UNIVERSIDAD CATÓLICA ANDRÉS BELLO

VICERRECTORADO ACADÉMICO

DIRECCIÓN GENERAL DE LOS ESTUDIOS DE POSTGRADO

ÁREA DE DERECHO

POSTGRADO DE DERECHO PROCESAL

VALORACIÓN QUE UN JUEZ DEBE DAR A LOS DISTINTOS MEDIOS PROBATORIOS QUE PUEDEN EMPLEARSE PARA PROMOVER O DESCONOCER UN CORREO ELECTRÓNICO EN UN PROCESO JUDICIAL

Presentado por

Bello Toro, Yael de Jesús

Para Optar al Título de

Especialista en Derecho Procesal

Asesor – Tutor

Romero Mendoza, Alfredo

Caracas. Septiembre 2012.

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
DIRECCIÓN GENERAL DE LOS ESTUDIOS DE POSTGRADO
ÁREA DE DERECHO
POSTGRADO EN DERECHO PROCESAL

APROBACIÓN DEL ASESOR

En mi carácter de Asesor del Trabajo Especial de Grado, presentado por la ciudadana Abogada Yael de Jesús Bello Toro, para optar al Grado de Especialista en Derecho Procesal, cuyo título es: "**Valoración que un Juez debe dar a los distintos medios probatorios que pueden emplearse para promover o desconocer un correo electrónico en un proceso judicial**"; considero que dicho Trabajo reúne los requisitos y méritos suficientes para ser sometido a la evaluación por parte del jurado examinador que se designe.

En la Ciudad de Caracas, a los 3 días del mes de Septiembre de 2012.

_____

Alfredo Romero Mendoza

CI. 6.324.982

DEDICATORIA

A Dios y a mi familia, por estar presentes a lo largo de mi vida.

AGRADECIMIENTOS

A Alfredo Romero Mendoza por brindarme su asesoría y apoyo en la redacción del presente Trabajo de Grado; a Alberto Rengifo porque sin él hubiera sido imposible realizar esta investigación; y a Alexander Coiro por ayudarme con las no menos importantes revisiones de estilo.

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
DIRECCIÓN GENERAL DE LOS ESTUDIOS DE POSTGRADO
ÁREA DE DERECHO
POSTGRADO DE DERECHO PROCESAL

VALORACIÓN QUE UN JUEZ DEBE DAR A LOS DISTINTOS MEDIOS PROBATORIOS QUE PUEDEN EMPLEARSE PARA PROMOVER O DESCONOCER UN CORREO ELECTRÓNICO EN UN PROCESO JUDICIAL

Autor: Abg. Yael de Jesús Bello Toro.

Tutor - Asesor: Abg. Alfredo Romero Mendoza.

Fecha: Septiembre - 2012.

RESUMEN

La investigación persigue analizar la valoración que un Juez debe dar a los medios para promover o desconocer un correo electrónico. La situación problemática que se analiza se presenta por cuanto en esta era de la información en donde muchas comunicaciones se realizan a través de correos electrónicos o mensajes de datos, se hace necesario considerar aquellas situaciones en las cuales se requiera otorgarles eficacia a los elementos que demuestren la existencia o no de una relación jurídica entre las partes. En Venezuela, el Decreto Ley sobre Mensajes de Datos y Firma Electrónica es la principal norma que regula la eficacia probatoria de los mensajes de datos o correos electrónicos. El principal aporte de ésta investigación radica en presentar soluciones al vacío que deja dicho Decreto Ley en cuanto a los medios probatorios que deben utilizarse para promover un correo electrónico que no cumpla con los requisitos exigidos en dicha norma, así como la valoración que el Juez en un proceso deberá otorgar a esos medios probatorios. El trabajo consiste en una investigación monográfica a nivel descriptivo, en el cual se utilizarán las técnicas de análisis de contenido y comparativo.

Palabras clave: Correo electrónico, Medios Probatorios, Valoración.

ÍNDICE

SIGLAS

World Wide Web	WWW
Advanced Research Projects Agency Network	ARPANET
National Science Foundation	NSF
Hyper Text Markup Language	HTML
Constitución de la República Bolivariana de Venezuela	CRBV
Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas	DLMDFE
Código de Procedimiento Civil	CPC
Comisión Nacional de Telecomunicaciones	CONATEL
Superintendencia de Servicios de Certificación Electrónica	SUSCERTE
Ministerio del Poder Popular para la Ciencia, Tecnología e Industrias Intermedias	MPPCTII
Proveedores de Servicios de Certificación	PSC
United Nations Comission on International Trade Law	UNCITRAL
Fundación Instituto de Ingeniería para la Investigación y Desarrollo Tecnológico	FIIDT

Electronic Data Interchange EDI

INTRODUCCIÓN

El objeto de este trabajo de investigación es analizar la valoración que un Juez debe dar a los distintos medios probatorios que pueden emplearse para promover o desconocer un correo electrónico en un proceso judicial. Para lo cual, se contrastó la regulación del correo electrónico como medio probatorio en el marco legal venezolano, y la valoración que de acuerdo a ese marco legal le debe otorgar el Juez en un juicio, con las diversas situaciones en las que el correo electrónico puede ser utilizado en una relación jurídica, y que por lo tanto puede demostrar hechos relacionados con esa relación jurídica en la cual fue utilizado como medio de comunicación. Determinando de esa forma, cual es la forma de demostrar esos hechos con un correo electrónico, por cuanto dicho mensaje de datos es un medio de comunicación, cuyo aspecto tecnológico es desconocido tanto para los abogados litigantes, como para los jueces que deben valorarlo en un proceso judicial.

A los efectos de lograr lo indicado anteriormente, en el presente trabajo se analizaron las distintas situaciones que pueden generarse en cuanto a la autoría y contenido del correo electrónico, y se ubicaron en el derecho positivo venezolano los medios probatorios que pueden ser utilizados para promover el correo electrónico en un proceso judicial, qué se demuestra con ellos, y cuál es la valoración que les debe otorgar un Juez en un proceso judicial.

La razón que motivó la realización de ese contraste entre el marco legal a aplicar y la realidad existente, es que en la actualidad el correo electrónico puede ser utilizado como prueba de una infinidad de relaciones jurídicas, debido al uso cada vez más frecuente que se hace del mismo, pero al momento de trasladar esa prueba a un proceso judicial se enfrenta al obstáculo de que en la mayoría de los casos los correos electrónicos no cumplen con los requisitos establecidos en el Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas para la firma electrónica o certificado

electrónico, y por lo tanto serán valorados por el Juez de acuerdo a su sana crítica, y no de acuerdo a un valor tarifado de forma previa por la ley.

De la misma forma, la investigación realizada explicó la validez de los medios probatorios previstos en instrumentos legales distintos al Decreto Ley sobre Mensajes de Datos y Firma Electrónica, para promover los correos electrónicos en un proceso judicial, o para demostrar hechos relacionados con el contenido y autoría del correo electrónico, así como la valoración que debe dar el Juez a cada uno de estos medios probatorios.

En ese sentido, se analizó como se ha regulado el correo electrónico como medio de prueba tanto por el derecho venezolano, como por el derecho comparado; y se presentó la justificación legal para el empleo de determinados medios probatorios con el objeto de demostrar los distintos hechos que puedan evidenciarse del contenido y autoría de un correo electrónico, y la valoración que le otorgaría un Juez a cada uno de esos medios probatorios en un proceso judicial.

Con el objeto de realizar el análisis de la valoración probatoria de los correos electrónicos, se plantearon los siguientes objetivos específicos: definir conceptos básicos para comprender el correo electrónico como medio de transmisión de información; analizar sistemas para garantizar la autoría y contenido del correo electrónico; determinar si el correo electrónico es una prueba fidedigna; establecer los medios probatorios para hacer valer un correo electrónico; establecer como ejercer el control y contradicción del correo electrónico. A tal efecto, se utilizó como base legal en primer orden la Constitución de la República Bolivariana de Venezuela, y en segundo termino, el Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas, así como otros textos legales relacionados.

El trabajo consiste en una investigación monográfica a nivel descriptivo, en el cual se utilizaron las técnicas de análisis de contenido y comparativo. El instrumento utilizado es una matriz de análisis de contenido sobre la información recogida durante el desarrollo del trabajo, a través de la categorización de la información atendiendo a las características del contenido.

El principal aporte de la investigación radica en aclarar el silencio que existe legalmente sobre la valoración probatoria de un correo electrónico que no cumpla con los requisitos del Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas.

CAPÍTULO I. ASPECTOS GENERALES SOBRE LA PRUEBA ELECTRÓNICA

Actualmente, muchas de las relaciones jurídicas se realizan mediante el correo electrónico, más conocido por sus siglas anglosajonas *e-mail* (*electronic mail*), el cual es uno de los sistemas que ofrece Internet para la transmisión de información, facilitando el intercambio de mensajes de texto, imagen y sonido, entre los distintos usuarios de dicha red.

El correo electrónico forma parte de las llamadas tecnologías de información, las cuales se distinguen por utilizar medios electrónicos y redes nacionales e internacionales, que constituyen una herramienta ideal para realizar intercambios de información sin necesidad de utilizar documentos escritos, lo que permite ahorro de tiempo y dinero.

El uso del correo electrónico en las relaciones jurídicas entre personas se ha desarrollado ampliamente, por ser éste parte de una evolución tecnológica a nivel mundial, la cual ha revolucionado todas las áreas del conocimiento y de las actividades humanas.

Tan importante ha sido el desarrollo de las tecnologías de información en las actividades del hombre, que en el derecho se han creado nuevos campos de investigación en el ámbito jurídico, tales como la Jurimetría definida como la "…aplicación de los computadores en el campo del Derecho, específicamente para el pronunciamiento de sentencias por parte de los jueces" (Rico, 2005, p. 7); la Iuscibernética cuyo objeto de estudio es "… las formas en que se relacionan la Cibernética y el Derecho" (Rico, 2005, p. 8); la Informática Jurídica definida como "… técnica que facilita la aplicación del Derecho, que nada tiene que ver con problemas de tipo legal" (Rico, 2005, p. 8); el Derecho Informático que "… trata la

relación existente entre el Derecho y la Informática desde una óptica jurídica ocupándose de estudiar los problemas legales que se derivan de esta interrelación" (Rico, 2005, p. 9); y el Derecho de las Tecnologías de la Información y las Comunicaciones que se ocupa del "… estudio de los fenómenos tecnológicos y su influencia en el campo jurídico" (Rico, 2005, p. 10).

DEFINICIÓN DEL CORREO ELECTRÓNICO (MENSAJE DE DATOS)

El presente trabajo de investigación enfoca una realidad que evoluciona tecnológicamente de forma constante, como lo es el intercambio de información entre las personas y las consecuencias que ello conlleva, desde el punto de vista del derecho procesal. Por lo que, aunado a que se analiza en qué consiste el correo electrónico, la garantía de la certeza de su autoría y contenido, también se estudian conceptos tecnológicos necesarios para comprender al correo electrónico como una herramienta que nos permite demostrar diversas relaciones jurídicas.

A partir de los años sesenta, a nivel mundial, se originaron muchos cambios en la ciencia de la información, los cuales por su novedad generaron que el derecho existente quedara obsoleto para regular las diversas situaciones que se generaban con la nueva tecnología.

El surgimiento de la llamada ciencia de la información o tecnología de la información, creó nuevas formas de guardar, procesar, y utilizar grandes cantidades de información, lo cual al surgir las telecomunicaciones permitió el envío de dicha información sin las barreras de distancia y tiempo que son frecuentes en otro tipo de comunicaciones. Es por ello, que hoy en día el correo electrónico es el medio electrónico que transfiere información de la forma más rápida posible, y capaz de recorrer las mayores distancias.

Tal como lo señala la autora Di Totto (2005, p. 2), la *World Wide Web* (WWW) o Internet, que es el medio electrónico mediante el cual los correos electrónicos llegan a su destino, tuvo su origen en los Estados Unidos de América, cuando el sector militar inició la creación de redes que conectaran distintas computadoras entre si, lo cual ocurrió durante el mandato del presidente Eisenhower, y fueron reforzados por el presidente Kennedy. El proyecto originario se denominó *Advanced Research Projects Agency Network* (ARPANET), la cual tenía como objeto que la información que debía transferirse entre los centros de mando llegase a su destinatario, aún cuando algunos puntos de conexión estuviesen inhabilitados como consecuencia de un ataque bélico. Posteriormente, en los años setenta, la red ARPANET fue transferida a la *Nacional Science Foundation* (NSF) para lograr que las universidades y centros de investigación de ese país se conectaran entre sí, y pudieran divulgar los conocimientos adquiridos.

En los ochenta, la conexión entre las computadoras se vuelve de acceso público, con la creación del lenguaje *Hyper Text Markup Language* (lenguaje de marcación de hipertexto HTML), teniendo en ese entonces también un acceso a otras redes a nivel mundial. Finalmente en 1990, Internet se convirtió en el medio de comunicación más popular a la hora de enviar información.

Ese contexto tecnológico, nos lleva al concepto del correo electrónico o *e-mail*. Al respecto, el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (DLMDFE, 2001) define los mensajes de datos como “Toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio”. Lo cual, de acuerdo a la autora Di Totto (2005) es “…un elemento de convicción que está contenido dentro de sistemas o dispositivos que funcionan mediante la tecnología de información y al cual sólo puede accederse a través del uso de esta tecnología”, por lo que señala que es una prueba electrónica (p. 10).

El correo electrónico es un medio de comunicación virtual vía Internet, el cual sirve para transmitir y recibir información mediante un dispositivo electrónico (computadora, celular, tablas, entre otros dispositivos).

En el portal web www.wikipedia.com se define al correo electrónico como:

> Correo electrónico (correo-e, conocido también como e-mail), es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos. Principalmente se usa este nombre para denominar al sistema que provee este servicio en Internet, mediante el protocolo SMTP, aunque por extensión también puede verse aplicado a sistemas análogos que usen otras tecnologías. Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos digitales dependiendo del sistema que se use. Su eficiencia, conveniencia y bajo coste están logrando que el correo electrónico desplace al correo ordinario para muchos usos habituales.

Por su parte, los autores Rueda y Perreti (2008) sostienen que “el correo electrónico es el más moderno mecanismo de comunicación, a través del cual las personas pueden transmitir y obtener información, mediante el uso de una computadora personal conectada a la red de la internet” (p. 328).

A su vez, el correo electrónico según Rico (2005), consiste en un medio innovador que permite el intercambio de información de una forma rápida usando los

medios informáticos para la transmisión de datos tales como es el computador. En concreto, sostiene lo siguiente:

> El correo electrónico, es comúnmente conocido por sus siglas anglosajonas e-mail (electronic mail), es uno de los sistemas que ofrece Internet para la transmisión de información, facilitando el intercambio de mensajes entre distintos usuarios de la Red.
>
> El correo electrónico funciona por medio de procedimientos de almacenamiento y reenvío de mensajes. Los mensajes recibidos se almacenan en un "buzón electrónico" que reside en la memoria del computador servidor donde está situada la cuenta de correo con las direcciones individualizadas de los usuarios, transmitiéndose automáticamente a éstos a través de un protocolo específico de recuperación de mensajes, denominado POP (Post Office Protocol). Mediante el correo electrónico se pueden enviar datos binarios que permiten anexar archivos de texto, imagen y sonido, para ello es necesario un software adecuado y tener cuenta activa en el servidor de correo en la Red que es quien recibe el correo en el buzón correspondiente hasta que es recuperado por su destinatario.
>
> A diferencia de la interactividad que ofrece el sistema Web al permitir que las transacciones se efectúen en tiempo real, las operaciones de correo electrónico se consideran offline en el sentido que el destinatario no necesita estar frente a la pantalla del computador cuando se envía el mensaje, ya que lo recibirá en el momento de revisar su buzón personal donde ha sido almacenado (p. 35).

La legislación venezolana define a los correos electrónicos como mensajes de datos, y en ese sentido la sentencia dictada por la Sala de Casación Social del

Tribunal Supremo de Justicia, con ponencia del magistrado Alfonso Valbuena Cordero, de fecha 5 de marzo del 2007, (caso Luis Alberto Nava Jiménez v. Vencemos C.A.), expone lo siguiente:

> La revolución de la Informática ha sido a nivel mundial, y en Venezuela, la era de la informática se ha hecho presente. El ordenamiento jurídico está normando estas situaciones a través de la creación de leyes especiales, a los fines de garantizar un marco jurídico mínimo indispensable que permita a los diversos agentes involucrados, desarrollarse y contribuir con el avance de las nuevas tecnologías. En efecto, en el año 2001 la Asamblea Nacional dictó el Decreto-Ley Sobre Mensajes de Datos y Firmas Electrónicas; y recientemente en Diciembre de 2004 se creó el Reglamento Parcial de dicho Decreto-Ley. Para la Ley venezolana, los documentos electrónicos se denominan mensajes de datos así, que el correo electrónico es una información inteligible (mensaje de datos electrónico) elaborada en lenguaje binario compuesta por combinación de dígitos, que al ser traducidos por un computador, pueden ser perfectamente leídos por el ser humano.
>
> (…Omissis…)
>
> El servicio de correo electrónico se proporciona a través del protocolo SMTP (Simple Mail Transfer Protocol), y permite enviar mensajes a otros usuarios de la red. A través de estos mensajes no sólo se puede intercambiar texto, sino también archivos binarios de cualquier tipo. Generalmente los mensajes de correo electrónico no se envían directamente a los ordenadores personales de cada usuario, puesto que en estos casos puede ocurrir que esté apagado o que no esté ejecutando la aplicación de correo electrónico. Para evitar este problema se utiliza un ordenador más grande como

> almacén de los mensajes recibidos, el cual actúa como servidor de correo electrónico permanentemente. Los mensajes permanecerán en este sistema hasta que el usuario los transfiera a su propio ordenador para leerlos de forma local.
>
> El correo electrónico está consagrado en la legislación venezolana, pero bajo el nombre de MENSAJE DE DATOS, definiéndolo como "toda información inteligible en formato electrónico o similar, que puede ser almacenada o intercambiada por cualquier medio". (Artículo 2 LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRÓNICAS).
>
> Incluso la Ley Especial contra los Delitos Informáticos expresa una definición sobre mensaje de datos. En su artículo 2 ordinal primero lo define como "cualquier pensamiento, idea, imagen, audio, data, información, expresados en un lenguaje conocido que puede ser explícito o secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones".

En conclusión, el correo electrónico que es denominado por el ordenamiento jurídico venezolano como mensaje de datos, es uno de los medios de comunicación más importantes en la actualidad, debido a que gracias a ese medio las personas pueden enviar y recibir información de una forma rápida, eficaz y sencilla a través de dispositivos electrónicos, dejando a un lado el uso de las cartas, telegramas, y otros medios menos eficaces.

CONCEPTOS TECNOLÓGICOS VINCULADOS CON EL CORREO ELECTRÓNICO

Usuario.

Es el nombre (o alias) que se le asigna a cada persona para ser identificado por el servidor o proveedor del servicio de mensajería de datos o correo electrónico, de esta manera el proveedor de Internet o de correo electrónico lo identifica, es único en cada servidor, y cada usuario tiene asignado un *password* o contraseña para poder acceder a su cuenta.

Arroba.

Es la simbología que separa el nombre de usuario del nodo o dominio. Este símbolo identifica el correo por Internet.

El arroba (@) es un símbolo utilizado en las direcciones de correo electrónico para separar el nombre del usuario del nombre del dominio, ambos necesarios para transmitir los *e-mails*.

Dominio.

El nombre del proveedor o dominio identifica la ruta o máquinas designadas para el envío y recepción de mensajes de forma correcta a través de Internet.

Organización.

Identifica a qué tipo de organización (educación, comercial, militar, etc.).

Extensión de país.

Identifica el país en que se encuentra alojado el dominio. Si el servidor no está en los Estados Unidos de América se le asignan dos letras para identificar a los países, en Venezuela las letras asignadas son "ve" ([1]).

USO DE LAS TECNOLOGÍAS DE INFORMACIÓN EN LA CONSTITUCIÓN DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA

Con la promulgación de la Constitución de la República Bolivariana de Venezuela (CRBV, 2009), se fomenta la aplicación del uso de las Tecnologías de Información, con el fin de contribuir al desarrollo humano. Para ello, dicho instrumento exige al Estado venezolano garantizar a los ciudadanos el acceso a los avances tecnológicos. Sobre este particular, la autora Rico (2005), expuso lo siguiente:

> En el propio texto constitucional se puede apreciar la influencia de la tecnología en el ámbito jurídico, al consagrarse dentro de los derechos fundamentales del individuo, el derecho al acceso a las tecnologías, a tal efecto, el artículo 108 de la CRBV, establece la obligación del Estado de garantizar los servicios de radio, televisión y redes de bibliotecas y de informática, con el fin de permitir el acceso universal a la información, imponiendo a los centros educativos el deber de incorporar el conocimiento y aplicación de las nuevas tecnologías en los procesos de enseñanza (p. 87).

[1] Para más información sobre éstas definiciones recomendamos la visita a la página web de Tecnología de Información y la Comunicación – Correo Electrónico, http://tutoriales.igluppiweb.com.ar/ecorreo.pdf

Aunado a lo anterior, el artículo 110 de la CRBV establece lo siguiente:

> El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Para el fomento y desarrollo de esas actividades, el Estado destinará recursos suficientes y creará el sistema nacional de ciencia y tecnología de acuerdo con la ley. El sector privado deberá aportar recursos para los mismos. El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía.

Ahora bien, con base a esto el Estado es el principal garante de hacer valer los principios éticos y legales que están inmersos en el uso de las tecnologías de la información. Además, el DLMDFE en su artículo 5 hace referencia a que "los Mensajes de Datos estarán sometidos a las disposiciones constitucionales y legales que garantizan los derechos a la privacidad de las comunicaciones y de acceso a la información personal".

A su vez, la Ley Orgánica de Telecomunicaciones expone en su artículo 1° como su objeto lo siguiente:

> Esta Ley tiene por objeto establecer el marco legal de regulación general de las telecomunicaciones, a fin de garantizar el derecho humano de las personas a la comunicación y a la

> realización de las actividades económicas de telecomunicaciones necesarias para lograrlo, sin más limitaciones que las derivadas de la Constitución y las leyes.
>
> Se excluye del objeto de esta Ley la regulación del contenido de las transmisiones y comunicaciones cursadas a través de los distintos medios de telecomunicaciones, la cual se regirá por las disposiciones constitucionales, legales y reglamentarias correspondientes.

No obstante, la CRBV no sólo hace referencia al fomento del acceso libre de las tecnologías de información para el desarrollo de los ciudadanos, también en su artículo 60 establece una limitante al uso de la informática, protegiendo el honor y la intimidad de las personas así como el ejercicio de sus derechos, con el fin de evitar posibles abusos que se puedan generar hacia la persona.

Por otra parte, a raíz del avance de las Tecnologías de Información y Comunicación en Venezuela, así como a nivel global, se han creado nuevos mecanismos para el uso de estas tecnologías, tales como el uso de dispositivos electrónicos, los cuales permiten al usuario acceder a la información de una manera mucho más rápida. Las comunicaciones a nivel mundial han mejorado notablemente, debido a que el uso de estas tecnologías tales como el Internet, permiten que las personas se comuniquen recíprocamente de formas más eficientes y rápidas.

