UNIVERSIDAD CATOLICA ANDRES BELLO
DIRECCION GENERAL DE LOS ESTUDIOS DE POSTGRADO
AREA DE DERECHO
ESPECIALIDAD EN DERECHO PROCESAL

LA FIRMA ELECTRONICA Y SU USO EN EL PROCEDIMIENTO CIVIL VENEZOLANO

Autor: Abogado José A. Menegaldo V.
Asesor: Dr. Alberto J. La Roche
Fecha: Diciembre de 2005

RESUMEN

Este trabajo se enfocó en determinar cuál es el régimen jurídico que en nuestro país se aplica a las firmas electrónicas y su uso en el procedimiento civil, basado en la transmisión y almacenamiento electrónico de datos, tomando para ello como base las disposiciones normativas contenidas en el ordenamiento jurídico venezolano. Se partirá principalmente de métodos cualitativos, como el documental, con apoyo de una amplia revisión bibliográfica y el uso de categorías, elaboración de fichas de trabajo, inducción, deducción y síntesis. El instrumento a utilizar en esta investigación será una matriz de análisis de contenido, necesaria para registrar y analizar el contenido de la información suministrada por las fuentes documentales. Los resultados obtenidos permitieron concluir de forma general que en el derecho venezolano existe un régimen especial aplicable a las firmas electrónicas, para regular diversos aspectos jurídicos relevantes atinentes a los contratos comerciales celebrados por medios electrónicos. La revisión documental del presente estudio contribuye con el impulso jurídico para el uso de la firma electrónica dentro del proceso civil venezolano.

INTRODUCCION

La irrupción de los microprocesadores en casi todos los órdenes de la vida en sociedad, y la utilización de los más diversos soportes magnéticos u ópticos para guardar y transmitir datos e informaciones, ha determinado en el mundo jurídico la aparición de algunos interrogantes conceptuales, relacionadas con el valor probatorio de la firma electrónica. En función de ello, los distintos países han realizado esfuerzos por reglamentar las condiciones bajo las cuales puede admitirse jurídicamente la firma electrónica, entre ellos Venezuela.

Con la promulgación del Decreto con fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas en el año 2001, (en lo adelante "LSMDFE"), que emanó del Poder Ejecutivo, conforme a la Ley Habilitante, algunas de las lagunas que han existido en materia procesal desaparecerán, en la medida que se otorga y reconoce eficacia y valor jurídico a la firma electrónica, al mensaje de datos y a toda información inteligible en formato electrónico.

Esta nueva legislación añade un componente esencial del cambio de paradigma que se ha efectuado en el mundo gracias a los avances de las telecomunicaciones y la tecnología de la información. Por ello, es necesario reconocer que el Ejecutivo Nacional acertó al promulgar este

instrumento. Asimismo, se debe al Ministerio de Ciencia y Tecnología la gestación y promoción de este nuevo instrumento, el cual ha contado con el respaldo de VENAMCHAM (Cámara Venezolano Americana de Comercio e Industria), CAVECOM-E (Cámara Venezolana de Comercio Electrónico) y CAVEDATOS (Cámara Venezolana de Empresas de Tecnologías de la Información), entre muchos otros actores de la vida nacional.

Ahora es prioritario asegurar su eficacia mediante distintas acciones de tipo legislativo: una de ellas es la incorporación de los mensajes Electrónicos y dar cumplimiento a la Constitución. En consecuencia, a la luz del sistema de la ley resulta un aspecto interesante el análisis de la admisibilidad de la firma electrónica como elementos de prueba, investigando su valor o eficacia probatoria.

Es indudable que la Ley Sobre Mensajes de Datos y Firmas Electrónicas (2001) ha introducido un elemento valioso que contribuye enormemente en la seguridad que deben tener las interacciones por medio de la red. Sin embargo, aun falta por recorrer algo más del camino en materia legislativa para brindar un marco normativo que se traduzca en mayores grados de seguridad jurídica. A los fines del presente trabajo se determinó el uso de la Firma Electrónica en el Procedimiento Civil

Venezolano. Este trabajo se estructuró en cinco capítulos, los cuales incluyen la siguiente configuración:

El Capitulo I, aborda el análisis del concepto de firma electrónica, exponiendo sus antecedentes, la evolución histórica de la firma, la firma electrónica en el Derecho Comparado y los aspectos técnicos y jurídicos relativos a la misma. Seguidamente, el Capitulo II, analiza los requisitos para la validez de la firma electrónica, especificando los requisitos jurídicos y técnicos en general, así como los establecidos dentro del ordenamiento jurídico venezolano.

Con respecto al Capítulo III, éste presenta un análisis del uso de la firma electrónica en el procedimiento civil venezolano, estableciéndose las condiciones procesales bajo las cuales es posible la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad. El Capítulo IV enfoca un análisis de los riesgos de las firmas electrónicas en el procedimiento civil venezolano, especificando los relativos al emisor, receptor y los asociados a los proveedores de servicios de certificación.

Asimismo, el Capítulo VI presenta un análisis de los medios de prueba de la firma electrónica, especificando las condiciones bajo las cuales las mismas pueden ser admitidas de acuerdo con la materia

procesal civil. Finalmente, se presentan las conclusiones derivadas del estudio, en función de las normativas analizadas.

CAPITULO I

ANALISIS DEL CONCEPTO DE FIRMA ELECTRONICA

Respecto al análisis del concepto de firma electrónica, es esencial enfocar los antecedentes históricos que dan soporte a la misma, la evolución de la firma desde el punto de vista jurídico y el concepto de firma electrónica considerando la doctrina, el desarrollo de los ordenamientos jurídicos en el derecho comparado y los aspectos técnico-jurídicos de la firma electrónica.

1.- Antecedentes Históricos.

La era digital ha cambiado el abordaje jurídico, especialmente, debido a la creciente demanda de operaciones electrónicas por medio de las llamadas redes abiertas. Para enfrentar estas nuevas situaciones, que en muchos casos generan consecuencias legales de grandes magnitudes, se viene regulando el uso de la firma electrónica, así como de las firmas y certificados digitales.

Al respecto, en Venezuela se ha aprobado una serie de cambios legislativos que permiten el uso de tales elementos técnicos, con la finalidad de acreditar fehacientemente a las personas que manifiestan voluntades por medios electrónicos y evitar de esta forma el repudio de

sus operaciones, siendo interesante analizar los antecedentes históricos de la materia.

Para efectos de este trabajo, es interesante analizar en que consiste la firma electrónica. De acuerdo con Irabien, J. (2002, 1), el concepto de firma digital fue introducido por Diffie y Hellman en 1976, preocupados por el adecuado manejo de las claves, aportaron la idea que hasta la fecha subsiste, consistente en que la clave pública se asociara efectivamente a la persona o usuario que decía ser su titular, de tal manera que se hiciera pública su identidad, ligada a su clave pública, lo cual se hace actualmente en directorios publicados por los Proveedores de Servicios de Certificación, (CA), Certification Authorities. Ellos fueron los responsables del surgimiento de la firma digital como una aplicación de codificación de clave pública.

Años después, explican Tuzio, A. y Palazzi, P. (2005, p. 17) que en el plano internacional tienen lugar múltiples actividades y debates en torno a los aspectos legales de la firma digital, entre ellos el Comité de Seguridad de la Información de la Sección de Ciencia y Tecnología de la American Bar Association (ABA-Asociación de Abogados de los EE.UU.) redactó su Normativa de Firma Digital en 1996, en la que participaron casi ochenta profesionales de las disciplinas del derecho, la informática y la criptografía de los sectores público y privado, en la que especifica un

mecanismo de firma digital a base a criptografía asimétrica, los certificados de clave pública y los certificadores de clave pública.

Agregan los autores antes mencionados que, la Comisión Europea redactó su borrador final de Directiva de Firma Digital (Propuesta de Directiva del Parlamento Europeo y el Consejo sobre un Marco Común Para las Firmas Electrónicas) del 13 de mayo de 1998, publicado en el Diario Oficial de las Comunidades Europeas del 23 de octubre de 1998, que establece las pautas para la utilización de la firma digital por los Estados miembros.

Asimismo, la Comisión de las Naciones Unidas para el Derecho Comercial Internacional (UNCITRAL) aprobó una Ley-Modelo sobre Comercio Electrónico y preparó varias normas uniformes en materia de firma digital, cuyas directivas fueron tomadas como base por la mayoría de los países latinoamericanos que legislaron en la materia, por su ductilidad para adaptarse a sus necesidades. Del mismo modo, la Organización de Cooperación y Desarrollo Económico (OCDE) emitió algunas pautas de política criptográfica de 1997, mientras organizaciones internacionales, como la Organización Mundial del Comercio (OMC), se interesaron en el tema.

La magnitud de las transformaciones generadas con el uso de las tecnologías de información y comunicación en todos los ámbitos a nivel

mundial, generó un compromiso gubernamental, así como un replanteamiento y ajuste de las regulaciones vigentes en Venezuela para adecuarlas al nuevo entorno, a fin de redefinir el papel del gobierno y la participación de otros actores, especialmente del sector privado, de favorecer la competencia en el mercado e impulsar la inversión privada.

En este sentido, Venezuela, siguiendo el ejemplo de otros países de América Latina, inició un proceso para elaborar y aprobar una Ley sobre Mensajes de Datos y Firmas Electrónicas. En este sentido, el Decreto – Ley sobre Mensajes de Datos y Firmas Electrónicas Venezolana se promulgó el 28 de febrero de 2001 en el marco de la Ley Habilitante otorgada al Presidente de la República Bolivariana de Venezuela.

El Decreto-Ley reconoce en su artículo 1, la 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, 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).

Desde el punto de vista doctrinal, básicamente, Frossini (1993, 173) indica que una firma electrónica es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje. Aparentemente estos se consiguen con los criterios de autenticidad e integridad, pero estos no son suficientes si se pretende equiparar a la firma manuscrita que además tiene las propiedades de ser barata y fácil de producir, fácil de reconocer tanto por el propietario como por otros y ser imposible de rechazar por el propietario.

Como puede observarse con diversos los esfuerzos nacionales e internacionales en el ámbito del desarrollo de ordenamientos jurídicos armónicos, en materia de firma electrónica, resaltándose que en Venezuela la misma es aplicable a la materia regida por los preceptos del Derecho Civil.

2.- Evolución de la Firma.

No existe en el Derecho Venezolano, una amplia teoría sobre la firma, sus elementos, consecuencias o su concepto, por lo cual las referencias que existen son obras de Derecho Notarial.

Indica Reyes, A. (2002, 1) que en Roma, existía la Manufirmatio, que consistía en una ceremonia en que leído el documento por su autor, o el funcionario, se colocaba desenrollando y extendido sobre la mesa del escribano y luego de pasar la mano abierta sobre el pergamino en actitud de jurar, pero sin hacerlo, se estampaba el nombre, signo, o una o tres cruces, por el autor o el funcionario en su nombre, haciéndolo seguidamente los testigos. Más que in requisito, la Manufirmatio era en sí misma parte del espectáculo solemne en que se realizaba el acto.

En la Edad Media, explica el autor antes señalado, se inscribía una cruz a la que se le añadían diversas letras y rasgos. Estos signos se utilizaban como firma. Debido a que no sabían leer ni escribir, los nobles remplazaron esta práctica con el uso de sellos. La diferenciación entre “firmas” y “signos” hizo que se empezase a entender que aquellas eran, más que simples “signos”, la inscripción manuscrita del nombre o de los apellidos.

En ese tiempo, pocas eran las personas que sabían leer y escribir, por lo que generalmente los particulares estampaban en los documentos que suscribían diversos signos o sellos, la extensión de la instrucción y el desenvolvimiento de las transacciones comerciales, hicieron que la firma fuera adquiriendo la importancia y uso que con el transcurso del tiempo se fue consagrando como un símbolo de identificación y de enlace entre el autor de lo escrito o estampado y su persona.

Rodríguez, G. (2002, 2) indica que 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.

Explica la misma autora antes mencionada, que 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.

Agrega Rodríguez, G. (2002, 3), que 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.

Por su parte, Illescas, R. (1997, 32) indica que 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 de manera inmediata. Se produce así el fenómeno que se ha dado en llamar electronificación o digitalización de las relaciones jurídicas.

La Real Academia Española (2001) indica que la firma es “el nombre y apellido o título de una persona que ésta pone con rúbrica al pié 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, Avellán (1999, 159) afirma que 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.

Agrega Palazzi, P. (1998, s/p) que la firma es “el trazo particular por el cual el sujeto consigna habitualmente su nombre y apellido, o sólo su apellido, a fin de hacer constar las manifestaciones de su voluntad”. La firma en este caso cumple diversas funciones, lo cual dependerá de la naturaleza del documento: establecer la autoría del propio texto, aceptar las obligaciones que surgen de un texto, adherir a lo expresado por otro y determinar la presencia del mismo. Cuando un Escribano certifica una firma lo que está asegurando es que la persona que firma es quien dice ser, que lo hizo libre y conscientemente, que firmó dicho documento en un lugar y día determinado.

