UNIVERSIDAD DEL AZUAY.
FACULTAD DE CIENCIAS JURÍDICAS.

ESCUELA DE DERECHO.

LOS MENSAJES DE DATOS, LA FIRMA ELECTRÓNICA Y LOS CERTIFICADOS DE FIRMA ELECTRÓNICA DENTRO DEL ORDENAMIENTO JURÍDICO ECUATORIANO.

TRABAJO DE GRADUACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO DE LOS TRIBUNALES DE JUSTICIA DE LA REPÚBLICA DEL ECUADOR.

AUTOR: JAIME LUCERO DÍAZ.

DIRECTOR: DR. ANTONIO MARTÍNEZ BORRERO.

CUENCA – ECUADOR

2010

Dedicatoria.

Dedico este trabajo
a toda mi familia por
apoyarme incondicionalmente
en todos los ámbitos de mi vida.

.

Agradecimientos.

Al doctor Antonio Martínez Borrero, por dedicar su valioso tiempo y aportar con sus ilustrados conocimientos, a la elaboración de este trabajo de grado.

A mis padres y mi familia, por haber confiado siempre en mí.

A la Universidad del Azuay y sus profesores, por haber inculcado en mí sólidas bases teóricas y morales para afrontar los problemas sociales.

A mis compañeros, por hacer más ameno el aprendizaje dentro de las aulas.

Índice de Contenidos.

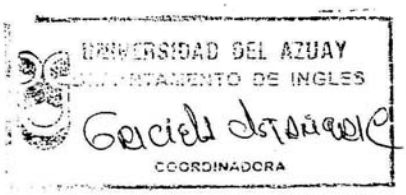
Índice de Ilustraciones y Cuadros.

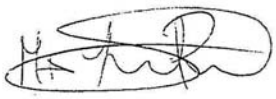
RESUMEN.

La informática ha incursionado en todos los ámbitos de nuestras vidas. Como consecuencia de este fenómeno, el uso de medios de comunicación, como el internet, se han generalizado con el pasar del tiempo. El internet sin lugar a dudas otorga varias ventajas a sus usuarios, pero al mismo tiempo es un instrumento del que se valen muchas personas para atentar contra una gran variedad de derechos como son: la propiedad, la honra, la libertad de pensamiento, etc. Por este motivo nuestro ordenamiento jurídico reconoce y regula a los mensajes de datos, a la firma electrónica y a los certificados de firma electrónica, otorgando a cada una de estas figuras validez jurídica y eficacia probatoria, con el fin de brindar seguridad a aquellas personas que intervienen en el intercambio de información por la vía telemática. En este trabajo analizaremos el tratamiento jurídico que nuestra legislación brinda a cada una de las figuras que acabamos de mencionar, para de esta forma saber si realmente éstas solventan el problema de la inseguridad en las relaciones telemáticas, y además establecer si el marco legal es el adecuado.

ABSTRACT

The Internet, without doubt, provides a lot of advantages for its users. However, at the same time, it is a tool which many people use to assault a wide range of rights such as, property, honor, free thought, etc. For this reason our legal system recognizes and regulates all the data messages, electronic signatures and certificates of electronic signature giving each of them legal and juridical validity and approbatory effectiveness. The objective is to offer security to those people who participate in the virtual interchange of information. This project analyses the juridical treatment that our system has for the aforementioned subjects, in this way it is possible to know if the legislation solves the problem of insecurity in virtual relations as well as establishing if the legal framework is appropriate.





INTRODUCCIÓN.

El incesante desarrollo de las nuevas tecnologías ha sido un factor determinante para la evolución de las relaciones telemáticas, esto es, aquellas relaciones que se verifican a distancia, entre dos o más personas, mediante el uso de las nuevas tecnologías. En la actualidad este tipo de relaciones proliferan, en especial si tomamos en consideración que el Internet, como medio de comunicación, es una herramienta cada día más accesible al público.

El internet brinda varias ventajas a sus usuarios, como por ejemplo, permitir que se concreten negocios con personas que pueden encontrase al otro lado del mundo, permite también el intercambio de información mediante servicios como el correo electrónico, brinda a las empresas la posibilidad de promocionar sus productos, etc.

No obstante lo anotado, es preciso señalar que el internet no solo brinda ventajas a sus usuarios, pues muchas personas, valiéndose de la novedad y del creciente número de usuarios de este medio de comunicación, lo utilizan para vulnerar los derechos de las demás personas, mediante mensajes o publicaciones que atentan a la honra por ejemplo, o cometiendo estafas mediante contratos que no brindan seguridad alguna.

Como sabemos el derecho no puede permanecer indiferente respecto de los nuevos problemas que se presentan dentro de la sociedad, pues es su deber regular todas aquellas nuevas situaciones que aparecen con el devenir de los años, es por ese motivo que en el Ecuador se encuentra vigente la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos desde el año 2002.

La Ley de Comercio Electrónico reconoce y regula a los mensajes de datos, a las firmas electrónicas y a los certificados de firma electrónica, con el fin de brindar a las personas herramientas con las que puedan participar dentro del ámbito de las relaciones telemáticas sin ningún riesgo, y además otorgar medios de prueba eficaces, con los que las personas puedan justificar la veracidad de la información que haya sido generada o que esté siendo almacenada por un medio electrónico, y que lesione sus derechos.

En definitiva, podemos manifestar que el fin que persigue la Ley de Comercio Electrónico al regular a los mensajes de datos, a la firma electrónica y los certificados de firma electrónica es brindar seguridad a las personas que intercambian datos mediante los modernos sistemas de información, entre ellos el internet. Pues como lo manifestaba Luis Recasens Siches, la seguridad es la motivación radical de lo jurídico.

El objetivo que perseguimos con este trabajo, es determinar si es que estas figuras establecidas por la ley, desempeñan eficientemente su función, que como ya lo manifestamos, consiste en brindar seguridad a las personas que intervienen en el intercambio de información, mediante la vía telemática. Además analizaremos la normativa legal ecuatoriana, para verificar si es eficaz en el tratamiento de estas figuras.

CAPÍTULO 1.

LOS MENSAJES DE DATOS.

1.1 Introducción

Tradicionalmente la información ha sido archivada en el papel, pero con el tiempo esta forma de guardar la información ha ido perdiendo vigencia. Pues la rapidez de acceso a la información, el ahorro de dinero, el ahorro de espacio físico e incluso razones ecológicas, han determinado que la información se archive, cada vez con mayor frecuencia, en los denominados medios electrónicos. Cuando la información es procesada o archivada en un medio electrónico, la ley califica a esta información como mensaje de datos, siempre que esta figura se enmarque dentro del concepto de mensaje de datos establecido por la ley.

En este capítulo, luego de analizar el concepto de mensaje de datos, nos referiremos al valor legal y a la eficacia que tienen los mensajes de datos dentro del ordenamiento jurídico ecuatoriano, así como al valor que tiene aquella información que originariamente constara en el papel pero fue trasladada a un
la definición que da nuestra Ley de Comercio Electrónico, en cuanto a la medio electrónico. Analizaremos además, la forma en que podemos dejar sin efecto, con la sola presencia de un mensaje de datos, aquella exigencia legal en virtud de la cual debemos presentar cierta información por escrito, o debemos justificar un determinado hecho presentando el documento original.

El análisis de estos temas nos permitirá, al final de este capítulo, establecer si es que es beneficioso que la información conste como mensaje de datos, además podremos determinar si la normativa legal es eficaz al regular a los mensajes de datos.

1.2 Definición.

Para analizar el concepto de mensaje de datos debemos recurrir a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos que rige en nuestro

país desde el año 2002; y al respecto la antes mencionada ley dentro de la disposición general novena, que contiene un glosario de términos, manifiesta lo siguiente al definir a los mensajes de datos:

> "Es toda información creada, generada, procesada, enviada, recibida, comunicada o archivada por medios electrónicos, que puede ser intercambiada por cualquier medio. Serán considerados como mensajes de datos, sin que esta enumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, télex, fax e intercambio electrónico de datos."

La ley 527 de 1999 de la República de Colombia, la cual se encarga de definir y reglamentar el uso de los mensajes de datos, entre otros temas relacionados con el comercio electrónico, también contiene, en su artículo dos un conjunto de definiciones, dentro de las cuales se halla una referente a los mensajes de datos:

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

Las definiciones sobre mensaje de datos, que traen estas dos legislaciones poseen un contenido es similar, pues ambas manifiestan que el mensaje de datos es toda información, en esto debemos hacer hincapié pues el mensaje de datos es esencialmente información, que se haya generado, procesado, recibido, enviado o archivado en un determinado medio electrónico. Aquí cabe referirnos, aunque sea a breves rasgos, a lo que debemos entender por medio electrónico, para este efecto vamos a citar el concepto de medio electrónico que da la Ley Sobre el Uso de Medios Electrónicos y Firma Electrónica para el Estado de Guanajuato y sus Municipios en el numeral décimo segundo de su artículo tres: "Medios electrónicos: Los dispositivos tecnológicos para transmitir o almacenar datos e información, a través de computadoras, líneas telefónicas, enlaces dedicados, microondas, o de cualquier otra tecnología."

Estos medios se diferencian de los medios impresos básicamente en su soporte; pues mientras los medios impresos tienen como soporte al papel, los medios electrónicos tienen como soporte a los sistemas de información creados por las nuevas tecnologías. También es pertinente comentar el hecho de que la ley al manifestar que el mensaje de datos es "toda información", admite la posibilidad de que la simple información contenida en un medio electrónico pueda considerarse mensaje de datos, así esta información no esté destinada a ser comunicada.

Siguiendo con las definiciones, tenemos que la ley 527 de 1999 de la República de Colombia además de los medios electrónicos agrega "o medios ópticos o similares"; respecto de estos medios ópticos podemos acotar que son dispositivos que sirven para almacenar datos o información como por ejemplo el CD-ROM.

Finalmente Nuestra ley de Comercio Electrónico añade que esta información debe tener la posibilidad de ser intercambiada por cualquier medio.

A continuación, creo oportuno definir algunas de las figuras que constituyen mensajes de datos según nuestra legislación.

Patricia Herrmann define al documento electrónico como "un soporte electrónico donde se encuentra una declaración de voluntad del autor, sin importar si lo ha firmado digitalmente o no." (Herrmann, 2007, P. 80)

Esta misma autora al referirse a los registros electrónicos manifiesta que éstos constituyen "una pequeña unidad de almacenamiento destinada a contener cierto tipo de datos que puede estar en la propia memoria central o en unidades de memoria de acceso rápido." (Herrmann, 2007, P. 80)

Como podemos apreciar este tipo de mensajes de datos entrañan una gran importancia, pues al contener una manifestación de voluntad, en el caso de los documentos electrónicos, y al almacenar ciertos tipos de datos, como lo hacen los registros electrónicos; bien pudieran servirnos como medios de prueba dentro de un juicio, por estas razones más adelante nos referiremos al valor y a la eficacia de los mensajes de datos.

Respecto del correo electrónico podemos decir que es aquel servicio que permite el envío y recepción de mensajes entre personas que se hayan conectadas a una red electrónica.

En cuanto al intercambio electrónico de datos cuyas siglas en inglés son EDI (*Electronic Data Interchange*), vamos a tomar el concepto de Santiago Marimón quien define a esta figura como "La transferencia de datos estructurados, mediante mensajes estándar, de una aplicación informática a otra, por medios electrónicos, con el mínimo de intervención humana". (Marimón, 1999, P. 219) Para este autor el Intercambio Electrónico de Datos no se trata de cualquier transferencia de datos sino que únicamente podríamos referirnos a esta figura cuando estamos frente a datos que sean estructurados, con el fin de ser trasmitidos electrónicamente, en mensajes de formato estandarizado, además, que salgan de una determinada aplicación informática para ingresar a otra, y por último, que todo este proceso se efectúe con una escasa o sin intervención humana. (Marimón, 1999, P. 219)

Con relación al fax Patricia Herrmann manifiesta lo siguiente: "El método y aparato de transmisión – recepción de documentos, mediante la red telefónica conmutada, que se basa en la conversión a impulsos de las imágenes leídas por el emisor, impulsos que son traducidos en puntos –formando imágenes- en el receptor. " (Herrmann, 2007, P. 80)

1.3 Valor y eficacia de los mensajes de datos.

Para hablar acerca del valor y de la eficacia que poseen los mensajes de datos dentro del ordenamiento jurídico ecuatoriano, debemos acudir necesariamente a la Ley de Comercio electrónico, Firmas Electrónicas y Mensajes de Datos; pues este cuerpo legal en su artículo segundo reconoce a los mensajes de datos el mismo valor jurídico que los documentos escritos: "Los mensajes de datos tendrán igual valor jurídico que los documentos escritos."