LEGISLACIÓN APLICABLE

Al transformarse el correo electrónico en una herramienta para celebrar diversas relaciones jurídicas, el mismo se ha convertido en un importante elemento de prueba tanto de la celebración de esas relaciones jurídicas, como de las condiciones y términos de las mismas.

Sin embargo, nuestra legislación principal en materia probatoria, que es el Código de Procedimiento Civil (CPC, 1990), sobre el cual se basan las normas procesales especiales en materias distintas a la civil, fue concebido en un momento histórico en donde sólo existían dos formas de celebrar relaciones jurídicas: oral y escrita, pero no la forma electrónica, que incluso ha sido definida por algunos autores como actos jurídicos electrónicos, tal como señala Rico (2005), cuando se refiere a que:

> …los actos jurídicos electrónicos no serían más que una manifestación de voluntad instrumentada a través de medios electrónicos, contenidos en un soporte distinto del papel –en algunos casos intangible- donde el signatario expresa su conformidad de manera diferente a la forma tradicional, mediante la sustitución de su firma autógrafa por una firma electrónica u otros medios alternativos de autenticación, hablándose en este sentido de documentos y contratos electrónicos (p. 93).

Aunado a que, la Constitución Nacional que reconoce el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información, en el año 2000, la Comisión Nacional de Telecomunicaciones (CONATEL) ([2]) estructura el Plan Nacional de Telecomunicaciones. Dicho Plan tiene como objeto incorporar a Venezuela en la actual tecnología de la información, fomentando para ello el uso de Internet a todos

[2] La Comisión Nacional de Telecomunicaciones fue creada el 5 de septiembre de 1991, mediante el Decreto N° 1.826 (Gaceta Oficial N° 34.801 del 18 de septiembre de 1991), y se encuentra adscrita al Despacho del Ministerio de Transporte y Comunicaciones, actual Ministerio del Poder Popular para la Infraestructura con rango de Dirección General Sectorial y función de Servicio Autónomo con autonomía de gestión administrativa, financiera y presupuestaria.

los niveles, así como impartiendo formación tanto para el conocimiento como el uso de las tecnologías de la información y de las comunicaciones.

El 25 de mayo de 2000, se publicó en Gaceta Oficial el Decreto N° 825 sobre Internet como Prioridad. Dicho Decreto declara el uso de Internet como política prioritaria del Estado para el desarrollo cultural, económico, social y político del país. El objeto principal de este Decreto es fomentar el uso de las tecnologías de información en la Administración Pública Nacional.

El 10 de febrero de 2001, fue promulgado por el Ejecutivo Nacional el Decreto N° 1.024, que fue publicado el 28 de febrero de 2001, en la Gaceta Oficial Nº 37.148, que contiene el Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas (DLMDFE), el cual de acuerdo a lo señalado en su exposición de motivos surge por cuanto:

> …se hace necesaria e inminente la regulación de las modalidades básicas de intercambio de información por medios electrónicos, a partir de las cuales han de desarrollarse 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 avance de las nuevas tecnologías en Venezuela.

Este Decreto Ley, en su artículo 4º, le otorga al correo electrónico el mismo valor que el de la prueba documental, siempre que cumpla con los elementos de certeza del contenido y su autoría, para lo cual establece el sistema de las firmas electrónicas y de los certificados electrónicos. Señalando, únicamente en cuanto a los correos electrónicos que no cumplan con los requisitos previstos en ese Decreto Ley

para la firma digital o el certificado digital, que serán valorados de acuerdo a la sana crítica, tal como lo establece en su artículo 17 cuando expresa que:

> La Firma Electrónica que no cumpla con los requisitos señalados en el artículo anterior no tendrá los efectos jurídicos que se le atribuyen en el presente Capítulo, sin embargo, podrá constituir un elemento de convicción valorable conforme a las reglas de la sana crítica.

Debido a que en el trabajo de investigación se tocaron instituciones referidas a los mensajes de datos, Internet, delitos informáticos, y relaciones jurídicas que pueden ser demostradas mediante un correo electrónico, son los fundamentos legales de la misma, primeramente el DLMDFE, el cual como nos indica su exposición de motivos pretende ser un:

> …instrumento legal que regule estos mecanismos de intercambio de información, los haga jurídicamente trascendentes a la administración de justicia, y les permita apreciar y valorar estas formas de intercambio y soporte de información, con el objeto de garantizar el cumplimiento de las obligaciones asumidas mediante dichos mecanismos y constituirse en un aporte necesario e indispensable que permita construir la base jurídica para el desarrollo de estas tecnologías.

Este Decreto Ley regula varios aspectos del correo electrónico como mensajes de datos, entre los cuales tenemos la integridad del mensaje de datos, lo cual tal como lo señala en su artículo 7, hace referencia a que cuando la Ley exige que la información sea presentada o conservada en su forma original, ello se considerará

cumplido "…si se mantiene inalterable desde que se generó, salvo algún cambio de forma propio del proceso de comunicación, archivo o presentación."

Dicho Decreto Ley también exige para que un mensaje de datos conste por escrito, que cumpla con los requisitos señalados en su artículo 8, los cuales son los siguientes:

> 1. Que la información que contengan pueda ser consultada posteriormente.
> 2. Que conserven el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida.
> 3. Que se conserve todo dato que permita determinar el origen y el destino del mensaje de datos, la fecha y la hora en que fue enviado o recibido.

A los efectos de determinar la oportunidad de la emisión del correo electrónico, el Decreto Ley al que se hace referencia, en su artículo 10, le da prioridad al acuerdo entre las partes, y en caso de no existir acuerdo señala que "…se tendrá por emitido cuando el sistema de información del Emisor lo remita al Destinatario".

A su vez, para determinar la recepción del correo electrónico, establece en su artículo 11, que salvo acuerdo en contrario entre las partes, se deben seguir las siguientes reglas:

> 1. Si el destinatario ha designado un sistema de información para la recepción de mensajes de datos, la recepción tendrá lugar cuando el mensaje de datos ingrese al sistema de información designado.

> 2. Si el destinatario no ha designado un sistema de información, la recepción tendrá lugar, salvo prueba en contrario, al ingresar el mensaje de datos en un sistema de información utilizado regularmente por el destinatario.

En cuanto a la determinación del lugar de emisión y recepción del correo electrónico, el Decreto Ley *in commento* en su artículo 12, señala que, salvo prueba en contrario, "se tendrá por emitido en el lugar donde el Emisor tenga su domicilio y por recibido en el lugar donde el Destinatario tenga el suyo".

Finalmente, el Decreto Ley en su artículo 13 establece un sistema de acuse de recibo, el cual consiste en:

> El emisor de un mensaje de datos podrá condicionar los efectos de dicho mensaje a la recepción de un acuse de recibo emitido por el destinatario. Las partes podrán determinar un plazo para la recepción del acuse de recibo, si no se recibe dicho acuse de recibo dentro del plazo convenido, se tendrá el mensaje de datos como no emitido. En el caso de que las partes no establezcan un plazo para la recepción del acuse de recibo, el mensaje de datos se tendrá por no emitido si el destinatario no envía su acuse de recibo en un plazo de veinticuatro (24) horas a partir de su emisión.

Igualmente, dicho Decreto Ley señala que cuando el emisor reciba el acuse de recibo del destinatario, el mensaje de datos surtirá todos sus efectos. De acuerdo a su artículo 14, el acuse de recibo consistirá en toda comunicación del destinatario, automatizada o no, que señale la recepción del mensaje de datos; o todo acto del destinatario que resulte suficiente a los efectos de demostrar al emisor que ha recibido su mensaje de datos.

En cuanto a la certeza de la autoría de la información transmitida por correo electrónico o *e-mail*, el DLMDFE establece en su artículo 9º, que a falta de acuerdo entre las partes, se entenderá que un mensaje de datos proviene del emisor cuando dicho mensaje haya sido enviado por el propio emisor, una persona autorizada para actuar en nombre del emisor, o por un sistema de información programado por el emisor o con autorización del mismo.

También señala en su artículo 38 que:

> El certificado electrónico garantiza la autoría de la firma electrónica que certifica así como la integridad del mensaje de datos, pero 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.

La vigencia de dicho certificado electrónico será determinada de acuerdo a lo establecido en el artículo 39 de dicha ley, el cual indica que la vigencia del mismo la determinarán el proveedor de servicios de certificación y el signatario.

En cuanto al ente encargado de aplicar el contenido del DLMDFE, éste Decreto creó a la Superintendencia de Servicios de Certificación Electrónica (de ahora en adelante SUSCERTE) ([3]), la cual se encuentra adscrita al Ministerio del Poder Popular para la Ciencia, Tecnología e Industrias Intermedias (MPPCTII).

[3] La SUSCERTE es un servicio desconcentrado sin personalidad jurídica, creado mediante el Decreto Ley sobre Mensajes de Datos y Firmas Electrónicas, publicado en la Gaceta Oficial de la República Bolivariana de Venezuela N° 37.148 del 28 de febrero de 2001.

La SUSCERTE “Quiénes somos” (http://www.suscerte.gob.ve/index.php/la-institucion) tiene entre sus objetivos coordinar e implementar el modelo jerárquico de la Infraestructura Nacional de Certificación Electrónica, también acredita, supervisa y controla a los Proveedores de Servicios de Certificación (de ahora en adelante PSC), y es el ente responsable de la Autoridad de Certificación Raíz del Estado Venezolano. Así mismo, tiene como alcance proveer estándares y herramientas para implementar una tecnología de información óptima en las empresas del sector público, a fin de obtener un mejor funcionamiento y proporcionar niveles de seguridad confiables.

El 12 de diciembre de 2004, el Ejecutivo Nacional dictó el Reglamento Parcial del Decreto Ley de Mensajes de Datos y Firmas Electrónicas N° 3.335, publicado en la Gaceta Oficial N° 38.086 de fecha 14 de diciembre de 2004, con el objeto de establecer la normativa que regule la acreditación de los PSC, la creación del Registro de Auditores y los estándares, planes y procedimientos de seguridad exigidos para la prestación del servicio.

En julio de 2008, la SUSCERTE acreditó a los dos (2) primeros PSC en el país: la Fundación Instituto de Ingeniería para la Investigación y Desarrollo Tecnológico ([4]), y la empresa privada Procert, C.A.

En cuanto a las distintas relaciones y situaciones jurídicas que pueden demostrarse con el correo electrónico, otro fundamento legal del presente trabajo de grado es la Ley Orgánica Procesal del Trabajo, la cual permite que el Juez utilice los

[4] La Fundación Instituto de Ingeniería para Investigación y Desarrollo Tecnológico (FIIIDT) es una fundación del Estado Venezolano adscrita al MPPCTII. El Instituto de Ingeniería fue creado en 1980 mediante el Decreto N° 733 de la Presidencia de la República, con la participación de las principales industrias públicas nacionales y la Academia: CONICIT (Consejo Nacional de Investigaciones Científicas y Tecnológicas ¬ actualmente FONACIT), PDVSA (Petróleos de Venezuela, S.A), CADAFE (C.A. De Administración y Fomento Eléctrico), CANTV (C.A. Nacional Teléfonos de Venezuela), CVG-VENALUM (Industria Venezolana de Aluminio), IVIC (Instituto Venezolano de Investigaciones Científicas), y USB (Universidad Simón Bolívar), como sus entes fundadores.

medios electrónicos al momento de dejar constancia de los hechos, tal como se observa expresamente en el Capítulo XI de las Inspecciones Judiciales, cuando en su artículo 114 señala que “el Juez ordenará la reproducción del hecho por cualquiera de los medios, instrumentos o procedimientos fotográficos, electrónicos, cinematográficos o mecánicos, si ello fuere posible”. Igualmente, incorpora el uso del correo electrónico para practicar las notificaciones correspondientes en el proceso judicial, tal como lo señala en su artículo 126.

Igualmente, el Código Orgánico Procesal Penal establece el correo electrónico como un mecanismo válido para practicar la citación de la víctima, expertos, intérpretes y testigos, en caso de urgencia, tal como lo señala en su artículo 169.

Asimismo, el Código Orgánico Tributario de 2001, también permite la utilización de medios electrónicos para notificar los actos dictados sobre la materia que regula, cuando en su artículo 125 señala el “uso de medios electrónicos o magnéticos para recibir, notificar e intercambiar documentos, declaraciones, pagos o actos administrativos y, en general, cualquier información”. Igualmente, en su artículo 162, establece en materia de notificaciones el uso válido del correo electrónico como medio para practicarlas, siempre que se deje constancia de su recepción en el expediente.

A su vez, mediante un correo electrónico o *e-mail* podría ser demostrada la comisión de un delito, tal como se observa en el caso de la Ley Especial Contra los Delitos Informático, publicada en Gaceta Oficial N° 37.313, de fecha 30 de octubre de 2001, la cual tipifica los delitos contra la privacidad de la data o información de carácter personal, definiéndolos en su artículo 20, como aquellos en los que una persona:

> (…) por cualquier medio se apodere, utilice, modifique o elimine, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información.

Asimismo, dicha Ley define los delitos de violación de la privacidad de las comunicaciones en su artículo 21, cuando señala que son aquellos en que una persona "mediante el uso de tecnologías de información, acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena".

También, el artículo 22 de dicha Ley define el delito de revelación indebida de data o información de carácter personal, señalando que es aquel en que una persona:

> (…) revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos precedentes, aún cuando el autor no hubiese tomado parte en la comisión de dichos delitos.

A su vez, la Ley de Comercio Marítimo del 5 de Enero de 2006, en sus artículos 31, 104 y 233, regula los medios electrónicos para efectuar notificaciones, y también para el caso de las "protestas de mar"[5].

[5] Artículo 5. Para los efectos de esta Ley, se entiende por Protesta de Mar, el acto mediante el cual el Capitán o las personas que tienen conocimiento de un hecho, que puede generar su responsabilidad, la de sus principales y dependientes, deben informar por cualquier medio las circunstancias de dichos eventos por ante la Autoridad Acuática o consular competente en el primer puerto de arribo del buque. Las protestas de mar deberán formularse, dentro de las 24 horas siguientes de la arribada del buque a puerto, mediante intercambio electrónico de datos o por cualquier otro medio que permita hacerlo.

También la Ley de Registro Público y del Notariado del 22 de diciembre de 2006, permite la incorporación de medios electrónicos para la gestión y automatización de los Registros y Notarías, tal como se observa cuando en sus artículos 23 y 24, le otorga validez a la firma electrónica de los Registradores y Notarios.

Por otra parte, el Decreto con Rango, Valor y Fuerza de Ley Orgánica de la Administración Pública del 31 de julio de 2008, en sus artículos 6, 9, 11, 151 y 162, le otorga a los documentos electrónicos la misma validez y eficacia que el documento original, siempre y cuando esté garantizada la autenticidad, integridad, e inalterabilidad de la información contenida en esos documentos electrónicos.

Otra ley que regula hechos que pueden ser demostrados mediante el correo electrónico es Ley para la Defensa de las Personas en el Acceso a los Bienes y Servicios, publicado en Gaceta Oficial N° 39.358 del 1° de febrero de 2010. Dicha Ley en su Capítulo V delimita el comportamiento esperado del proveedor en un ambiente electrónico; ordena la presentación de información en forma clara, precisa y accesible; regula la recepción de mensajes de datos no solicitados; ordena la difusión de información adecuada respecto a la pertenencia del proveedor a algún esquema relevante de autorregulación; resguarda la privacidad de las transacciones; limita la explotación de la data recabada de consumidores; y obliga a proveedores a disponer medios de pago seguros.

La Ley de Reforma de la Ley de Contrataciones Públicas del 6 de septiembre 2010, en su artículo 79, establece el uso de los medios electrónicos para la selección de contratistas, cuando expresamente señala que “medios y tecnologías de información y comunicaciones que garanticen la transparencia, honestidad, eficiencia, igualdad, competencia, publicidad, autenticidad, seguridad jurídica y confidencialidad necesarias”.

Actualmente, la mayoría de las normas jurídicas venezolanas incorpora a los medios electrónicos para actividades tales como realizar notificaciones, mejorar y automatizar la gestión de los entes de la Administración Pública, y algunos le dan valor probatorio a los documentos electrónicos. Podemos señalar como ejemplo de ellas, la Ley de Tarjetas de Crédito, Débito, Prepagadas y demás Tarjetas de Financiamiento y Pago Electrónico; Ley General de Bancos y Otras Instituciones Financieras; Ley de Impuesto a las Transacciones Financieras de las Personas Jurídicas y Entidades Económicas sin Personalidad Jurídica; Ley de Impuesto al Valor Agregado; Ley Orgánica de Aduanas; Ley Orgánica de la Contraloría de la República y del Sistema Nacional de Control Fiscal; Ley Orgánica contra el Tráfico Ilícito y el Consumo de Sustancias Estupefacientes y Psicotrópicas; Ley Orgánica del Poder Ciudadano; Ley Orgánica de Telecomunicaciones y; la Ley Orgánica del Turismo, entre otras.

Del marco jurídico arriba reseñado, se observa que cada vez más el correo electrónico adquiere una gran importancia a los efectos de cumplir con obligaciones legales, por lo que se convierte de gran relevancia al momento de demostrar la existencia de hechos y relaciones jurídicas.

PRINCIPIOS QUE RIGEN LA PRUEBA ELECTRÓNICA

El DLMDFE establece en su exposición de motivos los principios que regularan todo lo relacionado con los mensajes de datos y las firmas electrónicas. Cabe destacar, que dichos principios no son creación de nuestra legislación venezolana, sino que han sido aplicados en el ámbito internacional.

El objeto de estos principios es precisamente que se le otorgue a los mensajes de datos y firmas electrónicas valor probatorio, no sólo en un proceso judicial, sino en

el marco jurídico nacional, a los efectos de que constituyan plena prueba de las situaciones y relaciones jurídicas que cada vez más son plasmados en ellos.

Estos principios, fueron inicialmente consagrados por la Ley Modelo de UNCITRAL ([6]) sobre Firmas Electrónicas, y consisten básicamente en lo siguiente:

1) Eficacia probatoria – Equivalencia funcional.

2) Neutralidad tecnológica.

3) Respeto a las formas documentales existentes.

4) Respeto a las firmas electrónicas preexistentes.

5) Otorgamiento y reconocimiento jurídico de los mensajes de datos y las firmas electrónicas.

6) Funcionamiento de las firmas electrónicas.

7) No discriminación del mensaje de datos firmado electrónicamente.

8) Libertad contractual.

9) Responsabilidad.

[6] La *United Nations Comission on International Trade Law* (UNCITRAL) es el principal órgano jurídico del sistema de las Naciones Unidas en el ámbito del derecho mercantil internacional. Dicha comisión es un órgano jurídico de composición universal, dedicado a la reforma de la legislación mercantil a nivel mundial durante más de 40 años, cuya función consiste en modernizar y armonizar las reglas del comercio internacional.

A continuación, se realiza el análisis de lo que significa cada principio anteriormente señalado, por cuanto los mismos no sólo tienen gran relevancia a nivel internacional en relación con los correos electrónicos, sino que además han sido implementados a nivel nacional por el DLMDFE.

Eficacia probatoria – Equivalencia funcional.

Específicamente, el DLMDFE hace referencia al principio de eficacia probatoria y equivalencia funcional de los mensajes de datos y firmas electrónicas, cuando señala en su exposición de motivos lo siguiente:

> 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, en el artículo 4 se atribuye a éstos el valor probatorio que la ley consagra para los documentos escritos, los cuales gozarán de tarifa legal y producen plena prueba entre las partes y frente a terceros de acuerdo a su naturaleza (…). Todo lo concerniente a su incorporación al proceso judicial donde pretendan hacerse valer, se remite a las formas procedimentales reguladas para los medios de pruebas libres, contenidas en el Artículo 395 del CPC. De esta forma ha sido incorporado el principio de equivalencia funcional, adoptado por la mayoría de las legislaciones sobre 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.

Por otra parte, tenemos que el DLMDFE en sus artículos 4 y 17, establece la eficacia probatoria de los mensajes de datos y firmas electrónicas, así como señala

que en los casos en que la firma electrónica no cumpla con los requisitos indicados por la ley el Juez deberá valorar esa prueba de acuerdo a su sana crítica.

Tal como se observa del texto parcialmente trascrito, el DLMDFE le otorga a los mensajes de datos y firmas electrónicas el mismo valor probatorio que tienen los documentos escritos en el ordenamiento jurídico venezolano, por lo que los mismos deberán ser valorados por el Juez de acuerdo al sistema de tarifa legal, constituyéndose así en plena prueba en el proceso no sólo entre las partes sino también frente a terceros.

Sin embargo, cuando el referido Decreto se refiere a las formas procedimentales para promover como prueba a los mensajes de datos y firmas electrónicas, se remite a las normas previstas para la prueba libre. Igualmente, señala que la firma electrónica que no cumpla con los requisitos establecidos en dicha norma deberán ser valoradas por el Juez de acuerdo al sistema de valoración de la prueba de la sana crítica.

En ese sentido, el DLMDFE regula en cuanto a los mensajes de datos y firmas electrónicas el valor probatorio que tienen en un proceso, los sistemas que deben utilizarse para valorar la prueba, y la forma procedimental para su promoción y evacuación en el proceso.

La Ley Modelo de UNCITRAL de Comercio Electrónico cuando desarrolla el principio de equivalencia funcional, establece cinco aspectos del mismo, los cuales son los siguientes: el documento, la firma electrónica, originales y copias, la prueba y la conservación de los mensajes de datos.

Ahora bien, un elemento fundamental para que los mensajes de datos puedan tener valor probatorio en un proceso judicial, es que los mismos puedan conservarse

en el tiempo. Al respecto, el DLMDFE establece expresamente en su artículo 8 que: "Cuando la ley requiera que la información conste por escrito, ese requisito quedará satisfecho con relación a un mensaje de datos, si la información que éste contiene es accesible para su ulterior consulta". Igualmente, dicho artículo indica cuáles son las condiciones necesarias para que se entienda que el mensaje de datos ha sido efectivamente conservado en el tiempo:

> 1) Que la información que contengan pueda ser consultada posteriormente.
>
> 2) Que conserven el formato en que se generó, archivó o recibió o en algún formato que sea demostrable que reproduce con exactitud la información generada o recibida.
>
> 3) Que se conserve todo dato que permita determinar el origen y el destino del mensaje de datos, la fecha y la hora en que fue enviado o recibido.

El objeto de la exigencia arriba indicada es que el mensaje de datos pueda efectivamente ser equiparado a un documento escrito, siendo el caso que una de las grandes virtudes del documento escrito en un proceso judicial, es que el mismo tiene una gran permanencia en el tiempo, es decir permite plasmar de forma permanente la voluntad de las partes en relación con un negocio, relación o situación jurídica.

En relación con éste principio, Rico (2005), señala que "la equivalencia funcional permite aplicar a los mensajes de datos con firma electrónica un principio de no discriminación respecto de las declaraciones de voluntad, independientemente de las formas en que hayan sido expresadas" (pp. 66-69).