Aplicado al ordenamiento jurídico en 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, la cual se concreta con la Ley sobre Mensajes de Datos y Firmas Electrónicas Venezolana promulgada el 28 de febrero de 2001, la cual otorgó validez a

las firmas electrónicas y para establecer mayor certeza jurídica en cuanto a la validez de las mismas.

Rodríguez, G. (2002, 3) indica que la firma manuscrita es similar a la firma electrónica en tanto requieren una actividad del firmante, resultan de aplicar un procedimiento, sus elementos que se agregan a un documento, requieren información de conocimiento del Firmante, su finalidad directa es identificar al firmante e indirecta dar seguridad y confianza; y, significan que el firmante aprueba el contenido del documento. En ambos casos, deben ser verificables por terceras partes y requieren consenso social.

En el caso de la firma dactilar, la autora antes indicada afirma que esta se refiere a la firma que estampan las personas con alguna dificultad, de cualquier índole, para leer o escribir, y quienes 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.

Dicha forma tiene por tanto, la misma validez que la firma manuscrita e inclusive la firma electrónica.

Respecto a la firma electrónica, Ruiz, F. (2005, s/p) señala que es un conjunto de datos electrónicos que identifican a una persona en concreto. Suelen unirse al documento que se envía por medio telemático, como si de la firma tradicional y manuscrita se tratara, de esta forma el receptor del mensaje está seguro de quién ha sido el emisor, así como que el mensaje no ha sido alterado o modificado.

El mismo autor indica que, la firma electrónica puede utilizarse en el sector privado, para contratación privada por vía electrónica, entre empresa y consumidor (por ejemplo, la compra de un libro o un compacto por Internet) y entre empresas (por ejemplo, realizar un pedido a un distribuidor) o incluso entre los mismos consumidores finales. El mismo autor asevera que, la firma electrónica funciona mediante la encriptación o cifrado de los datos que la componen, de forma que si no se tiene la clave, el documento se convierte en ilegible.

Para ello, es necesario contar con un par de claves: clave privada y clave pública que se corresponden de forma matemática. Con esta encriptación se consigue que la información enviada bajo la firma electrónica sólo pueda leerse por la persona autorizada que posea la

clave y acreditar la identidad de quien firma el documento electrónicamente. En el análisis del concepto de firma electrónica, deben abordarse las conceptualizaciones de los distintos tipos de firmas existentes. En la actual normativa existen dos tipos: la firma no certificada y la certificada.

La firma no certificada es la que corresponde a la información creada por un mensaje de datos, a tenor de lo señalado en el artículo 16 de la Ley Sobre Mensajes de Datos……"lo que permitirá vincular al Signatario con el mensaje de datos y atribuir la autoría de éste". Por su parte, la firma certificada es aquella avalada por el Proveedor de Servicios de Certificación, autorizado por la Superintendencia de Certificación Electrónica, lo cual implica la encriptación asimétrica que garantiza la seguridad necesaria.

Otros autores hablan de firma básica y la avanzada. Ramos, F. (2000, 23) indica que la firma electrónica básica contiene un conjunto de datos recogidos de forma electrónica que formalmente identifican al autor y se incorporan al propio documento, pero este sistema tiene algunos problemas.

El mismo autor indica que, para tener la certeza de que los datos enviados hayan sido creados por la persona que lo firma o que

verdaderamente lo ha firmado él y no una tercera persona haciéndose pasar por él, se creó la firma electrónica avanzada, a la que el ordenamiento atribuye plena eficacia jurídica y valor probatorio en juicio.

Dicha firma electrónica avanzada permite la identificación del emisor del mensaje ya que está vinculada de manera única al que firma el documento y a los datos que incorpora, debido a que es el signatario quien únicamente posee el control exclusivo de estas claves, además de que permite saber si estos datos han sido modificados posteriormente o en su transcurso.

Por tanto, la firma electrónica básica no garantiza la identidad de la información recibida. Los datos que se adjuntan a la información no aseguran que el envío se haya realizado desde un emisor conocido; mientras que la firma electrónica avanzada sí garantiza la seguridad, porque asegura que el envío se realiza por parte del emisor conocido, siempre a través de la relación complementaria entre sus claves privada y pública.

Agrega Ramos, F. (2000, 23) que la firma digital consiste en la utilización de un método de encriptación llamado asimétrico o de clave pública. Este método consiste en establecer un par de claves asociadas a un sujeto, una pública, conocida por todos los sujetos intervinientes en el

sector, y otro privada, sólo conocida por el sujeto en cuestión. De esta forma, cuando se desea establecer una comunicación segura con otra parte basta con encriptar el mensaje con la clave pública del sujeto para que a su recepción sólo el sujeto que posee la clave privada pueda leerlo.

La criptología se define como aquella ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones. Abarca por tanto a la criptografía (datos, texto e imágenes), la criptofonía (voz) y el criptoanálisis, ciencia que estudia los pasos y operaciones orientados a transformar un criptograma en el texto claro original pero sin conocer inicialmente el sistema de cifrado utilizado y/o la clave.

Cifrar por tanto, consiste en transformar una información (texto claro) en otra ininteligible (texto cifrado o cripto) según un procedimiento y usando una clave determinada, pretendiendo que sólo quién conozca dicho procedimiento y clave pueda acceder a la información original. La operación inversa se llamara lógicamente descifrar.

Explica Ramos, F. (2000, 25) que se está ante un criptosistema simétrico o de clave secreta cuando las claves para cifrar y descifrar son idénticas, o fácilmente calculables una a partir de la otra. Por el contrario, si las claves para cifrar y descifrar son diferentes y una de ellas es

imposible de calcular por derivación de la otra entonces se trata de un criptosistema asimétrico o de clave pública (el aceptado uniformemente en la actualidad).

Esto quiere decir que si se utiliza un criptosistema de clave secreta o simétrico necesariamente las dos partes que se transmiten información tienen que compartir el secreto de la clave, puesto que tanto para encriptar como para desencriptar se necesita una misma clave u otra diferente pero deducible fácilmente de la otra. La peculiaridad de estos sistemas de encriptación es que son rápidos en aplicarse sobre la información.

Coincidiendo con lo mencionado, Mateo y Ros (2000, 45) indican que la firma electrónica es una manera de representación y confirmación de la identidad de un sujeto en el medio electrónico. Técnicamente, es un conjunto de datos únicos encriptados (transformados en códigos). Establecen dos tipos de firmas la electrónica que autentifica la identidad de la persona y la avanzada que autentifica la identidad, pero además permite llevar a cabo transacciones comerciales avanzadas y contratos. La diferenciación entre ambas clases de firmas está hecha en función de la protección legal que ellas producen.

Los efectos jurídicos que ella produce son consecuencia de ser un medio apto al que se le atribuye la cualidad de contener la voluntad de la persona. Quienes conceden el uso de una firma electrónica y garantiza que cada firma corresponde a ese usuario y no otro, son las Autoridades de Certificación Digital, que necesitan cumplir con unos requisitos muy concretos impuestos

Por tanto, se puede indicar que las firmas electrónicas en su esencia son total y absolutamente diferentes a las firmas autógrafas y dactilares. Una firma electrónica es producida por un software y una firma autógrafa o dactilar es una manifestación de la personalidad o de un rasgo físico individual de la persona.

Sin embargo, la finalidad las tres firmas es la misma, es decir, atribuir la autoría de un documento y la aceptación del contenido del mismo, sea en papel o forma de mensaje de datos. La ley venezolana, por tanto, las asimila solo en lo que refiere a sus efectos y consecuencias al atribuirle a la firma electrónica, la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa o digital.

3.- La firma Electrónica en el Derecho Comparado.

En el análisis de la firma electrónica en el Derecho Comparado, es esencial considerar las tendencias de diversos marcos jurídicos en la materia. Para efectos de este trabajo, se han considerado tres países, uno de América del Norte, uno perteneciente a la Unión Europea y uno de Latinoamérica, distinto a Venezuela, el cual es analizado en el presente trabajo. Un breve repaso por las tendencias de cada uno de estos países en torno a la firma electrónica es presentado seguidamente:

a) Estados Unidos: La primera ley en materia de Firma Digital en el Mundo fue la denominada “Utah Digital signatura Act”, publicada en mayo de 1995 en el Estado de UTAH, en Estados Unidos. Su objetivo es facilitar mediante mensajes electrónicos y firmas digitales las transacciones, procurar las transacciones seguras y la eliminación de fraudes y establecer normas uniformes relativas a la autenticación y confiabilidad de los mensajes de datos, en coordinación con otros Estados.

Su ámbito de aplicación son las transacciones mediante mensajes electrónicos, su confiabilidad, así como las firmas digitales. Esta ley, define a la Firma Digital como la “transformación de un mensaje empleando un criptosistema asimétrico tal, que una persona posea el

mensaje inicial y la clave pública del firmante pueda determinar con certeza si la transformación se creó usando la clave privada que corresponde a la clave pública del firmante, y si el mensaje ha sido modificado desde que se efectuó la transformación."

Al Criptosistema Asimétrico lo define como aquel "algoritmo o serie de algoritmos que brindan un par de claves confiable." Al Certificado, lo conceptualiza como aquel registro basado en la computadora que identifica a la autoridad certificante que lo emite; nombra o identifica a quien lo suscribe; contiene la clave pública de quien lo suscribe, y está firmado digitalmente por la autoridad certificante que lo emite.

En cuanto a la Supervisión y al control, estos recaen sobre la División, quien actúa como autoridad certificadora. También formula políticas para la adopción de las tecnologías de firma digital y realiza una labor de supervisión regulatoria. La emisión de los certificados corre a cargo de la autoridad certificadora que ha sido acreditada.

Asimismo, se equipara el valor probatorio de un mensaje de datos que uno en papel siempre y cuando contenga una firma digital confirmada mediante la clave pública contenida en un certificado que haya sido emitida por una autoridad certificadora autorizada. En esta ley, no se contempla el reconocimiento de certificados extranjeros, solo se menciona

que la División puede reconocer la autorización emitida por Autoridades Certificadoras de otros Estados y no contempla sanciones.

Otros documentos soportan la materia legislativa, en tal sentido, el Comité de Seguridad de la Información, de la División de Comercio Electrónico, de la American Bar Association, emitió, en agosto de 1996, la "Guía de Firmas Digitales". Así mismo, el 15 de agosto de 1997, la Conferencia Nacional de Comisionados sobre Derecho Estatal Uniforme, elaboró la "Uniform Electronic Transactions Act" (UETA), la cual se aprobó el 30 de julio de 1999.

Aunado a ello, el 4 de agosto del 2000 se aprobó la "Uniform Computer Information Transactions Act" (UCITA), la cual se encuentra en proceso de adopción por los diversos Estados de la Unión Americana. Asimismo, el 30 de junio el 2000 se emite la "Electronic Signatures in Global and Nacional Commerce Act" (E-Sign Act.) vigente a partir del 1 de octubre del 2000 (otorgando a la firma y documento electrónico un estatus legal equivalente a la firma autógrafa y al documento en papel).

Estados Unidos es uno de los países más avanzados en materia de firma electrónica. Sus leyes establecen la presunción de que una firma digital tiene el mismo efecto legal que una firma manuscrita si se cumplen ciertas existencias; una de las exigencias es que la firma digital sea

verificada por referencia a una clave pública incluida en un certificado válido emitido por una autoridad de certificación con licencia.

b) Italia: Delpiazzo, C. (2000, 16) indica que Italia fue el primer país de Europa en dictar reglamentación sobre firma digital y lo hizo con el "Regolamento contenente modalitá di applicazione dell' artícolo 15, comma 2, della lege 15 marzo 1997, n° 59, in formazione, archivazione e trasmissione di documenti con strumenti informatici e telematici".

Este reglamento da diversos conceptos en su art. 1°, como por ejemplo: firma digital, par de claves asimétricas, clave privada y certificado. En el art. 2° se establece la validez y eficacia del documento electrónico. Este reglamento no regula a las Autoridades Certificantes, las define como sujetos públicos o privados que certifican y guardan las claves públicas de firma por 10 o más años.

La Ley de 15 de marzo de 1997 número 59, es la primera norma del ordenamiento jurídico italiano que recoge el principio de la plena validez de los documentos informáticos. El reglamento aprobado por el Consejo de Ministros el 31 de octubre de 1997, si bien para el efectivo reconocimiento del valor jurídico de la documentación informática y de las firmas digitales será necesario esperar a que sea operativo en virtud de la

emanación de los posteriores e indispensables reglamentos técnicos de actuación.

Cadone (1998, p. 48) refiere que el 23 de enero del 2002 se publicó la ley sobre firma electrónica, quedando regulada la materia en su amplitud, lo cual adjudica validez jurídica a la firma electrónica. Se define la firma digital como el resultado del proceso informático (validación) basado en un sistema de claves asimétricas o dobles, una pública y una privada, que permite al suscriptor transmitir la clave privada y al destinatario transmitir la clave pública, respectivamente, para verificar la procedencia y la integridad de un documento informático o de un conjunto de documentos informáticos.