Esto quiere decir que todas aquellas figuras a las que nuestra ley califica como mensaje de datos, tienen la misma valoración y los mismos efectos legales que tienen, dentro de nuestro ordenamiento jurídico, los documentos escritos.

Este principio que recoge la Ley de Comercio Electrónico, nace inspirado en el artículo cinco de la Ley Modelo de la Comisión de las Naciones Unidas (CNUDMI) para el Derecho Mercantil Internacional sobre Comercio Electrónico, que establece el principio de no discriminación a los mensajes de datos y que manifiesta lo siguiente: "No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos."

Uno de los puntos en donde indudablemente adquiere trascendental importancia esta disposición es en la prueba; además si tomamos en consideración que el artículo cuarenta y cinco de la Ley de Comercio Electrónico establece que los contratos también pueden instrumentarse mediante mensajes de datos; y que no por el hecho de haberse formado mediante uno o varios mensajes de datos debe disminuírsele validez o fuerza obligatoria.

Ahora bien, nuestro ordenamiento jurídico reconoce varios tipos de prueba, con las que una persona que figure dentro de un proceso judicial como parte, puede justificar que lo que ella afirma ha sucedido, y ha sucedido de la manera que ella lo relata. Uno de estos tipos de prueba es la instrumental o documental, y es precisamente dentro de este grupo donde se encuentran los documentos escritos.

La prueba instrumental o documental puede consistir en instrumentos públicos e instrumentos privados, a continuación vamos a citar el concepto que trae nuestro Código de Procedimiento Civil respecto de instrumento público y de instrumento privado: "Art. 168. Instrumento público o auténtico es el autorizado con las solemnidades legales por el competente empleado. Si fuere otorgado ante notario e incorporado en un protocolo o registro público, se llamará escritura pública." Respecto del instrumento privado el mismo código manifiesta lo siguiente en su artículo ciento noventa y cinco: "Instrumento privado es el escrito hecho por personas particulares, sin intervención de notario ni de otra persona legalmente autorizada, o por personas públicas en actos que no son de su oficio."

Estas dos figuras, el instrumento público y el privado, constituyen, dentro de nuestro ordenamiento jurídico, la denominada prueba documental o instrumental. Nuestra Ley de Comercio Electrónico al establecer que los mensajes de datos gozan del mismo valor jurídico que los documentos escritos, permite incluirlos dentro de esta clasificación.

Ahora, como es obvio no todos los documentos escritos gozan de la misma eficacia probatoria, por lo que en primer lugar habrá que distinguir si el mensaje de datos constituye un instrumento público, o si dicho mensaje mejor debería ser considerado instrumento privado, pues de esto dependerá la fuerza y la eficacia probatoria del mensaje de datos. La razón por la que planteamos esta distinción es porque nuestra Ley de Comercio Electrónico en su artículo cincuenta y uno admite la posibilidad de que un mensaje de datos pueda constituir instrumento público: "Se reconoce la validez jurídica de los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmados electrónicamente."

Alexander Díaz García citado por Patricia Herrmann en su obra Comercio Electrónico define al instrumento público electrónico como "un mensaje de datos en soporte electrónico, en donde se registra la voluntad humana. Es otorgado por una autoridad competente, así puede ser el llamado notario virtual o a quien la ley de las facultades para hacerlo" (Herrmann, 2007, P.71)

Estos instrumentos públicos electrónicos tienen necesariamente que observar los requisitos y solemnidades que la ley y demás normas exijan para cada caso.

Entonces para que un mensaje de datos, que haya sido otorgado por o ante el funcionario competente, pueda constituir instrumento público, es necesario que haya sido otorgado con apego a lo que la ley establezca para cada caso; además el mensaje de datos deberá, según lo dispuesto en el antes aludido artículo, estar firmado electrónicamente.

Como ya indicamos, el hecho de que la ley otorgue a los mensajes de datos el mismo valor que tienen los documentos escritos, permite que estos puedan ser clasificados

dentro de la prueba instrumental en uno de sus dos grupos: instrumentos públicos e instrumentos privados; así la eficacia probatoria del mensaje de datos dependerá del grupo al que el mensaje de datos ingrese.

Por lo anotado en el párrafo anterior, creo que es pertinente analizar, aunque sea a breves rasgos, la fuerza probatoria tanto de los instrumentos públicos como de los instrumentos privados.

En primer lugar vamos a referirnos a los documentos o instrumentos públicos, es decir aquellos que son otorgados de conformidad con las solemnidades legales y ante el competente empleado, y que cuando se otorgan ante un notario y son incorporados a un registro público toman el nombre de escritura pública. Este tipo de documentos hacen plena fe únicamente en cuanto al hecho de haberse otorgado y a su fecha, es decir, hacen fe incluso contra terceros en cuanto a estos dos aspectos. Pero en cuanto a la veracidad del contenido del instrumento, éste hace fe únicamente respecto de sus otorgantes y de las personas a quienes se les haya transferido a título singular o a título universal las obligaciones o descargos contenidos en el instrumento. Considero importante anotar que no se puede utilizar ningún otro medio de prueba para justificar la ejecución de un determinado acto o la celebración de un contrato, cuando la ley exija que esto se lo haga mediante un instrumento público; pues si es que se evade esta exigencia la ley mirará simplemente como si nunca se hubiera celebrado el contrato o ejecutado el acto.

Ahora nos compete referirnos al instrumento privado, es decir aquel documento escrito, que haya sido elaborado por personas particulares, sin que haya intervenido en su elaboración ninguna persona pública, o que haya sido elaborado por personas públicas en actos que no son de su oficio. El Código de Procedimiento Civil al referirse a los instrumentos privados enumera, en su artículo ciento noventa y siete a los siguientes documentos que constituyen instrumentos privados: los vales simples y las cartas, las partidas de entrada y las de gastos diarios, los libros administrativos y los de caja, las cuentas extrajudiciales, los inventarios, tasaciones, presupuestos extrajudiciales y asientos privados y, los documentos a los que se refiere el artículo ciento noventa y seis y el artículo ciento noventa y ocho del Código de Procedimiento Civil.

En cuanto a los documentos mencionados en el artículo ciento noventa y seis del Código de Procedimiento Civil, debemos manifestar que estos se refieren a todos aquellos actos y contratos que pueden otorgarse en escritura privada, por no exigir la ley que se otorguen mediante escritura pública.

Los documentos indicados en el artículo ciento noventa y ocho se refieren a aquellos instrumentos en que una persona se obliga a dar, hacer o no hacer una cosa, o acepta haber recibido una cosa o estar satisfecha con el cumplimiento de una determinada obligación. Además debemos anotar que estos instrumentos pueden gozar de la misma eficacia probatoria de la que gozan los instrumentos públicos en los siguientes casos: cuando el autor del documento reconoce su autoría ante cualquier juez de lo civil o mediante escritura pública; cuando el autor del instrumento se niega a reconocerlo a pesar de que existe orden judicial; cuando por haber muerto el autor del instrumento, por haber negado su autoría sobre el instrumento, o por hallarse fuera de la república, comparecen dos testigos ante el juez de lo civil y declaran haber visto a esta persona otorgar el instrumento; finalmente, el instrumento privado goza de la misma fe probatoria que el instrumento público cuando la parte contra quien se presenta el instrumento no alega la falsedad del mismo, ni objeta su legitimidad, dentro de los tres días contados desde que se le citó y notificó la presentación del instrumento, aunque no lo haya reconocido expresamente o se halla probado con testigos.

Otro tema que, sin duda, merece ser tratado es el de la incorporación por remisión de la que habla nuestra Ley de Comercio Electrónico en su artículo tercero; este punto es importante porque se refiere a toda aquella información que no está contenida de una forma directa en el mensaje de datos principal; pero sin embargo, al existir una especie de vinculo o anexo dentro del mensaje de datos principal, permite que dicha información pueda ser revisada por medio de un enlace electrónico; nuestra ley además exige que esta información sea conocida y aceptada de una forma expresa por las partes:

> “Art. 3.- Incorporación por remisión.- Se reconoce validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que

> figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes."

El artículo cinco de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre Comercio Electrónico, en su inciso segundo, contiene un principio de no discriminación respecto de la información que conste a manera de remisión en un mensaje de datos:

> "No se negarán efectos jurídicos, validez ni fuerza obligatoria a la información por la sola razón de que no esté contenida en el mensaje de datos que se supone ha de dar lugar a este efecto jurídico, sino que figure simplemente en el mensaje de datos en forma de remisión."

Como un ejemplo de la incorporación por remisión a la que nos hemos referido, podemos citar el caso de una transacción en la que una persona, a la cual llamaremos A, mediante un correo electrónico invita a otra persona, quien será B, a celebrar un contrato, ofreciéndole la entrega de un determinado producto, siempre que B pague una determinada suma de dinero, cabe recalcar que esta oferta consta en un correo electrónico. Sin embargo, en el correo electrónico existe un hipervínculo[1], el cual permite acceder a la información en la que se detallan todas las características de dicho producto, es decir esta información, no aparece en el correo electrónico, sino que B debe ingresar a dicha información mediante el hipervínculo que se encuentra en el correo electrónico principal.

En nuestra legislación según el artículo tres de la Ley de Comercio Electrónico que ya lo citamos, la información que contiene los detalles del objeto que A ofrece a B, y a la que se accede por medio del hipervínculo, goza de validez jurídica, pues a pesar de que no se encuentre directamente en el mensaje de datos principal, es decir en el correo electrónico, nuestra ley da la posibilidad de que ésta goce de validez jurídica, cumpliendo con ciertos requisitos que la misma Ley de Comercio Electrónico determina en su artículo tres.

[1] Hipervínculo: enlace que se encuentra en una determinada página web o un archivo, que tiene como función permitir el acceso a otra página web u otro archivo.

Corresponde ahora analizar los requisitos a los que nos hemos referido, y podemos establecer como un primer requisito el hecho de que la información conste en forma de remisión en el mensaje de datos, mediante un enlace electrónico directo; en el caso del ejemplo que hemos citado en líneas anteriores se estaría cumpliendo con este requisito, pues existe la información que consta en forma de remisión y a la cual se accede por medio del hipervínculo que se encuentra en el correo electrónico.

El segundo requisito que debe cumplirse, para que la información por remisión pueda tener validez jurídica, es que ésta sea conocida y aceptada por las partes; pero la aceptación que hacen las partes de la información por remisión, no se trata de una simple aceptación, sino que debe ser manifestada de una forma inequívoca y mediante otro mensaje de datos en el que se confirme la aceptación de dicha información. Este requisito además está recogido en el segundo inciso del artículo uno del Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos que a continuación lo cito textualmente:

> "La aceptación que hacen las partes del contenido por remisión deberá ser expresada a través de un mensaje de datos que determine inequívocamente tal aceptación. En el caso del contenido incorporado por remisión a través de un enlace electrónico, no podrá ser dinámico ni variable y por tanto la aceptación expresa de las partes se refiere exclusivamente al contenido accesible a través del enlace electrónico al momento de recepción del mensaje de datos."

Creo que con esta disposición no queda duda respecto de lo que ya había manifestado; pues la información por remisión debe ser conocida por las partes y debe ser aceptada expresamente, mediante otro mensaje de datos, de esta forma se está manifestando inequívocamente la intención de las partes de aceptar la información por remisión.

Cuando el artículo uno del Reglamento a la Ley de Comercio Electrónico expresa que el contenido que se haya incorporado por remisión no puede ser ni dinámico ni variable, lo que está buscando es brindar seguridad a la partes, de modo que si se da

la aceptación de un determinado contenido, que conste a manera de remisión en un mensaje de datos, lo que se esté aceptando sea ése contenido, y no ningún otro que posteriormente pudiera aparecer.

