, relativas a su estatus civil e incluso de su relación con el Estado.

Las razones por las cuales la actividad contractual por vía electrónica ha cobrado la preponderancia que se evidencia casi por entero en la comunidad internacional, y que en países como Venezuela comienza a hacerse también patente, se hermana a las razones de practicidad, economía, celeridad, y en general a todas las facilidades que el empleo tecnológico ha impuesto al mundo contemporáneo. Ahora bien, la inclusión del carácter electrónico en la actividad negocial, se ha producido a un ritmo claramente más veloz, a aquel en que el legislador ha podido prever tal hecho; y más aún, regularizarlo en términos de tratamiento adjetivo.

Así, en Venezuela, para que la firma electrónica tenga efectos jurídicos de firma autógrafa, y en corolario un eficaz mecanismo de seguridad, se requiere la concurrencia de los requisitos *ut retro* señalados: a) que los datos utilizados para su generación se puedan producir una sola vez, b) ofrecer seguridad suficiente de que la firma no pueda ser falsificada y c) no alterar la integridad del mensaje de datos; ello de conformidad con el artículo 16 de la Ley de Mensaje de Datos y Firmas Electrónicas. Sin embargo, en caso de no cumplir con todos esos requisitos, puede constituir un elemento de convicción valorable conforme al principio de la sana crítica.

En virtud de que el certificado electrónico actúa sobre la firma, este mecanismo opera en el sentido confirmatorio o asegurativo de la identidad de quienes se ven involucrados en el documento (autenticidad), y del contenido del mismo (integridad), apareciendo entonces claramente el carácter que la misma Ley ha querido conferirle, a aquel documento que cuenta con dicha seguridades; es decir, se estaría frente a la figura de un potencial documento público electrónico, siempre y cuando participe un Notario Público o Registrador avalando el acto jurídico, tal como lo dispone la Ley de Registro Público y del Notariado. Así pues, el certificado electrónico se constituye como elemento insuperable para la formación de lo que en el futuro será el documento público electrónico; estableciéndose una relación inseparable entre las ideas de la firma electrónica que es certificada, y la intervención del Estado para la vigilancia y certeza de quienes participan en la formación del documento, materializada precisamente en los institutos emisores de la certificación (PSC), desapareciendo sutilmente las diferencias que existirían con el documento público común (en papel) y éste.

Referencias

Avellán, Aurelio (1999). *La contratación electrónica en la Argentina. Documento electrónico y firma digital.* Buenos Aires. S/e.

Álvarez-Cienfuegos, José María (2000). *La firma y el comercio electrónico en España***.** Pamplona.

Arango, Adriana (2005). Aproximación a la formación de contratos en Internet**.** En: *Internet, comercio electrónico & telecomunicaciones* e *informática*. Colombia. Legis.

Arias Rincón, Maria Inés (1999). El valor probatorio de los documentos suscritos electrónicamente. En: *Revista Tachirense de Derecho*. Táchira, Venezuela. Editorial UCAT.

Asamblea Nacional Constituyente. *Constitución de la República Bolivariana de Venezuela* (1999). Gaceta Oficial Nº 36.860 Caracas-Venezuela.

Carrascosa, Javier y Escudero Oya (1991). *Introducción al Derecho Internacional Privado.* Madrid-España. Editorial Comares.

Chacón Gómez, Nayibe (2005). *La aplicación de los sistemas de certificación electrónica en la actividad comercial.* Caracas-Venezuela. Ediciones UCV.

Fernández, C.; Hernández, R. y Baptista, P. (1994). *Metodología de la investigación.* México. Mc Graw-Hill Interamericana.

Finol de Navarro, Teresita y Nava de Villalobos, Hortensia (1996). *Procesos y productos en la investigación documental.* Maracaibo-Venezuela. Editorial de la Universidad del Zulia.

Flores, María de la Sierra (2002). *Impacto del comercio electrónico en el Derecho de la contratación.* Madrid-España. Editorial DIJUSA.

Font, Andrés (2000). *Seguridad y certificación en el comercio electrónico***.** Madrid. Fundación Retevisión.

La Roche, Alberto J. (2002). *La prueba en materia de contratación electrónica.* Maracaibo-Venezuela. CEJUZ.

Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI)

Ley Nº 527 de 1999. Colombia. Artículo: 2.

Ley Nº 59/2003 sobre Firma Electrónica. España.

Morles Hernández, Alfredo (2006). *Curso de Derecho Mercantil. Los contratos mercantiles.* Tercera Edición. Tomo IV. Caracas-Venezuela. Publicaciones UCAB.

Real Decreto-Ley Español Nº 14/1999, sobre Firma Electrónica.

República Bolivariana de Venezuela. Poder Ejecutivo Nacional. *Decreto con Fuerza de Ley de Mensaje de Datos y Firmas Electrónicas* (2001). Gaceta Oficial N° 37.148. Caracas-Venezuela.

República Bolivariana de Venezuela. *Ley de Registro Público y del Notariado* (2006). Gaceta Oficial N° 5.833 Extraordinario. Caracas-Venezuela. Artículo: 23 y 24.

Rico Carrillo, Mariliana (2005). *Comercio electrónico, internet y Derecho.* Segunda Edición. Bogotá-Colombia. Editorial Legis.

Rincón Cárdenas, Erick (2006). *Contratación electrónica.* Bogotá-Colombia. Centro Editorial Universidad del Rosario.

Rodriguez, Gladys Stella (2004). *El comercio electrónico (E-Commerce).* Barquisimeto-Venezuela. Editorial Jurídicas Rincón.

Zubieta, Herman (2005). Los mensajes de datos y las entidades de certificación. En: *Internet, comercio electrónico & telecomunicaciones e informática.* Colombia. Legis.