En el reglamento la firma digital está basada exclusivamente en el empleo de sistemas de cifrado llamados asimétricos. El art. 2 del Reglamento italiano establece que los documentos informáticos serán válidos y eficaces a todos los efectos legales si son acordes a las exigencias del Reglamento.

En concreto, el art. 10.2 equipara la firma digital sobre un documento informático a la firma escrita en soporte papel; y el art. 11.1 establece que los contratos realizados por medios telemáticos o informáticos mediante el uso de la firma digital según las disposiciones del

reglamento serán válidos y eficaces a todos los efectos legales; pero téngase en cuenta que el art. 8 establece que cualquiera que pretenda utilizar la criptografía asimétrica con los efectos del art. 2 debe conseguir un par de claves adecuado y hacer pública una de ellas a través del procedimiento de certificación efectuada por un certificador.

Regulan la Ley y el Reglamento entre otras cosas: La validez del documento informático; el documento informático sin firma digital; el documento informático con firma digital; los certificadores; los certificados; autentificación de la firma digital; el "cybernotary"; los actos públicos notariales; la validación temporal; la caducidad, revocación y suspensión de las claves; la firma digital falsa; la duplicidad, copia y extractos del documento; y la transmisión del documento.

c) Perú: Espinoza (2003, 21) indica que en Perú existe la Ley No. 27269 Ley de Firmas y Certificados Digitales (2000). Su Objetivo es utilizar la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación de voluntad. Su ámbito de aplicación son aquellas firmas electrónicas que, puestas sobre un mensaje de datos puedan vincular e identificar al firmante, y garantizar su integridad y autenticación.

En este marco jurídico, se define como firma digital aquella que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada. Como Certificado Digital a aquel documento electrónico generado y firmado digitalmente por una entidad de certificación, la cual vincula un par de claves con una persona determinada confirmando su identidad.

Por su parte la Entidad de Certificación es aquella que cumple con la función de emitir o cancelar certificados digitales. Existe una Entidad de Registro o Verificación que es la encargada de recolectar y comprobar la información del solicitante del Certificado, además identifica y autentica al suscriptor de firma digital y acepta y autoriza las solicitudes de emisión y cancelación de certificados digitales. La Supervisión y el Control, corren a cargo de la autoridad administrativa designada por el Poder Ejecutivo.

Las Entidades de certificación intervienen en la emisión de certificados y pueden asumir las funciones de entidades de registro o verificación y deberán de contar con un Registro. Esta ley no establece el Valor probatorio de la Firma Electrónica, indicando que para reconocer un Certificado Extranjero este debe contar con el aval de una entidad nacional y no existen sanciones expresas en la Ley.

La Ley 27269, Ley de Firmas y Certificados Digitales, marca un hito importante, en el desarrollo legislativo jurídico-informático peruano, por cuanto, permite el uso de la firma electrónica en general, tal como se señala expresamente, en el artículo primero de la mencionada norma; y aún cuando después, regule únicamente las firmas y certificados digitales, reconociéndose la validez y eficacia jurídica de las firmas generadas mediante la aplicación de técnicas criptográficas asimétricas, es decir, aquellas que usan un par de claves: la clave pública, que debe ser conocida por todos, y, la clave privada, que únicamente es conocida por su propietario.

Con la aprobación del Reglamento de la Ley 27269, se cumple la gran función de otorgar seguridad jurídica a las personas que incursionarán en redes abiertas o en medios electrónicos en general, al reconocerse la validez de las firmas generadas bajo la Infraestructura Oficial de Firma Electrónica o Firma Digital, sin desconocer el uso de otras firmas electrónicas generadas fuera de la Infraestructura Oficial. En tal sentido, Perú cuenta con las herramientas jurídicas que permitirán a los usuarios realizar operaciones seguras en materia de comercio electrónico y contratación electrónica en general.

Los aspectos regulados por la Ley de Firmas y Certificados Digitales han permitido que en el Perú comience un desarrollo legislativo

paulatino y constante, a través de la aprobación de una serie de normas con carácter jurídico-informático, que vienen siendo aplicables a los diferentes ámbitos de la vida en sociedad.

Por tanto, se visualiza que los distintos países, ha realizado esfuerzos concretos en legislar la materia referida a las firmas electrónicas. Bajo este entorno, es indiscutible que las nuevas tecnologías de la información se presentan como una oportunidad inmejorable para que los países menos desarrollados o emergentes puedan achicar la brecha que los separa con los denominados países del primer mundo.

En este sentido, la firma electrónica es un instrumento más que permite la adaptación a este nuevo paradigma socio-económico-cultural, que posibilita la expansión del comercio dentro de esta nueva economía digital globalizada, rediseña las relaciones laborales y la interacción humana y, a su vez, en el ámbito administrativo o gubernamental, optimiza la eficiencia a un bajo costo, con intervención y participación de los administrados (ciudadanos), lo cual impone la necesidad de adecuar y armonizar los ordenamientos jurídicos de las naciones.

4.- Aspectos Técnicos y Jurídicos de la Firma Electrónica.

El problema fundamental que plantean las transacciones a través de Internet, desde un punto de vista jurídico se puede resumir en el

criterio de Rodríguez, G. (2002, 4) en cuatro grandes puntos, que han sido puestos de manifiesto por numerosos expertos en la materia: autenticidad, integridad, confidencialidad y no repudio.

La autenticidad significa que la información sea enviada por quien aparece como emisor y recibida por aquel a quien va dirigida. La integridad, hace referencia al hecho de que la información no pueda ser manipulada en el proceso de envío. La confidencialidad, asegura el secreto de las comunicaciones contenidas en los mensajes. Por su parte, el no repudio, viene a asegurar que no se pueda negar la autoría del mensaje enviado.

Para garantizar el cumplimiento de estos cuatro requisitos, opina Rodríguez, G. (2002, 4) se plantean dos grandes alternativas:

a) Sistemas de Criptografría Simétrica, que obliga a los interlocutores a utilizar la misma clave para encriptar y desencriptar el mensaje, técnica que fue desarrollada por IBM (sistema “DES”), pero que fracasó debido a su inseguridad en cuanto al secreto y confidencialidad de dicha clave. No obstante, este sistema, ha sido el más utilizado históricamente.

Dependiendo de la naturaleza de la aplicación utilizada tiene cuatro variantes para su implementación: EBC (Electronic Codebook mode),

para mensajes cortos de menos de 64 bits; CBC (Cipher Block Chaining Mode), para mensajes largos; CFB (Cipher Block Feedback) para cifrar bit por bit; y el OFB (Output Feedback mode) análogo al CFB, pero permite evitar la propagación de errores. La experiencia práctica se ha encargado de poner de manifiesto las carencias de estos sistemas para la transmisión de información de alta de seguridad.

b) Sistemas de Criptografía Asimétrica, consistentes en la asignación de dos claves, una pública y otra privada, asociadas a un solo interlocutor. Este sistema, parece el más adecuado, para el cumplimiento de los requisitos anteriores, y es el más utilizado en la práctica, bajo la denominación RSA, que se debe a las iniciales de sus creadores (Rivest, Shamir y Adelman), y que es el contemplado en el documento de la ISO (International Standard Organisation), 7498-2, de Julio de 1988, que señala la arquitectura de seguridad para proteger las comunicaciones de los usuarios de las redes.

Se puede definir como una cadena de caracteres que se agrega a un archivo digital que hace el mismo papel que la firma convencional que se escribe en un documento de papel ordinario. El esquema resumido de este sistema se puede resumir en los siguientes pasos: a cada usuario se le un número entero que funciona como su clave pública, cada usuario posee una clave privada que solo él conoce, y que es distinta para cada

uno, existe un directorio de claves públicas que pueden ser conocidas y el emisor envía el mensaje con la clave pública del destinatario encriptándola con su clave privada. El destinatario solo podrá abrir el mensaje con la clave pública junto con su clave privada.

Opina Martín (2001, 2) que el éxito de este sistema se debe a que garantiza la seguridad y confidencialidad de las comunicaciones telemáticas. En otras palabras, la firma basada en RSA, provoca que el contenido del mensaje sea irreversible, único e invariable. Además facilita una perfecta identificación de remitente y destinatario. Esta última función se realiza a través de los llamados “terceros de confianza”, que han sido denominados por algún sector de la doctrina especializada, como Notarios Electrónicos.

Señala el autor in comento que, para poder utilizar la firma electrónica es necesario haber obtenido previamente un certificado digital. El funcionamiento de la firma electrónica se basa en un par de números —la clave privada y la clave pública— con una relación matemática entre ellos. Estos números o claves se generan a partir de un navegador de Internet y del certificado digital emitido por la entidad certificadora.

Martín (2001, 2) señala que la clave privada se almacena en un dispositivo de uso privado, siendo una tarjeta criptográfica o normalmente

el disco duro de un ordenador. La clave pública, en cambio, se distribuye junto con el mensaje firmado, fichero, entre otros.

Sobre la firma electrónica recibida, el receptor aplicará la clave pública del emisor a fin de descifrarla. El resultado será una huella que debe coincidir con la huella del mensaje. Si esto se produce, hay garantía de que el mensaje no ha sido modificado y de que ha sido emitido por el titular de la firma.

En la Exposición de Motivos de del Decreto-Ley sobre Mensajes de Datos y Firmas Electrónicas (2001), se indica que Venezuela avanza aceleradamente hacia la actualización en materia de tecnologías de información y de las comunicaciones. La particularidad de estas tecnologías de información es que utilizan medios electrónicos y las redes nacionales e internacionales adecuadas para ello, y constituyen una herramienta ideal para realizar intercambios de todo tipo incluyendo el comercial a través de la transferencia de informaciones de un computador a otro sin necesidad de la utilización de documentos escritos en papel, lo que permite ahorros de tiempo y dinero.

Agrega que, en consecuencia, se hace necesaria e inminente la regulación de las modalidades básicas de intercambio de información por medios electrónicos, de las cuales han de desarrollarse todas las nuevas modalidades de transmisión y recepción de información, conocidas y por

conocerse, a los fines de garantizar un marco jurídico mínimo indispensable que permita a los diversos agentes involucrados desarrollarse y contribuir con el desarrollo de las nuevas tecnologías en Venezuela.

Se indica además en la Exposición de Motivos de la ley in comento que el instrumento legal debe regular estos mecanismos de intercambio de información, hacerlos jurídicamente trascendente a la administración de justicia, que le permita apreciar y valorar estas formas de intercambio y ser un soporte de información, a fin de garantizar el cumplimiento de las obligaciones asumidas mediante estos mecanismo, constituye un aporte necesario.

En esta nueva modalidad de relacionarse hacen falta establecer dos elementos principales: identificación de las partes e integridad del documento o mensaje, de allí se derivan responsabilidades, entre ellas la de índole civil, que son comunes a los actos y negocios normales previstos en nuestro ordenamiento jurídico actual.

CAPITULO II

REQUISITOS PARA LA VALIDEZ DE LA FIRMA ELECTRÓNICA

Respecto a los requisitos para la validez de la firma electrónica, se analizan dos puntos esenciales, el cumplimiento de los requisitos jurídicos y de los requisitos técnicos, que a su vez le adjudican valor probatorio a la firma electrónica.

1.- Requisitos Jurídicos.

Rodríguez (2002, 4) indica que 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”.

Por consiguiente, 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 técnicos que la Firma debe poseer.

2.- Requisitos Técnicos.

Para efectos de comprobar la validez de la Firma electrónica, Rodríguez (2002, 4) plantea que 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, agrega la autora antes mencionada, que 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, se puede 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.

3.- Requisitos de la Firma Electrónica en Venezuela.

El Legislador Patrio consagró una serie de requisitos para dar validez y Eficacia probatoria a la firma, así lo consagra en el artículo 16 de la Ley Sobre Mensajes de Datos y Firmas Electrónicas que establece:

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.

Los procesos de creación y verificación de las firmas electrónicas deben cumplir para su validez y surtir efectos legales con dos requisitos esenciales: autenticación del signatario y autenticación del mensaje de datos. Con respecto a la autenticación del signatario, si el par de claves públicas o privadas está asociado a una persona especial, el certificado del mensaje de datos atribuye el mismo a esa persona y no a otra porque la firma no puede ser adulterada, salvo que el signatario haya perdido el

control de la clave privada, que está bajo su responsabilidad, supone que el signatario es quien envía el mensaje por lo cual goza de autenticación.

En cuanto a la autenticación del mensaje de datos, la firma electrónica identifica el mensaje firmado, con certeza, porque la verificación revela cualquier intento de adulteración, ya que la comparación del mensaje, obtenido en el proceso de firmarlo y en el proceso de verificación, debe mostrar que los mensajes entre emisor y destinatario son iguales.

Ovidio, J. (2002, 2), señala que la Ley Sobre Mensajes de Datos y firmas Digitales (2001) es en su naturaleza una Ley Especial. Por tanto, debe ser aplicada con preferencia sobre cualquier otra norma en todo lo que refiere al reconocimiento, eficacia y valor jurídico de la Firma electrónica, los mensaje de datos y toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas.