Para clarificar este punto, vamos a acudir nuevamente al ejemplo al que nos referimos en líneas anteriores , en el que A ofrece un producto a B mediante un correo electrónico, el mismo que posee un hipervínculo a través del cual se puede acceder a otro documento que contiene las características del producto, constituyéndose este contenido, en la información por remisión; información que solo tendría valor si B acepta celebrar el contrato con A, y ambos conocen y aceptan la información por remisión, mediante la forma prevista en la ley, es decir B envía un mensaje de datos para aceptar expresamente el contenido por remisión que A le envía en su correo electrónico; y siendo exclusivamente éste el contenido que tendría valor, es decir el que constaba en el momento en que B envió el mensaje de datos para aceptarlo.

Es preciso anotar que, en virtud del reglamento a la Ley de Comercio Electrónico, cuando una persona efectúe operaciones, o en fin tenga algún tipo de relación con los consumidores por medio de un mensaje de datos, esta persona tiene la responsabilidad de asegurar que los anexos o remitidos que consten en su mensaje de datos, tengan la suficiente disponibilidad, para que el consumidor, cuando lo crea pertinente, pueda acceder a ellos mediante un medio aceptable; además todo anexo o remitido que se refiera o que involucre derechos, garantías u obligaciones de los consumidores debe observar y respetar lo que dispone la Ley Orgánica de Defensa al Consumidor. Tratándose de otro tipo de relaciones, las partes pueden acordar la forma en la que se accederá a la información por remisión.

Otro punto de importancia que vale la pena resaltar es el que se refiere a las modificaciones que pudieran presentarse en la información por remisión. Para estos casos el Reglamento a la Ley de Comercio Electrónico, establece que de darse alguna modificación en el anexo o remitido esta debe ser comunicada al receptor del mensaje de datos; pero no basta con el simple comunicado que el emisor haga al receptor, sino que debe notificarse mediante otro mensaje de datos, o por escrito; además el emisor debe resaltar los aspectos que hayan sido modificados en el anexo

o remitido, para que el destinatario pueda apreciar sin dificultades las modificaciones efectuadas.

Si es que la notificación se da mediante un mensaje de datos, debe incorporarse en el mismo un enlace que permita al destinatario acceder al contenido original del anexo o remitido; este enlace debe estar ubicado en un lugar visible para que el destinatario pueda acceder a su contenido.

Ahora, si es que se modifica un anexo o remitido de un mensaje de datos que tenga que ver con algún tipo de relación en la que esté involucrado un consumidor, y el emisor procede, conforme corresponde, a comunicar al consumidor de la modificación que ha sufrido el anexo o remitido, no por este hecho quiere decir que el consumidor está aceptando el nuevo contenido del anexo; pues para que la aceptación por parte del consumidor se perfeccione es preciso que sea expresa, y el Reglamento a la Ley de Comercio Electrónico faculta al consumidor a comunicar su aceptación tanto por medios electrónicos como físicos.

Por último debemos señalar que cuando la ley exija que cierta información esté incorporada directamente en el mensaje de datos, ésta no puede constar como anexo o remitido en el mensaje de datos. Un ejemplo de esta situación lo podemos encontrar en la Ley Orgánica de Defensa al Consumidor, la misma que en el inciso primero de su artículo cuarenta y uno expone lo siguiente:

> "Art. 41.- El contrato de adhesión.- El contrato de adhesión deberá estar redactado con caracteres legibles, no menores a un tamaño de fuente de diez puntos, de acuerdo a las normas informáticas internacionales, en términos claros y comprensibles y no podrá contener remisiones a textos o documentos que, no siendo de conocimiento público, no se faciliten al consumidor previamente a la celebración del contrato."

1.4 Información escrita, e información original.

Este es un tema realmente interesante que nos presenta la Ley de Comercio Electrónico, y se refiere a todos aquellos casos en que la ley requiere o exige que

cierto tipo de información conste por escrito. Para estos casos, la Ley de Comercio Electrónico ha previsto la posibilidad de que dicha exigencia quede cumplida con un mensaje de datos, siempre y cuando la información que esté incorporada en el mensaje de datos pueda ser accesible para su posterior consulta.

Entonces cuando la ley exija que determinada información conste por escrito, pero dispongamos de un mensaje de datos en el cual esté incorporada dicha información, no será necesario el documento escrito, siendo éste reemplazado por el mensaje de datos en virtud de la ley. Un ejemplo de esta situación lo podemos encontrar en la Ley Modelo de la Comisión de las Naciones Unidas (CDUDMI) para el Derecho Mercantil Internacional sobre Arbitraje Comercial Internacional, que en su artículo siete se refiere a los acuerdos de arbitraje, definiéndolos de la siguiente manera:

> "El acuerdo de arbitraje es un acuerdo por el que las partes deciden someter a arbitraje todas las controversias o ciertas controversias que hayan surgido o puedan surgir entre ellas respecto de una determinada relación jurídica, contractual o no contractual."

Según este mismo artículo, el acuerdo, para someter una controversia a arbitraje, debe constar por escrito, pero el inciso cuarto de éste mismo artículo manifiesta lo siguiente:

> "El requisito de que un acuerdo de arbitraje conste por escrito se cumplirá con una comunicación electrónica si la información en ella consignada es accesible para su ulterior consulta. Por "comunicación electrónica" se entenderá toda comunicación que las partes hagan por medio de mensajes de datos."

Ahora, si bien un mensaje de datos puede cumplir aquella exigencia de la ley, en virtud de la cual determinada información debe constar por escrito, surge una necesidad, esta es, averiguar cuando la información que se encuentra comprendida en un mensaje de datos es considerada accesible para su posterior consulta, pues solo cuando esta información es accesible para su posterior consulta, el mensaje de

datos puede suplir al documento escrito, así la ley exija que sea el documento físico el que contenga determinada información.

El Reglamento a la Ley de Comercio Electrónico establece en su artículo dos que para que un mensaje de datos, sus anexos o sus remitidos puedan considerarse como accesibles para su posterior consulta, deben brindar la posibilidad de recuperar en forma íntegra la información que éstos poseen, en cualquier momento, y mediante los métodos que hayan sido previstos para tal efecto; estos métodos o procedimientos deben estar detallados y proporcionados en forma independiente al mensaje de datos, para que mediante su uso pueda garantizarse la posterior consulta del contenido de los mensajes de datos, anexos o remitidos.

En definitiva podemos decir que cuando la ley exija que cierta información conste por escrito, esta exigencia podrá cumplirse con un mensaje de datos; pero siempre y cuando la información contenida en el mensaje de datos sea susceptible de posterior consulta.

Según lo que hemos anotado, para que un mensaje de datos sea considerado accesible para su posterior consulta, éste debe cumplir con los siguientes requisitos: en primer lugar la información que el mensaje de datos posee debe tener la posibilidad de ser almacenada en un lenguaje electrónico/informático que tanto las partes que intercambian información, a través de los mensajes de datos, como sus correspondientes sistemas informáticos tengan la posibilidad de entenderla; en segundo lugar debe existir la posibilidad de que el contenido del mensaje de datos sea recuperado en forma íntegra y en cualquier momento; y por último debe proporcionarse, independientemente al mensaje de datos, los métodos o procedimientos con los que se podrá acceder a la información que el mensaje de datos posee.

Todo lo dicho se refiere a los documentos escritos. Ahora nos compete referirnos a la situación de los documentos originales, y al respecto vamos a manifestar que cuando la ley requiera o exija que un documento deba ser presentado en su forma original, ésta exigencia quedará cumplida con el mensaje de datos, siempre que se

pueda comprobar que el mensaje de datos que se generó por primera vez no ha sufrido modificación alguna desde entonces.

La Ley de Comercio Electrónico en el artículo siete, inciso segundo establece las circunstancias en que el mensaje de datos se considera íntegro: "Se considera que un mensaje de datos permanece integro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación."

Para complementar la disposición antes transcrita el Reglamento a la Ley de Comercio Electrónico establece lo siguiente en su artículo seis:

> "Integridad de un mensaje de datos.- La consideración de integridad de un mensaje de datos, establecida en el inciso segundo del artículo 7 de la Ley 67, se cumple si dicho mensaje de datos está firmado electrónicamente. El encabezado o la información adicional en un mensaje de datos que contenga exclusivamente información técnica relativa al envío o recepción del mensaje de datos, y que no altere en forma alguna su contenido, no constituye parte sustancial de la información.
>
> Para efectos del presente artículo, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún cambio que sea inherente al proceso de comunicación, archivo o presentación."

Por todo lo anotado concluimos en que cuando la ley exija que determinada información sea presentada en su forma original, esta exigencia puede ser obviada con la presencia de un mensaje de datos, mensaje de datos que debe cumplir con una condición para que pueda suplir la exigencia del documento original; esta condición se refiere a que exista la posibilidad de comprobar que el mensaje de datos que se generó por primera vez permanece integro, y que por consiguiente no ha sido objeto de ninguna modificación. Entonces para poder sustituir al documento físico original por el mensaje de datos, debemos demostrar la integridad de éste último; nuestra ley considera que un mensaje de datos permanece íntegro cuando su contenido se

mantiene completo e inalterable desde la fecha en que el mensaje de datos fue creado, con la única salvedad de aquellos cambios que pudiera sufrir el mensaje de datos en cuanto a su forma, y que sean propios del proceso de comunicación.

Estas disposiciones de la Ley de Comercio Electrónico adoptan la política establecida por la Guía para la Incorporación al Derecho Interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, política que aspira reducir el uso de la información plasmada en papeles. Pues esta guía en su literal "e", que se refiere al criterio del "equivalente funcional", manifiesta que aquellos requisitos legales que exigen el uso o la presentación de documentos en forma escrita o en su forma original, son los causantes de que los medios de comunicación modernos no puedan progresar. Este criterio de equivalencia funcional, que se aplica para los mensajes de datos, pretende que todas las funciones que desempeña el documento escrito, sean desempeñadas por el mensaje de datos, es por ello que se han dictado estas normas, que buscan eliminar aquella forma tradicional de presentar la información en el papel.

1.5 Documentos desmaterializados.

Antes de iniciar con este tema, voy a recurrir al glosario de términos que se encuentra en la disposición general novena de la Ley de Comercio Electrónico, con el único fin de tener una idea clara sobre lo que constituye la desmaterialización de los documentos: "Desmaterialización electrónica de documentos: Es la transformación de la información contenida en documentos físicos a mensajes de datos."

Ahora que tenemos claro lo que es la desmaterialización voy a permitirme citar textualmente lo que establece el inciso tercero del artículo siete, de la Ley de Comercio Electrónico: "Por acuerdo de las partes y cumpliendo con todas las obligaciones previstas en esta ley, se podrán desmaterializar los documentos que por ley deban ser instrumentados físicamente."

Esta disposición otorga la facultad a las partes de acordar la desmaterialización de los documentos físicos, es decir convertir estos documentos físicos en mensajes de

datos, trasladando la información contenida en el papel a un soporte electrónico; a pesar de que la ley exija que cierta información conste por escrito.

Los documentos desmaterializados son conocidos también como documentos electrónicos derivados, debido a que la información que se halla contenida en los mismos, originariamente estuvo plasmada en papel.

Pero no es suficiente el acuerdo entre las partes para que un documento sea correctamente desmaterializado, pues si nos acogemos a lo que establece la Ley de Comercio Electrónico en el inciso cuarto de su artículo siete, tenemos que es necesario cumplir con dos requisitos para que la desmaterialización sea eficaz. En primer lugar los documentos desmaterializados deben poseer las firmas electrónicas respectivas, y además el documento desmaterializado debe ser conservado de conformidad con lo que establece la ley.

Con relación al primer requisito, como habíamos manifestado ya, el documento desmaterializado debe contar con las firmas electrónicas de las partes, firmas que deben estar acompañadas de su respectivo certificado, el mismo que debe ser emitido por una de las entidades de certificación que se encuentre acreditada por el Consejo Nacional de Telecomunicaciones. Del estudio de las firmas electrónicas nos ocuparemos en el segundo capítulo de este trabajo, y de los certificados de firma electrónica en el tercer capítulo. En cuanto a las entidades de certificación el artículo veinte y nueve de la Ley de Comercio Electrónico las define como:

> "Las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República."

El artículo siete de la Ley de Comercio Electrónico exige, como segundo requisito, que el documento desmaterializado sea conservado de conformidad con lo que establece el artículo ocho del mismo cuerpo legal; nos referiremos a la conservación de los documentos desmaterializados más adelante.