Muci (2003) expresa sobre la equivalencia funcional de la firma electrónica que:

> ENTONCES, LEGALMENTE la firma electrónica que tiene equivalencia funcional con la autógrafa es la firma digital, aquella que se construye gracias a la conjugación de claves públicas o privadas y que al menos cubre los requerimientos contenidos en el Art. 16 de la LMDFE.
>
> LA EQUIVALENCIA FUNCIONAL mantiene vigentes las funciones tradicionales de la firma autógrafa: a) identificar a una persona; b) proporcionar certidumbre respecto a su participación personal en el acto de una firma; y, c) vincular a la persona con el contenido del documento. Sin la cobertura de tales funciones, no habrá equivalencia funcional y estaremos en presencia de una firma electrónica desprovista de validez y eficacia jurídica.

Neutralidad tecnológica.

El DLMDFE establece en su exposición de motivos que “No se inclina a una determinada tecnología para las firmas y certificados electrónicos. Incluirá las tecnologías existentes y las que están por existir”.

Asimismo dicho Decreto, regula este principio cuando en su artículo 1° señala lo siguiente:

> El Decreto-Ley será aplicable a los mensajes de datos y firmas electrónicas, independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en el futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los mensajes de datos y firmas electrónicas.

En virtud de la realidad tecnológica que varia constantemente, lo cual afecta los sistemas y tecnología que se implementa en la elaboración de mensajes de datos, firmas electrónicas y certificados electrónicos, el marco jurídico que los regule no puede atarse a una tecnología específica. De ser eso así, la norma jurídica perdería vigencia al ser desplazada dicha tecnología por otra más moderna, y sería de imposible aplicación.

El error arriba indicado fue cometido por la propia Ley Modelo de UNCITRAL, por cuanto establece regulaciones expresas sobre la tecnología del intercambio electrónico de datos (EDI, siglas en inglés de *Electronic Data Interchange*), la cual si bien estuvo plenamente vigente al momento en que se elaboró dicha Ley, actualmente ha sido desplazada por nuevas tecnologías.

Este principio de neutralidad tecnológica ha sido adoptado en otras normas jurídicas en Venezuela, tal como se observa en el artículo 108 de la Constitución, que consagra como un derecho humano el acceso a la tecnología, haciendo especial énfasis en la promoción de la educación sobre nuevas tecnologías y su aplicación.

Asimismo, se observa que la Ley Orgánica de Telecomunicaciones del 2012, cuando define en su artículo 4 a las telecomunicaciones como “toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza, por hilo, radioelectricidad, medios ópticos, u otros medios electromagnéticos afines, inventados o por inventarse”, no se refiere a una determinada o específica forma de tecnología, sino que busca ampliar su objetivo, de forma que cualquier modificación tecnológica que pueda ocurrir en el futuro se encuentre comprendida dentro de su regulación.

Sobre este principio, Rico (2005) señala que como la mayoría de las firmas electrónicas siguen el esquema de la clave pública, basada en la criptografía asimétrica, es sumamente difícil redactar un marco jurídico que sea neutro tecnológicamente. Asimismo, hace referencia al caso de España, en donde la firma electrónica está basada en la tecnología de la clave pública.

Respeto a las formas documentales existentes o no alteración del derecho preexistente de obligaciones y contratos.

El DLMDFE en su referida exposición de motivos menciona que:

> 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.

El principio de alteración del derecho preexistente de obligaciones y contratos implica que un contrato electrónico realizado virtualmente, no debe ser modificado posteriormente por una de las partes, ya que debe considerarse como si se hubiera perfeccionado a través de un medio tradicional. Es decir, deben respetarse los principios de intangibilidad de los contratos y el cumplimiento de buena fe de parte de los participantes que integran el negocio jurídico virtual.

Rico (2005) expresó que “Según este principio los elementos esenciales del negocio jurídico no deben modificarse cuando el contrato se perfecciona por vía

electrónica, ya que se trata de un nuevo medio de representación de la voluntad negocial" (p. 71).

En ese sentido, se mantienen en el mensaje de datos y firma electrónica los principios que existen en materia contractual, tales como el principio de buena fe.

Rico (2005) menciona que el principio de buena fe es una consecuencia del principio de la no alteración del derecho preexistente de las obligaciones y contratos, por cuanto en dicho derecho prevalece la buena fe en los acuerdos entre las partes.

La buena fe es un atributo que debe estar presente en las relaciones contractuales, y más aún cuando se trate de la transmisión de información vía Internet, en donde la identidad de las personas es de difícil conocimiento. Es por ello que se debe mantener y brindar la confianza entre las personas que se benefician del uso de las Tecnologías de Información.

Otorgamiento y reconocimiento jurídico de los mensajes de datos y las firmas electrónicas.

El DLMDFE señala en su exposición de motivos en relación con éste principio lo siguiente:

> Asegura el otorgamiento y reconocimiento jurídico de los mensajes de datos, 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 que cumplirán dichos proveedores de servicios de certificación, incluida su responsabilidad.

Este principio establece que los mensajes de datos, las firmas electrónicas y los servicios de certificación, además de los mecanismos reconocidos a nivel internacional, serán aceptados en el ordenamiento jurídico venezolano. Dicho esto, los proveedores de servicios de certificación serán responsables de cumplir lo preceptuado en el DLMDFE, así como otras leyes que regulen el uso de tecnologías.

Funcionamiento de las firmas electrónicas.

En cuanto al funcionamiento de las firmas electrónicas como principio el DLMDFE expone que:

> 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.

Con base a este principio el DLMDFE, trata de garantizar el buen funcionamiento de la firma electrónica, como mecanismo de autenticidad de estos documentos. Esto se logra a través de una regulación que permita establecer criterios adecuados que garanticen la validez jurídica de un documento realizado electrónicamente.

No discriminación del mensaje de datos firmado electrónicamente.

A su vez, el Decreto *in commento* menciona que “garantiza la fuerza ejecutoria, el efecto o la validez jurídica de una firma electrónica que no sea cuestionado por el solo motivo de que se presente bajo la forma de mensaje de datos”.

Dicho principio consiste en que un documento realizado y firmado con su respectiva firma electrónica debidamente autorizada por un proveedor de servicios de certificación, tiene la misma validez y eficacia que un documento con firma autógrafa. Por lo tanto, no se podrían desechar dichos documentos sin antes analizarlos, por el simple hecho de considerarlos documentos electrónicos. En este sentido, el DLMDFE es explícito, ya que establece en su artículo 4 que estos documentos tendrán el mismo valor probatorio que se le otorga a los documentos escritos.

Libertad contractual.

El DLMDFE establece en su exposición de motivos el principio del respeto a las firmas electrónicas preexistentes, el cual se encuentra relacionado con el principio de libertad contractual, por cuanto permite que “las firmas electrónicas utilizadas en grupos cerrados en los que 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”.

Además, el DLMDFE, establece que se “permite a las partes escoger la modalidad de sus transacciones, es decir, si aceptan o no las firmas electrónicas”.

Este principio permite a las partes elegir la forma en que van a realizar sus operaciones, la adopción de procedimientos electrónicos para la ejecución de ciertos y determinados contratos. Es decir, se enfoca en la libertad contractual que tienen las partes y por otro lado, la libertad que tienen para incluir la forma que consideren conveniente para regir sus relaciones contractuales.

Adicionalmente, este principio tiene relevancia, ya que son las partes las que tienen la potestad de decidir cómo van a realizar un negocio jurídico de acuerdo a las condiciones que ambas establezcan. Esto último, está estrechamente vinculado al principio de la autonomía de voluntad de las partes, en donde ellas son libres de elegir el modo de realizar sus contratos, siempre y cuando no vayan en contra del orden público, las buenas costumbres y la ley.

En relación con este principio, Rico (2005) menciona que:

> Este principio se encuentra consagrado en la exposición de motivos del DLMDFE al permitir a las partes convenir la forma de realizar sus transacciones y decidir si acuerdan o no adoptar los procedimientos electrónicos para celebrar sus contratos. La libertad contractual, por una parte, la elección del medio empleado en las negociaciones y por otra, la libertad para incluir las cláusulas o convenios que consideren necesarios a efectos de regir sus relaciones (p. 73).

Responsabilidad.

El principio de responsabilidad se refiere a que toda persona que haga uso de certificados y firmas electrónicas podrá eximirse de responsabilidad, siempre y cuando logre demostrar que ha actuado de una manera prudente y de acuerdo a las circunstancias que así lo ameriten. Por otro lado, los proveedores de servicios de certificación electrónica, pueden limitar su responsabilidad en lo que respecta a la creación de los certificados electrónicos, dadas las condiciones, límites y restricciones establecidas para su uso adecuado. Así, el DLMDFE expone que:

> 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.

Dicho principio se refleja expresamente en los artículos 19 y 35 del DLMDFE, que establecen las obligaciones de los usuarios o signatarios y de los PSC.

LA PRUEBA ELECTRÓNICA

Ahora bien, el ordenamiento jurídico venezolano no define el concepto de prueba, pero de acuerdo a lo señalado por el autor Pierre (1977), la legislación venezolana estructuró toda la materia probatoria acogiendo tres posiciones dogmáticas, las cuales son las siguientes:

> …a) atendiendo a los distintos medios de apreciación ofrecidos por las partes, o recogidos por el Juez en el curso de la contraversión (así se dice prueba documental, prueba testimonial, etc.); b) observando la acción de probar, y se dice entonces que al actor corresponde la comprobación de su demanda y al demandado la de su defensa; y c) contemplando el estado de espíritu creado por el Juez por las diligencias aportadas y en este sentido un hecho se considera probado o no según que los elementos de juicio sean o no considerados suficientes para formar la convicción del magistrado, pues las partes pueden haber producido en los autos abundantes pruebas sin lograr engendrar con ellas persuasión en el órgano jurisdiccional (p. 30).

Rengel Romberg (2004) define la prueba “como la actividad de las partes dirigida a crear en el Juez la convicción de la verdad o falsedad de los hechos alegados en la demanda o en la contestación” (p. 218).

A su vez, Midón (2007) expresó que la prueba “es el medio a través del cual el litigante presenta al Juez la verdad del hecho afirmado” (p. 34).

De igual forma, el reconocido autor Devis Echandía (1993) expresó que “probar es aportar al proceso por los medios y procedimientos aceptados en la ley, los motivos o las razones que produzcan el convencimiento o la certeza del Juez sobre los hechos” (p. 34).

Del mismo modo, el profesor Rivera (2004) expresó lo siguiente:

> Probar en este sentido es convencerse y convencer de la existencia de un hecho, o de la verdad de algo. Probar es, pues, producir un estado de incertidumbre en la mente de una o varias personas de la existencia o inexistencia de un hecho, o de la verdad o falsedad de una proposición (p. 3).

En comparación con estos otros autores, el maestro Carnelutti (2000) sostiene que:

> En el lenguaje común, prueba se usa como comprobación, de la verdad de una proposición; solo se habla de prueba a propósito de alguna cosa que ha sido afirmada y cuya exactitud se trata de comprobar; no pertenece a la prueba el procedimiento mediante el cual descubre una verdad no afirmada sino, por el contrario, aquel

> mediante el cual se demuestra o se halla una verdad afirmada (p. 38).

De las consideraciones anteriores, podemos concluir que el término “prueba”, se considera como la forma en que las partes demuestran al Juez la verdad o falsedad de los hechos que se pretenden hacer valer en el proceso.

Las pruebas son un factor preponderante en cualquier proceso. Esto es debido a que son la principal herramienta que las partes tienen para demostrar los hechos ocurridos, creando en el Juez una concepción de los hechos que ocurrieron en un pasado.

Dada esta variedad de definiciones, se considera apropiado lo comentado por Rivera, en virtud de que las partes tienen la tarea de convencer al Juez sobre situaciones que se han presentado en el pasado, sobre la existencia o inexistencia de un hecho y de esta manera poder adjudicarle un valor a lo que se prueba.

El ordenamiento jurídico venezolano tampoco define el concepto de medio probatorio, sino que establece cuales son los medios de prueba, y las condiciones para la promoción de los mismos. Por lo que, de acuerdo al autor Pierre (1977), el medio de prueba es:

> …la persona o la cosa y, excepcionalmente, también los hechos que, a través de la percepción, la representación y la deducción o inducción, suministran al Juez los conocimientos necesarios para que pueda determinar la verdad o falsedad de un tema de prueba o hecho litigioso (p. 150).

En cuanto a los distintos medios de prueba que existen, se tiene que el artículo 395 del Código de Procedimiento Civil, establece cuatro grupos de medios de prueba, los cuales están situados en un mismo plano, y consisten en instrumentos que se otorgan a los sujetos procesales para trasladar al proceso hechos que verifiquen las afirmaciones de las partes, o permitan averiguar la existencia de una situación fáctica.

El primer grupo de medios de prueba consiste en las pruebas tradicionales enumeradas en el Código Civil (instrumentos públicos y privados, las tarjas, la confesión, el juramento decisorio y el deferido de oficio, la prueba testimonial, la experticia, la inspección ocular, y las presunciones legales y *hominis*).

El segundo grupo de medios probatorios está formado por las contempladas exclusivamente en el CPC (reconstrucción de hechos, reproducciones, inspección judicial, interrogatorio libre y sin juramento de las partes, experticia, y prueba de informes).

El tercer grupo de medios probatorios está constituido por las establecidas en leyes distintas al Código Civil y al CPC.

Y el cuarto grupo lo forman todos aquellos instrumentos capaces de trasladar hechos al proceso y que no están contemplados en ley alguna, determinados por el principio de libertad probatoria.

Estos medios probatorios deben ser valorados por el Juez al momento de dictar sentencia en un proceso judicial. La valoración de las pruebas consiste en la labor del Juez para establecer la fuerza de convicción que tiene cada medio de prueba debidamente promovido, admitido y evacuado en el proceso judicial, apreciado tanto individualmente como en comparación con las otras pruebas aportadas al proceso.

Existen distintos sistemas que un Juez puede emplear para valorar las pruebas en un proceso judicial, entre los cuales tenemos el de tarifa legal, que consiste de acuerdo a lo señalado por el autor Pierre (1977), en "…el señalamiento anticipado que la ley le hace al Juez del grado de eficacia que tiene los medios de prueba o le dice como y de que manera debe tenerse por probado un hecho" (p. 342).

En contra de este sistema surgió el de la libre apreciación de la prueba razonada, el cual consiste de acuerdo con el autor Pierre (1977) en "…que la ley señala al Juez los medios que pueden ser admitidos como pruebas y las formalidades procesales para su validez, pero deja al magistrado en libertad para apreciar las que estén comprendidas en la enumeración legal" (p. 342).

Aplicando los conceptos de medio probatorio y valoración de pruebas al correo electrónico, se observa que tanto en el derecho venezolano como en el comparado, existe una preocupación por garantizar la autenticidad del contenido y de la autoría del correo electrónico. Esto se debe a que es un medio tecnológico que fácilmente puede ser alterado, por lo cual aparte de que tecnológicamente se han creado sistemas de seguridad como la firma electrónica, también legalmente se le ha otorgado valor a aquellos correos electrónicos que posean una firma electrónica, la cual sea certificada por una empresa que se encargue de prestar esos servicios, y que sea reconocida legalmente.

Es por ello, que el DLMDFE le da una eficacia probatoria a los correos electrónicos igual a la de documentos escritos, siempre y cuando cumplan con los requisitos de tener una firma electrónica que a su vez cumpla con lo exigido por dicho Decreto Ley.

Sin embargo, la información contenida en un correo electrónico que sea reproducida en un formato impreso, tendrá la misma eficacia probatoria que le otorga

el CPC a las copias o reproducciones fotostáticas, es decir se tendrán por fidedignas si no son impugnadas por la parte contraria en el proceso judicial. En cuanto, a la promoción, control, contradicción y evacuación como medio de prueba, remite a las normas del CPC para las pruebas libres.

Ahora bien, en cuanto a los correos electrónicos que no tengan una firma electrónica, o si la misma no cumple con los requisitos exigidos por el Decreto Ley, no se le otorgará el valor de una documental, sino que será un elemento de convicción valorable conforme a las reglas de la sana crítica.

Por lo tanto, el sistema legal vigente que regula el correo electrónico en Venezuela no establece en el caso de que un correo electrónico no cumpla con los requisitos de la firma electrónica, los medios probatorios mediante los cuales se le puede aportar al Juez un conjunto de elementos de convicción del objeto de prueba. De igual forma, si bien remite a las reglas de la sana crítica, no señala cual es la valoración que le debe otorgar un Juez al correo electrónico si el mismo es promovido con otro grupo de medios probatorios que demuestren la certeza del contenido y la autoría del mismo.

Cabe destacar, que la forma tradicional para realizar una probanza es mediante la utilización de instrumentos escritos. Es decir, un documento en forma escrita representa los hechos ocurridos con anterioridad, que si son demostrados correctamente por quienes los invoquen, podrían ser valorados sin ningún inconveniente.

Ahora bien, la prueba electrónica presenta el mismo objetivo que la prueba escrita tradicional. Sin embargo, tiene la particularidad de que ésta es emanada de una fuente informática, lo que puede llevar al debate sobre si surte o no efectos legales.

La respuesta a lo anterior debe ser afirmativa, ya que el CPC, en su artículo 395, expresa la posibilidad de aportar en el proceso cualquier medio probatorio que las partes consideren pertinentes y que no sea prohibido por la ley.

Adicionalmente, existen numerosas sentencias que hacen referencia a este punto e incluso el DLMDFE, es claro al respecto, en el sentido de que las pruebas electrónicas, como es el caso de los correos electrónicos, sí pueden tener valor probatorio en un proceso, ya que es una prueba legal consagrada en el artículo 2 del DLMDFE concatenada con el mencionado artículo 395 del Código de Procedimiento Civil.

MEDIOS INFORMÁTICOS COMO MEDIO DE PRUEBA, OBJETO DE PRUEBA Y FUENTE DE PRUEBA

Fuente de prueba.

La fuente de prueba es el elemento donde queda plasmado un hecho ocurrido. Es decir, corresponde a la circunstancia que permite observar el hecho concreto como se originó, dándole así una representación mental al Juez, con el fin de que pueda reconstruir los hechos ocurridos.

Ahora bien, en el caso de los medios informáticos, son aquellos dispositivos electrónicos que almacenan cualquier tipo de información (i.e. un computador), con la finalidad de poder representar posteriormente situaciones registradas por el hombre, haciendo uso de estos dispositivos electrónicos. Por lo tanto, según expresa Muñoz (1997), la fuente de prueba es “el elemento en el cual ha quedado estampada o grabada la huella del hecho histórico que vamos a intentar reconstruir en el proceso” (p.479).

Del mismo modo, Rivera (2004) menciona que fuente de prueba se refiere a:

> Es el hecho propiamente dicho que quedó estampado en las personas y cosas anteriores al proceso y que registraron el hecho. Por ello, lo que se lleva al proceso es información o registro sobre el hecho no el hecho en sí, porque este es el del pasado e irrepetible. En ocasiones el hecho fuente es el mismo que quiere probarse (p. 903).

Medio de prueba.

El medio de prueba es el vehículo por el cual se transportan al proceso los hechos ocurridos. Aunado a esto, permite la reconstrucción de lo alegado tanto para el Juez como para las partes involucradas en el proceso, con el fin de demostrarle al Juez el hecho debatido. Además, se puede decir que es una persona o cosa que permite probar hechos pertinentes al proceso. Aquéllos pueden ser testigos, prueba de peritos, inspección judicial, entre otros; y éstos comprenden las cosas, por ejemplo, los documentos.

Sin embargo, cuando se habla de medios informáticos como medio de prueba nos referimos a la forma en que serán reproducidos los hechos ya ocurridos, permitiéndole al Juez elegir la forma correcta de apreciación de la prueba promovida por la parte promovente, de acuerdo a lo que establezca la ley o, en caso de ser necesario, la sana critica del Juez.

Sobre este particular, Rivera (2004) expresó lo siguiente:

> Los medios de pruebas son los caminos o instrumentos que se utilizan para conducir al proceso los hechos y posibilitar la

> reconstrucción de los acontecidos en “la pequeña historia”, que es pertinente al proceso que se ventila. Son aquellos que transportan los hechos al proceso. Son los instrumentos regulados por el derecho para la introducción en el proceso de la fuente de prueba. Visto así son instrumentos de intermediación requeridos en el proceso para dejar constancia material de los datos de hechos (p. 387).

Objeto de prueba.

Con respecto al objeto de la prueba el autor Devis Echandía (1993), sostiene que es “aquello sobre lo que puede recaer la prueba” (p. 143).

Con base a lo anterior, se puede decir que corresponde a los hechos que son aducidos en el proceso haciendo uso de algún medio de prueba. El hecho en concreto y el medio se vinculan para demostrar el contenido de la prueba.

Siguiendo este orden de ideas, es preciso mencionar un medio probatorio muy importante para muchas legislaciones a nivel mundial así como para la nuestra. Su relevancia como prueba resulta uno de las más efectivas al momento de demostrar una pretensión en un proceso, ya que es una forma practicada desde hace siglos en nuestra civilización, lo que la hace eficiente en toda su extensión en esta era moderna. Este medio lleva la particularidad del empleo de la escritura y su estampado en papel, lo que permite durabilidad a lo largo de los años y la posibilidad de demostrar lo que en él se contiene.

Este medio probatorio es el denominado “documento”. A continuación se explicará su propósito y tipos para, posteriormente, abarcar otra clasificación del documento que será objeto de estudio a lo largo de este trabajo.

EL DOCUMENTO

El documento, en su expresión más amplia, y siguiendo lo establecido por Rivera (2004) es un instrumento en el que se plasman hechos y la forma en que ocurrieron.

Una particularidad de los documentos, es que los hechos son demostrados haciendo uso del papel. Es decir, los negocios o actos jurídicos del hombre quedan estampados mediante el uso de los documentos escritos, los cuales permiten que su propósito perdure en el tiempo, y también hace muy difícil su modificación por quienes pretendan hacer un uso distinto al que ya poseen.

Para Rivera (2004) el documento es “todo objeto o materia en el cual se incorpora el pensamiento humano mediante signos gráficos, simbólicos, imagen o pictóricos con el objeto de representar hechos o actos jurídicos relevantes por sus consecuencias” (p. 723).

Por otro lado, de acuerdo al tratadista italiano Carnelutti (2000) “el documento no es solo una cosa, sino una cosa representativa capaz de representar un hecho” (p. 156).

Por su parte, Devis Echandía (1993), expresa que el documento puede ser considerado como “toda cosa que sea producto de un acto humano, perceptible con los sentidos de la vista y el tacto, que sirve de prueba histórica indirecta y representativa de un hecho cualquiera” (p. 486).

Asimismo, el maestro Couture (1976) se expresa de la siguiente manera “es el objeto normalmente escrito, en cuyo texto se consigna o representa alguna cosa apta

para esclarecer un hecho o se deja constancia de una manifestación de voluntad que produce efectos jurídicos" (p. 239).

Por lo tanto, y vistas las definiciones anteriormente señaladas, se puede concluir que el documento es cualquier aspecto o cosa realizada por el hombre en donde plasma una información y/o contenido, con el fin de perdurar en el tiempo y de esta manera, de ser el caso, poder demostrar algún hecho en el futuro.

Ahora bien, dependiendo de la naturaleza jurídica del negocio jurídico, existen dos tipos de documentos, el documento privado y el documento público, los cuales se evalúan a continuación.

Documento público.