Como se ha señalado, la única diferencia de los hechos llevados a cabo en la Red de aquellos perfeccionados en el mundo tridimensional es el medio electrónico a través del cual se desarrollan, por tanto, las leyes ordinarias del mundo físico se aplican en lo que corresponden a los hechos provenientes de Internet salvo la presencia de una ley especial,

como es el caso de la Ley Sobre Mensajes de Datos y Firmas Electrónicas (2001), que será de aplicación preferente en lo que respecta a las materias de su especialidad.

En Venezuela la Ley Sobre Mensajes de Datos y Firmas Electrónicas (2001) ha pasado a constituir una herramienta indispensable para que el país se mantenga a la vanguardia regional en materia de derecho adaptado y aplicado a las nuevas tecnologías. Los principios y procedimientos adoptados por esta Ley son muy similares a los de otras legislaciones nacidas en momentos similares.

El proceso de identificación establecido en la Ley Sobre Mensajes de Datos y Firmas Electrónicas (2001) consta de cinco elementos: el mensaje de datos, la firma electrónica, el certificado electrónico, el proveedor de servicios de certificación y la Suscerte.

El mensaje de datos que presente todos los elementos del régimen de identificación, es decir aquel que tenga una firma electrónica que ha generado un certificado electrónico que ha sido provisto por un proveedor de servicios de certificación acreditado ante Suscerte, es el que va a tener la misma validez y eficacia probatoria que la ley otorga a los documentos firmados en forma autógrafa. La falta de alguno o varios de estos elementos trae como consecuencia que el documento no tenga valor de

plena prueba. Sin embargo, siempre tendrá un valor probatorio que deberá ser apreciado por el juez.

Cabe señalar que si bien la Ley Sobre Mensajes de Datos y Firmas Electrónicas (2001) es tecnológicamente neutra, no lo es así el reglamento. En cuanto a la ley, era determinante que esta no favoreciera una tecnología sobre otra, a fin de que permanezca vigente con independencia de los estándares que imponga el mercado.

Sin embargo, el reglamento está claramente orientado hacia la tecnología de criptografía asimétrica, tecnología que actualmente es el estándar. No obstante, para no favorecer a ningún proveedor de tecnología, en lugar de los términos de uso comercial “clave privada” y “clave pública”, la ley se refiere a los genéricos “datos de generación y datos de verificación de firma”.

Por tanto, la Ley Sobre Mensajes de Datos y Firmas Electrónicas (2001), no obliga a la utilización de la firma electrónica en lugar de la manuscrita, sino que su utilización es voluntaria, por lo cual el otorgamiento de validez y eficacia de los mensajes firmados electrónicamente no se pretende establecer su obligatoriedad.

Lo anterior supone que el mismo sea un medio alternativo, voluntario entre las partes, que haya consentimiento en su empleo, puesto

que no está en el ánimo del legislador alterar las restantes formas de los diversos actos jurídicos, registrales y notariales, sino que se propone que un mensaje de datos firmado electrónicamente no carezca de validez jurídica por la naturaleza de su soporte y de su firma.

CAPITULO III
ANÁLISIS DEL USO DE LA FIRMA ELECTRÓNICA EN EL PROCEDIMIENTO CIVIL VENEZOLANO

1.- Principios que rigen el Uso de la Firma Electrónica.

En el ámbito del Derecho Procesal Civil, mediante la Ley Sobre Mensajes de Datos y Firmas Electrónicas (2001), es posible la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica, en tal sentido, la manifestación de voluntad, es expresa cuando se realiza en forma oral o escrita, a través de cualquier medio directo, manual, mecánico, electrónico u otro análogo.

Esto alude al principio de autonomía y voluntad, el cual se refiere a que debe prevalecer la libertad contractual entre las partes, quienes de mutuo acuerdo decidirán o no el empleo de la firma electrónica, sea certificada o no certificada. Dicha relación contractual se rige por las disposiciones contenidas en el artículo 1133 del Código Civil (1982), indicando que es una convención entre dos o más personas para constituir, reglar, transmitir, modificar o extinguir entre ellos un vínculo jurídico.

Ahora bien, la aceptación de la firma electrónica certificada o no, implica la declaración de voluntad formulada por la persona a quien va dirigida la proporción para la validez de la misma y su aceptación o rechazo es su consentimiento, su declaración de voluntad de que el documento privado tenga dicha cualidad o no.

En el artículo 1368 del Código Civil (1982) se manifiesta la autonomía de voluntad en los instrumentos privados, el cual no tiene validez si no está suscrito por el obligado, puesto que si la escritura no tiene firma no hace fé contra nadie, por lo tanto es indispensable que se encuentre firmada por quienes han contraído la obligación. En principio la sola voluntad de las partes es suficiente para crear el vínculo jurídico, hacer nacer las obligaciones, transformarlas, modificarlas o extinguirlas.

Avellán, A. (1990, 90) señala que se contempla el uso de firmas digitales en las facturas electrónicas y se le considera como un sustituto digital cifrado (encriptado) de la firma manuscrita que, en el marco del intercambio electrónico de datos, permite al emisor y al receptor de un mensaje electrónico, verificar con certeza la identidad proclamada por el transmisor, impidiendo este último desconocer su autoría.

Entre los principios que guían al Decreto-Ley sobre Mensajes de Datos y Firmas Electrónicas, señalados en la exposición de Motivos de la Ley mencionada, se destacan los siguientes:

a) Eficacia Probatoria. A los fines de otorgar la seguridad jurídica necesaria para la aplicación del Decreto-Ley, así como la adecuada eficacia probatoria a los mensajes de datos y firmas electrónicas. Se le atribuye a los mismos el valor probatorio que la Ley consagra para los instrumentos escritos, los cuales gozan de tarifa legal y producen plena prueba entre las partes y frente a terceros de acuerdo a su naturaleza.

b) Tecnológicamente neutra. No se inclina a una determinada tecnología para las firmas y certificados electrónicos. Incluirá las tecnologías existentes y las que están por existir.

c) Respeto a las Formas Documentales Existentes. Es importante destacar que este Decreto-Ley no obliga a la utilización de la firma electrónica en lugar de la manuscrita, sino que su utilización es voluntaria. Tampoco se pretende alterar las restantes formas de los diversos actos jurídicos, registrales y notariales, sino que se propone que un mensaje de datos firmado electrónicamente no carezca de validez jurídica únicamente por la naturaleza de su soporte y de su firma.

d) Respeto a las firmas electrónicas preexistentes. Las firmas electrónicas utilizadas en grupos cerrados donde existan relaciones contractuales ya establecidas pueden ser excluidas del campo de aplicación del Decreto-Ley. En este contexto debe prevalecer la libertad contractual de las partes.

e) Reconocimiento Jurídico de las Firmas Electrónicas. Asegura el reconocimiento jurídico de las firmas electrónicas y los servicios de certificación provistos por los proveedores de servicios de certificación, incluyendo mecanismos de reconocimiento a nivel internacional. Establece las exigencias esenciales a cumplir por dichos proveedores de servicios de certificación, incluida su responsabilidad.

f) Funcionamiento de las firmas electrónicas. El Decreto-Ley busca asegurar el buen funcionamiento de las firmas electrónicas, mediante un marco jurídico homogéneo y adecuado para el uso de estas firmas en el país y definiendo un conjunto de criterios que constituyen los fundamentos de su validez jurídica.

g) No discriminación del mensaje de datos firmado electrónicamente. Garantiza la fuerza ejecutoria, el efecto o la validez jurídica de una firma electrónica no sea cuestionado por el solo motivo de que se presenta bajo la forma de mensaje de datos.

h) Libertad contractual. Permite a las partes convenir la modalidad de sus transacciones, es decir, si aceptan o no las firmas electrónicas.

i) Responsabilidad. Se excluye la responsabilidad siempre que el sujeto pueda demostrar que ha tomado las diligencias necesarias según las circunstancias. Los Proveedores de Servicios de Certificación Electrónica pueden limitar su responsabilidad, incluyendo en los certificados que emitan las restricciones, condiciones y límites establecidos para su utilización.

Dichos principios rigen la aplicación de la ley que rige la firma electrónica en Venezuela, y se establecen de acuerdo con las presunciones de legalidad que garantizan la autenticidad, integridad y no repudio.

2.- La Firma Digital como Prueba Libre.

La actual regulación expresa sobre esta materia expuesta en la Ley Sobre Mensajes de Datos y Firmas Electrónicas (2001), conduce a considerar la admisibilidad y el uso de las firmas electrónicas en el sistema legal venezolano. El régimen probatorio actual permitiría que documentos electrónicos con firmas electrónicas sean presentados en juicio bajo la categoría de las pruebas libres, erigidas en el Artículo 395

del Código de Procedimiento Civil (1987) pero ello probablemente se reduce a instrumentos que no son públicos.

El Código Civil, en su artículo 1.356, establece la clásica división entre instrumentos públicos e instrumentos privados. Los primeros se encuentran definidos en el artículo 1.357 del Código Civil.

> "Instrumento público o auténtico es el que ha sido autorizado con las solemnidades legales por un Registrador, por un Juez u otro funcionario o empleado público que tenga facultad para darle fe pública, en el lugar donde el instrumento haya sido autorizado."

La definición de instrumento privado no está expresamente establecida por la ley pero podría definirse como todo aquel instrumento que no es un instrumento público, y que está suscrito por el obligado (Artículo 1.368 del Código Civil). Por suscrito debe entenderse que esté firmado. No existe una definición de firma pero se ha interpretado que se trata de una firma ológráfica.

Más aún, en el único aparte de este artículo 1.368 dispone que si el otorgante (del documento privado) no sabe o no puede firmar, el instrumento deberá estar suscrito por persona mayor de edad que firme a ruego de aquél, y, además, por dos testigos". Esta interpretación se

fortalece cuando se lee el artículo 1.375 del Código Civil (1982), el cual establece:

> "El telegrama hace fe como instrumento privado, cuando el original lleva la firma de la persona designada en él como remitente, o cuando se prueba que el original se ha entregado o hecho entregar en la Oficina Telegráfica en nombre de la misma persona, aunque ésta no lo haya firmado, siempre que la escritura sea autógrafa. Si la firma del original se ha autenticado legalmente, se aplicarán las disposiciones establecidas respecto de los instrumentos privados. Si la identidad de la persona que lo ha firmado o que ha entregado el original se ha comprobado por otros medios establecidos en los reglamentos telegráficos, se admitirá la prueba contraria".

Esta disposición aclara el requisito de firma en instrumentos privados, al tratarse de un medio tecnológico que no permite una firma ológráfica, con lo cual, no podría, bajo el régimen actual, clasificarse un documento electrónico con una firma electrónica como instrumento privado.

Por lo tanto, en un juicio, los documentos suscritos con firmas electrónicas, podrán ser apreciados por el Juez bajo la categoría de pruebas libres, que son todas aquellas pruebas no prohibidas expresamente por la ley, y que las partes consideren conducentes a la demostración de sus pretensiones (artículo 395 del Código de Procedimiento Civil, 1987).

Por su parte, Curto, J. (2000, s/p) indica que el principio de libertad de medios postula que los elementos de prueba puedan ser introducidos

al proceso con amplitud. Este sistema permite al juzgador admitir u ordenar los medios de prueba que considere idóneos para formar su convicción, aunque no se encuentren expresamente regulados. Enuncia los medios de prueba clásicos, pero expresa o tácitamente permite la producción de otros no regulados.

El mismo autor antes mencionado agrega que este sistema a su vez, presenta dos modalidades; la primera de ellas es la que enumera los medios de prueba clásicos utilizables y consagra en una disposición expresa la facultad del juzgador de admitir u ordenar otros que estime convenientes. Así ocurre en el orden procesal nacional que establece que cuando se ofreciese un medio de prueba idóneo y pertinente no previsto de modo expreso por la ley, el Tribunal establecerá la forma de diligenciarlo, usando el procedimiento determinado para otras pruebas que fueren analógicamente aplicables"

En consecuencia, la firma electrónica en un documento electrónico tiene su concepto, estructura y naturaleza en el documento, y en el proceso civil, el documento electrónico resulta admisible como elemento de prueba, debiendo tener similar tratamiento y ponderación, en cuanto no resulte incompatible por sus particularidades, al medio previsto para la prueba documental en todas sus fases: presentación, ofrecimiento, sustanciación, impugnación, producción y valoración.

CAPITULO V
ANÁLISIS DE LOS RIESGOS DE LAS FIRMAS ELECTRÓNICAS EN EL PROCEDIMIENTO CIVIL VENEZOLANO

En el análisis de los riesgos de las firmas electrónicas en el procedimiento civil venezolano, se analizan los riesgos asociados al emisor-receptor, así como aquellos vinculados con el proveedor de Servicios de Certificación.

1.- Riesgos Asociados al Receptor-.Emisor.

Dentro del procedimiento civil venezolano, la firma electrónica goza de autentificación de las partes (yo y el otro son quienes dicen ser), se garantiza la integridad del documento (la totalidad del documento es verídica, y se mantendrá íntegra) y se garantiza que los firmantes no podrás repudiarlo (no podrán negar su existencia y validez legal). Técnicamente hablando, la firma electrónica es más segura que la firma en papel, pues está encriptada y es más difícil de plagiar. Esto es lo que quiere proteger la ley.