El reglamento a la Ley de Comercio Electrónico también tiene normas bastante claras que se refieren a la desmaterialización de los documentos, así en su artículo cuatro este reglamento manifiesta que tanto los mensajes de datos como los documentos desmaterializados deben ser, cuando la ley así lo exija o dependiendo de cada caso, certificados ante un notario, o ante la autoridad competente, o por la persona autorizada por la firma electrónica.

Este mismo artículo declara, en cuanto al valor que tienen los documentos desmaterializados dentro de nuestro ordenamiento jurídico, que éstos se considerarán copia idéntica del documento físico del cual nacieron, así manifiesta que los documentos desmaterializados surten los mismos efectos que las copias impresas certificadas por autoridad competente; pero deben contener la indicación de ser documentos desmaterializados.

Como ya manifestamos la ley autoriza a las partes a pactar la desmaterialización de un documento físico, pero este acuerdo entre las partes debe constar en un documento físico o electrónico, con sus correspondientes firmas y con la admisión de que el documento desmaterializado es idéntico al original; adicionalmente cuando la ley lo exija o exista acuerdo entre las partes, debe existir una certificación electrónica por parte de un notario o autoridad competente, estos certificarán al documento con su respectiva firma electrónica.

1.6 Conservación de los mensajes de datos.

Como habíamos manifestado ya en líneas anteriores, para que un documento físico sea correctamente desmaterializado existen ciertos requisitos que deben ser inexorablemente observados.

Uno de los requisitos a los que nos referimos en el párrafo anterior se encuentra establecido en el artículo siete de la Ley de Comercio Electrónico, que establece que el documento desmaterializado sea conservado de conformidad con lo que establece el artículo ocho del mismo cuerpo legal.

El artículo ocho de la Ley de Comercio Electrónico establece que toda información que sea regulada por este cuerpo legal puede ser sometida a conservación; conservación que se verifica con el archivo del mensaje de datos. Ahora, si bien la ley manifiesta que con el archivo del mensaje de datos se está cumpliendo con la conservación del mismo, y por ende, la desmaterialización del documento físico sería eficaz, por respetar esta exigencia legal; el mismo artículo ocho de la Ley de Comercio Electrónico se encarga de establecer como condiciones para el archivo del mensaje de datos las siguientes:

"a. Que la información que contenga sea accesible para su posterior consulta."

Este primer requisito, que se refiere a que la información contenida en el mensaje de datos sea accesible para su posterior consulta, ya lo analizamos cuando tratamos el tema de los documentos escritos y de los documentos originales, por lo que nos limitaremos a anotar de una forma muy sintética que para que un mensaje de datos pueda ser considerado accesible para su posterior consulta éste debe, en primer lugar, estar almacenado en un sistema electrónico/informático que tanto las partes como sus sistemas informáticos tengan la posibilidad de entenderlos, además debe brindar la posibilidad de recuperar en forma íntegra su contenido, en cualquier momento, y finalmente debe proveerse en forma independiente al mensaje de datos los métodos o procedimientos con los que se podrá recuperar la información.

"b. Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable que reproduce con exactitud la información generada, enviada o recibida."

En cuanto a este segundo requisito, que exige que el mensaje de datos sea conservado en el formato en el que se haya generado, o cualquier otro formato, siempre y cuando este nuevo formato brinde la posibilidad de demostrar que su contenido es idéntico al del mensaje de datos original, podemos manifestar que tiene por única finalidad brindar a las partes seguridad jurídica, pues si la ley facultara a las personas para que conserven sus mensajes de datos en cualquier formato, aunque éste formato no permitiera verificar su contenido, la ley estaría generando una gran incertidumbre en las partes involucradas, al no estar seguras del contenido exacto del mensaje de datos que se está conservando. Por lo que considero que es prudente la

posición que adopta la ley al exigir que el mensaje de datos se conserve en el mismo formato o en uno distinto pero que permita establecer que su contenido es idéntico al del mensaje de datos originario.

"c. Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado."

Este tercer requisito que exige que se conserve todo dato concerniente tanto al origen como al destino del mensaje de datos, así como fecha y hora en que fue creado, enviado y archivado, es de gran importancia; pues como ya dijimos, los mensajes de datos gozan de la misma eficacia probatoria que los documentos escritos, siempre que cumplan con los requisitos ya analizados, y si por ejemplo utilizáramos en un juicio un mensaje de datos para justificar una determinada situación, jugarían un papel crucial los datos referentes al origen y destino del mensaje de datos así como la fecha y hora de su creación, envío o archivo.

"d. Que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley."

Como último requisito la ley exige que se garantice la integridad del mensaje de datos por el tiempo que el Reglamento a la Ley de Comercio Electrónico haya establecido; respecto de esta exigencia creo conveniente recordar el inciso segundo del artículo siete de la Ley de Comercio Electrónico que manifiesta lo siguiente: "Se considera que un mensaje de datos permanece integro, si se mantiene completo e inalterable su contenido, salvo algún cambio de forma, propio del proceso de comunicación, archivo o presentación."

El Reglamento a la Ley de Comercio Electrónico en su artículo seis también se refiere a la integridad de los mensajes de datos, y en su inciso segundo manifiesta lo siguiente: "Para efectos del presente artículo, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún cambio que sea inherente al proceso de comunicación, archivo o presentación."

De lo anotado se desprende que en cuanto a la integridad de los mensajes de datos nuestra ley es bastante clara, pero si recordamos el último requisito de la conservación de los mensajes de datos, tenemos que se debe garantizar su integridad por el tiempo que establezca el Reglamento a la Ley de Comercio Electrónico, y el reglamento expone lo siguiente: "En los procesos de conservación de los mensajes de datos, se debe garantizar la integridad de los mismos al menos por el mismo tiempo que las leyes y reglamentos exijan su almacenamiento."

El artículo ocho de la Ley de Comercio Electrónico en su inciso final otorga la facultad a cualquier persona para que pueda conservar un mensaje de datos mediante los servicios de un tercero; estos servicios que brindan terceras personas se denominan Registros Electrónicos de Datos. El Reglamento a la Ley de Comercio Electrónico, en su artículo nueve, establece las actividades que pueden realizar los Registros Electrónicos de Datos:

> "a. Conservación, almacenamiento y custodia de la información en formato electrónico con las debidas seguridades;
> b. Preservación de la integridad de la información conservada;
> c. Administración del acceso a la información y la reproducción de la misma cuando se requiera;
> d. Respaldo y recuperación de información; y,
> e. Otros servicios relacionados con la conservación de los mensajes de datos."

1.7 Protección de datos.

Del Peso Navarro (2003) señala que la información siempre ha sido un bien valioso, pero hoy en día no solo que es un bien valioso, sino que es un bien absolutamente necesario; por lo que ha llegado a manifestarse que actualmente vivimos en una sociedad de la información.

En la actualidad las empresas si desean ingresar a los distintos mercados, deben previamente obtener la debida información respecto de aquellos; y dentro de esta información han cobrado especial importancia los datos de carácter personal. De esta

forma se han creado numerosas redes sociales, en las cuales se incluyen precisamente estos datos de carácter personal, como una forma de captación de clientes, pues con estos datos se puede, por ejemplo, enviar publicidad personificada, resultando ser ésta más eficaz e incluso más económica. Esto ha originado a su vez una mayor circulación de correspondencia tanto postal como electrónica, generándose un gran volumen de esta última.

Es por esta razón que nuestra Ley de Comercio Electrónico establece que cuando se requiera elaborar, transferir o utilizar bases de datos que procedan de la transferencia o utilización de mensajes de datos, debe existir el consentimiento del titular de los mismos, y será él quien seleccione la información que será compartida con terceros, de esta forma aquella información que no seleccione simplemente no podrá ser compartida.

Nuestra Ley de Comercio Electrónico se preocupa de que los derechos de las personas no se vean vulnerados por el uso de los mensajes de datos, pues en su artículo nueve declara que en la recopilación y uso de datos personales se deben respetar los derechos de intimidad, confidencialidad y privacidad.

La Ley de Comercio Electrónico, en su glosario de términos contenido en la disposición general novena, al referirse a los datos personales indica que son "Aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley"

Estos datos únicamente pueden ser utilizados previa autorización de la persona a quien pertenecen, o por orden de autoridad competente. Por esto es importante que la ley establezca que tipo de datos ha de ser considerado como personal, y de esta forma evitar que para la utilización de cualquier tipo de datos, aunque no tenga el carácter de personal, deba contarse con el permiso de su titular.

Ahora bien, como sabemos toda regla general tiene su excepción, y en el inciso tercero del artículo nueve de la Ley de Comercio Electrónico está la excepción a esta regla:

> "No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato."

Éste mismo artículo, en su inciso final, establece que el consentimiento que presta una persona para que se utilicen sus datos, puede ser revocado en cualquier momento por la persona titular de los mismos, pero en todo caso esta revocatoria no puede tener efecto retroactivo.

1.8 Procedencia e Identidad de un Mensaje de Datos, Excepciones.

Para determinar la procedencia e identidad de un mensaje de datos, nuestra Ley de Comercio Electrónico ha establecido una presunción legal. Pues el artículo diez de la Ley de Comercio Electrónico, presume, a no ser que exista prueba en contrario, que un mensaje de datos proviene de aquella persona que ha enviado el mensaje de datos; además autoriza al destinatario del mensaje de datos para que actúe de conformidad con el contenido del mismo, siempre que de la verificación exista concordancia entre la dirección ip y la firma electrónica del emisor. Esta regla tiene excepciones, y a continuación las vamos a enunciar.

La primera excepción se presenta en los casos en que se da aviso que un mensaje de datos no proviene de quien consta como emisor; en estos casos el comunicado debe realizase antes de que el destinatario actúe de conformidad al contenido del mensaje de datos. Si es que no se logra dar aviso de esta situación, y el destinatario ya actúa conforme al contenido del mensaje de datos, la persona que conste como emisor debe justificar que el mensaje se envió sin su autorización o el mismo fue alterado.

La otra excepción se refiere al hecho de que el receptor o destinatario de un mensaje de datos no hubiere realizado de una manera diligente la verificación referente a la coincidencia entre la identidad del autor del mensaje de datos y su firma electrónica, o simplemente no le dio importancia a su resultado.

Ya que hablamos acerca de la verificación de la coincidencia entre la identidad del emisor de un mensaje de datos y su firma electrónica, considero de utilidad recurrir al Reglamento de la Ley de Comercio Electrónico que manifiesta en su artículo siete que para la verificación de la concordancia entre la identidad y la firma electrónica del emisor de un mensaje de datos, se tendrá en cuenta la vigencia y los datos que contenga el certificado de firma electrónica que respalde a su firma.

Otro aspecto importante que se haya contenido en esta norma es aquel que se refiere al aviso que debe hacerse respecto de un posible riesgo que pueda tener un mensaje de datos, la firma electrónica o su certificado de firma electrónica por parte del titular de los mismos al destinatario. Este aviso puede realizarse a través de cualquier medio, y debe tener la posibilidad de prevenir al destinatario, para que tome las medidas necesarias con el fin de evitar que sus intereses se vean menoscabados.

Entonces, si actuamos de conformidad con el Reglamento a la Ley de Comercio Electrónico, la verificación, que debemos hacer respecto de la concordancia entre la identidad del emisor del mensaje de datos y su firma electrónica, debemos efectuarla comprobando la vigencia y los datos del certificado de firma electrónica que respalde la firma del emisor. Tratándose de otro tipo de firma o sistema de identificación se verificará esta concordancia con los correspondientes registros que se requieran dependiendo del caso.

1.9 Envío y Recepción de los Mensajes de Datos.

Respecto del envío y de la recepción del mensaje de datos, nuestra Ley de Comercio Electrónico manifiesta en su artículo once que de no existir pacto en contrario, se presumirá que el tiempo y lugar de emisión y recepción de un mensaje de datos son los siguientes:

> "a) Momento de emisión del mensaje de datos.- Cuando el mensaje de datos ingrese a un sistema de información o red electrónica que no esté bajo control

> del emisor o de la persona que envió el mensaje en nombre de éste o del dispositivo electrónico autorizado para el efecto."

Esto quiere decir que el momento en que la ley presume se emitió el mensaje de datos es cuando éste ingresa al sistema de un tercero.