Rivera (2004) hace referencia a una jurisprudencia venezolana de la antigua Corte Federal, sentencia del 26 de mayo de 1952, la cual fue tomada del autor Borjas Arminio, en donde menciona una definición de documento público expresando lo siguiente "Es aquel que es autorizado por funcionario competente para dar fe pública y que tiene como finalidad comprobar la veracidad de los actos que el contiene y la firma de las personas que intervienen" (p. 723).

Por otro lado, el Código Civil venezolano en su artículo 1.357 expresa lo siguiente:

> 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 se haya autorizado.

De lo anterior, se puede concluir que un documento público es aquel que ha sido revisado y conocido por un funcionario competente, quien tiene la obligación de profundizar en los aspectos de forma y fondo, con el fin de darle veracidad a lo contenido en el documento y otorgarle fe pública.

En este punto, cabe resaltar el contenido de la sentencia de la Sala de Casación Civil de la extinta Corte Suprema de Justicia del 24 de febrero de 1988, citada en sentencia del Juzgado Segundo de Primera Instancia en lo Civil, Mercantil y del Tránsito de la Circunscripción Judicial del Estado Mérida del 09 de marzo de 2011 (Caso Gustavo Veltrán contra Félix Escolar), que expone lo siguiente:

> El documento público a que se refiere el artículo 376 [hoy derogado] del Código de Procedimiento Civil vigente, es el documento que conlleva cuatro fases a saber: evidencia-solemnidad-objetivación y coetaneidad; estas cuatro fases las cumple el registrador, no el notario, el registrador da fe de que conoce a los otorgantes, averigua la capacidad jurídica de los otorgantes, califica el acto, lee el documento y lo confronta con los otorgantes y testigos, ordena su inserción en los protocolos respectivos y si todo coincide, los otorgantes emiten su consentimiento. Por ello la función del Registrador es superior a la del Notario: estas cuatro fases que cumple el documento ante el registro es lo que le da el carácter de público y la fuerza erga omnes, fuerza que no tiene el documento notariado solamente ya que este solo surte efectos entre las partes y no frente a terceros.

De tal modo, un documento público como bien lo sostienen los citados autores, la Ley y la jurisprudencia, es aquel que emana de un funcionario público investido de autoridad para darle fe pública al documento.

Documento privado.

Por otra parte, el documento privado es la contrapartida de lo anterior, ya que éste tipo de documento no nace del funcionario competente, sino que son las partes quienes lo elaboran, por lo que sólo tiene efectos entre las partes que intervienen en él. Sin embargo, dicho documento puede ser autenticado, lo cual significa que un funcionario (notario) da fe pública de que el acto se realizó cumpliendo los requisitos establecidos en la Ley de Registro Público y Notariado, pero sin que el funcionario conozca sobre el fondo del documento.

Con fundamento a lo anterior, Borjas (1964) sostiene que el documento privado es "todo escrito firmado o no, que pueda servir para dar constancia de algún hecho o acto y en cuyo otorgamiento no hayan sido llenados los requisitos que la ley exige para los que sean públicos" (p. 275).

Habiendo definido el documento público y privado, es necesario hacer hincapié en las diferencias existentes entre estos dos tipos de documentos.

Diferencias entre documento público y documento privado.

Respecto a las diferencias que existen entre estos dos tipos de documentos, Rivera (2004) sostiene que en primer lugar el documento privado emana de las partes sin la participación de un funcionario público, mientras que el documento público goza de fe pública otorgada por un funcionario público presente al momento de su otorgamiento. En segundo lugar, el documento público tiene efectos *erga omnes* por cuanto afecta a terceros distintos a las partes que suscriben el documento, mientras que el documento privado únicamente surte efectos entre las personas que lo suscriben.

De acuerdo a Rivera (2004) nuestra legislación si bien no tiene una definición legal de documento privado, contempla las formalidades legales que deben respetarse. A diferencia del documento público, que sí se encuentra definido por el anteriormente citado artículo 1357 del Código Civil, y las formalidades que debe contener para que tenga plena validez están consagradas en los artículos siguientes al ya enunciado artículo.

Por su parte, en cuanto al documento privado, la forma en que debe elaborarse el mismo, así como las formalidades de su reconocimiento por las partes para que surta efecto frente a terceros y por ende, para que tenga valor probatorio, deberá regirse por lo establecido en los artículos 1363 ([7]) y 1368 ([8]) del Código Civil.

DOCUMENTO ELECTRÓNICO

El documento electrónico es un documento que ha sido creado haciendo uso de las tecnologías de la información, en donde es grabado en una memoria interna de algún dispositivo electrónico, pudiendo ser reproducido fácilmente por cualquier interesado que posea un medio digital.

Existen numerosas definiciones que han desarrollado expertos en la materia, entre las cuales se tienen las siguientes:

[7] Artículo 1.363. El instrumento privado reconocido o tenido legalmente por reconocido, tiene entre las partes y respecto de terceros, la misma fuerza probatoria que el instrumento público en lo que se refiere al hecho material de las declaraciones; hace fe, hasta prueba en contrario, de la verdad de esas declaraciones.

[8] Artículo 1.368. El instrumento privado debe estar suscrito por el obligado, y, además debe expresarse en letras la cantidad en el cuerpo del documento, en aquéllos en que una sola de las partes se obligue hacia otra a entregarle una cantidad de dinero u otra cosa apreciable en dinero. Si el otorgante no supiere o no pudiere firmar, y se tratare de obligaciones para cuya prueba se admiten testigos, el instrumento deberá estar suscrito por persona mayor de edad que firme a ruego de aquél, y, además, por dos testigos.

Rodríguez (1997) sostiene que “el tipo de documento en soporte electrónico, informático y telemático es un documento con las mismas características, en principio y en cuanto a la validez jurídica, que cualquier otro de los que tradicionalmente se aceptan en soporte en papel” (p. 4).

Asimismo, Ruíz (1999) lo define de esta manera: “el documento electrónico o informático, se concibe como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica, informática y telemática” (p. 319).

Por su parte, para el autor Falcón (2003), se puede definir al documento electrónico como:

> Aquel que ha sido creado sobre un ordenador, grabado en un soporte informático y que puede ser reproducido. Pero, en síntesis, el documento electrónico es un conjunto de campos magnéticos aplicados a un soporte, de acuerdo con un determinado código. El medio de recuperación puede ser el medio probatorio, pero en muchos casos se necesitara una prueba pericial compleja para llegar a conocerlo o determinar su autenticidad (p. 898).

Para Rico (2005) el documento electrónico es:

> En sentido estricto [documento informático] se define como la representación idónea capaz de reproducir una cierta manifestación de voluntad, materializada a través de las tecnologías de la información sobre soportes magnéticos, como un disquete, un CD ROM, una tarjeta electrónica u otro soporte de esta naturaleza, que

> se expresa a través de mensajes digitalizados que requieren de máquinas para ser percibidos y comprendidos por el hombre (p.100).

La misma autora también expone que:

> La amplitud de la definición de documento y el tratamiento por medios informáticos, permiten la sustitución del tradicional soporte en papel por uno de naturaleza electrónica, hablándose en tal sentido de un nuevo tipo de documento: “el Documento Electrónico” (p. 97).

De acuerdo a Bello y Bello (2007), los documentos electrónicos:

> Son un conjunto de cartas que son remitidas de una persona a otra, haciendo uso de medios de comunicación como lo es el correo electrónico, los cuales son representativos ya que expresan hechos jurídicos que podrían tener valor probatorio y cuya representación ininteligible se encuentra en un formato electrónico (p. 23).

Además, el documento electrónico también ha sido definido jurisprudencialmente. Como ejemplo de ello, se cita a continuación la sentencia de la Sala de Casación Civil del Tribunal Supremo de Justicia N° 460 del 5 de octubre de 2011, (Caso Transporte Doroca, C.A., contra Cargill de Venezuela, S.R.L.), en la que se expresa lo siguiente:

> Debemos precisar que el documento electrónico está previsto en la Ley sobre Mensajes de Datos y Firmas Electrónicas, y en sentido amplio, debe entenderse como cualquier tipo de documento

> generado por medios electrónicos, incluyendo en esta categoría los sistemas electrónicos de pago, la red de internet, los documentos informáticos y telemáticos, entre otros. También es catalogado como un medio atípico o prueba libre, por ser aquél instrumento que proviene de cualquier medio de informática o que haya sido formado o realizado por éste, o como el conjunto de datos magnéticos grabados en un soporte informático susceptible de ser reproducidos que puede fungir como objeto de prueba y su reproducción, independientemente de su denominación, debe ser considerada otro documento que actúa como medio para su traslado al expediente.

Vistas las definiciones expuestas, se puede afirmar que el documento electrónico, es aquel documento realizado mediante el uso de un medio informático como lo es un computador, en donde la persona estampa cierta información que es transformada en un lenguaje matemático dentro del computador y aparece reflejado en un dispositivo digital como un monitor.

En este punto, es evidente que un documento electrónico es cualquier escrito realizado usando un dispositivo electrónico, que permita expresar la voluntad de una parte o varias partes, plasmarla en ese dispositivo y luego poder visualizarla en un formato electrónico. Siendo esto así, desaparece el soporte escrito en papel, ya que no se reflejará en este medio, sino que estará reflejado en un medio ó soporte informático como lo es un computador o su equivalente (entiéndase que ya no es únicamente el computador, debido a que existen otros dispositivos electrónicos en donde puede verse reflejado un documento).

En el entorno global, ésta ramificación de documento -el realizado electrónicamente- ha sido aceptada por gran parte de la legislación mundial. Esto

debido a los grandes avances tecnológicos llevados a cabo en las últimas décadas, lo que implica que numerosos países tales como Alemania, Canadá, Estados Unidos de América, Suecia, Francia y Gran Bretaña, se viesen obligados a regular este nuevo documento y aceptar el valor probatorio que tienen los mismos.

Este nuevo esquema virtual denominado documento electrónico, corresponde a un avance en la tecnología moderna, es decir, implica un desarrollo tanto en el ámbito no jurídico como en el jurídico. Y es precisamente en este punto donde adquiere mayor relevancia este tema, ya que en el derecho interno no es muy común la utilización de los medios informáticos para hacer valer una pretensión en un proceso. Este aspecto es importante debido a que en la era moderna, la tecnología crece cada vez más aceleradamente, por lo que se debe conocer cómo es la utilización de este medio, su valoración y apreciación en un proceso judicial venezolano.

Cabe destacar, que el documento electrónico trae consigo múltiples beneficios tales como la rapidez en su creación y envío a uno o varios destinatarios simultáneamente, entre otros. Así como ciertas desventajas en determinados casos, sobre todo en los puntos referidos a su valor probatorio, como el caso de la facilidad para alterar su contenido.

Siendo esto así, surge la interrogante sobre si un documento electrónico extraído de un computador, podría ser considerado como prueba por una de las partes en el proceso. Este tema se trata en el siguiente capítulo, el cual tiene como objeto el desarrollo de la definición del correo electrónico y sus implicaciones. Además de esto, se ahonda en cómo puede dársele autenticidad a un correo electrónico tomando en cuenta si posee una firma electrónica o no.

CAPÍTULO II. CORREO ELECTRÓNICO, FIRMA ELECTRÓNICA Y ENTE REGULADOR

INNOVACIÓN TECNOLÓGICA DE LA PRUEBA ELECTRÓNICA: EL CORREO ELECTRÓNICO EN VENEZUELA Y EL IMPACTO DE SU USO POR LOS VENEZOLANOS

Hoy en día, el uso del documento electrónico no representa un problema para los venezolanos, ya que la innovación tecnológica que ha emergido los últimos años, ha traído consigo que cada vez más personas utilicen medios tales como las computadoras, celulares, tablas, y otros, para realizar determinadas actividades como negocios, compras "*online*" y transmisión de información vía correos electrónicos, entre otros.

No obstante, el hecho de promover un documento conformado con elementos electrónicos, trae como interrogante, cómo comprobar la autenticidad de su contenido y autoría. Debido a que, tal como se expuso anteriormente, desde los inicios del derecho probatorio se ha sostenido que la mejor forma de representación de un documento es cuando éste se realiza en un papel con la firma autógrafa de quien lo suscribe, que representa la autoría de tal documento.

Cabe preguntarse, si tendrá el mismo valor probatorio un documento escrito emanado por las partes con su debida firma autógrafa, que un documento realizado en un soporte electrónico. Es aquí donde deben aplicarse ciertas leyes reguladoras en esta materia, tales como el CPC, el DLMDFE, la Ley Especial contra los Delitos Informáticos, así como diferentes opiniones jurisprudenciales referidas a este caso de estudio.

Los medios de prueba electrónicos constituyen un gran avance en la forma de probar los hechos por las partes en un proceso. Esto, se debe al progreso de los sistemas de información, que obligan al abogado a profundizar y estudiar como son los mecanismos y formas que se deben tener presentes al momento de promover una prueba electrónica.

No obstante, debe hacerse un estudio de lo que se pretende probar, ya que no cualquier documento generado por un sistema computarizado, puede tener plena validez en un proceso.

De tal forma, para poder usar estos documentos electrónicos como medio probatorio se debe cumplir con una serie de requisitos tales como la pertinencia, licitud, conducencia, legalidad, legitimidad y temporaneidad, y así de esta forma el Juez podrá determinar si es procedente o no tal prueba en el proceso.

Por lo tanto, si una prueba no cumple con los requisitos mencionados, el Juez debe desecharla, ya que son requisitos que debe cumplir cualquier medio probatorio que sea interpuesto por las partes y así está estipulado en el CPC.

PRINCIPALES VENTAJAS DEL CORREO ELECTRÓNICO

Sobre las ventajas del correo electrónico, Rico (2005) señalaba que el mensaje de datos permitía enviar y recibir información contenida en archivos, imágenes e incluso sonidos, de una forma sencilla, rápida y a un bajo costo. Por otra parte, el correo electrónico transmite información no sólo a una persona, sino a varias personas simultáneamente. Adicionalmente, el correo electrónico tiene una ventaja ecológica como es el no uso del papel para enviar o recibir un mensaje.

Por otra parte, también surge un problema en cuanto a la ausencia de seguridad en la confidencialidad del mensaje enviado, el cual una vez remitido a otra persona, puede ser modificado en su trayecto por cualquier individuo, dándose el caso de que se puede acceder sin ningún permiso al contenido del mismo y de esta manera modificarlo. De ahí a que en la actualidad, hayan surgido nuevos mecanismos para proteger la información enviada vía correo electrónico.

En cuanto a los sistemas que existen a nivel nacional e internacional para garantizar la autoría y contenido de un correo electrónico, Hance (1996) señala lo siguiente:

> En la mayoría de los países de la Unión Europea y de América del Norte, se considera a la privacía como un valor que merece protegerse. Aunque los medios legales de protección varían de un país a otro –en algunos, la privacía está protegida por ley; en otros, por la jurisprudencia. Estas formas generales de protección implican penalización en el caso de la difusión de mensajes que pueden divulgar información (texto, imágenes, etcétera) que constituya una invasión a la privacía. Además, esta queda protegida contra monitoreo electrónico por autoridades gubernamentales y por individuos privados. Por último, está estrictamente regulado el procesamiento de datos personales, lo cual representa una genuina amenaza a la privacía (tanto en el sector privado como en el público, bajo la legislación europea, y en el sector público bajo la estadounidense y la canadiense), o está sujeto a autorregulación (con referencia al sector privado en Canadá y en Estados Unidos) (p. 132).

Ahora, específicamente en cuanto a los medios que tienen los usuarios de la mensajería del correo electrónico para garantizar la autenticidad del contenido y autoría del correo electrónico, dicho autor nos señala lo siguiente:

> Una de las consecuencias de una red abierta como Internet son los problemas de seguridad y confidencialidad. Debido al incremento de las transacciones comerciales y de la transmisión de información delicada (digamos, información financiera o datos protegidos por secreto profesional), 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 (p. 180).

Dicha información es complementada con lo señalado por Martínez (2000), en cuanto a que:

> En pleno desarrollo de la sociedad de la información, con aplicación de las nuevas tecnologías para el desarrollo de verdaderas transacciones comerciales, la firma electrónica, junto con los certificados y las entidades de certificación se ofrecen, desde el punto de vista técnico, como elementos para conseguir un comercio electrónico seguro a gran escala, en cuanto permiten solucionar los problemas de autenticidad, integridad, no rechazo en origen, e, incluso, en algunos casos, confidencialidad, inherentes a las comunicaciones electrónicas. Desde el punto de vista jurídico, estas soluciones técnicas plantean algunas dudas e incertidumbres

> para cuya resolución existen distintas iniciativas legislativas (p. 17).

En cuanto a los mecanismos existentes para alterar la autoría y el contenido de un correo electrónico, Orta (2005) hace referencia a lo que se denomina "ciberterrorismo", cuando señala que "Es la forma de terrorismo que usa conocimientos y recursos informáticos para intimidar o realizar coerción a otros" (p. 3).

Al respecto, dicho autor también señala que:

> Las tecnologías de información han ayudado a la evolución del ser humano, y su utilización con fines de guerra y delictual debe ser severamente castigada. La comisión de delitos y de actos contra las tecnologías hace que los usuarios desconfíen de los sistemas produciéndose un retraso en los ciclos de mejoramiento y desarrollo de este tipo de tecnologías.
>
> El uso de la informática como medio de comisión o como facilitadores para la perpetración y continuación de cualquier tipo de delitos debe ser considerado en el futuro por las legislaciones penales como un agravante de los delitos existentes.
>
> Con la aparición de nuevas tecnologías, estas se convierten de inmediato en herramientas para cometer nuevos delitos y en nuevos medios de comisión o de ayuda o facilitación de nuevos delitos (p. 22).

Información que se complementa con lo indicado por la autora Di Totto (2005), la cual señala que:

> Es así que, independientemente de nuestro nivel de conocimiento o de utilización eficiente de la tecnología de información, muchos de nuestros datos personales más sensibles están registrados en los sistemas automatizados de las universidades donde estudiamos o impartimos conocimientos, en los bancos donde tenemos cuentas o tarjetas de crédito, en las organizaciones a las cuales hemos prestado servicios, en los centros de salud donde nos han atendido, y desde luego, en las empresas de las que somos clientes. Lo cierto es que muchos aspectos de nuestra vida pueden ser revisados con solo 'hacer click' en un comando de un computador y los gobiernos e instituciones privadas no se quedan atrás en cuanto a la vulnerabilidad que entraña, hasta para su propia supervivencia, que sus bases de datos lleguen a ser obtenidas o malutilizadas por personas no autorizadas, o que sus sistemas sean objeto de daño o sabotaje que puedan poner en peligro la confiabilidad de sus operaciones (p. 5).

Es por esta razón que surgen mecanismos como la denominada "firma electrónica" y el "certificado electrónico", los cuales han causado furor en numerosos países a nivel mundial, adoptando en gran parte de ellos, una normativa que permite atribuirle mayor seguridad en el envío de información, aplicando algoritmos matemáticos que impiden a los denominados "*hackers*", tergiversar los contenidos de estos mensajes.

CERTIFICACIÓN ELECTRÓNICA

La certificación electrónica principalmente se enfoca en demostrar la identidad del firmante de un documento electrónico. La SUSCERTE "Certificado

Electrónico" (http://www.suscerte.gob.ve/index.php/es/certificacion), expone sobre la certificación electrónica lo siguiente:

> La Certificación Electrónica es un área que involucra políticas, procedimientos, infraestructura, estándares y equipamiento, que hacen posible el ciclo de vida de un certificado y su uso, con las garantías que dictan los estándares de seguridad electrónica. Esto permite al usuario confiar en operaciones como la firma electrónica, correo electrónico seguro, fecha y hora certificada, entre otras.

Concatenado a esto, Martínez (2000) sostiene que la certificación electrónica permite "vincular un dato de verificación de firma (una clave pública, en el caso de criptografía asimétrica) a una persona determinada" (p. 103).

Por su parte, Rico (2005) lo trata como "requisito necesario para equiparar jurídicamente la firma electrónica con la tradicional" (p. 239).

Se considera apropiada la definición del autor Martínez, ya que el requisito de la criptografía asimétrica es la esencia de un certificado electrónico. De esta forma permite vincular a una determinada persona la verificación de una firma electrónica.

Por su parte, la SUSCERTE define al certificado electrónico "Certificado Electrónico" (http://www.suscerte.gob.ve/index.php/es/certificacion) como:

> Es un documento electrónico emitido por un Proveedor de Servicios de Certificación, que vincula a un usuario (signatario) con su firma electrónica, el mismo está compuesto por dos elementos (clave pública y clave privada), con el cual se identifica

al propietario del mismo y permite la generación de firmas electrónicas. Para ello para firmar electrónicamente se requiere de un certificado electrónico.

Beneficios del Certificado Electrónico.

De acuerdo a la SUSCERTE "Certificado Electrónico" (http://www.suscerte.gob.ve/index.php/es/certificacion), los beneficios que conlleva el uso de un certificado electrónico se clasifican de la siguiente manera:

1. Se reducen los costos en impresión de documentos que necesiten aprobación mediante firma manuscrita.

2. Garantiza la identidad del ciudadano que realiza una gestión electrónica.

3. Proporciona confidencialidad, integridad y seguridad en Internet.

4. El contenido del documento electrónico no puede ser alterado.

5. Se agilizan los procesos de aprobación para documentos que requieran firma manuscrita.

6. El ciudadano puede realizar trámites y gestiones electrónicamente y obtener una respuesta inmediata sin tener que desplazarse.

7. Se apalanca efectivamente la lucha contra la burocracia y la corrupción.

8. Tiene el mismo valor jurídico que la firma manuscrita.

Proveedores de Servicios de Certificación (PSC).

El DLMDFE establece en su artículo 18, que la firma electrónica deberá ser debidamente certificada por un Proveedor de Servicios de Certificación (PSC), y en su Capítulo VI regula todo lo concerniente a requisitos para ser un PSC; acreditación ante la SUSCERTE; actividades de los PSC; obligaciones de los PSC; contraprestación del servicio; y notificación de cese de actividades.

De acuerdo al marco normativo anteriormente señalado, se debe concluir que los PSC son personas naturales o jurídicas que cumplan con los requisitos expresamente previstos en el artículo 31 del DLMDFE, y que se encuentren debidamente acreditados ante la SUSCERTE de acuerdo al artículo 32 del referido Decreto, cuyo objeto sea crear y certificar las firmas electrónicas mediante el otorgamiento de los Certificados Electrónicos, y que realicen las actividades previstas en el artículo 34 del DLMDFE.

El artículo 31 del DLMDFE señala como requisitos para ser un PSC los siguientes:

> 1. La capacidad económica y financiera suficiente para prestar los servicios autorizados como Proveedor de Servicios de Certificación. En el caso de organismos públicos, éstos deberán contar con un presupuesto de gastos y de ingresos que permitan el desarrollo de esta actividad.
> 2. La capacidad y elementos técnicos necesarios para proveer Certificados Electrónicos.
> 3. Garantizar un servicio de suspensión, cancelación y revocación, rápido y seguro, de los Certificados Electrónicos que proporcione.