Rodríguez (2002, 5) indica que 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:

> Artículo 22. La Superintendencia de Servicios de Certificación Electrónica tendrá las siguientes competencias:
>
> 1. Otorgar la acreditación y la correspondiente renovación a los Proveedores de Servicios de Certificación una vez cumplidas las formalidades y requisitos de este Decreto-Ley, sus reglamentos y demás normas aplicables.
> 2. Revocar o suspender la acreditación otorgada cuando se incumplan las condiciones, requisitos y obligaciones que se establecen en el presente Decreto-Ley.
> 3. Mantener, procesar, clasificar, resguardar y custodiar el Registro de los Proveedores de Servicios de Certificación públicos o privados.
> 4. Verificar que los Proveedores de Servicios de Certificación cumplan con los requisitos contenidos en el presente Decreto-Ley y sus reglamentos.

5. Supervisar las actividades de los Proveedores de Servicios de Certificación conforme a este Decreto-Ley, sus reglamentos y las normas y procedimientos que establezca la Superintendencia en el cumplimiento de sus funciones.
6. Liquidar, recaudar y administrar las tasas establecidas en el artículo 24 de este Decreto-Ley.
7. Liquidar y recaudar las multas establecidas en el presente Decreto-Ley.
8. Administrar los recursos que se le asignen y los que obtenga en el desempeño de sus funciones.
9. Coordinar con los organismos nacionales o internacionales cualquier aspecto relacionado con el objeto de este Decreto-Ley.
10. Inspeccionar y fiscalizar la instalación, operación y prestación de servicios realizados por los Proveedores de Servicios de Certificación.
11. Abrir, de oficio o a instancia de parte, sustanciar y decidir los procedimientos administrativos relativos a presuntas infracciones a este Decreto-Ley.
12. Requerir de los Proveedores de Servicios de Certificación o sus usuarios, cualquier información que considere necesaria y que esté relacionada con materias relativas al ámbito de sus funciones.
13. Actuar como mediador en la solución de conflictos que se susciten entre los Proveedores de Servicios de Certificados y sus usuarios, cuando ello sea solicitado por las partes involucradas, sin perjuicio de las atribuciones que tenga el organismo encargado de la protección, educación y defensa del consumidor y el usuario, conforme a la ley que rige esta materia.
14. Seleccionar los expertos técnicos o legales que considere necesarios para facilitar el ejercicio de sus funciones.
15. Presentar un informe anual sobre su gestión al Ministerio de adscripción.
16. Tomar las medidas preventivas o correctivas que considere necesarias conforme a lo previsto en este Decreto-Ley.
17. Imponer las sanciones establecidas en este Decreto-Ley.
18. Determinar la forma y alcance de los requisitos establecidos en los artículos 31 y 32 del presente Decreto-Ley.
19. Las demás que establezcan la ley y los reglamentos.

Illescas, R. (1997, 33) señala con acierto que la confianza descansa no sólo en la seguridad que ofrezca la técnica, sino también en la seguridad jurídica. Con el Decreto – ley 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.

En efecto, en nuestro derecho la suscripción tradicional por sí sola no es suficiente para demostrar la autoría y la fe probatoria de un documento si falta su reconocimiento en juicio, expreso o tácito (ver artículo 444 del Código de Procedimiento Civil, en concordancia con el artículo 1.363 del Código Civil).

De hecho, si la firma es negada toca a la parte que produjo el instrumento (documento) probar su autenticidad a través de otros medios de prueba como el cotejo (experticia) y la prueba testimonial. De allí que, la autoría de un documento electrónico no firmado digitalmente, podría ser demostrada a través de cualquier medio de prueba pertinente.

En las transacciones electrónicas, Viloria (2001, 7) indica que la utilización de la firma electrónica no es obligatoria, por lo que la verdadera dificultad que surge en esta materia, es cuando se quiere garantizar el “cierre” del contrato. En efecto, de acuerdo con los principios generales

del Derecho Civil y comercial la firma tradicional garantiza el cierre de la contratación en un doble sentido, ya que asegura que el contenido del contrato es idéntico al texto suscrito e impide la reapertura de nuevas condiciones contractuales a las ya concluidas y aceptadas. De allí que la ventaja de utilizar una firma electrónica es que a través de ella se garantiza tanto el intercambio de voluntades como el “cierre” del contrato, en los mismos términos que una firma tradicional.

Ciertamente, opina la autora que, para desvirtuar la idea de que los documentos electrónicos o mensajes de datos están expuestos a una fácil manipulación por parte de los usuarios de las computadoras, así como a una reproducción indiscriminada del original, de tal modo que se hace imposible distinguirlo de los duplicados, la parte que pretenda valerse de un documento electrónico deberá, entonces, producir elementos suficientes que convenzan al juzgador de la veracidad y de la certeza de su contenido, para lo cual podrá valerse de cualquier medio de prueba que considere idóneo (por ejemplo: con un justificativo para perpetua memoria, testificales, posiciones juradas, experticias técnicas, entre otros).

Alsina (2000, 127) indica respecto al problema de la autenticidad de los documentos y datos informáticos originados en elaboradores electrónicos de las partes o de terceros cabe precisar que, si bien intervienen distintos sujetos en las fases de programación, toma a ingreso

y su recuperación, todos son perfectamente individualizadles a través de códigos de identificación atribuidos "ad personan" o mediante auditorias de sistemas.

Tal circunstancia interesa no sólo por la imputación de responsabilidad penal en el supuesto de delitos, sino para desvirtuar la falsa idea de que los datos electrónicos resultan de procedimientos anónimos o, peor aún, de máquinas inimputables. En virtud de la incompatibilidad de los medios informáticos con la exigencia de normas que trabaría la operatividad y la celeridad que los caracteriza ha de puntualizarse la existencia de métodos sustitutivos de ella para comprobar la autoría.

Por ejemplo, en el sistema SWIFT de transferencia internacional de fondos por vía electrónica, se exige la identificación recíproca para expedir órdenes y mensajes. La confiabilidad judicial en los sistemas informáticos puede apoyarse en la circunstancia de que poseen técnicas de control para evitar errores, cuyo funcionamiento debe ser verificado en caso necesario. La inalterabilidad y el carácter indeleble de los datos son condiciones que responden precisamente a exigencias de la fiabilidad de la información. Los soportes que por su índole pueden ser re inscriptos, no brindan garantías de credibilidad y su valor probatorio ha de ser, ciertamente, menor.

Font (2000, 210), 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 autentica, todo ello confiere una ventaja a la Firma digital.

Dadas las condiciones que anteceden, Martínez, A. (1998, 34), al hacer referencia a las técnicas de seguridad de la información que pueden resultar adecuadas para hacer frente a los riegos señaló:

> "… las nuevas tecnologías están haciendo posible el uso de firmas electrónicas para autenticar y preservar la integridad de las transacciones y documentos; generalmente, implica el uso de tecnologías basadas en la criptografía, como el cifrado (para la obtención de confidencialidad) y las firmas digitales (a efectos de autenticación, integridad y no repudiación); firmas digitales que, como veremos, nos llevan a certificados y autoridades de certificación."

De igual modo se ha pronunciado el autor Hance, 0. (1996, 180), al afirmar lo siguiente:

> "Debido al incremento de las transacciones comerciales y de la transmisión de información delicada... usuarios, autores y hombres de negocios desean ser capaces de garantizar la seguridad y confidencialidad. Uno de los medios más seguros de lograrlo es utilizar la criptografía, una técnica basada en un algoritmo matemático que transforma un mensaje legible a su equivalente en un formato ilegible para cualquier usuario que no cuente con la clave secreta para desencriptarlo."

Por su parte, Martínez A. (1998, 42) al hacer referencia a la criptografía, la definió como:

> “...la ciencia que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlos a su forma original... La criptografía utiliza generalmente un algoritmo matemático para cifrar datos para hacerlos ininteligibles para cualquier persona que no posea cierta información secreta (clave criptográfica)”.

Así mismo, la autora citada se refirió por una parte a la criptografía simétrica o de clave secreta, donde las partes en el proceso de cifrado y descifrado deben compartir una clave común que se ha acordado de forma previa, y por la otra, a la criptografía asimétrica o de clave publica, basada en el uso de un par de claves asociadas: una clave privada, conocida solo por su titular, y una clave pública, relacionada matemáticamente con ella, y que puede ser accesible para cualquiera.

El sistema de criptografía asimétrica permite confidencialidad, pues se pueden enviar mensajes secretos a través de Internet, sin necesidad de comunicación previa de una clave secreta compartida; además, permite realizar firmas digitales, que proporcionan autenticidad, integridad y no rechazo de origen (pp. 42-47).

En ese mismo orden se ha pronunciado Hall, J. (1999, 26), quien señalo:

> “...los métodos de encriptado por clave publica no solo garantizan la inviolabilidad del contenido de un documento, sino que también certifican la identidad del originante. Esta combinación de i) la certeza respecto del contenido del documento, y ii) la certeza respecto de la identidad del

documento permiten utilizar a la criptografía de clave publica como firma digital."

Por su parte, Davara, M. (1996, 149), al referirse a las firmas digitales expresa:

> "Las firmas digitales proporcionan una nueva dimensión al mundo de la información. En estos tiempos en que las grandes masas de información se tratan a través de ordenadores, es imprescindible incorporar el concepto de firma que autentique de una forma inequívoca al autor y La integridad del documento. Las firmas digitales se consiguen con sistemas criptográficos en clave pública, encriptando la información con La clave privada del autor del documento, y verificando con la clave pública de dicho autor. Aplicaciones como correo electrónico seguro y firmas digitales de documentos son posibles en un entorno de comunicaciones abierto gracias a La clave publica."

En el marco de las observaciones anteriores, la autora Sanchis, C. (1999, 93) preciso la diferencia entre las expresiones firma digital y firma electrónica, al señalar:

> "Por firma electrónica se entiende 'cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita'. Así tanto es firma electrónica La firma manuscrita digitalizada, como las firmas que, con tecnología más avanzada, se crean utilizando sistemas de criptografía. Sin embargo solo estas últimas se conocen hoy en día como digitales."

Por consiguiente, se puede considerar que la firma electrónica sea admitida o no por el emisor,

2.- Riesgos Asociados a los Proveedores de Certificación.

La firma digital en sí, es un elemento básico de los protocolos autoverificables, ya que no precisa de la intervención de una Autoridad de Certificación para determinar la validez de una firma. La Autoridad o Entidad de Certificación debe reunir los requisitos que determine la ley, conocimientos técnicos y experiencia necesaria, de forma que ofrezca confianza, fiabilidad y seguridad.

Las autoridades de Certificación pueden emitir diferentes tipos de certificados:

a) Los certificados de Identidad, que son los más utilizados actualmente dentro de los criptosistemas de clave pública y ligan una identidad personal (usuario) o digital (equipo, software, etc.) a una clave pública.

b) Los certificados de Autorización o potestad que son aquellos que certifican otro tipo de atributos del usuario distintos a la identidad.

c) Los Certificados Transaccionales son aquellos que atestiguan que algún hecho o formalidad acaeció o fue presenciada por un tercero.

d) Los Certificados de Tiempo o estampillado digital de tiempo permiten dar fe de que un documento existía en un instante determinado de tiempo.

Autores como Martínez A. (1998, 83) han destacado la necesidad de la implementación de las autoridades de certificación, al señalar:

> "…la criptografía necesita una nueva entidad: una tercera parte de confianza, la cual actuará, fundamentalmente, para asegurar el vinculo entre la clave pública y el titular de la clave privada, además de desarrollar, en su caso, otras funciones igualmente importantes (como, por Ej., autenticar fechas y horas de determinadas acciones y transacciones, Se pone así de manifiesto el papel emergente e importante de las autoridades de certificación, y los certificados, en el comercio electrónico seguro: las partes sin unas relaciones comerciales preestablecidas pueden optimizar su usa de firmas digitales y criptografía de forma segura si una autoridad de certificación de confianza asegura la autenticidad e integridad de sus mensajes a través de la certificación de sus claves publicas."

Es importante destacar que en diversos ordenamientos jurídicos se están realizando grandes esfuerzos para reducir los riesgos asociados a las transacciones comerciales basadas en la transmisión y almacenamiento electrónico de datos, a través de creación de leyes relativas al comercio electrónico en general, o a las firmas digitales y autoridades de certificación en particular.

Así por ejemplo, en los Estados Unidos existe gran actividad en materia de legislación sobre firma electrónica. En algunos países de Europa se han aprobado normas en materia de firma digital como es el caso de Italia y Alemania, mientras que en otros países existen proyectos en discusión.

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). Opina Rodríguez (2002, 6) que en nuestro ordenamiento jurídico, 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 ingrese 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 el empleo de los proveedores de servicios

de certificación y la efectiva seguridad que estos impriman a sus procesos.

Por otra parte, la Ley sobre Mensajes de Datos y Firmas Electrónicas prevé la figura de los Proveedores de Servicios de Certificación y todo lo relativo a los certificados electrónicos. De acuerdo con la Ley, la figura de los proveedores de certificados electrónicos se crea con el objeto de otorgar mayor seguridad en el comercio y comunicaciones electrónicas.