> "b) Momento de recepción del mensaje de datos.- Cuando el mensaje de datos ingrese al sistema de información o red electrónica señalado por el destinatario. Si el destinatario designa otro sistema de información o red electrónica, el momento de recepción se presumirá aquel en que se produzca la recuperación del mensaje de datos. De no haberse señalado un lugar preciso de recepción, se entenderá que ésta ocurre cuando el mensaje de datos ingresa a un sistema de información o red electrónica del destinatario, independientemente de haberse recuperado o no el mensaje de datos."

Según este literal el momento de la recepción se produce cuando el mensaje de datos ingresa a la red electrónica o sistema señalado por el destinatario, si el destinatario ha señalado otra red o sistema la recepción se efectúa en el momento en que el destinatario recupera el mensaje de datos, y por fin si el destinatario no ha señalado una red o sistema preciso la recepción se efectúa cuando el mensaje de datos entra en la red del destinatario, independientemente de que haya recuperado o no el mensaje de datos.

> "c) Lugares de envío y recepción.- Los acordados por las partes, sus domicilios legales o los que consten en el certificado de firma electrónica, del emisor y del destinatario. Si no se los pudiere establecer por estos medios, se tendrán por tales, el lugar de trabajo, o donde desarrollen el giro principal de sus actividades o la actividad relacionada con el mensaje de datos."

1.10 Conclusiones.

Una vez que hemos concluido el análisis de todos los aspectos referentes a los mensajes de datos, podemos determinar si es que existe o no algún beneficio en el hecho de que la información conste como un mensaje de datos.

Gracias a los principios de no discriminación y de equivalencia funcional, que se hayan recogidos por nuestro ordenamiento jurídico, el mensaje de datos puede producir los mismos efectos jurídicos que producen los documentos escritos. Por lo que no existe diferencia alguna entre los mensajes de datos y los documentos escritos, en lo que se refiere a los efectos jurídicos que estos producen. Lo único que diferencia a un mensaje de datos de un documento escrito es su soporte, siendo el papel el soporte de los documentos escritos; y los medios electrónicos el soporte de los mensajes de datos.

Entonces, partiendo del hecho de que los mensajes de datos producen los mismos efectos jurídicos que los documentos escritos, puedo decir que existen ciertos beneficios cuando la información consta en un mensaje de datos; pues en primer lugar el mensaje de datos tiene el mismo valor legal que tienen los documentos escritos dentro de nuestro ordenamiento jurídico, y no por el hecho de constar en un medio electrónico puede negársele validez. Además el soporte de la información de un mensaje de datos, es decir los medios electrónicos, brinda a las personas ciertos beneficios como son la rapidez con la que se puede acceder a esta información, el ahorro de espacio físico, existe una menor probabilidad de que esta información se pierda o se destruya, se puede mantener esta información de una manera más ordenada que si constara en papel, e incluso existen beneficios ecológicos al guardar la información como un mensaje de datos, pues de esta forma se evita un desperdicio de papel; por estas razones los países están adoptando políticas en virtud de las cuales se pretende reemplazar el papel por los mensajes de datos.

En cuanto al marco legal vigente respecto de los mensajes de datos creo que es muy conveniente tener en cuenta la definición que respecto de los mensaje de datos da nuestra Ley de Comercio Electrónico, pues como manifestamos, éste cuerpo legal se refiere de una manera taxativa a las figuras que constituyen mensajes de datos; con lo que se descarta la posibilidad de que modernas formas que pudieran aparecer en el futuro, sean calificadas como mensajes de datos. Con esta disposición se obliga al legislador a realizar un eficaz seguimiento respecto de aquellas figuras que pudieran aparecer en el futuro y que deberían ser consideradas mensajes de datos, para que en base a este seguimiento puedan ser contempladas dentro de la normativa legal, y así evitar vacíos legales; o simplemente debería cambiarse la forma en que se redacta el artículo tres de la Ley de Comercio Electrónico, que contiene el concepto de mensaje

de datos, de manera que se permita que estas nuevas figuras puedan ser calificadas como mensajes de datos.

CAPÍTULO 2.

LA FIRMA ELECTRÓNICA.

2.1 Introducción.

Las principales causas por las que varios de los negocios que se llevan a cabo mediante la vía telemática no se llegan a concretar, se refieren a la incertidumbre que existe en las partes respecto de la identidad de la contraparte, o la falta de garantías que existe en cuanto a la obligatoriedad de los ofrecimientos que efectúan las partes.

Para solventar estos inconvenientes la Ley de Comercio Electrónico reconoce y regula a la firma electrónica, como una figura que produce los mismos efectos que produce la firma ológrafa en los documentos escritos, pero dentro del ámbito de las relaciones telemáticas.

En este capítulo analizaremos los efectos de la firma electrónica, así como los requisitos que ésta debe reunir para que produzca estos efectos, estudiaremos las garantías que brinda la firma electrónica, el funcionamiento de la firma electrónica, para que luego de analizar estos aspectos podamos establecer si efectivamente la firma electrónica, brinda seguridad a las partes que intervienen en los contratos que se celebran mediante la vía telemática. Determinaremos además si es que la normativa legal que regula a la firma electrónica es adecuada.

2.2 Definición.

Para empezar este capítulo, creo conveniente referirme a un tema que considero de importancia, y que se refiere a los tipos de relaciones que tienen las personas dentro del ámbito comercial. Hocsman (2005) manifiesta que las relaciones entre las personas pueden ser de dos tipos: físicas y telemáticas. Siguiendo a este autor podemos decir que las relaciones telemáticas son aquellas que se desarrollan a la distancia y a través de las nuevas tecnologías, como por ejemplo el Internet. En

cambio las relaciones físicas constituyen todas aquellas operaciones que se desarrollan con la presencia de las partes que intervienen en tales operaciones.

Es indudable, que el desarrollo tecnológico ha traído como consecuencia un incremento incesante de las relaciones telemáticas, y gracias al desarrollo de estas relaciones hoy en día es posible que se concreten varios negocios a través del Internet, esto es lo que se conoce como contratación electrónica. A continuación diferenciaremos al contrato electrónico del contrato informático; Yánez (1999), expone que el contrato electrónico es aquel acuerdo de voluntades que se lo efectúa por medio de elementos electrónicos, mientras que el contrato informático es aquel acuerdo de voluntades en el cual el objeto de la negociación recae sobre bienes que tengan que ver con la informática, como por ejemplo un computador, software, periféricos, etc.

Las contrataciones electrónicas nos permiten efectuar transacciones con empresas o individuos que se encuentren en cualquier lugar del planeta, esto es, sin lugar a dudas, una gran ventaja; pero sin embargo éste tipo de contratos implican grandes riesgos, riesgos que se relacionan precisamente con la distancia existente entre las partes, pues nadie les garantiza que los ofrecimientos efectuados por la contraparte serán cumplidos, además el hecho de no saber a ciencia cierta con quien están negociando impide que exista seguridad en las contrataciones electrónicas.

El derecho debe brindar las herramientas necesarias para garantizar la seguridad dentro de los contratos electrónicos, es por esta razón que nace la figura de la firma electrónica.

Antes de definir a la firma electrónica vamos a empezar por definir a la firma ológrafa o manuscrita; Patricia Herrmann Fernández define a la firma como "Cualquier método o símbolo que expresa la intención de vincularse el autor del mismo o autenticar un documento." (Herrmann, 2007, P.109)

Para Herrmann (2007) existen varias técnicas que se usan para firmar un documento, como la firma ológrafa, o la firma manual que está plasmada en un sello o

digitalizada, o la clave de una tarjeta de crédito; pero lo que diferencia a estas técnicas es que cada una de ellas brinda diferentes seguridades.

Guillermo Cabanellas de Torres define a la firma de la siguiente manera: “Nombre y Apellido, o título que se pone al pie de un escrito, para acreditar que procede de quien lo suscribe, para autorizar lo allí manifestado, para obligarse a lo declarado.” (Cabanellas, 1998, P. 169)

De conformidad con los conceptos que hemos citado, podemos concluir en que la firma es aquel método en virtud del cual las personas escriben su nombre en un documento con la finalidad de indicar que el mismo es de su autoría y hacerse cargo de las obligaciones contenidas en el documento suscrito.

Ahora, si nos fijamos con detenimiento en los conceptos citados; podemos apreciar que la firma cumple con ciertas funciones como por ejemplo, dar autenticidad a un documento, aprobar su contenido, obligarse a lo declarado en el documento, o para indicar que el documento procede de quien lo firma. Estas funciones, que cumple la firma ológrafa, se tornan necesarias dentro del comercio electrónico, pues como hemos manifestado ya, la actual evolución de las transacciones telemáticas, exigen del Estado figuras que garanticen que estas transacciones van a ser seguras. Para garantizar la seguridad dentro de estas operaciones, nuestra Ley de Comercio Electrónico regula a la firma electrónica, esta es una figura que cumple con las funciones de la firma ológrafa pero dentro de las operaciones que se efectúen electrónicamente.

Cabe decir que no se puede aspirar a una seguridad absoluta, pues esta no se da ni en las transacciones ordinarias, pero, a pesar de ello, la firma electrónica reduce considerablemente la inseguridad en las relaciones telemáticas, pues pensemos cuan grave sería que una persona no pueda quedar obligada a lo que se compromete dentro de un contrato electrónico, simplemente no habría forma de hacer que la misma cumpla con lo que ofrece; la firma electrónica busca precisamente que este tipo de situaciones no se den en la práctica.

Según Hocsman (2005) para que la firma electrónica pueda cumplir con las funciones a las que ya nos hemos referido, ésta debe reunir dos características básicas: en primer lugar la firma debe brindar la posibilidad de identificar de una manera inequívoca a quien suscribió el documento, haciendo sea difícil el intento de reproducción o copiado de la firma por parte de otra persona; y en segundo lugar debe identificar el contenido del documento firmado, haciendo imposible que se pueda alterar el contenido del mismo, sin que se pueda verificar que se ha producido tal alteración.

A continuación vamos a tomar el concepto de firma electrónica que nos trae la Ley de Comercio Electrónico en su artículo trece:

> "Firma electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos."

La Comunidad Europea mediante la directiva 1999/93/CE del Parlamento Europeo y del Consejo define a la firma electrónica de la siguiente manera: "Los datos en forma electrónica anexos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación."

El concepto de firma electrónica que brinda nuestra Ley de Comercio Electrónico es un concepto amplio, y me parece que es prudente la postura que tiene nuestra legislación, pues de esta forma se admite la posibilidad de que nuevas modalidades con las que se pueda firmar un documento electrónicamente puedan entrar dentro de esta definición; pues como sabemos la tecnología avanza incesantemente, y siempre habrá innovaciones dentro del campo de las relaciones telemáticas.

2.3 Encriptación de datos.

Para poder entender cómo funciona una firma electrónica, considero que es de vital importancia referirnos a una ciencia que guarda íntima relación con el tema, ésta es

la criptografía. Aunque nos parezca un poco raro, la criptografía es una técnica que ya se había venido utilizando hace aproximadamente cuatro milenios, pues en Egipto se utilizaban jeroglíficos en las tumbas de los reyes que fallecían, en la India el gobierno utilizaba claves para comunicarse con una red de espías que se hallaban en todo su territorio, en Mesopotamia también se utilizó la criptografía mediante la escritura cuneiforme. En la Grecia antigua también existió la criptografía y una prueba de ello es el "método de Polibio", en la "La Ilíada" cuando uno de sus personajes es enviado ante un rey con una tabla secreta en la que se manifestaba que este debía matarlo; en Roma Julio Cesar para enviar mensajes secretos corría dos letras de su lugar en el alfabeto, Justiniano utilizaba como clave el rapado en las cabezas.

Etimológicamente la palabra criptografía viene de las voces griegas Krypto "secreto", y grapho "escritura", por lo que podemos concluir en que la criptografía es el arte de la escritura secreta.

Juan Carlos Galende Díaz define a la criptografía como "El arte de escribir en un lenguaje convenido mediante el uso de claves o cifras." (Galende, 1995, P.15) El doctor Heriberto Hocsman en su obra, "Los Negocios en el Internet" define a la criptografía como "La ciencia de usar la matemática para encriptar y desencriptar información, de manera tal que solo el destinatario pueda leerla." (Hocsman, 2005, P.363) En definitiva podemos decir que la criptografía es la ciencia que utiliza las matemáticas para transformar los mensajes legibles en ilegibles; esto con la finalidad de que terceras personas no puedan acceder a esta información, garantizando al destinatario que el mensaje que ha recibido no haya sido alterado.