> 4. Un sistema de información de acceso libre, permanente, actualizado y eficiente en el cual se publiquen las políticas y procedimientos aplicados para la prestación de sus servicios, así como los Certificados Electrónicos que hubiere proporcionado, revocado, suspendido o cancelado y las restricciones o limitaciones aplicables a éstos.
>
> 5. Garantizar que en la emisión de los Certificados Electrónicos que provea se utilicen herramientas y estándares adecuados a los usos internacionales, que estén protegidos contra su alteración o modificación, de tal forma que garanticen la seguridad técnica de los procesos de certificación.
>
> 6. En caso de personas jurídicas, éstas deberán estar legalmente constituidas de conformidad con las leyes del país de origen.
>
> 7. Personal técnico adecuado con conocimiento especializado en la materia y experiencia en el servicio a prestar.
>
> 8. Las demás que señale el reglamento de este Decreto-Ley.
>
> El incumplimiento de cualesquiera de los requisitos anteriores dará lugar a la revocatoria de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica, sin perjuicio de las sanciones previstas en este Decreto-Ley.

Tal como se observa del artículo anterior, los PSC pueden ser públicos o privados, tal como lo indica Chacón (2005) cuando señala que “pueden ser de naturaleza pública o privada, en el primer supuesto será un funcionario público que tenga delegada una función pública. Y en el segundo caso, atiende a un profesional libre que actúa en el mercado de la libre competencia” (p. 73).

Cabe destacar, que la certificación electrónica por parte de un PSC de un mensaje de datos le otorga el valor probatorio de un documento privado entre las partes, por cuanto los PSC no tienen las facultades delegadas por parte de la Administración Pública para dar fe pública a un documento.

Al respecto, Jedlicka (2004) señala que:

> Los PSC no están investidos legalmente de las facultades necesarias para dar fe pública por lo que, solo si el mensaje de datos es autorizado o generado electrónicamente por un Registrador, Juez o Notario, o algún otro funcionario público que efectivamente esté investido de dicha facultad para dar fe pública, es que verdaderamente se podría equiparar el mensaje de datos a un documento público, ello independientemente de que dicho mensaje haya sido certificado o no por un PSC (p. 197).

En cuanto a la acreditación de los PSC por parte de la SUSCERTE, tal como se exige en el artículo 32 del DLMDFE, el artículo 3 del Reglamento Parcial del DLMDFE señala expresamente cuales son los documentos y recaudos que deben presentar las personas que quieran acreditarse como PSC. Los referidos documentos y recaudos están dirigidos a demostrar los requisitos exigidos por el DLMDFE, tales como que tenga la capacidad económica y financiera para prestar los servicios como PSC, descripción detallada de la infraestructura física y tecnológica, personal calificado, sistemas de seguridad que utilicen, herramientas y estándares adecuados a los usos internacionales, entre otros.

El artículo 34 del DLMDFE señala que las actividades que deben realizar los PSC, en relación con los mensajes de datos, firmas electrónicas y certificados electrónicos son las siguientes:

1. Proporcionar, revocar o suspender los distintos tipos o clases de Certificados Electrónicos.

2. Ofrecer o facilitar los servicios de creación de Firmas Electrónicas.

3. Ofrecer servicios de archivo cronológicos de las Firmas Electrónicas certificadas por el Proveedor de Servicios de Certificación.

4. Ofrecer los servicios de archivo y conservación de mensajes de datos.

5. Garantizar Certificados Electrónicos proporcionados por Proveedores de Servicios de Certificación extranjeros.

6. Las demás que se establezcan en el presente Decreto-Ley o en sus reglamentos.

Los Certificados Electrónicos proporcionados por los Proveedores de Servicios de Certificación garantizarán la validez de las Firmas Electrónicas que certifiquen, y la titularidad que sobre ellas tengan sus Signatarios.

En cuanto a las obligaciones de los PSC, el DLMDFE en su artículo 35, señala lo siguiente:

1. Adoptar las medidas necesarias para determinar la exactitud de los Certificados Electrónicos que proporcionen y la identidad del Signatario.

2. Garantizar la validez, vigencia y legalidad del Certificado Electrónico que proporcione.

3. Verificar la información suministrada por el Signatario para la emisión del Certificado Electrónico.

4. Mantener en medios electrónicos o magnéticos, para su consulta, por diez (10) años siguientes al vencimiento de los Certificados Electrónicos que proporcionen, un archivo cronológico con la información relacionada con los referidos Certificados Electrónicos.

5. Garantizar a los Signatarios un medio para notificar el uso indebido de sus Firmas Electrónicas.

6. Informar a los interesados en sus servicios de certificación, utilizando un lenguaje comprensible en su página en la Internet o en cualquier otra red mundial de acceso público, los términos precisos y condiciones para el uso del Certificado Electrónico y, en particular, de cualquier limitación sobre su responsabilidad, así como de los procedimientos especiales existentes para resolver cualquier controversia.

7. Garantizar la integridad, disponibilidad y accesibilidad de la información y documentos relacionados con los servicios que proporcione. A tales efectos, deberán mantener un respaldo confiable y seguro de dicha información.

8. Garantizar la adopción de las medidas necesarias para evitar la falsificación de Certificados Electrónicos y de las Firmas Electrónicas que proporcionen.

9. Efectuar las notificaciones y publicaciones necesarias para informar a los signatarios y personas interesadas acerca del vencimiento, revocación, suspensión o cancelación de los Certificados Electrónicos que proporcione, así como de cualquier otro aspecto de relevancia para el público en general, en relación con dichos Certificados Electrónicos.

10. Notificar a la Superintendencia de Servicios de Certificación Electrónica cuando tenga conocimiento de cualquier hecho que pueda conllevar a su Inhabilitación Técnica.

El incumplimiento de cualesquiera de los requisitos anteriores dará lugar a la suspensión de la acreditación otorgada por la Superintendencia de Servicios de Certificación Electrónica, sin perjuicio de las sanciones establecidas en el presente Decreto-Ley.

En el artículo 12 del Reglamento Parcial del DLMDFE, se establecen igualmente otras obligaciones para los PSC:

1. Comprobar presencialmente la identidad de los solicitantes de los Certificados Electrónicos y verificar cualesquiera otras circunstancias relevantes, en forma previa a la expedición, conservando la documentación que respalda dicha identificación por el tiempo señalado en el numeral 4 del artículo 35 del Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas.

2. Mantener a disposición permanente del público en su página Web o en cualquier otra red mundial de acceso público y con un acceso desde su página inicial, la declaración de prácticas de certificación y las políticas de certificados vigentes.

3. Cumplir cabalmente con las políticas de certificados y la declaración de prácticas de certificación vigente.

4. Informar en la forma establecida en el numeral 4 del artículo 31 y numeral 6 del artículo 35 del Decreto Ley Sobre Mensajes de Datos y Firmas Electrónicas, el nivel de confiabilidad de sus certificados electrónicos, los límites de responsabilidad del Proveedor de Servicios de Certificación y las obligaciones que el signatario asume como usuario del servicio de certificación.

5. Garantizar la prestación permanente e ininterrumpida del servicio. Quedan a salvo las suspensiones que autorice la Superintendencia de Servicios de Certificación Electrónica de conformidad con la Ley y sus reglamentos.

6. Garantizar de manera fácil y permanente el acceso de los signatarios y terceros al repositorio.

7. Informar a la Superintendencia de Servicios de Certificación Electrónica de manera inmediata, cualquier evento que comprometa la prestación del servicio.

8. Abstenerse de almacenar los datos de generación de firma del signatario y garantizar un método de creación de los mismos, que impida mantener copia una vez que éstos hayan sido entregados al signatario.

9. Mantener actualizado el registro de los certificados electrónicos revocados.

10. Informar al signatario dentro de las veinticuatro horas siguientes de la suspensión o revocatoria de su Certificado Electrónico.

11. Mantener el control exclusivo de sus datos de generación de firma electrónica como Proveedor de Servicios de Certificación, y establecer las medidas de seguridad necesarias para que ésta no se divulgue o comprometa.

Otro aspecto en el que hace énfasis el Reglamento Parcial del DLMDFE, es e la obligación que tienen los PSC de crear y aplicar políticas, planes y procedimientos de seguridad, tal como lo indica en su artículo 34:

1. Políticas y procedimientos de seguridad de las instalaciones físicas y los equipos.

2. Políticas de acceso a los sistemas e instalaciones del proveedor y monitoreo constante de los mismos.

3. Planes y procedimientos de actualización de hardware y software, utilizados para la operación de Proveedores de Servicios de Certificación.

4. Planes y procedimientos de contingencia en cada uno de los riesgos potenciales que atenten en contra del funcionamiento del Proveedor de Servicios de Certificación, según estudio que se actualizará periódicamente.

5. Plan de manejo, control y prevención de virus informático.

Tal como se indicó anteriormente, en la actualidad solo existen dos PSC en el país acreditados por la SUSCERTE, los cuales son: la Fundación Instituto de Ingeniería para la Investigación y Desarrollo Tecnológico, y la empresa privada Procert, C.A.

FIRMA ELECTRÓNICA

El DLMDFE define en su artículo 2 a la firma electrónica de la forma siguiente “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”.

Una definición básica de la firma electrónica es que consiste en una firma realizada por medios electrónicos, específicamente códigos que pueden ser caracteres. Es decir, la firma electrónica es un esquema matemático, o un método criptográfico que contiene datos electrónicos que permiten identificar a la persona que la suscribe, vincular a dicha persona con el mensaje de datos, y garantizar que el contenido del mensaje de datos no fue alterado.

La Ley Modelo de UNCITRAL sobre comercio electrónico en su artículo 2 define la firma electrónica como “datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información recogida en el mensaje de datos”.

Por otra parte, la Ley Española 59/2003 de Firma Electrónica, en su artículo 3.2 señala que la firma electrónica:

> (…) permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Asimismo, la Ley Española 59/2003 de Firma Electrónica define a la firma electrónica en su artículo 3.3, como una especie de firma “basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma”.

El DLMDFE en cuanto al cumplimiento de solemnidades y formalidades señala en su artículo 6 que el requisito de la firma autógrafa en los actos o negocios jurídicos, quedará satisfecho cuando los mensajes de datos tengan asociada una firma electrónica.

Lo expuesto anteriormente, es ratificado por el artículo 16 del DLMDFE cuando establece que:

> 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.
>
> A los efectos de este artículo, la Firma Electrónica podrá formar parte integrante del Mensaje de Datos, o estar inequívocamente asociada a éste; enviarse o no en un mismo acto.

El artículo 18 del DLMDFE señala que los requisitos arriba expuestos se cumplirán en los casos en que la firma electrónica esté debidamente certificada por un PSC. Estableciendo en su artículo 17, la consecuencia de que una firma electrónica no cumpla con esos requisitos, la cual consiste en que el Juez de un proceso judicial la valorará de acuerdo a su sana crítica.

Ahora bien, a pesar de que la firma electrónica debe ser certificada por un PSC, ello no implica que los usuarios o signatarios de la misma no tienen responsabilidades y obligaciones. Al respecto, el artículo 19 del DLMDFE establece las siguientes obligaciones:

> 1. Actuar con diligencia para evitar el uso no autorizado de su Firma Electrónica.
>
> 2. Notificar a su Proveedor de Servicios de Certificación que su Firma Electrónica ha sido controlada por terceros no autorizados o indebidamente utilizada, cuando tenga conocimiento de ello.

> El Signatario que no cumpla con las obligaciones antes señaladas será responsable de las consecuencias del uso no autorizado de su Firma Electrónica.

Por otra parte, también existe la posibilidad de que en un proceso judicial se le pida a un tercero (propietario o administrador del sistema informático en que se encuentre el correo electrónico), aunque dicho tercero no esté certificado por la SUSCERTE. Siendo el caso que la respuesta que se obtenga de ese tercero podrá certificar o invalidar la autoría de la persona o por lo menos identificación de la computadora de donde se emitió el mensaje, las transacciones que se realizaron, y la fecha y hora de las mismas. En ese caso, el medio probatorio a utilizar previsto en el CPC así como en otras normas procesales especiales es la prueba de informes.

A su vez, Rico (2005) señala que "el legislador venezolano reconoce el uso de la firma electrónica en forma amplia y le otorga valor jurídico independientemente de las características tecnológicas empleadas para firmar en respeto al principio de neutralidad tecnológica" (p. 201).

Ahora bien, el hecho de que una firma electrónica esté debidamente certificada por un PSC adscrito a la SUSCERTE representa para el usuario una serie de ventajas, tales como la garantía de autenticidad del origen del mensaje, no repudio por parte del autor del mensaje, imposibilidad de suplantación por otro contenido, integridad de la información, e identificar y rastrear las operaciones realizadas, de las cuales no podría ser beneficiario sino aplica dicho mecanismo.

CRIPTOGRAFÍA Y FIRMA DIGITAL

De acuerdo a Martínez (2000), la criptografía es la ciencia que se encarga de la transformación de un mensaje, a tal punto de hacerlo ininteligible para posteriormente, devolverlo a su estado inicial.

Concatenado a esto, la autora Rico (2005) expone que la criptografía es "el cifrado de la información es un instrumento de seguridad que permite la transformación de un mensaje ininteligible (en claro), en otro ininteligible (texto cifrado), mediante ciertas operaciones matemáticas denominadas algoritmos" (p. 189).

Por lo tanto, corresponde a una de las formas más eficientes para la protección y confidencialidad de la información transferida usando las denominadas redes electrónicas abiertas.

Dicho esto, existen dos tipos de criptografía, la Criptografía Simétrica y la Criptografía Asimétrica.

Criptografía simétrica.

Este esquema de criptosistema simétrico corresponde a la utilización de dos claves entre el emisor y el receptor. Es decir, deben compartir una misma clave que es acordada entre ellos para cifrar y descifrar un mensaje, lo que implica que no puede ser divulgada a terceros, ya que en ese caso el mensaje transmitido podría no ser auténtico.

El autor Martínez (2000), explica la Criptografía Simétrica de la siguiente manera:

> Con los criptosistemas simétricos, en el proceso de cifrado y descifrado las partes deben compartir una clave en común que es usada para cifrar y descifrar, y que es acordado de forma previa. Esta clave debe ser secreta para evitar el acceso no autorizado a datos confidenciales (p. 46).

Por su parte, la autora Rico (2005) define la criptografía simétrica como:

> Los sistemas simétricos son conocidos también como sistemas clásicos, convencionales, de clave única, compartida o de clave secreta en razón que precisan de una clave única, común e idéntica, conocida tanto por el emisor como por el receptor del mensaje, utilizándose esta para cifrar y descifrar la información. La autenticidad de los mensajes se consigue siempre y cuando los usuarios mantengan la clave en secreto (p. 191).

Cabe destacar, que la transmisión de información entre las partes que hacen uso de esta criptografía resultaría eficaz, únicamente si ellas (emisor y receptor de un mensaje) mantienen en secreto la clave privada o la clave acordada previamente. Es la única manera que tienen para determinar la autenticidad de la misma.

Por otro lado, tenemos otro tipo de criptografía, que es quizás la más usada por los que manejan estas tecnologías, ya que es mucho más segura al momento de la transmisión de datos, garantizando así la confidencialidad, integridad y no repudio. Esta es la llamada criptografía asimétrica.

Criptografía asimétrica.

Este tipo de criptografía es mucho más definida, ventajosa y válida tanto para el derecho como para el comercio electrónico. Es un mecanismo que se emplea para dar seguridad y autenticidad al documento que permite mediante un conjunto de claves asociadas, que se pueda mantener un mensaje que no sea modificado por una persona, salvo por quien creó el mensaje.

De acuerdo a Martínez (2000), este esquema de criptografía se basa principalmente en un par de claves asociadas entre sí, siendo el caso que "si bien las claves están relacionadas entre sí por el criptosistema asimétrico, hace virtualmente imposible que personas que conozcan la clave pública puedan derivar de ella la clave privada" (p. 50).

La clave privada solo es conocida por el titular de la misma, e incluso puede que no la conozca, ya que puede estar contenida en un dispositivo biométrico, *token* o incluso puede darse mediante un huella digital. Esta clave debe permanecer en secreto, ya que si se conoce por terceros haría ineficaz el uso de esta criptografía. Por otro lado tenemos la clave pública, la cual es de conocimiento público y es matemáticamente relacionada con la primera.

En relación a esto, Rico (2005) expresa lo siguiente:

> En los sistemas asimétricos, el emisor y el receptor del mensaje disponen cada uno de dos claves matemáticamente relacionadas entre si: una pública que deben revelar y publicar y otra privada que deben mantener en secreto. Una vez que los números primos (que actúan como clave pública) se multiplican entre sí, se obtiene otro de longitud aún mayor (la clave privada) resultando casi

> imposible determinar cuáles fueron los dos números primos que dieron origen a este último (p. 193).

Continúa exponiendo que “la clave privada se utiliza para firmar el mensaje y descifrar lo que se recibe con la correspondiente clave pública, mientras que la clave pública solo permite cifrar la información y descifrarla si ha sido cifrada con su pareja correspondiente (la clave privada)” (p. 193).

De acuerdo a Martínez (2000), con el uso del criptosistema asimétrico, una persona que tenga el mensaje inicial y la clave pública del firmante puede determinar de manera segura lo siguiente:

> Si la transformación fue realizada usando la clave privada que corresponde a la clave pública del firmante; y se satisface así la necesidad de autenticación, porque si un mensaje fue firmado con la clave privada de un sujeto, solo puede ser verificado por el receptor utilizando la clave pública de ese mismo sujeto.
>
> Si el mensaje inicial ha sido alterado desde la transformación; y se satisface la exigencia de integridad, pues, si el mensaje ha sido alterado en lo más mínimo, su resumen no coincidirá con el resumen firmado del mismo descifrado aplicando la clave pública de su emisor; y si el mensaje firmado ha sido alterado no coincidirá con el resumen del mensaje en claro (p. 52).

REGULACIÓN DE LAS FIRMAS ELECTRÓNICAS SEGÚN EL DECRETO LEY SOBRE MENSAJES DE DATOS Y FIRMAS ELECTRÓNICAS

Las firmas electrónicas deben cumplir con una serie de requisitos que permitan atribuirles eficacia probatoria, para de esta forma poder considerarlas una firma segura.

En este orden, el DLMDFE establece ciertos requisitos necesarios para otorgarle al documento electrónico el mismo valor probatorio que a la firma autógrafa, para lo cual su artículo 16 norma lo siguiente:

> 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.

De lo anterior, se puede resaltar que el artículo enuncia tres requisitos, los cuales son esenciales para darle autenticidad a un documento electrónico y así darle la misma eficacia probatoria que un documento escrito con firma autógrafa. Ahora bien, dentro de los requisitos se puede encontrar que el mensaje de datos debe permanecer íntegro, por lo que la firma electrónica busca sostener la probidad de los documentos electrónicos, a fin de prevenir y localizar cualquier modificación posterior.

Sin embargo, hoy en día resulta sencillo alterar un mensaje de datos, es por ello que la ley busca ofrecer seguridad a los documentos electrónicos a través del uso de la firma electrónica. Siendo el caso que, una vez enviado el mensaje de datos con su respectiva firma debidamente certificada por la autoridad competente, según lo

establecido en el artículo 18 del DLMDFE, se le garantiza al receptor que el contenido del mensaje no podrá ser alterado. En caso de reenviar o modificar el contenido del mismo buscando otro propósito, inmediatamente perderá su autenticidad, ya que no podría atribuírsele la autoría al mensaje.

Ahora bien, el artículo 17 del DLMDFE hace referencia a que cuando la firma electrónica no cumpla con los requisitos antes mencionados no tendrá los mismos efectos jurídicos que el DLMDFE le otorga en cuanto a su valor probatorio. Sin embargo, si no cumple con los requisitos del artículo anterior, no implica que dicho documento no pueda ser usado como medio de convicción en el proceso, de acuerdo a las reglas de la sana crítica establecidas en el CPC.

Por otro lado, según lo establecido en el artículo 19 del DLMDFE el signatario de una firma electrónica es aquella persona que emite un mensaje electrónico. El signatario es quien, según el precitado Decreto Ley, debe guardar la suficiente prudencia para que de esta manera, terceros o personas no autorizadas se abstengan del uso no permitido de la firma electrónica.

Es responsabilidad del signatario notificar a su respectivo proveedor de certificados electrónicos, si su firma electrónica fue utilizada por otra persona sin su autorización o incluso apropiada indebidamente por un tercero. Si este no cumple con su deber, será el responsable por haberle dado un uso distinto a dicha firma. Esto último, implica el deber de todo poseedor de un certificado electrónico, a su cuidado y uso adecuado del mismo, toda vez que la imprudencia en su uso podría acarrear diversas consecuencias para el signatario.

Finalmente, vista la implicación legal que posee la firma electrónica en el ordenamiento jurídico venezolano, se deben tener claros ciertos aspectos que ayudan a entender con mayor facilidad lo relacionado a lo ofertado por los PSC.

SUPERINTENDENCIA DE SERVICIOS DE CERTIFICACIÓN ELECTRÓNICA (SUSCERTE) COMO AUTORIDAD DE CERTIFICACIÓN DE FIRMAS ELECTRÓNICAS

Existe un órgano en Venezuela encargado de velar por el uso de los llamados "certificados digitales" y "firma digital", que permite garantizar la autenticidad de un mensaje enviado a terceras personas que hagan uso de esta tecnología. Cabe destacar la importancia que tiene esta actividad, ya que como se ha explicado, un mensaje de datos (correo electrónico) sin firma electrónica, es un documento cuya valoración se complica debido a que es difícil comprobar la autoría de un mensaje enviado sin conocer quién es el emisor del mismo.

Por tal razón, la aplicación de una firma electrónica puede cambiar la situación mencionada, toda vez que, si se envía un mensaje de datos aplicando la llamada firma electrónica, se podría garantizar que la información contenida en el mensaje es auténtica en toda su extensión. Es decir, se tendría la seguridad de que el mensaje no sufrió ninguna transformación en el trayecto hacia su destino. Esto último, se garantiza gracias a un PSC, que avala tal certificado, y logra de esta manera el no repudio de la información contenida en un mensaje de datos.

Los PSC deben estar debidamente adscritos a la SUSCERTE, que es el órgano que certifica a su vez que los PSC cumplan con todo lo exigido por el DLMDFE para garantizar la autenticidad de la firma electrónica y el certificado electrónico.

La SUSCERTE "Quiénes somos" (http://www.suscerte.gob.ve/index.php/es/la-institucion) se define como institución de la siguiente manera:

> Es el encargado de coordinar e implementar el modelo jerárquico de la Infraestructura Nacional de Certificación Electrónica, también acredita, supervisa y controla a los Proveedores de Servicios de Certificación (PSC) y es el ente responsable de a Autoridad de Certificación Raíz del Estado venezolano.

La SUSCERTE es un órgano desconcentrado y sin personalidad jurídica, que fue creado mediante la promulgación del DLMDFE del año 2001. Este órgano es el encargado de velar por la implementación de todo lo relacionado con la Certificación Electrónica a los documentos digitales. A su vez, es un órgano que tiene como objetivos: otorgar, conferir y vigilar a los llamados PSC, y es a éste a quien se le atribuye la responsabilidad de garantizarle a los particulares que hacen uso de los certificados electrónicos, la autenticidad de los mensajes transmitidos. Dicho esto, es un órgano que ha tomado la iniciativa en fomentar el uso de las tecnologías de la información a empresas públicas y privadas, para mejorar su funcionamiento interno y proporcionar un manejo y uso seguro de la información que circula dentro de las mismas, garantizando la autenticidad de los mensajes de datos enviados.