En efecto, los proveedores son los sujetos que, siguiendo el procedimiento legalmente previsto, obtengan de la Superintendencia de Servicios de Certificación Electrónica, una autorización que les permita garantizar a los usuarios, la autoría de un mensaje de datos, a través de la certificación de la firma electrónica y la certificación de la integridad del mensaje.

Ahora bien, estas funciones de los proveedores de certificados electrónicos, bajo ningún concepto sustituyen las funciones de los notarios o registradores, cuando para determinados actos jurídicos se requiera su intervención; por lo que, cuando se trate de negocios o actos jurídicos que para su validez frente a terceros, la ley exija las formalidades de registro, dicho requisito en ningún modo se entenderá cumplido con la emisión de un certificado electrónico.

CAPITULO VI
ANÁLISIS DE LOS MEDIOS DE PRUEBA DE LA FIRMA ELECTRÓNICA

Toda pretensión jurídica invocada en juicio debe ser comprobada mediante las reglas dadas por el derecho probatorio, puesto que de esto depende la efectiva titularidad sobre el derecho discutido. La prueba en si constituye la base fundamental del proceso y es una condición de seguridad jurídica esencial para el pronunciamiento de una sentencia justa y objetiva.

Como consecuencia del reciente empleo de la tecnología informática como soporte material de hechos y actos jurídicos, es imprescindible conocer las condiciones bajo las cuales se consideran los medios de prueba de la firma electrónica.

La Ley Sobre Mensajes de datos y Firmas Electrónicas reglamenta la eficacia probatoria de la Firma electrónica dentro del ordenamiento jurídico venezolano. El artículo 4 se expresa lo siguiente:

> Artículo 4. Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, sin perjuicio de lo establecido en la primera parte del artículo 6 de este Decreto-Ley. Su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el Código de Procedimiento Civil.
>
> La información contenida en un Mensaje de Datos, reproducida en formato impreso, tendrá la misma eficacia

probatoria atribuida en la ley a las copias o reproducciones fotostáticas.

Dicho artículo en concordancia con el 1363 del Código de Procedimiento Civil (1987), indica que los mensajes de datos o archivos electrónicos son medios de prueba escritos, por lo cual tendrán el mismo valor probatorio que los instrumentos privados, sin embargo, pueden ser desconocidos por la parte a quien se opone en juicio, su contenido puede ser desvirtuado puesto que hace fé, hasta prueba en contrario de la verdad de sus declaraciones de acuerdo con lo estipulado por el artículo 1333 del Código de Procedimiento Civil, asimismo de lo establecido por el artículo 1364 del Código Civil donde se manifiesta que aquel contra quien se produce o a quien se exige el reconocimiento de un instrumento privado está obligado a reconocerlo o negarlo formalmente y si no lo hubiere se tendrá como reconocido.

En este proceso probatorio, los Proveedores de Servicios de Certificación, están en capacidad de dar fé de la autenticidad de las mismas, al emitir el certificado correspondiente, puesto que están autorizados y supervisados por la Superintendencia de Certificación Electrónica.

El artículo 444 del Código de Procedimiento Civil señala que la parte contra quien se produzca en juicio un instrumento privado como

emanado de ella o de algún causante suyo, deberá manifestar formalmente si lo reconoce o niega ya en el acto de contestación de la demanda. El silencio de las partes a este respecto, dará por reconocido el instrumento, es decir, que la parte podrá utilizar el procedimiento previsto en los artículos 444 al 450, ambos inclusive, del Código de Procedimiento Civil venezolano para la eficacia probatoria de los instrumentos electrónicos.

Con estas disposiciones se le atribuye a la firma electrónica el mismo valor probatorio de la firma autógrafa o documentos escritos, si están en su formato original, por lo cual gozarán de tarifa legal y producirán plena prueba entre las partes y frente a terceros de acuerdo con su naturaleza, salvo prueba en contrario.

En el caso de la firma no certificada, en su forma más simple contiene una clave pública y un nombre, a la cual otros pueden acceder. Por ello, para que tenga eficacia probatoria, salvo que las partes dispongan otra cosa, se exige el cumplimiento de los siguientes requisitos: garantizar que los datos utilizados para su generación puedan producirse solo una vez asegurando razonablemente su confidencialidad, ofrecer seguridad suficiente que no pueda ser falsificada con la tecnología y no alterar la integridad del mensaje de datos.

Sin embargo, a tenor de lo dispuesto en el artículo 17 de la ley sobre Mensajes de Datos y Firmas Electrónicas (2001) en el supuesto que no cumpla con estos requisitos puede constituirse en un elemento de convicción valorable bajo las reglas de la sana crítica y no perderá el valor que le atribuye la ley a las copias o reproducciones fotostáticas de acuerdo con lo señalado por el artículo 4 de la ley in comento.

Respecto a la eficacia probatoria de las firmas electrónicas certificadas, de acuerdo con el artículo 2 de la ley sobre Mensajes de Datos y Firmas Electrónicas (2001), emplea su propia clave secreta a través de un sistema criptográfico asimétrico y que solamente el conoce el acceso o clave, lo cual impide que después pueda negar su autoria, de tal manera que el signataria queda vínculo al documento electrónico enviado, por lo cual la validez del documento podrá ser probada en cualquier momento.

Por tanto, la firma electrónica certificada, por el solo hecho de se certificada tiene la validez jurídica y eficacia probatoria que la ley otorga a la firma manuscrita, puesto que en conformidad con el artículo 18 de la ley in comento “la firma electrónica debidamente certificada por un Proveedor de Servicios de Certificación, conforme a lo dispuesto en este Decreto-Ley, se considerará que cumple con los requisitos señalados en el artículo 16 de la misma ley.

De acuerdo con el artículo 16 de la recientemente promulgada Ley sobre Mensajes de Datos y Firmas Electrónicas, “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”, de esta manera si para determinados actos o negocios jurídicos la ley exige la suscripción autógrafa del documento, ese requisito quedará satisfecho en relación con un mensaje de datos (documento electrónico) al tener asociado una firma electrónica.

Ahora bien, para que esta firma posea la misma validez y eficacia probatoria de la firma manuscrita, deberá estar elaborada bajo ciertos mecanismos de seguridad que permitan a las partes contratantes garantizar que los datos utilizados para su generación puedan producirse sólo una vez y, asegurar razonablemente, su confiabilidad; así como ofrecer una seguridad razonable de que la firma no pueda ser falsificada con la tecnología existente para la fecha de la suscripción.

Así pues, esta Ley (cuyo proyecto fue originalmente elaborado en forma conjunta por Venamcham y Cavecom) viene a regular en el país, la eficacia y valor jurídico de la firma electrónica, de los mensajes de datos (e-mail) y toda información inteligible en formato electrónico, independientemente de su soporte material.

De acuerdo con el artículo 38 de la Ley Sobre Mensajes de Datos y Firmas Electrónicas (2001), el certificado electrónico garantiza la autoría e

integridad del mensaje, sin embargo, no confiere la autenticidad o fe pública que conforme a la ley otorguen los funcionarios públicos a los actos, documentos y certificaciones que con tal carácter suscriban.

En el supuesto que los menajes de datos sean presentados de manera impresa, tendrán el mismo valor que se atribuye a las copias o reproducciones fotostáticas, por lo que no podrán ser objeto de rechazo por el simple hecho que se presente bajo la forma de mensaje de datos.

Así mismo, su incorporación en el proceso judicial en el cual se pretenda hacer valer será realizado de acuerdo con las formas procedimentales reguladas por los medios de pruebas libres, contenidos y consagrados en el artículo 395 del Código de Procedimiento Civil (1990), con lo que se incorpora el principio de equivalencia funcional con respecto a la firma manuscrita, lo cual ha sido adoptado por la mayoría de las legislaciones en esta materia y los modelos que organismos multilaterales han desarrollado para la adopción por parte de los países de la comunidad internacional en su legislación interna.

Bajo estos preceptos debe mencionarse la opinión de Yunis, S. (2001, 14), el principio de integridad, el cual descansa en la presunción de la no modificación o alteración del mensaje de datos, que se ha firmado electrónicamente y que dicha firma es única para cada mensaje y de cambiarse alguna letra su alteración de comprobará inmediatamente.

Este principio se fundamenta en que los datos contenidos en el mensaje no han sido alterados, desde el momento en que se firmó el mismo, con lo cual se garantiza el mismo, ya que existe la presunción legal de que la firma electrónica fue suministrada por un Proveedor de servicios de Certificación Electrónica que cumple con los requisitos establecidos y en consecuencia se puede afirmar que los datos no han sido alterados desde el momento en que la firma fue añadida al texto, que la firma que aparece pertenece a la persona que realizó la firma y envió y solicitó que enviaran el mensaje y que la firma electrónica fue añadida al mensaje por la persona dueña de la firma con la intención de firmar los datos.

Para Yunis, S. (2001, 15), si se cumple con estos requisitos, se considera válido el mensaje de datos y por consiguiente y por consiguiente tiene eficacia probatoria, salvo que la parte en desacuerdo demuestre que se han incumplido las normas de seguridad establecidas para garantizar la información y que se ha alterado el mismo, pues la integridad lleva implícito el elemento de inalterabilidad.

A tenor de lo expresado en el artículo 7 de la Ley Sobre Mensajes de datos y firmas Electrónicas Venezolana se considera que el mensaje permanece integro cuando la información sea presentada o conservada en su forma original, si se mantiene inalterable desde que se generó salvo

algún cambio de forma del proceso de comunicación, archivo o presentación.

En el último aparte del artículo 16, de la Ley antes mencionada se señala que a efectos de los requisitos para la validez y eficacia probatoria de la firma electrónica, la misma podrá formar parte integrante del mensaje de datos o estar inequívocamente asociada a éste, envíese o no el mismo en el mismo acto, situación que coloca en entredicho la integridad de los datos.

Cabe destacar que el Máximo Tribunal de la República al instalar el "Seminario Taller del Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas organizado por el Tribunal Supremo de Justicia, la Cámara Venezolana Americana de Comercio e industria y la Universidad católica Andrés Bello reconoció a través de la ponencia del magistrado Dr. Rincón (2001) el valor jurídico de los medios electrónicos al afirmar en nombre del tribunal que:

> "Se reconoce y brinda valor jurídico a la firma electrónica, al mensaje de datos y a toda la información inteligible en formato electrónico, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los proveedores de servicios de certificación y certificados electrónicos, lo cual es esencial para el desarrollo del comercio por vía electrónica en cualquier lugar del mundo".

Los medios electrónicos se ubican en la categoría de pruebas libres consagradas en el artículo 395 del Código de Procedimiento Civil. Henríquez La Roche (1996) indica que la regla general de cualquier medio probatorio es válido y conducente al hacinamiento de la Prueba, salvo que esté expresamente prohibido en la ley.

Para la valoración como medio de prueba, el juez utilizará la sana crítica, a menos que exista una norma legal expresada en la ley para valorar el mérito de la prueba, a tenor de lo señalado en el artículo 507 del Código de Procedimiento Civil y además en conformidad con el artículo 509, los jueces deberán todas cuantas pruebas se hayan producido

Por tanto, la firma electrónica constituirá medios de prueba siempre y cuando cumpla con los requisitos establecidos en el Código Civil venezolano, el Código de Procedimiento Civil, la Ley Sobre Mensajes de Datos y Formas Electrónicas y las demás leyes de la República, considerándose medios de prueba válidos a los efectos legales, determinados en las leyes que regulan la materia.

En la definición de los medios probatorios, existen otras vías para acreditar la autoría del mensaje (la prueba testimonial). Viloria (2001, 8), indica que para demostrar el origen del documento electrónico, la parte promovente podrá por ejemplo, utilizar el testimonio de la persona encargada del envío o recepción del mensaje o registro electrónico.

Opina la autora que, la prueba testifical en estos casos sólo podrá ser admisible si con ella se pretende demostrar, por ejemplo, el origen del mensaje o documento electrónico; éste sería el caso en que el promovente de la prueba electrónica promueve también el testimonio del empleado o secretaria del autor del documento o mensaje, que haya sido el encargado de su envío.

Sin embargo, podría llegar a considerarse que el testimonio no tiene ningún valor probatorio, pues muy posiblemente la secretaria o el empleado del departamento de informática de la empresa desconozcan el contenido del documento que ha enviado y este es un hecho casi imposible de dejar pasar para cualquier litigante en la oportunidad de interrogar al testigo.

Viloria (2001, 8) señala que un testigo que no es el autor del documento no puede testimoniar o declarar sobre el contenido del mismo; en consecuencia, su testimonio podría ser invalidado, pues, no le consta el contenido del documento electrónico

Si se trata, por ejemplo, de un documento electrónico creado durante el curso normal de las actividades comerciales de una compañía, la persona que testifica sobre la confiabilidad del sistema puede ser un experto en computación (testigo-perito), o simplemente una secretaria o cualquier empleado siempre que esté familiarizado con el sistema y la confiabilidad del mismo. No existe ninguna exigencia legal que obligue a

la realización de pruebas técnicas a los sistemas de tecnologías para comprobar su confiabilidad; sin embargo, la parte promovente podrá valerse de experticias tecnológicas para ello.