Esta ciencia se encarga también de recuperar la información original, es decir transformar la información ilegible (encriptada) en legible (desencriptada), a esta parte de la criptografía se la conoce como criptoanálisis. Toda esta serie de procedimientos se realizan con el único fin de mantener la confidencialidad en el intercambio de la información, para que esta no pueda ser manipulada.

Existen dos tipos de criptografía: una simétrica y otra asimétrica, esta última es la más usada y es la que ha permitido el desarrollo de la firma electrónica. Respecto de

la encriptación simétrica podemos decir que es aquella en la que tanto el emisor como el receptor hacen uso de una misma clave, que le sirve al emisor para encriptar el mensaje y al receptor para desencriptar el mismo. En cambio la encriptación asimétrica es aquella en la que a una misma persona le corresponden dos tipos de claves, una pública y otra privada; la clave privada es conocida solo por su propietario, mientras que la clave pública es divulgada para que sea conocida por todos. En este tipo de encriptación, como ya lo mencionamos, tanto el emisor como el receptor tienen un par de claves; y al proceso de firmado lo vamos a resumir de la siguiente forma: el emisor envía su mensaje encriptándolo mediante la clave pública del receptor y emite su firma usando su clave privada, de esta forma el receptor podrá abrir el mensaje mediante la clave pública del emisor, y podrá desencriptar el mensaje usando su clave privada. Por lo que hemos anotado se evidencia que la coexistencia de las claves pública y privada tiene por finalidad hacer que la una sirva para encriptar el mensaje y la otra para desencriptar el mismo.

Una vez que ha concluido este proceso surge un problema: ¿Cómo sabe el destinatario si el mensaje que ha recibido no ha sido alterado? Para solventar este problema se ha desarrollado una técnica denominada Hashing. Para el doctor Heriberto Hocsman un hash es “un número que se obtiene haciendo una operación matemática sobre todos los datos del mensaje, de tal manera que si el mensaje variara aunque sea en un bit, el hash sería totalmente diferente”. (Hocsman, 2005, P.365) Esta es una función que permite al emisor obtener un resumen o extracto del mensaje de datos al aplicarla; de esta forma, cuando el destinatario reciba el mensaje, va a tener la posibilidad de verificar si el mensaje que ha recibido ha sido alterado o no; esto lo hará comparando el resumen que adjuntó el emisor a su mensaje, con el resumen que obtenga el destinatario al aplicar la función hash al mensaje que ha recibido; si es que los resúmenes son iguales el destinatario sabrá que el mensaje no ha sido alterado; pero si los resúmenes no coinciden sabrá que el mensaje ha sido alterado antes de que llegue a su poder.

Vale la pena anotar que cuando un mensaje ha sido alterado, aunque sea solo una coma la que se haya suprimido o aumentado, el resumen que obtenga el destinatario será totalmente distinto del original, lo que hace a esta función muy confiable al momento de verificar la integridad del mensaje de datos.

Para concluir con este tema debemos recordar que nos hemos referido al funcionamiento de la firma electrónica en base a la criptografía, que como ya lo habíamos mencionado, es la ciencia que permitió el desarrollo de la firma electrónica, especialmente la criptografía asimétrica, que hoy en día es la técnica más usada en todo el mundo para firmar los mensajes de datos. No obstante lo dicho, debemos hacer hincapié en el hecho de que la definición que trae nuestra legislación es una definición amplia, y por ende si es que en un futuro apareciera una técnica con la que también se puedan firmar electrónicamente los mensajes de datos, y esta encasilla dentro de la definición que trae nuestra Ley de Comercio Electrónico, no habría ningún problema para que esta técnica pueda ser usada.

Distinto es el caso del Estado de Utah, que en virtud de la Ley de Firma Digital del Estado de Utah del 1 de mayo de 1995, se concibió el concepto de firma electrónica bajo las características específicas de la criptografía asimétrica, definiendo de la siguiente forma a la firma electrónica: "La transformación de un mensaje usando un sistema de criptografía asincrónica tal que una persona, teniendo el mensaje inicial y la clave pública del firmante, puede determinar con precisión si la transformación ha sido creada usando la clave privada que corresponde a la clave pública, y si el mensaje ha sido alterado desde que se ha hecho la transformación." Como vemos en este caso la definición es una definición rígida, lo cual para mi punto de vista es un error, pues como ya habíamos apuntado, el incesante desarrollo tecnológico, permite el desarrollo de diversas técnicas o la implementación de nuevas tecnologías que puedan aplicarse para brindar mayor seguridad en el desarrollo de las relaciones telemáticas.

Para concluir debemos manifestar que no debemos confundir a la firma electrónica con otras técnicas que existen para firmar dentro del marco de las relaciones telemáticas, como por ejemplo el escaneo de la firma manuscrita, o un código secreto utilizado para identificar a una persona, o el escaneo de la huella digital por medio de instrumentos digitales; debemos tener claro que nuestra ley no se refiere a ninguna de estas técnicas, pues como bien dice la Ley de Comercio Electrónico, la firma electrónica no es más que, un bloque de caracteres asociado o lógicamente

adjuntado a un mensaje de datos, y que sirven para identificar al autor del mismo, y para expresar la aquiescencia del autor del mensaje con el contenido del mismo.

2.3 Garantías de la Firma Electrónica.

Como habíamos anotado en líneas anteriores el desarrollo de las relaciones telemáticas genera muchas ventajas para quienes optan por esta vía, pero este tipo de relaciones exigen cierta seguridad, como por ejemplo, el saber si cierto mensaje de datos proviene de una determinada persona, o el saber si esta persona aprueba el contenido del mensaje, para resolver este tipo de inconvenientes, que podrían suscitarse en las relaciones telemáticas, se utiliza la firma electrónica. Entonces, la firma electrónica es un método que permite establecer la autoría de un mensaje de datos, además de la aprobación del contenido del mensaje por parte del autor, otra de sus garantías es la integridad del mensaje, como también el dotar de autenticad al mismo. La firma electrónica está regida por algunos principios que consolidan las garantías que hemos anotado, estos principios son:

- Principio de analogía: este principio exige que a la firma electrónica se le apliquen los mismos conceptos que se le aplican a la firma ológrafa, es decir a la manuscrita, y está recogido en nuestra legislación en el artículo catorce de la Ley de Comercio Electrónico: “La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba enjuicio.”
- Principio de Integridad: como habíamos visto ya, a la firma electrónica se le aplican ciertas técnicas que permiten establecer si un determinado mensaje ha sido alterado o no, como por ejemplo, la denominada técnica Hashing, que brinda la posibilidad de constatar, aunque el mensaje original haya variado solo en un bit, si ha existido alguna modificación al mensaje que el emisor envió. Por esto es que una de las garantías de la firma electrónica es precisamente la integridad del mensaje firmado. Además existe dentro de nuestro ordenamiento jurídico una presunción, en virtud de la cual la ley considera que un mensaje de datos permanece íntegro desde que se emitió. Esta presunción la podemos encontrar en el artículo cincuenta y tres de la

Ley de Comercio Electrónico: “Cuando se presentare como prueba una firma electrónica certificada por una entidad de certificación de información acreditada, se presumirá que ésta reúne los requisitos determinados en la ley, y que por consiguiente, los datos de la firma electrónica no han sido alterados desde su emisión y que la firma electrónica pertenece al signatario.”

- Principio de Autenticidad: en virtud de este principio, se atribuye la autoría de un determinado mensaje de datos, cuando éste se encuentre con una firma electrónica, a quien sea titular de la firma electrónica. Como ya sabemos una de las funciones que la firma electrónica está llamada a cumplir es precisamente identificar al autor de un mensaje de datos, por lo que podemos manifestar que esta función se relaciona estrechamente con el principio de autenticidad.
- Principio de no repudio: este principio se complementa con el anterior, ya que es su consecuencia lógica, pues si con la firma electrónica se está garantizando que un determinado mensaje de datos pertenece a la persona que lo ha firmado, no sería correcto que al titular de la firma electrónica se le conceda la facultad de negar la autoría del mensaje; por eso, este principio establece que una persona que haya emitido una firma electrónica en un mensaje de datos, no puede negar su autoría respecto del mismo, consecuentemente, quedará forzado a cumplir con las obligaciones que puedan surgir del mencionado mensaje de datos. Vale la pena hacer mención nuevamente al artículo cincuenta y tres de la Ley de Comercio Electrónico, en el cual existe también una presunción respecto de la titularidad de la firma electrónica, pues según este artículo se presume que la firma electrónica pertenece a su signatario; y en virtud de este principio el signatario de la firma electrónica no puede negar que el mensaje de datos que tiene su firma le pertenece, por lo que debe hacerse cargo de las obligaciones contenidas en el mensaje.

Para concluir, podemos citar como garantías de la firma electrónica las siguientes:

- Igual valor jurídico que la firma ológrafa.
- Identifica al autor de un mensaje.

- El titular de una firma electrónica no puede negar la autoría de un mensaje que contenga su firma electrónica.
- Garantiza la integridad del mensaje.
- Aprobación del contenido del mensaje.
- Confidencialidad entre emisor y receptor del mensaje.

2.4 Partes que intervienen.

Dentro del proceso de la firma electrónica intervienen las siguientes partes:

- Emisor o Signatario: es la persona natural o jurídica, que emite un mensaje de datos, con su firma electrónica. En la disposición general novena de la Ley de Comercio Electrónico, que contiene un glosario de términos, podemos encontrar una definición de signatario: "Signatario: Es la persona que posee los datos de creación de la firma electrónica, quien, o en cuyo nombre, y con la debida autorización se consigna una firma electrónica."
- Receptor o Destinatario: es la persona natural o jurídica a quien está dirigido el mensaje de datos, que contiene la firma electrónica del emisor.

Dentro de este proceso también podríamos considerar como parte al tercero de confianza, es decir, a la autoridad de certificación, que son aquellas entidades que emiten los certificados de firma electrónica, otorgando las claves públicas y las claves privadas, a las personas titulares de una firma electrónica, cabe resaltar, sin embargo, que quien determina la clave privada es el titular de la firma mas no la entidad de certificación, pues como habíamos manifestado en líneas anteriores, la clave privada es solamente conocida por el titular de la firma electrónica, ni la autoridad de certificación puede conocer esta clave.

2.5 Valor y eficacia.

Para hablar acerca del valor y de la eficacia de la firma electrónica es preciso citar el artículo catorce de la Ley de Comercio Electrónico: "Efectos de la firma electrónica.- La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos

jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio."

Este es un artículo de gran importancia que recoge nuestra legislación, pues en él se plasma el principio de analogía y no discriminación de las firmas electrónicas; principio que exige que las mismas reglas que se aplican para la firma ológrafa sean aplicadas para la firma electrónica, es decir, la firma electrónica debe surtir los mismos efectos que surte la firma ológrafa, además este principio declara, que no se pueden negar los efectos jurídicos que derivan de la firma electrónica, por el solo hecho de que esta se halle en un formato electrónico.

Recordando el concepto de firma ológrafa podemos manifestar que ésta constituye aquel método o símbolo que utiliza una persona para identificarse como el autor de un determinado documento y hacerse cargo de las obligaciones contenidas en el documento suscrito. Con este concepto podemos recordar las funciones que cumple una firma que son las de identificar al autor de un documento, aprobar el contenido del documento, obligar al autor del documento a cumplir con lo que declara en el mismo, dar autenticidad al documento. Todos estos efectos que surte la firma manuscrita, debe también producir la firma electrónica, en virtud del principio de analogía y no discriminación que está recogido en el artículo catorce de nuestra Ley de Comercio Electrónico.

Esta es la eficacia de la firma electrónica; pues cuando emitimos una firma electrónica es exactamente igual que si estuviéramos firmando un documento por escrito, y los efectos tienen que ser los mismos. Vale la pena comentar que el artículo catorce de la Ley de Comercio Electrónico, establece que la firma electrónica tiene el mismo valor jurídico que la firma manuscrita, pero el artículo se refiere al valor que tiene la firma manuscrita cuando esta se halla vinculada a un determinado documento, pues sería ilógico pensar que una firma aislada pueda tener algún valor jurídico, por consiguiente es útil aclarar que la firma electrónica tiene el mismo valor que la firma manuscrita que se halle vinculada a un determinado documento. Además agrega el artículo que podrá ser utilizada como medio de prueba dentro de un juicio.