La SUSCERTE actualmente ha acreditado a dos instituciones, una de carácter público denominada Fundación Instituto de Ingeniería para la Investigación y Desarrollo Tecnológico (FIIDT), y otra privada que lleva por nombre Procert, C.A, los cuales son los encargados de proveer los certificados electrónicos para aquellas personas interesadas en adquirirlas.

Una vez determinados los mecanismos existentes en el ordenamiento jurídico venezolano para garantizar la autenticidad del correo electrónico, en el siguiente capítulo se especifican los medios probatorios para hacer valer un correo electrónico en un juicio, las formas de ejercer el control y contradicción de la prueba, y

finalmente la valoración de los mismos en el cuerpo normativo vigente, la doctrina y la jurisprudencia nacional.

CAPÍTULO III. LOS MENSAJES DE DATOS COMO MEDIO DE PRUEBA EN EL PROCESO CIVIL VENEZOLANO

Actualmente, a pesar de que existen dos PSC adscritos a la SUSCERTE en el país, y que pueden proveer a los particulares de certificados electrónicos, en la práctica los certificados electrónicos y las firmas electrónicas no son comúnmente utilizados entre los particulares al momento de realizar actuaciones mediante medios electrónicos. Sin embargo, cada vez son más frecuentes las relaciones y situaciones jurídicas que se configuran en las que se encuentran involucradas los medios electrónicos, y más específicamente los mensajes de datos o correos electrónicos.

En ese sentido, si bien tal como se ha indicado anteriormente el DLMDFE le otorga a la firma electrónica debidamente certificada por los PSC el mismo carácter de la firma autógrafa, y en consecuencia se equipara el documento electrónico al documento escrito, procesalmente la situación se vuelve compleja cuando el correo electrónico no cuenta con una firma electrónica o con un certificado electrónico.

Cabe destacar, que la legislación adjetiva venezolana que regula las normas y procedimientos en los procesos judiciales en diversas materias, así como en los procedimientos administrativos, tiene su base en el Código Civil y el CPC, los cuales fueron creados en una época donde no existía o no era para nada frecuente la utilización de medios electrónicos en los negocios jurídicos.

En consecuencia, si bien algunas normas procesales de reciente data involucran el uso de los medios electrónicos, las mismas usualmente señalan que en los asuntos no previstos por ellas se aplicarán las previsiones contenidas en el Código Civil y en el CPC.

Aunado a lo anteriormente expuesto, el DLMDFE es confuso cuando por una parte señala que los mensajes de datos tendrán el mismo valor probatorio que los documentos escritos, pero luego cuando se refiere a las formas procedimentales para promoverlo en un juicio indica que se aplicarán las normas previstas para las pruebas libres.

El ordenamiento jurídico venezolano se caracteriza por el principio de libertad probatoria, consagrado en nuestra Constitución, cuando en su artículo 49 señala que toda persona tiene derecho de disponer de los medios adecuados para ejercer su defensa. Este principio es ratificado en el CPC cuando se establece la prueba libre, que permite a las partes traer al proceso cualquier otro medio de prueba distinto a los expresamente previstos en las normas, siempre y cuando cumpla con determinados requisitos, los cuales se concentran en que básicamente la prueba no sea obtenida de forma ilegal, por cuanto la forma de su obtención no haya vulnerado los derechos de otras personas.

Específicamente, el artículo 395 del CPC es el que se refiere a la prueba libre, y de acuerdo a la exposición de motivos de dicho Código:

> Se consideró conveniente introducir una ampliación de los medios de prueba con el propósito de que el debate probatorio sea lo más amplio posible, y de que las partes puedan aportar cualquier otro medio no regulado expresamente en el Código Civil, haciendo posible de este modo, una mejor apreciación de los hechos por parte del Juez, y la posibilidad de una decisión basada en la verdad real y no solamente en la formal, procurándose además, de esto, una justicia más eficaz.

En cuanto al correo electrónico como un medio de prueba fidedigno, el autor Orta (2005) nos hace referencia a que:

> Uno de los grandes problemas con los que nos encontramos al tratar de incorporar estos hechos al proceso, es el pensar que las pruebas informáticas son fácilmente creadas, modificadas o destruidas y que por ello difícilmente podrían ser utilizados en un proceso judicial. La realidad es que dentro de la Criminalística o investigación científica judicial, se ha venido desarrollando una nueva disciplina denominada Informática Forense, la cual tiene como objeto el estudio de la Evidencia Digital (p. 1).

Igualmente, dicho autor señala que:

> En contraposición a lo que se piensa, es relativamente fácil determinar si una Evidencia Digital ha sido modificada o alterada a través de la comparación con su original o bien con el análisis de sus metadatos a los cuales haremos referencia más adelante.
>
> La Evidencia Digital no puede ser destruida fácilmente, tal como piensan los usuarios de ordenadores o computadoras, que creen que con ejecutar un comando de borrado (delete), ya ha desaparecido un documento o archivo objeto del mismo de la máquina (p. 3).

El artículo 2 del DLMDFE define el mensaje de datos, y establece que el mismo debe ser inteligible, que pueda ser almacenado o intercambiado por cualquier medio, y que debe contar con un soporte electrónico o similar.

Tal como se ha indicado anteriormente, el artículo 4 le atribuye a los mensajes de datos el mismo valor probatorio que se le otorga a los documentos escritos, más establece que su promoción, control, contradicción y evacuación se realizará conforme a lo previsto para las pruebas libres en el CPC.

Cabe destacar, que a pesar de que el DLMDFE les otorga el mismo valor probatorio a los mensajes de datos que a los documentos escritos, los mensajes de datos en la práctica se diferencian de los documentos escritos tanto en su forma de presentación, como en sus características. Esto genera como consecuencia, que cuando se pretende aplicar las normas procedimentales previstas para los documentos escritos se generan algunas confusiones o vacíos que deben ser complementados, lo cual debe realizarse no sólo bajo la figura de la prueba libre, sino promoviendo otros medios probatorios específicamente tarifados en el ordenamiento jurídico. Estos medios probatorios que se encuentran expresamente previstos hacen referencia a los documentos escritos, por lo que en muchas ocasiones pueden ser aplicados analógicamente a los mensajes de datos, tal como ocurre con la prueba de informes, exhibición de documentos y otras.

El DLMDFE es claro cuando señala que, dependiendo si el mensaje de datos cuenta con una firma electrónica certificada, el valor probatorio que le deberá otorgar el Juez es el de plena prueba, o de indicios en el caso en que no cuente con la firma electrónica certificada. Es decir, la eficacia probatoria de los mensajes de datos en un juicio dependerá de la forma en que se haya realizado.

Al respecto, Jedlicka (2004), señala que “los mensajes de datos tendrán eficacia probatoria en la medida en que se logre la convicción del Juez sobre la existencia, autenticidad e integridad de la información contenida en el mensaje” (p. 185).

Por su parte, Rico (2005) señala como requisitos de veracidad y autenticidad que un documento electrónico debe reunir para que sea admisible como medio de prueba los siguientes: 1) Calidad de los sistemas de elaboración y almacenamiento del documento; 2) Veracidad de la información; 3) Conservación del mensaje de datos para su posterior recuperación; 4) Legibilidad del mensaje de datos; 5) Identificación de los sujetos participantes y las operaciones realizadas; 6) Autenticidad del mensa de datos; y 7) Fiabilidad de los sistemas de autenticación del documento.

Es decir, en un proceso judicial la parte que promueve el mensaje de datos debe enfocarse en probar que el mismo es autentico, y para ello demostrar que se cumple con los requisitos indicados anteriormente por la doctrina. En ese sentido, se observa que no bastará con promover el mensaje de datos en su presentación tecnológica como prueba libre, o en una impresión como documental. Deberá entonces promoverse otros medios de prueba que le brinden al Juez la certeza de que el mensaje de datos se mantiene integro, por lo que la información que contiene es veraz; que se pueda identificar los sujetos participantes y las operaciones realizadas por ellos; y la autenticidad del mensaje de datos.

PROMOCIÓN DEL CORREO ELECTRÓNICO COMO PRUEBA Y MEDIOS DE IMPUGNACIÓN Y DESCONOCIMIENTO

En relación con los medios de promoción de pruebas con los cuales se puede hacer valer un correo electrónico en un proceso judicial, Di Totto (2005) señala lo siguiente:

> La gran versatilidad que caracteriza a la prueba electrónica le confiere a su vez una naturaleza múltiple, ya que comparte elementos propios de la prueba pericial, del documento y de la

> inspección o reconocimiento, según sean las circunstancias ocurridas y la calificación jurídica que merezcan los hechos punibles objeto de investigación.
>
> Cabe la posibilidad de que los rastros y soportes electrónicos deban presentarse, conjuntamente, como experticia, documento y reconocimiento o inspección, sin detrimento de su individualidad, cuando esa combinación aporte eficacia, utilidad y economía al proceso, sin embargo es menester revisarlos por separado con el objeto de distinguir cuándo sus características nos permiten elegir cuál de ellos proporciona la vía más idónea para convertir los soportes o rastros electrónicos en elementos de convicción procesal (p. 15).

Información que es complementada a su vez, por lo señalado por Orta (2005), cuando establece que:

> El Derecho Informático es un nuevo campo del Derecho, que agrega una nueva cantidad de elementos que pueden ser considerados probatorios. Las pruebas informáticas pueden plantearse independientemente en casos en los que los hechos jurídicos informáticos sean los principales de la causa, pero debemos tener presente que las pruebas sobre hechos informáticos pueden incidir sobre todo tipo de causas y procesos judiciales.
>
> A pesar de que se está tratando legal y doctrinariamente de enfocar las pruebas sobre hechos digitales hacia las pruebas libres, debemos tener en cuenta que los medios probatorios conocidos son útiles y conducentes. Las pruebas no electrónicas pueden servir también para probar los hechos informáticos, por lo que la promoción de experticias o pericias no debe ser el único medio de

> pruebas a tomar en consideración. La pericia informática puede ser insuficiente en muchos casos, por lo que es necesario aplicar la creatividad y el pensamiento crítico a efectos de poder buscar pruebas en el mundo informático (p. 33).

En cuanto a los medios probatorios mediante los cuales se puede promover en un juicio el correo electrónico, se tiene que el artículo 395 del CPC, establece cuatro grupos de medios de prueba, los cuales están situados en un mismo plano, y consisten en instrumentos que se otorgan a los sujetos procesales para trasladar al proceso hechos que verifiquen las afirmaciones de las partes, o permitan averiguar la existencia de una situación fáctica.

El DLMDFE en su exposición de motivos establece que en cuanto a la incorporación al proceso judicial el mensaje de datos tiene la misma eficacia probatoria de los documentos escritos, y se remite a las formas procedimentales reguladas para los medios de prueba libre, contenidas en el artículo 395 del CPC. Esto lo observamos específicamente en su artículo 4, en el cual se señala que los mensajes de datos tendrán la misma eficacia probatoria que la ley otorga a los documentos escritos, por lo que su promoción, control, contradicción y evacuación como medio de prueba, se realizará conforme a lo previsto para las pruebas libres en el CPC.

También, esta Ley señala que 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. Dicha eficacia consiste en que las mismas serán consideradas fidedignas si las mismas no son impugnadas por la parte contra quien se promueven en un juicio. Así, la eficacia de los documentos privados

está condicionada, tanto por el CC en su artículo 1363 ([9]), como por el CPC en su artículo 444 ([10]) a su previo reconocimiento.

También, la Ley Especial contra los Delitos Informáticos en su artículo 2, equipara el documento escrito a cualquier soporte o rastro que reúna los requisitos de fidelidad y perdurabilidad sobre los cuales se sustente la seguridad o certeza de su contenido.

Otro punto importante, a la hora de promover un correo electrónico como prueba, es que la misma puede ser ilegal si viola derechos y garantías constitucionales. Ello, por cuanto la Constitución en su artículo 48 establece el derecho a la inviolabilidad de la correspondencia en todas sus formas, por lo que comprende al correo electrónico.

En cuanto a la eficacia probatoria de los correos electrónicos, el DLMDFE en su artículo 4, le atribuye a los mensajes de datos y firmas electrónicas 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.

[9] Artículo 1363. El instrumento privado reconocido o tenido legalmente por reconocido, tiene entre las partes y respecto de terceros, la misma fuerza probatoria que el instrumento público en lo que se refiere al hecho material de las declaraciones; hace fe, hasta prueba en contrario, de la verdad de esas declaraciones.

[10] Artículo 444. 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 en que ha sido producido, cuando lo fuere posteriormente a dicho acto. El silencio de la parte a este respecto, dará por reconocido el instrumento.

En cuanto a la validez y eficacia de la firma electrónica, dicha Ley señala en su artículo 16 que tiene la misma validez y eficacia que la firma autógrafa siempre que cumpla con los requisitos exigidos por ella.

Sin embargo, a pesar de que la valoración del correo electrónico está establecida bajo el sistema de la tarifa legal, en los casos en que no cumpla con los requisitos señalados por la Ley, la Ley en referencia le permite al Juez valorar la prueba de acuerdo al sistema de la sana crítica, tal como lo establece en su artículo 17.

En relación con la forma de promover un mensaje de datos o un correo electrónico, la doctrina presenta dos vertientes, que se resumen en promoverlo de acuerdo a las normas previstas para los documentos escritos, o promoverlo de acuerdo a la prueba libre.

La corriente doctrinal que señala que el mensaje de datos debe promoverse bajo las normas aplicables a los documentos escritos, se ve representada por Rico (2005), quien señala que deben ser promovidos como una prueba documental, con la ayuda de otros medios probatorios como la experticia o inspección judicial para demostrar su integridad y autenticidad. Además explica que debe ser incorporado al proceso con la demanda, salvo los casos en que pueda incorporarse posteriormente al proceso. Finalmente, concluye que es importante contratar los servicios de un PSC por cuanto permitirá dejar constancia del momento, lugar, hora y fecha de remisión del mensaje de datos al tribunal.

Por otra parte, un autor que mantiene la posición de promover los mensajes de datos necesariamente como prueba libre es Jedlicka (2004), el cual señala que:

> De acuerdo a la tecnología vigente en este momento y, considerando el soporte electrónico o similar que tienen los mensajes de datos, en principio no es posible traer físicamente al expediente de un proceso judicial el original del mensaje de datos, para que repose en los autos de la misma manera que podría hacerlo el original de un documento escrito, cuyo soporte es instrumental (p. 185).

Esa imposibilidad física de traer el mensaje de datos al expediente como si fuera un documento escrito justifica, según afirma Jedlicka (2004), lo siguiente:

> La aplicación del procedimiento de pruebas libres para la producción de mensajes de datos en juicio pues, implica la utilización analógica de las reglas de promoción, control, contradicción y evacuación previstas para aquellos medios de prueba legales que más se asemejen al mensaje de datos de que se trate, estableciéndose así una de las diferencias fundamentales de este medio de prueba con los documentos escritos en papel (p. 186).

Ahora bien, un aspecto difícil de diferenciar en un proceso judicial es cuando se considera que el mensaje de datos es original y cuando es una copia. Además de lo expuesto en el artículo 7 del DLMDFE sobre la integridad del mensaje de datos, Rico (2005) indica como requisitos para considerar un mensaje de datos como original que se conserve íntegro y sin alteraciones desde su emisión; que pueda ser presentado ante terceros; y que pueda recuperarse posteriormente.

En el caso de las impresiones o reproducciones del mensaje de datos impresas en soporte de papel, el artículo 4 del DLMDFE establece que la información

contenida en un mensaje de datos tendrá la misma eficacia probatoria otorgada por la ley a las copias o reproducciones fotostáticas. En consecuencia, pareciera que de acuerdo al DLMDFE siempre serán necesarios otros medios probatorios que ratifiquen la validez del mensaje de datos en un proceso, a diferencia del documento escrito que es presentado en original en un juicio.

En relación con la impresión del mensaje de datos, Jedlicka (2004) señala que:

> Para el caso de mensaje de datos impresos que por sus características sean equivalentes a un documento privado, tendrá eficacia probatoria sólo en la medida en que dicha impresión sea reconocida por la parte contra la cual ha sido producida y, para el caso de mensajes de datos impresos cuya eficacia probatoria sea equivalente a un instrumento público o privado reconocido, tales impresiones podrían considerarse como copias fidedignas del mensaje de datos, de acuerdo al artículo 429 CPC, si no fueren impugnadas por el demandado en la contestación de la demanda, de haberse producido con el libelo, o dentro de los cinco días siguientes, si han sido producidas con la contestación o en el lapso de promoción de pruebas (p. 193).

Igualmente, Jedlicka (2004) sostiene que:

> El reconocimiento expreso o tácito realizado por la parte contra la cual se opone un mensaje de datos impreso, liberará la carga probatoria que tiene el promovente de demostrar el contenido, integridad y autenticidad del mensaje de datos y le atribuirá la misma eficacia probatoria que tendría un documento reconocido (p. 194).

Es decir, si el correo electrónico es promovido durante el juicio como una impresión, y de acuerdo a la ley aplicable tiene el mismo valor de una copia fotostática, el mismo estará sujeto a lo que establece el artículo 429 ([11]) del CPC, cuando señala que las copias fotostáticas se tendrán como fidedignas siempre que no sean impugnadas por la parte contra quien se promueven. Aunado a ello, tal como se indicó anteriormente se encuentra sujeta a las normas de reconocimiento del documento privado, y de tacha del documento público de ser el caso.

De acuerdo a lo anteriormente expuesto, el mensaje de datos debe ser promovido con la demanda o recurso, si se trata de un documento fundamental para demostrar la pretensión demandada o solicitada, tal como lo indica el artículo 340 del CPC. Cabe destacar, que el resto de las normas procesales en el ordenamiento venezolano ha adoptado este requisito procesal para la admisibilidad de las demandas, querellas o recursos.

En el caso de que el mensaje de datos no sea un documento fundamental del cual se desprenda el derecho alegado, el mismo podrá ser promovido en la etapa de promoción de pruebas.

---

[11] Artículo 429. Los instrumentos públicos y los privados reconocidos o tenidos legalmente por reconocidos, podrán producirse en juicio originales o en copia certificada expedida por funcionarios competentes con arreglo a las leyes.
Las copias o reproducciones fotográficas, fotostáticas o por cualquier otro medio mecánico claramente inteligible, de estos instrumentos, se tendrán como fidedignas si no fueren impugnadas por el adversario, ya en la contestación de la demanda, si han sido producidas con el libelo, ya dentro de los cinco días siguientes, si han sido producidas con la contestación o en el lapso de promoción de pruebas. Las copias de esta especie producidas en cualquier otra oportunidad, no tendrán ningún valor probatorio si no son aceptadas expresamente por la otra parte.
La parte que quiera servirse de la copia impugnada, podrá solicitar su cotejo con el original, o a falta de éste con una copia certificada expedida con anterioridad a aquella. El cotejo se efectuará mediante inspección ocular o mediante uno o más peritos que designe el Juez, a costa de la parte solicitante. Nada de esto obstará para que la parte produzca y haga valer el original del instrumento o copia certificada del mismo si lo prefiere.

En este sentido, las oportunidades y medios que tiene la contraparte para ejercer el control y contradicción de la prueba en el caso del mensaje de datos, serían los mismos que se tienen para desconocer un documento privado, es decir en la contestación de la demanda si este fue consignado con el libelo de la demanda, o a los cinco (5) días siguientes si es consignado posteriormente en el proceso. Igualmente, si el documento electrónico cumple con los requisitos legales para considerar que otorga fe pública, la contraparte deberá utilizar los medios de impugnación y desconocimiento del documento público.

Igualmente, la contraparte puede impugnar el mensaje de datos a los efectos de que la parte que lo aporta al proceso promueva los medios probatorios necesarios para verificar su autenticidad, entre los cuales de acuerdo al artículo 429 del CPC se tendría la inspección ocular para cotejar el documento.

Asimismo, la contraparte tiene la oportunidad procesal para oponerse a las pruebas por razones de impertinencia e ilegalidad, y contra la decisión que las admita podrá ejercer los recursos ordinarios y extraordinarios que le permita la Ley.

Ahora bien, para que se tenga éxito promoviendo un mensaje de datos en un proceso judicial, la parte no debe limitarse a promover la prueba como documental o prueba libre, sino que debe promover otros medios probatorios que aporten un valor probatorio adicional.

Entre estos otros medios probatorios que contribuyen a aportarle un valor de plena prueba al mensaje de datos, tenemos a las pruebas de informes, mediante las cuales se le solicita a personas jurídicas información sobre el contenido, lugar, fecha y hora de emisión de los mensajes de datos que estén almacenados en sus sistemas de información, y que a su vez remita un soporte impreso de dicho mensaje de datos.

El artículo 433 del CPC regula la prueba de informes en el ordenamiento jurídico venezolano, y señala que cuando sean hechos que consten en documentos, el tribunal podrá requerir a oficinas públicas, bancos, asociaciones gremiales, sociedades civiles o mercantiles que informen sobre los hechos litigiosos que aparezcan en dichos documentos, y que envíen copia de los mismos.

Se debe tomar en cuenta que, el referido artículo señala que se requerirá dicha información a personas jurídicas aunque no sean parte del juicio, lo cual de acuerdo al criterio de la investigadora no limita el uso de la prueba de informes a solicitar información exclusivamente de terceros que no sean parte en el juicio. Sin embargo, el criterio jurisprudencial vigente establece que únicamente la prueba de informes podrá utilizarse para requerir información sobre documentos a terceros que no forman parte del proceso, y que el medio idóneo para exigir que la contraparte aporte un documento al proceso es la exhibición de documentos.

En ese sentido, si el mensaje de datos se encuentra en poder de la parte demandada o la contraparte, deberá promoverse adicionalmente la prueba de exhibición de documentos de acuerdo al artículo 436 del CPC.

La exhibición de documentos tiene como ventaja que si se presentan pruebas de que el mensaje de datos está en poder de la contraparte, y ésta no lo exhibe en el proceso, se tendrá como exacto el texto del documento, y como ciertos los datos alegados por la parte promovente sobre el documento.

Por otra parte, la prueba de exhibición de documentos también puede utilizarse para solicitar que un tercero que no sea parte en el juicio traiga el documento al proceso, de acuerdo al artículo 437 del CPC.

Igualmente, el ordenamiento jurídico en materia procesal establece como medio probatorio a la prueba de experticia. Dicha prueba tiene como objeto verificar desde el punto de vista técnico información referente al contenido, lugar, hora y fecha de emisión o recepción del mensaje de datos; su integridad; certificar que el mismo no ha sido modificado o alterado desde que se generó; y la autenticidad del emisor.

La experticia puede ser utilizada no sólo para ratificar la veracidad del mensaje de datos promoviéndola adicionalmente a la prueba documental, y a la prueba libre, sino que también puede emplearse cuando la impresión del mensaje de datos haya sido desconocida o impugnada por la contraparte.

La prueba de experticia se encuentra prevista principalmente en los artículos 1.422 y siguientes del Código Civil, los cuales establecen que es el medio probatorio adecuado cuando se requiere de una apreciación o comprobación que exija conocimientos especiales. Igualmente, los artículos 451 y siguientes del CPC establecen la forma de promover y evacuar la prueba de experticia en un proceso judicial.