Por otra parte, si se quiere comprobar un hecho relevante a través de un documento electrónico cuyo autor no es parte en el juicio, la parte promovente deberá aportar el testimonio de su autor a los fines del control de la prueba por su contraparte, a tenor de lo dispuesto en el artículo 431 del Código de Procedimiento Civil. En estos casos, el tercero rendirá su testimonio acerca del contenido del documento y el reconocimiento de su autoría.

Abordando el correo electrónico (e-mail), Viloria (2001, 9) explica que éste permite a los usuarios con una dirección electrónica comunicarse entre sí de la misma manera en que lo hacen a través del servicio postal convencional. Ante esta similitud con las cartas o correos personales, consideramos que para la promoción en juicio de un mensaje de datos contentivo de un correo electrónico, la parte proponente del medio deberá observar las reglas y limitaciones establecidas para la utilización de las cartas misivas como medios de prueba, previstas en el Código Civil.

Ahora bien, de acuerdo con el referido Código:

“Artículo 1.371: Pueden hacerse valer en juicio como prueba o principio de prueba por escrito, las cartas misivas dirigidas por una de las partes a

la otra, siempre que en ellas se trate de la existencia de una obligación o de su extinción, así como de cualquier otro hecho jurídico relacionado con los puntos que se controviertan.

El autor de la carta puede exigir la presentación de esta a la persona a quien fue destinada o esta producirla en juicio para los efectos mencionados".

"Artículo 1.372: No puede una de las partes requerir la presentación de una carta dirigida a un tercero por alguno de los interesados en el juicio, o por personas extrañas, si el tercero y el autor de la carta no prestan su consentimiento para ello. El tercero tampoco puede valerse de la carta como prueba, contra la voluntad del autor de ella.

Las cartas misivas, dirigidas y recibidas entre terceros, no pueden en ningún caso, emplearse como medios de prueba en juicio por personas para los cuales los terceros no eran causantes o mandatarios. Los herederos y causahabientes de las personas que dirigieron o recibieron las cartas misivas antedichas, pueden emplearlas como medios de prueba en los mismos casos en que aquéllas podrían hacer uso de ellas.

Si se aplica por analogía a los correos electrónicos personales, Viloria (2001, 9) indica que las normas relativas a las cartas misivas como pruebas o principio de prueba por escrito, entonces, estos mensajes de datos sólo podrían aprovecharse en juicio entre las partes emisora y receptora del mensaje, o por personas extrañas, siempre que éstas hayan dado su consentimiento.

Por otra parte, si se trata de correos de carácter confidencial, es decir, que no se trata de los asuntos expresados en el artículo 1371 antes citado, no pueden publicarse ni presentarse en juicio sin el consentimiento de su autor y de la persona a quien fueron dirigidas (Artículo 1.371, ejusdem).

La fuerza probatoria de las cartas misivas producidas en juicio, se determina por las reglas establecidas en la ley para los instrumentos privados; “pero carecerán de valor las que no estén firmadas por la persona a quien se atribuyan, salvo que hayan sido escritas de su puño y letra, y remitidas a su destino” (Artículo 1.374, ejusdem)

En cuanto al requisito de la firma, vale destacar que la Ley sobre Mensajes de Datos y Firmas Electrónicas dispone que “Cuando para determinados actos o negocios jurídicos la ley exija la firma autógrafa, ese requisito quedará satisfecho en relación a un Mensaje de Datos al tener asociado una firma electrónica”, con esta previsión se incorpora a nuestro ordenamiento jurídico el principio de equivalencia funcional, respecto a las firmas electrónicas.

Si se aplica la normativa civil en cuanto a la valoración de las cartas misivas, un correo electrónico que esté asociado a algún mecanismo de seguridad que permita identificar el origen y autoría del mismo (como es el caso de una firma electrónica) tendrá la misma fuerza probatoria que un documento privado; pero, si en la elaboración, envío o

recepción del correo electrónico no se utilizó ningún método de seguridad que garantice el origen o autoría del mensaje, consideramos que ello no imposibilita su aprovechamiento en juicio, si se demuestra -incluso en forma indiciaria-, que el mensaje fue enviado o recibido por quien se atribuye su autoría o recepción; por ejemplo, podría demostrarse que la dirección electrónica que aparece en el mensaje de datos pertenece a la contraparte en juicio.

Ahora bien, Viloria (2001, 9) indica que si se trata de un correo electrónico enviado por un sujeto que no es parte procesal, considera que la ausencia de la firma electrónica quedaría subsanada con la aceptación expresa de su autoría, por parte de ese tercero.

La Ley sobre Mensajes de Datos y Firmas Electrónicas (2001), al reconocer que los mensajes electrónicos son medios de prueba libres, cuya eficacia probatoria es la misma que la ley reconoce a los documentos escritos, permite entonces acudir a las reglas para la promoción y evacuación de la prueba documental, entre las cuales se encuentran la prueba de exhibición de documentos y la prueba de informes.

En atención a la aplicación de las reglas que rigen la promoción y evacuación de los medios de prueba libres, se considera perfectamente posible aplicar por analogía la prueba de exhibición de documentos

prevista en nuestro ordenamiento jurídico a los mensajes o documentos electrónicos.

Así, si el original del documento electrónico promovido en juicio o su copia electrónica (disquete) y/o impresa, no se encuentra disponible por cualquier causa (por ejemplo, porque el formato en que se generó o recibió ya no existe en la Red o porque el formato electrónico que lo reproducía con exactitud fue destruido), pero se tiene conocimiento de que el original del mismo –o al menos una copia que reproduce con exactitud la información contenida en el mensaje o documento electrónico original- se encuentra en poder del adversario o de un tercero, la parte podrá solicitar su exhibición, de acuerdo con lo establecido en el artículo 436 y 437 del Código de Procedimiento Civil.

Como señala Montero, J. (2000, 71), la carga de la presentación de los documentos que se impone a las partes, presupone que éstas tienen la disponibilidad de los mismos. Ante los casos de no disposición por una de las partes la Ley reacciona imponiendo a quien tenga esa disposición el deber o la carga de exhibir el documento para que de ese modo pueda ser tenido en cuenta por el órgano jurisdiccional. En efecto, de acuerdo con el ordenamiento procesal civil: Artículo 436.- “La parte que deba servirse de un documento que según su manifestación, se halle en poder de su adversario podrá pedir su exhibición”.

A la solicitud de exhibición deberá acompañar una copia del documento, o en su defecto, la información de los datos que conozca el solicitante acerca del contenido del mismo y un medio de prueba que constituya por lo menos presunción grave de que el instrumento se halla o se ha hallado en poder de su adversario. El tribunal intimará al adversario la exhibición o entrega del documento dentro del plazo que le señalará bajo apercibimiento.

Si el instrumento no fuere exhibido en el plazo indicado, y no apareciere de autos prueba alguna de no hallarse en poder del adversario, se tendrá como exacto el texto del documento, tal como aparece de la copia presentada por el solicitante y en defecto de ésta, se tendrán como ciertos los datos afirmados por el solicitante acerca del contenido del documento.

Si la prueba acerca de la existencia del documento resultare contradictoria, el juez resolverá en la sentencia definitiva, pudiendo sacar de las manifestaciones de las partes y de las de las pruebas suministradas las presunciones que su prudente arbitrio le aconsejen.

Ahora bien, el deber de colaborar con el órgano decisor puede imponerse a la Administración Pública o a un tercero (respecto de la parte contraria, como apunta Sanchis, C. (1999, 83) sólo puede hablarse de carga). En este sentido, respecto a los terceros, el Código de Procedimiento Civil (1990) dispone: “Artículo 437.- El tercero en cuyo

poder se encuentren documentos relativos al juicio, está igualmente obligado a exhibirlos, salvo que invoque justa causa a juicio del juez".

La parte que no disponga de un mensaje de datos o documento electrónico, cuyo contenido es relevante para su defensa, podrá entonces (acudiendo a las formas de promoción de la prueba por escrito) solicitar la exhibición del documento que se encuentra en poder de su adversario o de un tercero, debiendo acompañar la impresión del mensaje de datos o la copia reproducida en disquete, o en su defecto, la información que conozca sobre el contenido del mensaje.

En este último supuesto, el promovente deberá, además, acompañar algún medio de prueba que haga presumir al juez o al árbitro que el mensaje de datos se halla o se ha hallado en poder de su adversario o del tercero.

Por otra parte, señala el Código de Procedimiento Civil en su artículo 433, que:

> “Cuando se trate de hechos que consten en archivos u otros papeles que se hallen en oficinas públicas, Bancos, Asociaciones gremiales, Sociedades civiles o mercantiles e instituciones similares, aunque éstas no sean parte en el juicio, el Tribunal a solicitud de parte, requerirá de ellas informes sobre los hechos litigiosos que aparezcan de dichos instrumentos, o copia de los mismos”.

Para Sentis (1990, 151), la prueba de informes es la forma a través de la cual las entidades públicas o privadas rinden su testimonio o declaración sobre determinados hechos de los cuales tienen conocimiento, sean o no parte en el juicio; por lo que, dicha prueba sólo podría ser solicitada a personas jurídicas.

De esta manera, explica el autor, la parte que pretenda valerse en juicio del contenido de un mensaje de datos y sólo cuente con la impresión del mismo, podrá acreditar la autenticidad de su contenido a través de una prueba de informes, con la finalidad de que el juez o el árbitro ordene a su contraparte, o a un tercero, la declaración escrita del conocimiento que éste posea sobre los hechos o datos contenidos en los archivos electrónicos de su computador.

En cuanto a la prueba de inspección judicial, la misma está regulada en los artículos 472 al 476 del Código de Procedimiento Civil (1990) y su finalidad es que el juez o el árbitro perciban de modo inmediato y a través de sus sentidos cosas, personas o sitios litigiosos; es decir, poner al juez en contacto directo con los hechos. Lo que implica que los hechos a inspeccionar no se encuentren materializados de forma escrita, pues en este caso estamos ante un documento que bien puede ser trasladado al proceso conforme a las reglas establecidas para la prueba por escrito.

En efecto, atendiendo a la finalidad de la prueba de inspección judicial, ésta sólo es eficaz en cuanto permita al Tribunal apreciar, por las exterioridades de la cosa inspeccionada, el hecho que se trata de averiguar; por lo que, necesariamente debe tratarse de un hecho actual y presente que el juez pueda conocer directamente y no, de un hecho pasado.

Ahora bien, conforme a lo expuesto la prueba de inspección judicial no parece ser la más idónea para la introducción procesal de los mensajes de datos. En esto cabe mencionar la opinión de Sanchis, C. (1999, 84) para quien no puede mantenerse que el juez perciba directamente hechos cuando para hacerlo deba llevar a cabo una labor mental de representación y actualización de información que, por otro lado, sólo intelectualmente se consigue, con lo que la percepción inmediata del juez no es más que una ilusión.

Sin embargo, si lo que se pretende probar es la imagen o el sonido de un determinado mensaje de datos que circulan por Internet se considera que la prueba de inspección judicial sí podría resultar adecuada, toda vez que el órgano jurisdiccional estaría empleando el sentido de la vista sólo para observar y no para leer, como sucedería en el caso de un mensaje escrito electrónicamente.

Respecto al control y contradicción de la promoción de los documentos electrónicos, conforme a nuestro ordenamiento procesal, los

medios de prueba libres se promoverán aplicando por analogía las disposiciones relativas a los medios de prueba semejantes contemplados en el Código Civil y en el Código de Procedimiento Civil; por ello la parte que quiera valerse del medio libre similar a uno legal, como es el caso del documento electrónico, deberá respetar las reglas de promoción, correspondiéndole al juez y a la contraparte, el examen de la legalidad de la adaptación.

Como contrapartida del derecho a la prueba judicial, se ubica al derecho del control de la prueba por la contraparte del promovente, quien podrá oponerse, por ilegalidad o impertinencia, a la admisión de la prueba promovida.

En efecto, como ya se expuso, siguiendo la opinión de Cabrera, J. (1999, 99) la oposición atiende a dos conceptos jurídicos: el de la impertinencia y el de la ilegalidad. Por pertinencia se entiende la congruencia que debe existir entre el objeto fáctico de la prueba promovida y los hechos alegados y controvertidos.

Por argumento a contrario, existe impertinencia cuando el medio promovido para probar el hecho litigioso, no se identifica con éste ni siquiera indirectamente. Para el derecho procesal venezolano, no es causa de impertinencia, la relación indirecta entre el hecho objeto de la prueba y los hechos controvertidos, al menos para el momento de la admisión de la prueba y, por ello, el Código de Procedimiento Civil (1990)

siempre ha ordenado que el juez rechace la prueba manifiestamente impertinente, dando entrada así a los medios que incorporarán a la causa posibles hechos indiciarios.