2.6 Requisitos de la firma electrónica.

Como habíamos manifestado ya, el concepto de firma electrónica que se encuentra en el artículo trece de la Ley de Comercio Electrónico es un concepto amplio, y que por ende, admite la posibilidad de que nuevas técnicas o métodos que puedan ser desarrollados en el futuro, puedan ser consideradas firmas electrónicas. Pero a pesar de ello nuestra ley exige que la firma electrónica reúna ciertos requisitos para que esa técnica pueda ser considerada firma electrónica. Estos requisitos se encuentran especificados en el artículo quince de la Ley de Comercio Electrónico:

> "Requisitos de la firma electrónica.- Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:
>
> a) Ser individual y estar vinculada exclusivamente a su titular;
> b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta ley y sus reglamentos;
> c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado;
> d) Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario, y,
> e) Que la firma sea controlada por la persona a quien pertenec*e."*

Estos son los requisitos que deben cumplirse inexorablemente para que una determinada técnica o método pueda constituir una firma electrónica. Pero, sin embargo, aquí juega un papel fundamental el artículo cincuenta y tres de la Ley de Comercio Electrónico que se encuentra en el capítulo cuarto del antes mencionado cuerpo legal, y que se refiere a la prueba; pues este artículo declara que cuando se presentare como prueba una firma electrónica, y ésta se hallare certificada, por una de las entidades de certificación de información acreditadas por el organismo competente, que en nuestro caso es el CONATEL, se presume que la firma electrónica reúne todos los requisitos exigidos por la ley.

Cuando una firma electrónica es presentada dentro de un juicio como prueba, el artículo cincuenta y tres de la Ley de Comercio Electrónico presume que ésta reúne todos los requisitos exigidos en el artículo quince del mismo cuerpo legal. Sin embargo, debemos preguntarnos si la presunción contenida en el artículo cincuenta y tres constituye una presunción legal o constituye una presunción de derecho. Para resolver este problema vamos a acudir al artículo treinta y dos del Código Civil:

> "Art. 32.- Se llama presunción la consecuencia que se deduce de ciertos antecedentes o circunstancias conocidas.
> Si estos antecedentes o circunstancias que dan motivo o la presunción son determinados por la ley, la presunción se llama legal.
>
> Se permitirá probar la no existencia del hecho que legalmente se presume, aunque sean ciertos los antecedentes o circunstancias de que lo infiere la ley; a menos que la ley misma rechace expresamente esta prueba, supuestos los antecedentes o circunstancias.
>
> Si una cosa, según la expresión de la ley, se presume de derecho, se entiende que es inadmisible la prueba contraria, supuestos los antecedentes o circunstancias."

Como vemos entre la presunción de derecho y la presunción legal existe una gran diferencia, pues mientras la presunción legal admite prueba en contrario, la presunción de derecho no lo hace; resulta por tanto de trascendental importancia determinar si la presunción contenida en el artículo cincuenta y tres de la Ley de Comercio Electrónico, constituye una presunción de derecho o una presunción legal. Siendo así, vamos a recurrir al tenor literal del mismo artículo treinta y dos del Código Civil que en su cuarto inciso manifiesta que si una cosa "según la expresión de la ley, se presume de derecho" no es admisible prueba en contrario. Según este inciso para que exista una presunción de derecho, la ley debe manifestar expresamente que una determinada situación constituye presunción de derecho, impidiendo de esta forma que se pueda probar lo contrario.

Además el inciso tercero del artículo treinta y dos del Código Civil permite probar la no existencia de un hecho que legalmente se presume, a no ser que la misma ley rechace expresamente esta posibilidad; en este caso no existe ninguna disposición que imposibilite probar que una determinada técnica no reúne los requisitos que debe cumplir para ser considerada firma electrónica.

Con los antecedentes que hemos señalado podemos llegar a la conclusión de que la presunción contenida en el artículo cincuenta y tres de la Ley de Comercio Electrónico, constituye una presunción legal, pues esta disposición no establece que esta presunción constituya una presunción de derecho, además existe la posibilidad de probar el no cumplimiento de los requisitos establecidos por la ley por parte de una firma electrónica, ya que no existe una prohibición expresa de la ley.

Si esta presunción constituyera una presunción de derecho, estaríamos frente a un grave problema; pues se podría presentar cualquier firma electrónica, por más que esta no cumpla con los requisitos establecidos en el artículo quince de la Ley de Comercio Electrónico, como prueba dentro de un juicio, y por ser la presunción del artículo cincuenta y tres de la Ley de Comercio Electrónico, una presunción de derecho, nos veríamos en la imposibilidad de probar que esta firma no reúne los requisitos que la misma ley exige.

Refiriéndonos ya a los requisitos exigidos por la ley para que pueda existir una firma electrónica, el primer requisito, que creo que es bastante claro, se refiere a que la firma electrónica puede tener solo un titular, pues sería ilógico pensar que varias personas pudiesen utilizar una misma firma electrónica; además se estaría causando un perjuicio al destinatario, quien no sabría a ciencia cierta con quien se está comunicando.

El segundo requisito que establece nuestra ley se haya vinculado íntimamente con una de las funciones que cumple la firma, esta es la de identificar plenamente la autoría e identidad del signatario, este requisito establece que debe haber la posibilidad de identificar al signatario por uno de los mecanismos de comprobación establecidos por la ley o su reglamento, este mecanismo son los llamados certificados de firma electrónica, a los que ya nos referiremos más adelante.

El tercer requisito exige que el método de creación y comprobación de la firma electrónica sea seguro, confiable e inalterable; se cumple con este requisito, por ejemplo, con el sistema de criptografía asimétrica o de claves públicas, con la aplicación de la técnica del *hashing*, para la verificación de la integridad del mensaje, pues como ya apuntamos, con este sistema basta que el mensaje haya sido alterado en una coma, para que el resumen que sirve para verificar la integridad del documento sea totalmente distinto del original, además el uso de las claves privadas que son únicamente conocidas por el titular, hace que la creación de la firma electrónica sea segura.

Como cuarto requisito tenemos que, al momento en que se crea una firma electrónica, los datos que sirven para la creación de la misma deben estar bajo el control del signatario; de conformidad con este requisito, una firma electrónica tendrá valor solo si el signatario es quien controla los datos que sirven para la emisión de la misma; es necesario entonces saber que son los datos que sirven para la creación de una firma electrónica, y para tal efecto vamos a acudir a la Ley de Comercio Electrónico que en su disposición general novena define a los datos de creación de la firma electrónica de la siguiente manera: "Son los elementos confidenciales básicos y necesarios para la creación de una firma electrónica." Como un ejemplo de los datos que sirven para la creación de una firma electrónica tenemos la clave privada, pues según nuestra ley, y creo que es lógico, si es que al momento de la emisión de una determinada firma electrónica existen dos o más personas que conozcan la clave privada del signatario, y se emite una firma electrónica, la misma carecería de valor.

Finalmente, la ley exige que la firma electrónica esté controlada por la persona a quien pertenece; este es un requisito que se vincula con el anterior, ya que estos dos últimos requisitos procuran brindar seguridad a los destinatarios, pues pensemos en la posibilidad de que la firma electrónica esté siendo controlada por otra persona que no sea el titular de la misma, sin duda sería un peligro para quien sea destinatario de un mensaje que se envíe con la firma electrónica que se encuentra bajo el control de esta otra persona, ya que el destinatario creerá que este mensaje efectivamente fue enviado por el titular de la firma electrónica, cuando en realidad es otra persona.

Concluimos en que para que una firma electrónica pueda gozar de plena validez, es necesario que concurran todos estos requisitos, caso contrario la firma electrónica no tendrá ningún valor, y no podrá surtir ningún efecto.

2.7 Obligaciones del titular de la firma electrónica.

El artículo diecisiete de la Ley de Comercio Electrónico se refiere a las obligaciones que tiene el titular de la firma electrónica en sus siete literales, y a continuación vamos a referirnos a cada una de estas obligaciones:

"a) Cumplir con las obligaciones derivadas del uso de la firma electrónica"

Esta es una de las obligaciones que se vincula directamente con el principio de no repudio de la firma electrónica, principio que establece que el titular de una firma electrónica no puede negar la autoría de un documento que contenga su firma electrónica; y como consecuencia debe cumplir con los compromisos que se deriven del documento firmado por él. Ésta es también una de las garantías que tiene el uso de la firma electrónica, pues si no hubiera la posibilidad de que el signatario cumpla con lo ofrecido en un documento que tenga su firma electrónica, ésta no tuviera ninguna razón de ser.

"b) Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada"

Esta obligación tiene su justificación, pues si la ley exige como requisito para la validez de la firma electrónica que los datos que sirven para la creación de la misma estén bajo el control de su titular; y que sea el titular de la firma electrónica quien la controle; la ley no puede dejar de exigir al titular de la firma que tome todas las medidas necesarias para que la firma electrónica permanezca bajo su control, y de esta forma evitar el uso indebido de la misma, porque de no hacerlo estaría arriesgándose a que su firma electrónica carezca de valor.

“c) Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente”

Esta obligación surge en el momento en el que el titular de la firma electrónica, por no cumplir eficazmente con la obligación contenida en el literal b, ha provocado que terceras personas tengan el control de su firma electrónica y como consecuencia existe el riesgo de que se produzca un uso indebido de tal firma. En este caso la ley exige al titular de la firma electrónica que notifique por cualquier medio a todas las personas que pudieran verse afectadas por esta situación, evitando así que se cause perjuicio a éstas por el mal uso de su firma electrónica.

“d) Verificar la exactitud de sus declaraciones”

La ley obliga al titular de la firma electrónica a verificar la exactitud de sus declaraciones, porque respecto de las firmas electrónicas rige el principio de no repudio, y además el literal a del artículo diecisiete de la Ley de Comercio Electrónico le exige que cumpla con las obligaciones que se deriven de las declaraciones que haya hecho en un documento que se encuentre con su firma electrónica. Por estas razones el signatario debe ser consciente de que los compromisos que adquiera en un documento con su firma electrónica deben ser fatalmente cumplidos, por lo que debe asegurarse de que sus declaraciones sean exactas.

“e) Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia”

El literal b del artículo diecisiete de La Ley de Comercio Electrónico, exige al titular de la firma electrónica que actúe diligentemente, y que tome las medidas de seguridad necesarias para que terceras personas no tengan control sobre su firma electrónica, y de esta manera evitar el uso indebido de su firma. Pero si es que el titular de la firma electrónica no ha cumplido con esta obligación, el literal e de este mismo artículo le obliga a cumplir con las obligaciones que se hayan generado por el uso no autorizado de su firma electrónica. Es decir, el titular de la firma también es responsable de las

obligaciones contraídas incluso por personas no autorizadas para usar su firma electrónica, si es que éste no ha tenido el debido cuidado para evitar que ello suceda; salvo que haya comunicado previamente al destinatario sobre este riesgo o que el destinatario no haya actuado con la debida diligencia.

"f) Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados"

Cuando el titular de una firma electrónica a permitido que terceras personas tengan el control de su firma electrónica, existiendo por tanto el riesgo de que éstas firmen sin su autorización, el titular de la firma electrónica tiene la obligación de notificar a la entidad de certificación de información que le proporcionó el certificado de firma electrónica, para que esta entidad proceda a cancelar este certificado.

Finalmente el artículo diecisiete señala en su literal g que el titular de la firma electrónica debe cumplir con las demás obligaciones que se encuentren señaladas en la ley y sus reglamentos.

2.8 Duración y extinción de la firma electrónica.

En cuanto a la duración de la firma electrónica, el artículo dieciocho de la Ley de Comercio electrónico es muy claro al manifestar que la firma electrónica tiene una duración indefinida. Y el artículo diecinueve del mismo cuerpo legal se encarga de establecer las causales por las que una firma electrónica se extingue:

"a) Voluntad de su titular;

b) Fallecimiento o incapacidad de su titular;

c) Disolución o liquidación de la persona jurídica, titular de la firma; y,

d) Por causa judicialmente declarada."

Es de importancia anotar que a pesar de que se extinga una firma electrónica por una de estas causales, las obligaciones que derivaron de su uso no se extinguen.