Además de la prueba de experticia, tenemos la inspección ocular que puede realizarse sobre el *software* y el *hardware* en el que se encuentre los programas o sistemas de información, que son otro medio comúnmente utilizado para promover información del contenido de mensajes de datos. Mediante esta prueba el Juez podrá conocer mediante un informe pericial de un experto en la materia el contenido de un mensaje de datos, así como el emisor, receptor, lugar, fecha y hora de emisión.

La prueba de inspección ocular se encuentra regulada principalmente por el Código Civil en los artículos 1.428 y siguientes, en donde se establece que el objeto de dicha prueba es dejar constancia de las circunstancias o el estado de los lugares o de las cosas. Asimismo, los artículos 472 y siguientes del CPC regulan la forma de

promover y evacuar dicha prueba, agregando que se puede acordar la inspección sobre personas, cosas, lugares o documentos a objeto de verificar los hechos que interesen o el contenido de los documentos.

Al ser el criterio jurisprudencial actual de que la promoción, control, contradicción y evacuación del correo electrónico como medio de prueba deberá regirse por lo que el legislador ha establecido para las pruebas libres en el CPC, para ejercer los mecanismos de control y contradicción de la prueba el Juez deberá emplear analógicamente las reglas previstas en el referido texto adjetivo sobre medios de prueba semejantes, o implementar los mecanismos que considere idóneos en orden a establecer la credibilidad del documento electrónico.

En consecuencia, es importante que la parte promovente conozca la amplia variedad de medios probatorios anteriormente indicados, que le pueden servir a la hora de traer el mensaje de datos al proceso como prueba, así como que no sólo promueva el mensaje de datos como prueba libre en el formato tecnológico en que se haya realizado, sino que además promueva una impresión del mismo como documental, que tendrá el valor de las copias fotostáticas, y haga uso de los demás medios probatorios antes señalados para dejar constancia de la autenticidad del referido mensaje de datos.

La recomendación de ésta investigación a los abogados litigantes es que a la hora de promover un mensaje de datos en un proceso judicial se utilicen todos los medios probatorios que se puedan relacionar con el mismo, y no se limiten a promoverlo como una documental o como prueba libre. Esto, por cuanto al existir distintos criterios doctrinales, y la posibilidad de cambios de criterios jurisprudenciales, el sujetarse a promover un único medio probatorio porque lo consideramos procesal y teóricamente correcto, puede generar que en la práctica la

prueba sea inadmitida o desechada, perdiendo así la oportunidad de demostrar la veracidad de los hechos alegados en el litigio.

VALORACIÓN DEL CORREO ELECTRÓNICO COMO PRUEBA

La escasa regulación de los correos electrónicos que no cumplen con los requisitos de la firma electrónica y el certificado electrónico (que garantizan la certeza de su contenido y autoría), es un vacío legislativo importante. Por lo que, quedan así a la sana crítica del Juez todos aquellos correos electrónicos que sin tener los requisitos legales de una firma electrónica o certificado electrónico, son elementos de prueba para demostrar comunicaciones en donde se asumen obligaciones, se establecen responsabilidades, e incluso se confiesan ilícitos o delitos.

Es por ello, que al momento de promover un correo electrónico como prueba de hechos que se alegan en un proceso judicial, no es suficiente promoverlo como prueba libre tal como lo establece el DLMDFE en su artículo 4º, sino que es necesario analizar otros medios probatorios tarifados legalmente, que permitan incorporar dicha prueba al proceso judicial de la forma más adecuada para que el Juez valore esa prueba de acuerdo a lo establecido legalmente, y no sólo de acuerdo a su sana crítica.

Por otra parte, hay que tomar en cuenta que al ser el correo electrónico un medio de comunicación de tecnología informática, está sometido a una rápida, constante y variable evolución tecnológica, por lo que fácilmente puede ser alterado en su autoría y contenido, y más aún si no se utilizan los sistemas de firma digital o certificado digital. Por ello, para que un Juez le otorgue a dicho correo electrónico la valoración probatoria que demuestre eficazmente el hecho objeto de la prueba, hay que constatar la veracidad de dicho correo electrónico tanto en su contenido como en su autoría, para lo cual no sólo basta con promoverlo mediante la prueba libre, sino que también hay que utilizar otros medios de prueba establecidos legalmente.

Igualmente, el DLMDFE en referencia no establece la forma y medios probatorios que se tienen para demostrar que un correo electrónico es falso tanto en su contenido como autoría, frente a lo cual se debe analizar los medios probatorios establecidos en otros instrumentos legales y adecuar su aplicación al correo electrónico.

En la mayoría de las normas procesales existentes a nivel internacional, el documento electrónico no se encuentra regulado de forma expresa, lo cual plantea problemas en cuanto a su admisión en un proceso judicial, la forma de incorporarlo a éste, y el valor probatorio atribuido en relación con los demás medios de prueba.

Entonces, los aspectos de la eficacia real que tiene el correo electrónico para demostrar relaciones jurídicas debido a la facilidad tecnológica de alterar su contenido y autoría, así como el hecho que de acuerdo al marco legal venezolano sólo aquellos correos electrónicos que tengan una firma digital o certificado digital que cumpla con los requisitos establecidos en el DLMDFE tendrán valor de una prueba documental, y que todos aquellos correos electrónicos que no cumplan con los requisitos previstos en esa Ley sólo serán valorados por el Juez en un proceso judicial de acuerdo a su sana crítica, nos plantean el presente problema: ¿Cuál es la valoración que un Juez debe dar a los distintos medios probatorios que pueden emplearse para promover o desconocer un correo electrónico en un proceso judicial?.

En cuanto a la valoración que le debe dar el Juez a cada uno de los medios probatorios utilizados para promover un correo electrónico en un proceso judicial, el autor Martínez (2000) nos plantea la situación en España cuando señala lo siguiente:

> A la vista de lo expuesto, puede concluirse que el Real Decreto-ley no cumple, al menos de forma inmediata, su objetivo de regular y

> dar seguridad al tema de la validez de los efectos jurídicos de la firma electrónica. Pues, para que sea admitida como medio de prueba, se exigen una serie de requisitos que requerirán de numerosas y difíciles pruebas periciales. Y, aún cuando es cierto que, de forma adecuada, el legislador español establece en el artículo 3.1, párrafo segundo, una presunción que elimina buena parte de esas dificultades probatorias, no es menos cierto tampoco que tal presunción no se puede aplicar, de momento, pues los elementos en que se basa están pendientes de regulación y desarrollo no sólo por las autoridades nacionales sino incluso también por las comunitarias. Y esta necesidad de desarrollo ulterior afecta, como hemos visto, a otras muchas cuestiones contempladas en el Real decreto (p. 312).

Al respecto el autor, Hance (1996) establece lo siguiente

> Estas situaciones nos presentan un problema considerable en un momento crucial. El problema es considerable porque los actores de Internet deben demostrar la legitimidad de su reclamo ante un Juez y en concordancia con las reglas de evidencia establecidas. No todo es evidencia admisible a los ojos de los tribunales. En algunos casos no se permite presentar correo electrónico, por ejemplo, y las siglas PGP no siempre se aceptan, El momento es crucial porque, si una parte falla al probar un hecho o un contrato ante el Juez, este la excluirá de la consideración a decidir el caso (p. 228).

Dicho autor hace un análisis detallado de como es la valoración del correo electrónico como prueba en distintos sistemas legislativos, y concluye con que en Francia el sistema aplicable es el siguiente:

> Bajo la legislación francesa, probar hechos (como la distribución de correo electrónico o la circulación de páginas Web) difiere de probar contratos firmados por Internet. La prueba de hechos, en asuntos civiles y comerciales, puede hacerse por cualquier medio legal y, por lo tanto, mediante documentos electrónicos, lo cual también es cierto para contratos comerciales cerrados por la red. Respecto a asuntos civiles, los contratos no necesitan probarse por medio de un documento original en papel firmado si el contrato respalda un valor menor a cinco mil francos, si existe un principio de evidencia en papel, en el caso de prácticas comunes, o de una admisión por la parte contraria. Por otro lado, para todos los demás contratos es necesario un documento en papel original y firmado. Que un documento electrónico firmado pueda considerarse un documento original firmado es una cuestión de debate. La tecnología permite un nivel de confiabilidad igual al de un documento original en papel y firmado tradicional, pero las actitudes aún no cambian (p.247).

En cuanto a la legislación aplicable en Inglaterra, dicho autor señala lo siguiente:

> De acuerdo con el nuevo régimen de la legislación inglesa, los documentos electrónicos son admisibles como tales. Todo el correo electrónico, mensajes de grupos de interés o páginas Web grabados electrónicamente y en circulación por Internet se admiten como evidencia, lo cual también es cierto para las copias electrónicas o impresiones de documentos digitalizados circulando por Internet. No obstante, estos documentos deben ser validados por diferentes

> procedimientos, dependiendo de si la parte que presenta la evidencia realiza un negocio o no (un concepto más amplio que el sentido ordinario de las palabras), o si pertenece a una autoridad pública. Más aún, aunque todos los documentos electrónicos que circulan por Internet son admisibles como tales, suponiendo que sean auténticos, no necesariamente tienen el mismo peso ante el tribunal (valor probatorio) (p. 247).

Y cuando hace referencia a la legislación en Estados Unidos y Canadá, señala lo siguiente:

> Bajo las legislaciones de Estados Unidos y Canadá, las reglas de evidencia pueden variar dependiendo del estado o provincia y de la jurisdicción. En términos generales, una parte puede presentar un documento electrónico bajo dos condiciones: el documento debe ser relevante (y, en particular, autenticado) y debe estar cubierto por una de las excepciones a dos reglas que constituyen obstáculos a la evidencia en forma de documentos electrónicos (la regla de mejor evidencia y la regla de prueba por referencia). Se ha facilitado la presentación de documentos electrónicos creados durante el curso normal de las actividades de una compañía por tales excepciones. Por último en lo que se refiere a venta de productos por Internet, debe tomarse en cuenta la legislación de las provincias de Canadá y de los Estados Unidos (actas de ventas de productos) (p. 248).

La doctrina ha señalado que dependiendo del cumplimiento de los requisitos exigidos legalmente por el mensaje de datos, el valor probatorio del mensaje de datos será de plena prueba, elemento de convicción o indicio. Al respecto, Salgueiro

(2006), señala que si el documento es público tendrá valor *erga omnes*, es decir frente a terceros ajenos a la suscripción del documento, y si el documento es privado será plena prueba entre las partes. Específicamente, dicho autor señala que el correo electrónico será plena prueba en un juicio en los supuestos siguientes:

1) El correo electrónico tiene una firma electrónica emitida por un PSC debidamente por la SUSCERTE.

2) El correo electrónico que tiene una firma electrónica emitida por un PSC que no esté acreditado por la SUSCERTE, pero que la firma electrónica cumpla con los requisitos exigidos por el artículo 16 del DLMDFE para su validez: a) Garantizar que los datos utilizados para su generación puedan producirse una sola vez y asegurar razonablemente su confidencialidad; b) Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento; y c) No alterar la integridad del mensaje de datos.

3) El correo electrónico que tiene una firma electrónica, que de acuerdo al artículo 16 del DLMDFE, permita vincular al signatario y atribuirle su autoría, cuando se prueben los requisitos de validez señalados en el párrafo anterior.

4) El correo electrónico que tiene una firma electrónica emitida por un PSC extranjero, cuando el certificado electrónico esté garantizado por un PSC debidamente acreditado por la SUSCERTE.

5) El correo electrónico que a pesar de que le falta alguno de los requisitos señalados en el DLMDFE, las partes convinieron que el mismo tendrá valor de plena prueba.

En consecuencia, el valor probatorio de plena prueba con efectos frente a terceros de un mensaje de datos dependerá de que el mismo pueda ser equiparado legalmente con un documento público auténtico, específicamente en los casos en que sean autorizados de forma electrónica por un funcionario público investido de la facultad de dar fe pública. Asimismo, podrá tener valor probatorio entre las partes cuando pueda equipararse con documentos privados reconocidos. De otra manera, si no son reconocidos por la parte que los suscribe serán equivalentes a un documento privado simple que, de ninguna forma puede considerarse que tenga el valor de plena prueba.

Al respecto, Chacón (2005) señala que el documento electrónico se considerará como público cuando así lo indique la ley expresamente. Tal como es el caso, de la Ley de Registro Público y Notariado que señala en su artículo 23 y 24 la existencia de la firma electrónica de Registradores y Notarios.

En el caso de que el mensaje de datos no contenga todos los elementos exigidos por el DLMDFE, y no cumpla con los requisitos previstos en el artículo 16, será en el proceso un elemento de convicción valorable por el Juez conforme a las reglas de la sana crítica, según lo establecen los artículos 17 y 44 del DLMDFE.

Al respecto, Brewer y Superlano (2004) señalaron que:

> La valoración del documento electrónico, es idéntica a la del documento tradicional. En consecuencia su valoración y eficacia como medio probatorio, será igual a la de cualquier documento convencional, sometido a las mismas reglas de apreciación y oposición que rige el sistema probatorio venezolano. Su tasación como plena prueba, o mero indicio probatorio, va a depender de las circunstancias y formalidades bajo las cuales fue otorgado dicho

> documento, que serán las mismas normas existentes para el otorgamiento de los documentos ordinarios o contenidos en papel. Así, el documento público electrónico será valorado igual que el documento público ordinario y el documento privado electrónico idéntico al documento privado convencional (p. 220).

Sin embargo, Salgueiro (2006) señala que los correos electrónicos serán valorados conforme a las reglas de la sana crítica en los siguientes supuestos:

1) El correo electrónico que tiene una firma electrónica emitida por un PSC que no está acreditado por la SUSCERTE, y que no cumple con los requisitos de validez establecidos en el artículo 16 del DLMDFE.

2) El correo electrónico que tiene una firma electrónica emitida por un PSC extranjero, más el certificado electrónico no está garantizado por un PSC acreditado por la SUSCERTE.

3) El correo electrónico que tiene una firma electrónica no certificada a través de un certificado electrónico emitido por un PSC.

A su vez, Newirovsky (2006) sostiene que la remisión que hace el DLMDFE al artículo 395 del CPC, indica que los correos electrónicos no son iguales a la prueba por escrito, pero al ser semejantes o similares se les debe aplicar por analogía las reglas de promoción y evacuación de las documentales.

Finalmente, existen casos en que los mensajes de datos serán valorados como simples indicios, lo cual ocurrirá cuando los mismos no tengan asociada una firma electrónica o cuando se encuentren en formato impreso.

Al respecto, Salgueiro (2006) establece que los correos electrónicos serán valorados como simples indicios en los siguientes casos:

1) El correo electrónico que no tiene una firma electrónica, ni un certificado electrónico. En consecuencia, deberá ser promovido conjuntamente con otros medios de prueba.

2) La impresión del correo electrónico, que tendrá la misma eficacia probatoria atribuida por Ley a las copias o reproducciones fotostáticas.

Por otra parte, Jedlicka (2004) hace referencia a lo establecido en los artículos 401 y 514 del CPC:

> (…) siempre existirá la posibilidad de que el Juez ordene a través de un auto complementario de pruebas o de un auto para mejor proveer, la evacuación de cualquier otro medio probatorio que considere pertinente, con el fin de lograr su convicción sobre la eficacia probatoria del mensaje de datos (p. 190).

En conclusión, se observa que el valor probatorio que un Juez le otorgará a un correo electrónico en el proceso judicial dependerá de los requisitos y formas que éste contenga, otorgándosele más peso a aquellos que cumplan con lo exigido por el DLMDFE para garantizar la autenticidad del mensaje de datos.

JURISPRUDENCIA NACIONAL

En la práctica a pesar de las posiciones doctrinales que puedan existir sobre la promoción y valoración del mensaje de datos o correo electrónico como prueba, es importante tomar en cuenta el criterio sostenido jurisprudencialmente por el Tribunal

Supremo de Justicia, ya que nos permitirá dilucidar como los máximos sentenciadores han dado respuesta al problema planteado en el presente trabajo de investigación.

En ese sentido, a continuación se hace referencia a varias sentencias del Poder Judicial venezolano que tratan sobre la promoción y valoración de un correo electrónico o la utilización de medios electrónicos en un juicio.

La Sala Constitucional del Tribunal Supremo de Justicia dictó sentencia el 1° de febrero de 2000, con ponencia del Magistrado Jesús Eduardo Cabrera, en el expediente N° 00-0010, nomenclatura de ese Tribunal, en el caso del Amparo Constitucional interpuesto por José Armando Mejías Betancourt, José Ángel Villavicencio y otros.

En dicha sentencia, se permite utilizar medios electrónicos, específicamente los correos electrónicos puros y simples (sin firma electrónica o certificado electrónico), para poder efectuar notificaciones judiciales exclusivamente en materia de amparo. Dicha decisión tuvo como fundamento el carácter urgente de la tramitación del proceso del amparo constitucional, por lo que le otorgó a estas notificaciones por correo electrónico la misma eficacia jurídica que la Ley otorga a las notificaciones judiciales escritas, realizadas conforme al CPC y la Ley Orgánica de Amparo sobre Derechos y Garantías Constitucionales.

Sin embargo, esta sentencia debe generar una reflexión sobre la necesidad de garantizar en el uso de los medios electrónicos para notificar a las partes en un proceso, el derecho al debido proceso tanto judicial como administrativo de ser el caso. En concreto, debe existir un mecanismo que permita verificar que efectivamente el correo electrónico fue recibido por el destinatario, de ser el caso que no se cuente

con una firma electrónica o certificado electrónico, a los efectos de que no se le violente a este último su derecho a la defensa.

La Sala Constitucional también dictó la sentencia N° 2031 el 19 de agosto de 2002, con ponencia del Magistrado Iván Rincón Urdaneta, en el expediente N° 02-175, nomenclatura de ese Tribunal.

En dicha sentencia, la Sala señaló que las publicaciones en la página Web del TSJ sólo tienen un carácter netamente informativo, por lo que la información relacionada con la actividad judicial puede ser modificada, enmendada o eliminada por el Tribunal.

La Sala Político-Administrativa del Tribunal Supremo de Justicia dictó la sentencia Nº 00157 del 13 de febrero de 2008, con ponencia del Magistrado Levis Ignacio Zerpa, en el caso PDV-FIT, PDV-Informática y Telecomunicaciones, S.A., contra INTESA Informática, Negocios y Tecnología, S.A. y SAIC (Bermuda) Ltd., en el Expediente N° 2004- 0183, nomenclatura de ese Tribunal.

En dicha sentencia, con relación a los correos electrónicos, la Sala decidió lo que sigue:

> De acuerdo a los dispositivos transcritos se colige que tratándose de mensajes que han sido formados y transmitidos por medios electrónicos, éstos tendrán la misma eficacia probatoria de los documentos.
>
> Sin embargo, su promoción, control, contradicción y evacuación deberá regirse por lo que el legislador ha establecido para las pruebas libres en el Código de Procedimiento Civil. Así, para tramitar la impugnación de la prueba libre promovida,

corresponderá al Juez emplear analógicamente las reglas previstas en el referido texto adjetivo sobre medios de prueba semejantes, o implementar los mecanismos que considere idóneos en orden a establecer la credibilidad del documento electrónico.

Dicho esto, y volviendo al caso de autos, observa la Sala que el valor probatorio de las impresiones de los correos electrónicos consignadas, es el que debe darse a las pruebas documentales. En este sentido, se aprecia que los referidos mensajes de datos fueron enviados por "FERRERO, HORST ALEJANDRO" a los ciudadanos Oswaldo Contreras y Jorge Baralt; además, cuentan con un logo de INTESA que deviene en firma electrónica, entendida en los términos expresados en su artículo 2:

…omissis…

Ahora bien, como aún no ha entrado en funcionamiento la Superintendencia de Servicios de Certificación Electrónica, servicio autónomo que el texto legal en estudio ordenó crear a los fines de la acreditación, supervisión y control de los proveedores de servicios de certificación públicos o privados, la firma electrónica contenida en los mensajes electrónicos no permite que éstos generen certeza de su forma y contenido.

No obstante lo dicho, estima la Sala que en razón de que la falta de certificación electrónica no puede ser atribuida a la parte que se quiere servir de las pruebas emitidas por medios electrónicos, lo procedente, en aplicación de los medios probatorios previstos en el Código de Procedimiento Civil, es analizarlas tomando en cuenta otros aspectos que se evidencian de su contenido.

Así, se observa que tanto el emisor como el destinatario ("FERRERO, HORST ALEJANDRO" en el primer caso, y los

> ciudadanos Oswaldo Contreras y Jorge Baralt, en el segundo) resultan ser terceros ajenos al juicio que ha dado lugar a este fallo, ambos debieron ratificarlos por vía testimonial a tenor de lo dispuesto en el artículo 431 del Código de Procedimiento Civil.
>
> Así, la ausencia de ratificación de las impresiones de los mensajes de datos tiene por consecuencia el que esta Sala desestime las referidas probanzas en el presente juicio.

Se observa de ésta sentencia que la Sala aplicó al mensaje de datos las normas probatorias previstas para el documento escrito, y expresamente señaló que la parte debió haber utilizado la ratificación mediante testimonial porque equivalía a un documento emanado de terceros. Igualmente, llama la atención que en un principio la sentencia parece confundir un logo con la firma electrónica, los cuales tal como se desarrollo en la presente investigación, son completamente diferentes.

La Sala de Casación Civil del Tribunal Supremo de Justicia dictó la sentencia N° 460 el 5 de octubre de 2011, en el caso (Transporte Doroca, C.A., contra Cargill de Venezuela, S.R.L.), en donde se expresa lo siguiente:

> Asimismo, esta Sala de Casación Civil, en sentencia dictada el 24 de octubre de 2007, caso: Distribuidora Industrial de Materiales C.A. contra Rockwell Automation de Venezuela C.A., dejó asentado que el documento electrónico debe entenderse como cualquier tipo de documento generado por medios electrónicos, incluyendo en esta categoría los sistemas electrónicos de pago, la red de internet, los documentos informáticos y telemáticos, entre otros.
>
> También ha sido catalogado como un medio atípico o prueba libre, por ser aquél instrumento que proviene de cualquier medio de

informática o que haya sido formado o realizado por éste, o como el conjunto de datos magnéticos grabados en un soporte informático susceptible de ser reproducidos que puede fungir como objeto de prueba y su reproducción, independientemente de su denominación, debe ser considerada otro documento que actúa como medio para su traslado al expediente.

…omissis…

La Sala en la sentencia antes referida (24 de octubre de 2007) dispuso que era evidente que los mensaje de datos son un medio de prueba atípico, cuyo soporte original está contenido en la base de datos de un PC o en el servidor de la empresa y es sobre esto que debe recaer la prueba.

…omissis…

De acuerdo a los dispositivos transcritos se colige que tratándose de mensajes que han sido formados y transmitidos por medios electrónicos, éstos tendrán la misma eficacia probatoria de los documentos escritos.

Sin embargo, su promoción, control, contradicción y evacuación deberá regirse por lo que el legislador ha establecido para las pruebas libres en el Código de Procedimiento Civil. Así, por ejemplo, para tramitar la impugnación de la prueba libre promovida, corresponderá al Juez emplear analógicamente las reglas previstas en el referido texto adjetivo sobre medios de prueba semejantes, o implementar los mecanismos que considere idóneos en orden a establecer la credibilidad del documento electrónico.