Ahora bien, señala Cabrera, J. (1999, 99) que en la mayoría de los medios de prueba, el promovente, al momento de anunciarlos debe indicar los hechos que trata de probar con ellos, por lo que resulta fácil comparar lo que se pretende probar con los hechos alegados controvertidos y, por tanto, calificar o no la pertinencia o la impertinencia manifiesta.

El mismo autor indica que la ilegalidad consiste en que con la proposición del medio se transgreden sus requisitos legales de existencia o admisibilidad, infracción que se verifica para el momento de su promoción o, excepcionalmente, para el momento de su evacuación.

Ahora bien, la ilegalidad como argumento para la oposición de la prueba promovida opera con mayor intensidad para el caso de las pruebas legales debido a que están reguladas por la ley y, por tanto, de sus normas se deducen sus requisitos; sin embargo, ello no significa que no pueda alegarse la ilegalidad en relación a los mensajes de datos, cuando, por ejemplo, se dejan de aplicar las reglas establecidas para la promoción de medios análogos o similares.

Por otra parte, vale destacar que de acuerdo con la Constitución de la República Bolivariana de Venezuela de 1999, no son válidas las pruebas obtenidas en violación al debido proceso (Artículo 49); por lo que, en aquellos casos en que el medio de prueba haya sido obtenido en violación garantías procesales o constitucionales, la contraparte del promovente podrá oponerse a su admisión bien por ilegalidad o bien por inconstitucionalidad. En estos casos, la ilegalidad o la inconstitucionalidad no es respecto del medio de prueba, sino de las formas utilizadas para la obtención de la fuente.

Cabrera, J. (1999, 100) señala que un ejemplo de lo anterior sería que el hecho que se pretenda probar este contenido en un correo electrónico de contenido personal y privado, interceptado por un sujeto distinto a quien iba dirigido. En este caso, el promovente del medio habría obtenido la prueba en violación a las normas legales y constitucionales que protegen la intimidad, el secreto e inviolabilidad de las comunicaciones; por lo que, la contraparte del promovente podría oponerse a su admisión.

Ahora bien, la ausencia de oposición no significa una convalidación de la impertinencia o ilegalidad, ya que, como bien lo apunta Cabrera, J. (1999, 100) se trata por ser conceptos jurídicos el juez -o arbitro- podrá tomarlos en cuenta de oficio y ordenar o negar que se reciba la prueba en autos.

Respecto a la impugnación y el desconocimiento de la prueba documental electrónica, explica el mismo autor antes señalado, que debe indicarse que el hecho de que la parte que pretenda valerse del documento electrónico demuestre en juicio la autenticidad y autoría del mensaje o registro contenido en un disquete o en un papel impreso, no impide a la contraparte en juicio impugnar la eficacia y validez probatoria del medio.

Así pues, en ocasiones la oposición al medio de prueba propuesto no es suficiente, por lo que el legislador otorga ofrece otra alternativa a los litigantes en materia de defensa procesal: La impugnación del medio, que no es más que un ataque dirigido a enervar la veracidad de un medio de prueba.

Explica Cabrera, J. (1999, 100) que este ataque al medio puede asumir dos formas: una activa (impugnación en sentido estricto: la tacha documental y la de testigos), con alegatos de hechos y con la carga de prueba sobre el impugnante; y otra pasiva (desconocimiento) donde también se alega un hecho, pero la carga de la prueba la tiene la contraparte del impugnante.

En el análisis de la tacha de falsedad de un documento o mensaje electrónico, las normas que resultan aplicables son las relativas a la tacha de instrumentos privados, la cual procede, conforme el artículo 443 del

Código de Procedimiento Civil (1990), por los motivos especificados en el Código Civil.

En cuanto al desconocimiento, Cabrera, J. (1999, 250) asevera que como ataque pasivo, es importante recordar que quien propone un documento electrónico o mensaje de datos debe demostrar su credibilidad. El que un documento emanó, por ejemplo, de determinada persona, es parte de la demostración que el proponente del medio tiene la carga de hacer, a menos que el mismo sea auténtico y que en consecuencia se presuma quien es su autor.

Ahora bien, nuestro legislador debido a la suscripción tradicional o a la escritura y a que éstos son elementos de imputación de la autoría a una de las partes, sus causantes o mandatarios, creo un procedimiento tendente a la obtención de la credibilidad del documento y que consiste en la declaratoria expresa o tácita de la autoría.

Así, de acuerdo con el artículo 444 del Código de Procedimiento Civil (1990):

> “La parte contra quien se produzca en juicio un instrumento privado como emanado de ella o de algún causante suyo, deberá manifestar formalmente si lo reconoce o lo niega, ya en el acto de la contestación de la demanda, si el instrumento se ha producido con el libelo, ya dentro de los cinco días siguientes a aquel e que se haya producido, cuando fuere posteriormente a dicho acto. El silencio de la parte al respecto, dará por reconocido el instrumento”.

De esta manera, la autenticidad del documento privado puede lograrse bien por el reconocimiento expreso o por el silencio de la contraparte. Cuando se niega formalmente la autoría del documento el reconocimiento electrónico, toca a la parte promovente demostrar su autenticidad (Artículo 445, ejusdem).

Como puede advertirse el desconocimiento de instrumentos privados es un procedimiento creado sobre la base algunos signos externos de la autenticidad (firma manuscrita o escritura), de los cuales –al menos tradicionalmente- carecen los documentos electrónicos.

No obstante lo anterior, Cabrera, J. (1999, 266) afirma que en atención al concepto amplio de documento y, siendo aún más precisos, con la asimilación que hace la Ley Sobre Mensajes de Datos y Firmas Electrónicas (2001), entre la firma tradicional o manuscrita y la firma digital (o cualquier otro medio de identificación de la persona autora del documento que en el futuro pueda surgir), es perfectamente posible que la parte contra quien se promueva un documento electrónico como emanada de ella o de algún causante suyo, lo desconozca, debiendo el proponente de la prueba demostrar su autenticidad.

Ahora bien, tratándose de documentos escritos en soporte informático, no es posible acudir al cotejo ni a ningún procedimiento similar a éste, por lo que rechazada la autoría del mensaje será necesario la realización de una prueba de experticia en la que técnicos

(especialistas informáticos) puedan determinar lo más exactamente posible la autenticidad de tal documento.

CONCLUSIONES

En función del análisis monográfico presentado, se señalan las siguientes conclusiones:

a) En el análisis de la firma electrónica, de debe indicar que la misma ha sido ampliamente conceptualizada desde la perspectiva de la doctrina y de la ley venezolana, e inclusive existen subcategorías de la misma que se determinan en función del nivel de certificación existente.

b) Respecto a los requisitos de la firma electrónica, en Venezuela los mismos están plasmados en Ley Sobre Mensajes de Datos y Firmas Electrónicas, los cuales permiten 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. Ello supone garantizar que los datos utilizados para su generación puedan producirse sólo una vez, y asegurar, razonablemente, su confidencialidad; ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento y no alterar la integridad del Mensaje de Datos.

c) Es amplio el uso de la firma electrónica en el procedimiento civil venezolano, siendo esencial la promulgación de la Ley Sobre Mensajes de Datos y Firmas Electrónicas, la cual constituye un importante avance

en materia probatoria, al definirse lo que constituye el equivalente a un documento escrito, la firma y el original en el entorno electrónico y, además, establecerse el régimen aplicable para la admisibilidad, promoción y evacuación en juicio de tales documentos (el de las pruebas libres); sin embargo, al remitirse a las formas procesales ordinarias previstas en el Código de Procedimiento Civil, la prueba de los hechos o actos contenido en un mensaje electrónico sigue siendo una prueba compleja.

d) Son diversos los riesgos implícitos en la firma electrónica, tanto desde el punto de vista técnico, como jurídico, sin embargo cabe destacar la existencia de medios concretos a través de los cuales se puede determinar la validez de la misma y su eficacia jurídica. La autenticidad de la firma electrónica puede demostrarse por medios técnicos y jurídicos.

e) Dado que toda pretensión jurídica invocada en juicio debe ser comprobada mediante las reglas dadas por el derecho probatorio, puesto que de esto depende la efectiva titularidad sobre el derecho discutido. La prueba en si constituye la base fundamental del proceso y es una condición de seguridad jurídica esencial para el pronunciamiento de una sentencia justa y objetiva, lo cual es aplicable a la firma electrónica.

Referencias Bibliográficas

Alsina, Jorge. (2000). Valor probatorio del Documento Electrónico. Revista El Derecho.

Cabrera, Jesús. (1997). Contradicción y control de la prueba legal y libre. Tomo I, Librería Jurídica venezolana. Caracas.

Cadone, Clara. (1998). Apuntes al anteproyecto de Ley sobre firma electrónica" Revista Electrónica de Derecho. Bologna (Italia), abril.

Código Civil Venezolano. (1982): Código Civil Venezolano. Gaceta Oficial de la República de Venezuela Nº 2990 Extraordinario

Código de Procedimiento Civil Venezolano (1990). Gaceta Nº 4.209 Extraordinaria 18 de septiembre de 1990

Curto, Jorge. (2000). El Documento Electrónico. Su Eficacia Probatoria. Colegio de Abogados de Córdoba. Córdoba.

Davara, Miguel. (1996). La Seguridad en las Transacciones Electrónicas: La Firma Electrónica. Ediciones Marcial Pons. Madrid.

Delpiazzo, Carlos. (2000). Validez y eficacia de la firma electrónica", en Tribuna del Abogado. Montevideo. Nº 117.

Diccionario De la Real Academia Española. Vigésima segunda edición. Madrid.

Espinoza, José. (2003). Régimen Jurídico de la Firma Electrónica en el Perú. Universidad de Lima. Primer Congreso Mundial de Derecho Informático. Lima. Perú.

Font, Andrés. (2000): Seguridad y Certificación en el Comercio Electrónico. Editorial Biblioteca Fundación retevision. Madrid.

Hall, Andrés. (1999), Fundamentos y Validez Legal de la Firma Digital y el Comercio Electrónico. Ediciones Civitas. Buenos Aires.

Hance, 0liver (1996) Leyes y Negocios en Internet. Editorial McGraw-Hill. México.

Irabien, José. (2002). Key Management y Certificación Digital. Revista de Derecho Informático. Edita: Alfa-Redi. No. 052 - Noviembre del 2002

Frosini, Vittorio (1993). Cibernética, Derecho y Sociedad, Tecnos, Madrid.

Illescas, Rafael. (1997). Derecho de la Contratación Electrónica. Ediciones Civitas. Madrid.

Ley No. 27269, Perú, artículo 1, primer aparte.

Ley Sobre Mensajes de Datos y Firmas Electrónicas de Venezuela (2001). Gaceta Oficial de la República Bolivariana de Venezuela Nº 37.148 del 28 de Febrero del 2001.

Ley Utah Digital signatura Act. (1995). Publicada en mayo en el Estado de UTAH, en Estados Unidos.

Ley Uniform Computer Information Transactions Act (UCITA), 4 de agosto del 2000

Martín, José (2001). Aspectos técnicos y Jurídicos de la Firma Electrónica. Universidad de Navarra. Proyecto Aequitas. Navarra.

Martínez, Apolonia. (1998). Firma electrónica, certificados y entidades de certificación**.** Revista de la Contratación Electrónica. Núm. 36.

Mateu, Rafael y Ros, Juan (2000). Derecho de Internet: Contratación electrónica y firma digital. Ediciones Aranzadi. Navarra.

Montero, Juan. (2000). La prueba en el proceso civil. Editorial Edit. Tirant lo Blanch, Valencia.

Palazzi, Pablo (1998). Firma digital y comercio electrónico en Internet, en Ponencias del VI Congreso Iberoamericano de Derecho e Informática, Montevideo, Uruguay.

Ovidio, José. (2002). Contratación Electrónica. Revista Alfa-Redi. Caracas.

Ramos, Fernando (2000). La firma digital. Aspectos técnicos y legales. publicado en Internet en Marketing y comercio. com. Número 14/00abr-firmadigital.htm. Año 2000.

Reyes, Alfredo. (2004). La Firma Electrónica. Universidad Panamericana. Panáma.

Ruiz, Fernando. (2005). El Documento Electrónico frente al Derecho Civil y Financiero. Publicado en Internet en la Sección Doctrinal del "Derecho.org.".

Rodríguez, Gladis. (2002). De la firma Autógrafa a la Firma Digital. Prespectiva Venezolana. La Universidad del Zulia. Facultad de Ciencias Jurídicas y Políticas. Instituto de Filosofía del Derecho "Dr. J.M. Delgado O". Presentado en el segundo Congreso Mundial de Derecho Informático. Madrid.

Sanchis, C. (1999). La Prueba por soportes informáticos. Ediciones Tirant lo blanch, Valencia-España.

Sentis, S. (1990). La prueba. Valletta Ediciones. Buenos Aires.

Tuzio, Alejandro y Palazzi, Pablo. (2005). Derecho Informático. Editorial Lexis Nexos. Buenos Aires.

Viloria, Mónica. (2001). Los Mensajes de Datos y la prueba de los negocios, actos y hechos con relevancia jurídica soportados en formatos electrónicos. Revista de Derecho informático. No. 036 - Julio del 2001.