…omissis…

Con base en todo lo anterior, el valor probatorio de las impresiones de los correos electrónicos consignadas, es el que debe

darse a las pruebas documentales. En este sentido, se observa que los referidos mensajes de datos fueron enviados, el primero, por "nina_odreman@cargill.com" para el remitente,transportedoroca@cantv.net el día 10 de enero de 2004, a las 3:23 de la tarde, con un asunto "Minuta reunión Sábado 10/1/2004"; el segundo, por "nina_odreman@cargill.com" para el remitente, transportedoroca@cantv.net el día 21 de enero de 2004, a las 5:09 de la tarde, con un asunto "Situación del 21/1/2004" y; el último, por "nina_odreman@cargill.com" para el remitente, transportedoroca@cantv.net el día 27 de diciembre de 2003, a la 1:06 de la tarde, con un asunto Facturas en tránsito".

…omissis…

De conformidad con la citada ley especial, el valor probatorio de los mensajes de datos, es asimilable al de los documentos escritos y están sujetos a las regulaciones que plantea el artículo 395 del Código de Procedimiento Civil en lo referido a la prueba libre, por lo que el Juez superior al apreciarlos con el mismo valor que se les da a las copias o reproducciones fotostáticas, aplicó correctamente el Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas, al caso concreto.

…omissis…

De la transcripción parcial de la sentencia recurrida se evidencia que el sentenciador de alzada estableció que la demandada acompañó junto con la contestación formatos impresos de correos electrónicos de fechas 10/1/2004, 21/1/2004, 27/12/2003 respectivamente, folios 120 al 123.

Respecto de ellos, consideró que hablar de documentos electrónicos en la era actual, no parece presentar ningún tipo de problema, ya que tales documentos son comunes en la vida

cotidiana, por lo que es normal que se reciban correos electrónicos y por este medio, se trate cualquier tipo de compromiso, que es un contrato en sentido estricto, así como la utilización de tarjetas de créditos para todo tipo de pago.

Asimismo, indicó que conforme el artículo 395 del Código de Procedimiento Civil, los medios de pruebas libres, deben promoverse y evacuarse aplicando por analogía las disposiciones relativas a los medios de pruebas semejantes, y en su defecto, en la forma que señale el Juez.

Sobre este particular, señaló que el valor probatorio de los mensajes de datos y firmas electrónicas, reproducidos en formato impreso, debían considerarse semejantes, en cuanto a su eficacia y valor probatorio, a las copias o reproducciones fotostáticas, de conformidad con lo establecido en el artículo 4 del Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas, razón por la cual le dio pleno valor probatorio a los correos electrónicos al amparo de lo establecido en el artículo 429 del Código de Procedimiento Civil, con base en que los mismos no fueron impugnados en su oportunidad legal.

Considera esta Sala, que el sentenciador de alzada, con su proceder respecto al valor probatorio de los mensajes de datos o correos electrónicos, aplicó el contenido del artículo 4 del Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas, en especial en lo referido al único aparte de la norma que establece "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", por cuanto el Juez superior al momento de apreciar y valorar la referida prueba estableció: "los expresados correos

electrónicos no fueron impugnados en su oportunidad legal por lo que se le da pleno valor probatorio según lo establecido en el artículo 429 del Código de Procedimiento Civil", norma ésta que regula el valor de las copias fotostáticas, de la siguiente manera:

…omissis…

Conforme con esta norma, las copias fotostáticas o reproducidas por cualquier medio mecánico, se reputarán fidedignas, siempre que se cumplan con ciertas condiciones, entre ellas, que no sean impugnadas por la contraparte, ya en la contestación a la demanda si han sido producidas con el libelo, ya dentro de los cinco días siguientes, si han sido producidas con la contestación o en el lapso de pruebas.

La Sala debe insistir, y en este sentido también darle la razón al Juez superior, que el adversario del promovente tiene la carga de impugnar las fotocopias simples de documentos, si dicha fotocopia se consigna en la demanda, contestación o lapso probatorio.

En este sentido, la Sala observa que la demandante no impugnó, dentro de los cinco días siguientes de producidas, las copias impresas de los correos electrónicos consignados junto con la contestación de la demanda, lo cual era su deber a tenor de lo establecido en la jurisprudencia de esta Sala, que en decisión No. 469 de fecha 16 de diciembre de 1992, Caso: Asociación La Maralla contra Proyectos Dinámicos El Morro, C.A., dejó asentado:

…omissis…

Recordemos además, en este punto, que conforme al Decreto con Fuerza de Ley Sobre Mensajes de Datos y Firmas Electrónicas, en su único aparte "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", de manera que con base en el contenido del artículo 429 del Código de Procedimiento Civil, resultó correcta la apreciación del Juez al considerar que los correos electrónicos, estimados por la ley especial con eficacia probatoria semejante al de las copias o reproducciones fotostáticas, son fidedignos para demostrar la "inconformidad de la empresa CARGILL requerida a TRANSPORTE DOROCA".

Esta última sentencia, ratifica no sólo la importancia de promover la impresión del mensaje de datos que se quiere hacer valer en el juicio de acuerdo a las normas previstas para los documentos escritos, sino que además establece que la contraparte debe ejercer los mecanismos de control y contradicción de la prueba previstos para los documentos escritos, a los efectos de desconocer o impugnar el correo electrónico. Específicamente, por cuanto si el mensaje de datos no es impugnado correctamente por la contraparte, la impresión del mismo se entiende como fidedigna y adquiere valor de plena prueba.

Las sentencias reseñadas previamente son una clara muestra de que cada vez más los medios electrónicos son comúnmente utilizados para dejar constancia de hechos, celebrar actos y negocios jurídicos que generan derechos y obligaciones.

Igualmente, se observa que las sentencias son contestes en equiparar el correo electrónico a un documento escrito, y en consecuencia valorar el uso de medio probatorios relacionados con la prueba documental, así como los medios de control y contradicción íntimamente vinculados con ella.

CONCLUSIONES

El marco legislativo venezolano presenta una regulación de mediana claridad en cuanto a los mensajes de datos o correos electrónicos que posean una firma electrónica o certificado electrónico que cumpla con los requisitos establecidos en el Decreto Ley sobre Mensajes de Datos y Firma Electrónica. Tal como se señaló anteriormente, dichos correos electrónicos tendrán el mismo valor probatorio que una prueba documental.

Ahora bien, en la práctica son muy pocos los usuarios de la firma electrónica y el certificado electrónico, por lo que son realmente escasos los hechos que se pretenden demostrar en un juicio con un correo electrónico que cumpla con esos requisitos.

El Decreto Ley sobre Mensajes de Datos y Firma Electrónica señala que aquellas firmas electrónicas que no cumplan con los requisitos exigidos por dicha norma serán valoradas por el Juez de acuerdo a su sana crítica, por lo que en algunos casos no tendrán mayor valor probatorio que el de indicios.

En ese sentido, la solución propuesta por la firma electrónica o certificado electrónico para otorgarle eficacia probatoria a un mensaje de datos en un juicio, se ha quedado corta para la amplitud de la realidad actual de hechos y negocios jurídicos que ocurren día a día mediante medios electrónicos.

Por otra parte, es evidente la falta de claridad aún en los casos de los correos electrónicos que poseen una firma electrónica o un certificado electrónico, en cuanto a la aplicación de las normas procesales para hacer valer dicho mensaje de datos en un juicio. Concretamente, se observa que en la doctrina se presentan dos corrientes, la

primera orientada a promover el correo electrónico como una prueba documental, y la segunda que considera que debe ser promovido como prueba libre.

Los abogados litigantes y los jueces han intentado colmar ese vacío normativo aplicando normas jurídicas que no sólo fueron creadas para regular medios probatorios con formas y contenidos distintos a los de un mensaje de datos o correo electrónico, sino que además fueron creadas en un momento histórico en el que o bien no existían los mensajes de datos y correos electrónicos, o su uso era sumamente escaso.

En consecuencia, por más que el Código de Procedimiento Civil nos brinde una amplitud probatoria con la regulación de la prueba libre para cualquier medio de prueba que no esté prohibido expresamente por la ley, las formas de los medios probatorios que el Juez debe aplicar por analogía para poder evacuar esas pruebas libres, no se encuentran adaptadas a los elementos que contiene un correo electrónico o mensaje de datos.

Es por ello, que es necesaria una reforma del Decreto Ley sobre Mensajes de Datos y Firma Electrónica, que incorpore una regulación amplia y detallada de los medios probatorios que se utilizarán para promover o desconocer el correo electrónico en un proceso judicial. Dicha reforma deberá abarcar el caso en el que el correo electrónico no cumpla con los requisitos de la firma electrónica o el certificado electrónico, y como deberán ser valorados los medios probatorios utilizados, en un proceso judicial con el objeto de que exista un instrumento legal actual que regule en su totalidad todos los aspectos del correo electrónico como medio de prueba.

Es necesario, que dicha reforma legal también abarque los mecanismos para demostrar los aspectos relacionados con la certeza de la autoría y contenido del correo electrónico, con la finalidad de que no sólo un instrumento legal regule a

cabalidad todos los aspectos del correo electrónico como prueba, sino que además dicho instrumento legal sea producto de un análisis de las actuales tecnologías y los aspectos procesales que implica demostrar hechos efectuados con las mismas.

A pesar que la propuesta principal de ésta investigación es que se reforme la norma existente, y ésta regule cabalmente los aspectos procesales del correo electrónico como medio de prueba, se plantea de igual forma que mientras no se lleve a cabo dicha reforma legal, se utilice toda la gama de medios probatorios previstos en el ordenamiento jurídico venezolano para hacer valer el correo electrónico en un proceso judicial.

Es decir, el correo electrónico debe ser promovido como una prueba documental en sus elementos que se asemejen al documento escrito, específicamente la impresión del referido mensaje de datos, utilizando para validar la autenticidad de su contenido y firma otros medios probatorios, tales como la exhibición de documentos, la ratificación documental, la prueba de informes, la experticia o la inspección ocular. Así mismo, debe utilizarse el medio probatorio de la prueba libre a los efectos de no limitar la valoración del correo electrónico como prueba a las formas expresamente previstas para las pruebas documentales, y los otros medios probatorios antes indicados, en cuanto a que el correo electrónico tenga características que difieran de la prueba documental.

En la práctica, los abogados litigantes cuando pretendan demostrar un hecho con un correo electrónico se encontrarán en un escenario donde deberán promover múltiples medios probatorios a los efectos de certificar la validez y autenticidad del contenido y autoría del mismo. Todo lo cual, representa procesalmente una inversión para la parte afectada tanto de tiempo, debido a los lapsos procesales que conlleva la evacuación de esos distintos medios probatorios, como de dinero por cuanto se

requerirá la participación de expertos o peritos que certifiquen el carácter fidedigno del correo electrónico.

Por lo tanto, la reforma legal originalmente propuesta debe realizarse con la participación de expertos en las tecnologías de comunicación, que permita crear un mecanismo para certificar la autenticidad del correo electrónico en un juicio, o impugnar el mismo, que no dependa exclusivamente de las figuras del correo electrónico y de la firma electrónica, sino que permita a las partes utilizar el correo electrónico para demostrar hechos en un juicio garantizando la celeridad y gratuidad que debe regir en todo proceso.

Un ejemplo de lo anteriormente expuesto, es que se tenga una lista de las personas jurídicas que prestan servicios de mensajes de datos o correos electrónicos, o una lista de expertos en dichas tecnologías, y el Juez deba corroborar con ellos la autenticidad del correo. Sin que se requiera para ello impulso de las partes, sino que se considere como una actuación necesaria del Juez cuando se traiga un correo electrónico al juicio, a los efectos de tener la verdad como norte de sus actos.

Asimismo, otra proposición es plantear que se establezca una obligación legal con sanción por su incumplimiento, para las personas jurídicas que brindan los servicios de mensajerías de datos y de correos electrónicos, de informar sobre la autenticidad o no de los mismos, en los casos en que así sean requeridos por el Poder Judicial.

REFERENCIAS BIBLIOGRÁFICAS

Bello, Humberto, y Bello, Isabel. (2007). *El documento electrónico y los medios de reproducción de imágenes y sonidos como medios de prueba judicial*. S.E. Caracas.

Bello Tabares, Humberto. (2008). *Las pruebas en el proceso laboral*. (2ª Edición). Caracas: Ediciones Paredes II, C.A.

Brewer, Albert, y Superlano, Rosa V. (2004). *La prueba documental en el comercio electrónico: El documento-e*. *En Aspectos Legales del Comercio Electrónico*, (pp. 213-222). Caracas: Cámara Venezolana de Comercio Electrónico.

Borjas, Arminio. (1964). *Comentarios al Código de Procedimiento Civil Venezolano*. (Segunda Edición). Caracas: Ediciones Sales.

Carnelutti, F. (2000). *La prueba civil*. Buenos Aires: Editorial Acayú.

Chacón Gómez, Nayibe. (2005). *La aplicación de los sistemas de certificación electrónica en la actividad comercial*. Caracas: Instituto de Derecho Privado Facultad de Ciencias Jurídicas y Políticas, UCV.

Couture, Eduardo. (1976). *Vocabulario jurídico*. Buenos Aires: Ediciones Desalma.

Devis, Hernando. (1993). *Teoría general de la prueba judicial.* Tomo II. Segunda Edición. Buenos Aires: Editorial Víctor P. de Zavalia.

Di Totto Blanco, B. (2005). *La "prueba electrónica" en el proceso penal venezolano.* [Libro en línea]. Disponible en: http://derechoinformatico.net.ve/imagenes/pruebaelectronica.pdf. [Consulta: 2006, Diciembre 2º].

Falcón, Enrique. (2003). *Tratado de la prueba: civil, comercial, laboral, penal, administrativa: principios y sistemas probatorios, carga de la prueba, factores psicológicos, la informática, el lenguaje, apreciación o valoración,*

prueba ilícita, medios probatorios documentales e informativos. Caracas: Editorial Astrea.

Hance, O. (1996). *Leyes y negocios en Internet*. México, D.F.: McGraw-Hill.

Jedlicka Zapata, Pedro A. (2004). *Comentarios de los mensajes de datos como medios de prueba*. *En Aspectos Legales del Comercio Electrónico*, (pp. 177-198). Caracas: Cámara Venezolana de Comercio Electrónico.

Martínez Nadal, A. (2000). *La Ley de Firma Electrónica*. Madrid: Civitas Ediciones, S.L.

Midón, Marcelo. (2007). *Derecho probatorio*: Parte General. Buenos Aires, Argentina: Ediciones Jurídicas Cuyo.

Muci, Gustavo. (2003). Equivalencia Electrónica. (2003, 25 de octubre). *Diario El Universal*. Disponible en: http://www.eluniversal.com/2003/10/25/opi_art_25490B.shtml

Muñoz, Luis. (1997). *Técnica probatoria*. Bogotá: Editorial Temis.

Newirosky, Hugo. (2006) *El valor probatorio del documento electrónico. En Tendencias Actuales del Derecho Procesal Constitución y Proceso*. (pp.165-176). Caracas: Universidad Católica Andrés Bello.

Orta, R. (2005). *Ciberterrorismo*. [Documento en CD-ROM]. Disponible en: http://tecnoiuris.com y http://experticias.com.

Orta, R. (2005). *Curso de introducción a la informática forense – IF100a. Glosario de Términos*. [Documento en CD-ROM]. Disponible en: http://tecnoiuris.com y http://experticias.com.

Orta, R. (2005). *Informática forense como medio de pruebas*. [Documento en CD-ROM]. Disponible en: http://tecnoiuris.com y http://experticias.com.

Pierre Tapia, O. (1977). *La prueba en el proceso venezolano*. Barcelona: Producciones Editoriales Avda. José Antonio, 800.

Rueda, Aníbal, y Perreti, Magaly. (2008). *La prueba*. Caracas: Vadell Hermanos.

Rengel Romberg, Arístides. (2004). *Tratado de derecho procesal civil venezolano, según el nuevo código de 1987*. Vols. III: Teoría General del Proceso. (11ª Edición). Caracas: Organización Gráficas Capriles, C.A.

Rico Carrillo, Mariliana. (2005). *La prueba electrónica*. (2ª Edición). Bogotá: Legis, S.A.

Rivera Morales, Rodrígo. (2004). *Las pruebas en el derecho venezolano*. San Cristóbal, Venezuela: Editorial Jurídica Santana.

Rodríguez, Gladys. (1997). *De la firma autógrafa a la firma digital: perspectiva venezolana*. Universidad del Zulia. Facultad de Ciencias Jurídicas y Políticas. Instituto de Filosofía del Derecho "Dr. J. M. Delgado O".

Ruíz, Fernando. (1999). *El documento electrónico frente al derecho civil y financiero*, *Revista de Derecho Informático en Alfa-Redi*, N° 16, noviembre de 1999.

Salgueiro, José O. (2006). *Contratación Electrónica*. *En Tendencias Actuales del Derecho Procesal Constitución y Proceso*. (pp.177-205). Caracas: Universidad Católica Andrés Bello.

REFERENCIAS LEGISLATIVAS

Constitución de la República Bolivariana de Venezuela. (2009). *Gaceta Oficial de la República Bolivariana de Venezuela*, 5.908 (Extraordinario), Febrero 19, 2009.

Código Orgánico Tributario. (2001). *Gaceta Oficial de la República Bolivariana de Venezuela*, 37.305, Octubre 17, 2001.

Código Civil. (1982). *Gaceta Oficial de la República de Venezuela*, 2.990 (Extraordinario), Julio 26, 1982.

Código de Procedimiento Civil. (1990). *Gaceta Oficial de la República de Venezuela*, 4.209 (Extraordinario), Septiembre 18, 1990.

Ley Orgánica del Poder Ciudadano. (2001). *Gaceta Oficial de la República Bolivariana de Venezuela*, 37.310, Octubre 25, 2001.

Ley Orgánica Procesal del Trabajo. (2002). *Gaceta Oficial de la República Bolivariana de Venezuela*, 37.504, Agosto 13, 2002.

Ley Orgánica contra el Tráfico Ilícito y el Consumo de Sustancias Estupefacientes y Psicotrópicas. (2005). *Gaceta Oficial de la República Bolivariana de Venezuela*, 38.337, Diciembre 16, 2005.

Ley Orgánica de la Contraloría General de la República y del Sistema Nacional de Control Fiscal. (2010). *Gaceta Oficial de la República Bolivariana de Venezuela*, 6.013, Diciembre 23, 2010.

Ley de Reforma de la Ley Orgánica de Telecomunicaciones. (2011). *Gaceta Oficial de la República Bolivariana de Venezuela*, 39.610, Febrero 7, 2011.

Ley Especial Contra Delitos Informáticos. (2001). *Gaceta Oficial de la República Bolivariana de Venezuela*, 37.313, Octubre 30, 2001.

Ley de Comercio Marítimo. (2006). *Gaceta Oficial de la República Bolivariana de Venezuela*, 38.351, Enero 5, 2006.

Ley de Registro Público y del Notariado. (2006). *Gaceta Oficial de la República Bolivariana de Venezuela*, 5.833 (Extraordinario), Diciembre 22, 2006.

Ley de Tarjetas de Crédito, Débito, Prepagadas y demás tarjetas de financiamiento y pago electrónico. (2008). *Gaceta Oficial de la República Bolivariana de Venezuela*, 39.021, Septiembre 22, 2008.

Ley para la Defensa de las Personas en el Acceso a los Bienes y Servicios. (2010). *Gaceta Oficial de la República Bolivariana de Venezuela*, 39.358, Febrero 1°, 2010.

Ley de Reforma Parcial de la Ley General de Bancos y Otras Instituciones Financieras. (2010). *Gaceta Oficial de la República Bolivariana de Venezuela*, 39.491, Agosto 19, 2010.

Ley de Reforma Parcial de la Ley de Contrataciones Públicas. (2010). *Gaceta Oficial de la República Bolivariana de Venezuela*, 39.503, Septiembre 6, 2010.

Decreto N ° 825 (Internet como prioridad). (2000). *Gaceta Oficial de la República Bolivariana de Venezuela*, 36.955, Mayo 25, 2000.

Decreto N° 1.204 (Ley sobre Mensajes de Datos y Firmas Electrónicas). (2001). *Gaceta Oficial de la República Bolivariana de Venezuela* Nº: 37.148, Febrero 28, 2001.

Decreto N° 5.212 (Ley de Reforma Parcial del Impuesto al Valor Agregado). (2007). *Gaceta Oficial de la República Bolivariana de Venezuela*, 38.632, Febrero 26, 2007.

Decreto N° 5.620 (Ley de Impuesto a Transacciones Financieras de las Personas Jurídicas y Entidades Económicas Sin Personalidad Jurídica). (2007). *Gaceta Oficial de la República Bolivariana de Venezuela*, 5.852 (Extraordinario), Octubre 5, 2007.

Decreto N° 5.879 (Ley Orgánica de Aduanas). (2008). *Gaceta Oficial de la República Bolivariana de Venezuela*, 38.875, Febrero 21, 2008.

Decreto N° 6.217 (Ley Orgánica de la Administración Pública). (2008). *Gaceta Oficial de la República Bolivariana de Venezuela*, 5.890 (Extraordinario), Julio 31, 2008.

Decreto N° 9.044 (Ley Orgánica de Turismo). (2012). *Gaceta Oficial de la República Bolivariana de Venezuela*, 6.079, Junio 15, 2012.

Decreto N° 9.042 (Código Orgánico Procesal Penal). (2012). *Gaceta Oficial de la República Bolivariana de Venezuela*, 6.078 (Extraordinario), Junio 15, 2012.

Reglamento N° 3.335 Parcial del Decreto-Ley sobre Mensajes de Datos y Firmas Electrónicas. (2004). *Gaceta Oficial de la República Bolivariana de Venezuela*, 38.086, Diciembre 14, 2004.

Ley Modelo de UNCITRAL Sobre El Comercio Electrónico. (1999). *Naciones Unidas*.

Real Decreto Ley 59/2003 de Firma Electrónica. (2003). *BOE Núm. 304*, Diciembre 20, 2003). Disponible en: http://belt.es/legislacion/reciente/pdf/ley_20_dic_03.pdf

REFERENCIAS JURISPRUDENCIALES

Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 07, de fecha 1° de febrero de 2000, con ponencia del Magistrado Jesús Eduardo Cabrera, Expediente N° 00-0010.

Tribunal Supremo de Justicia. Sala Constitucional. Sentencia N° 2031, de fecha 19 de agosto de 2002, con ponencia del Magistrado Iván Rincón Urdaneta, Expediente N° 02-175.

Tribunal Supremo de Justicia. Sala Político Administrativa. Sentencia N° 00157, de fecha 13 de febrero de 2008, con ponencia del Magistrado Levis Ignacio Zerpa, Expediente N° 2004-0183.

Tribunal Supremo de Justicia. Sala de Casación Social. Sentencia N° 0264, de fecha 5 de marzo de 2007, con ponencia del magistrado Alfonso Valbuena Cordero, Expediente N° 06-1657.

Tribunal Supremo de Justicia. Sala de Casación Civil. Sentencia N° 460, de fecha 5 de octubre de 2011, con ponencia de la Magistrada Isbelia Josefina Pérez Velásquez, Expediente N° 11-237.

Juzgado Segundo de Primera Instancia en lo Civil, Mercantil y del Tránsito de la Circunscripción Judicial del Estado Mérida. Sentencia de fecha 09 de marzo de 2011, dictada por el Juez Albio Contreras Zambrano, Expediente N° 10238.