2.9 Adquisición y manejo de la firma electrónica dentro del Ecuador.

Para concluir este capítulo, he creído conveniente, referirme al manejo de las firmas electrónicas dentro de nuestro país. Para ello vamos a empezar por señalar cuáles son los organismos encargados de la promoción y regulación de las firmas electrónicas.

En primer lugar tenemos al Consejo de Comercio Exterior e Inversiones (COMEXI) que constituye dentro de nuestro país el ente promotor del uso de las firmas electrónicas, pues así lo establece el artículo treinta y seis de la Ley de Comercio Electrónico.

Por otra parte, el Consejo Nacional de Telecomunicaciones (CONATEL) es el ente encargado de la regulación, autorización y registro de las entidades de certificación de información. Las entidades de certificación son los únicos organismos que pueden otorgar a una persona una firma electrónica, así como el certificado de firma electrónica respectivo. En definitiva podemos decir que las entidades de certificación son los organismos que tienen la facultad de desarrollar todas las actividades que se vinculen al uso de las firmas electrónicas.

En nuestro país contamos únicamente con una entidad de certificación acreditada por el CONATEL, ésta es el Banco Central del Ecuador. Esta entidad, que obtuvo su acreditación por parte del CONATEL mediante resolución número 481-20-2008, el ocho de octubre de 2008, es la única entidad dentro del Ecuador que tiene la facultad para emitir firmas electrónicas y su correspondiente certificado.

Para que la entidad de certificación de información del Banco Central del Ecuador pueda emitir un certificado de firma electrónica, es necesario en primer lugar dirigir una solicitud a dicha entidad, esta solicitud no es la misma para todos los casos, pues debe tenerse en cuenta si el solicitante es una persona natural, una persona jurídica de derecho privado, o un funcionario público, ya que el formulario es distinto para

cada caso. El formulario para la solicitud de emisión del certificado de firma electrónica se lo puede descargar de la siguiente página web: www.informatica.gov.ec.

Una vez que ha llenado la solicitud, la persona interesada en obtener una firma electrónica y su correspondiente certificado de firma electrónica, debe dirigirse a las oficinas de la entidad de certificación de información del Banco Central del Ecuador, ubicadas en Quito, Guayaquil y Cuenca; para que ahí se proceda a firmar el contrato de prestación de servicios.

En cuanto a los valores económicos que tiene que cubrir el solicitante tenemos los siguientes: 43.00 U.S.D. por concepto de emisión del certificado de la firma electrónica, 26.00 U.S.D. correspondientes al dispositivo *token*, lo que da un total de 69.00 U.S.D. que con el pago del I.V.A. (Impuesto al valor agregado) suma 77.28 U.S.D.

El certificado de firma electrónica tiene un tiempo de vigencia de dos años, al culminar el segundo año de vigencia del certificado de firma electrónica se lo puede renovar por dos años más; para ello, el titular de la firma electrónica deberá cancelar la cantidad de 22.00 U.S.D.

Así es como se ve un certificado de firma electrónica:

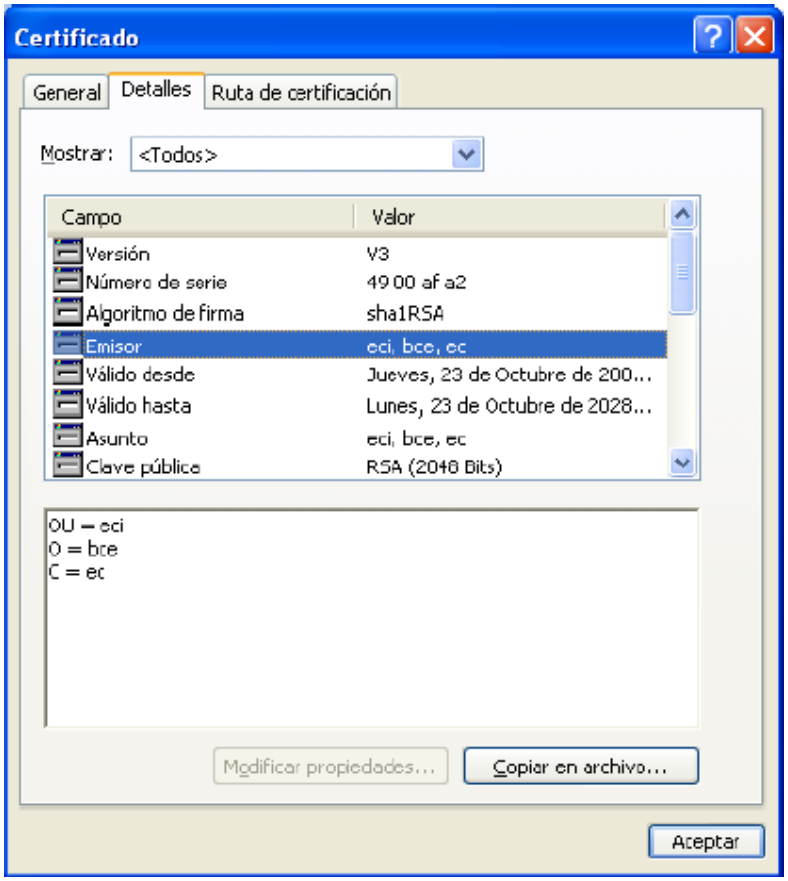


Ilustración 1.

El dispositivo *token*, que debe ser adquirido por la persona que desea obtener una firma electrónica, es necesario para poder firmar documentos, ya que este dispositivo es el que contiene el certificado de firma electrónica, el mismo que será enviado junto con el mensaje de datos al destinatario. Para que pueda emitirse una firma mediante este dispositivo debe instalarse el driver del dispositivo *token* en el ordenador que será utilizado por el titular de la firma electrónica para firmar sus documentos. Este driver lo podemos descargar de la página *web* del Banco Central del Ecuador: www.bce.fin.ec, ingresando a la opción entidad de certificación, y escogiendo la opción ocho: "driver del dispositivo portable seguro – *Token*". Ya con el driver instalado el titular de la firma podrá hacer uso de la misma.

Ilustración 2.

Finalmente, para poder firmar un documento, archivo o incluso imagen, existe una aplicación que se encuentra disponible en forma gratuita en la siguiente dirección: http://firmadigital.informatica.gov.ec. Esta aplicación nos permitirá firmar cualquier archivo.

El proceso de firmado mediante esta aplicación es muy sencillo: en primer lugar debemos ingresar a la página *web* antes indicada es decir: http://firmadigital.informatica.gov.ec. Luego damos un clic en la opción firma digital de documentos, a continuación escogemos el archivo que deseamos firmar, finalmente cuando ya hayamos seleccionado el archivo que deseamos firmar, damos un clic en el botón firmar archivo, debiendo ingresar la contraseña del dispositivo *token* para que este archivo finalmente sea firmado. Este es todo el proceso que se debe seguir para emitir una firma electrónica, y obviamente para que podamos realizar esta operación debe estar insertado el dispositivo *token* en el ordenador.

2.10 Conclusiones.

Una vez que hemos concluido este capítulo, podemos determinar si la firma electrónica efectivamente brinda seguridad a las personas que intervienen en las relaciones telemáticas, celebrando contratos mediante el internet por ejemplo.

En primer lugar debemos tener en cuenta que la firma electrónica cumple las mismas funciones que cumple la firma ológrafa, por lo que debemos señalar que en cuanto a los efectos no existe diferencia alguna entre la firma electrónica y la firma ológrafa. Debemos resaltar además uno de los principios que rigen a la firma electrónica como es el principio de no repudio, principio en virtud del cual, la persona que haya emitido una firma electrónica en un determinado documento, se encuentra, por ese

solo hecho, en la imposibilidad de negar su autoría respecto de dicho documento, y por ende debe hacerse cargo de las declaraciones que haya efectuado en dicho documento.

Por estos motivos me atrevo a decir que la firma electrónica brinda seguridad a las partes que intervienen en negocios que se celebran mediante la vía telemática. Pues la incertidumbre en cuanto a la identidad de una persona que celebra un contrato mediante el internet por ejemplo, desaparece con la presencia de la firma electrónica, ya que la misma está constituida por un bloque de caracteres que permiten identificar al firmante. Y en cuanto a la obligatoriedad de las declaraciones que se realicen en un determinado documento, si éste posee una firma electrónica, el cumplimiento de las declaraciones será de obligatorio cumplimiento para el firmante, además éste no podrá alegar que no es el autor de dicho documento en virtud del principio de no repudio.

En cuanto a la normativa legal aplicable a la firma electrónica, tenemos que hacer mención al artículo trece de la Ley de Comercio Electrónico que define a la firma electrónica; esta definición a diferencia de la definición de los mensajes de datos, es una definición en sentido amplio, que permite que cualquier técnica que cumpla con las exigencias legales y se enmarque dentro del concepto legal, pueda ser considerada como firma electrónica. Considero que es prudente la posición adoptada por nuestra legislación, pues no existe una técnica exclusiva con la que se pueda firmar los mensajes de datos, al contrario existen varias técnicas que han sido acogidas por las legislaciones del mundo; por lo que aceptar solo una de ellas sería un error y se estaría provocando inseguridad en las negociaciones.

CAPITULO III

CERTIFICADOS DE FIRMA ELECTRÓNICA.

3.1 Introducción.

Una vez que hemos concluido el tema de las firmas electrónicas, no podemos dejar de tratar aquel que se refiere a los certificados de firma electrónica.

Pues si decíamos que la firma electrónica está constituida por un bloque o conjunto de caracteres, adjuntados o lógicamente asociados a un determinado documento, y que tienen por finalidad identificar a la persona que haya firmado electrónicamente el documento; tenemos que la firma electrónica necesita de los certificados de firma electrónica para que mediante ellos las personas puedan identificar plenamente al firmante.

Mediante los certificados de firma electrónica una entidad de certificación da fe de la veracidad de los datos que constan en el certificado, para que de esta forma las personas que se comunican telemáticamente con el titular del certificado de firma electrónica tengan plena certeza respecto de su identidad.

En este capítulo definiremos a los certificados de firma electrónica, para luego poder referirnos a la utilidad de los mismos, a los requisitos que estos deben cumplir para poder tener valor legal, además analizaremos las causales por las que los certificados de firma electrónica se extinguen, son suspendidos y son revocados

Finalmente nos referiremos al reconocimiento internacional de los certificados de firma electrónica.

3.2 Definición.

Creo que es pertinente, en primer lugar recurrir a las siguientes definiciones que respecto de los certificados de firma electrónica, han sido elaborados por diversos autores:

El español Guillermo Díaz al definir a los certificados de firma electrónica manifiesta que son "dispositivos que posibilitan el almacenamiento de diversos datos relativos al propietario de los mismos (datos personales, claves, etc.) y permiten identificarlo en la red, garantizando tanto la emisión de los datos, como su recepción, la integridad de la información transmitida, la confidencialidad y lo más importante, el no repudio de la transacción." (Díaz, 2008, P. 9)

Por su parte el también español Francisco Javier García Mas define a los certificados de firma electrónica como: "Todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma electrónica." (García, 2004, P. 32)

García (2004) manifiesta que la función que cumple el certificado de firma electrónica es constatar que la clave pública del firmante le pertenece; y es el tercero de confianza, es decir, las entidades de certificación de información, sobre quien descansa la fiabilidad de todo el sistema de la firma electrónica.

Patricia Herrmann Fernández al referirse a los certificados de firma electrónica expone que: "El certificado de una firma electrónica es un registro electrónico que atestigua que una clave pública pertenece a determinada persona natural o persona jurídica. Por medio del certificado de firma electrónica podemos verificar que una clave pública pertenece a determinada persona. Uno de los fines del certificado de firma electrónica es evitar que alguien utilice una clave falsa intentando hacerse pasar por otro individuo." (Herrmann, 2007, P.124)

Nuestra Ley de Comercio Electrónico también posee una definición respecto de los certificados de firma electrónica en su artículo veinte, y a continuación la cito textualmente: "Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad."

Los conceptos que hemos citado nos permiten deducir ciertas características básicas que reúnen los certificados de firma electrónica. Así podemos indicar que los certificados de firma electrónica son, como bien lo menciona nuestra Ley de

comercio electrónico, mensajes de datos. Estos mensajes de datos cumplen una misión específica: garantizar a la sociedad que una firma electrónica pertenece a determinada persona, y que por consiguiente la respectiva clave pública pertenece efectivamente al firmante, pues de este hecho da fe una entidad de certificación mediante los certificados de firma electrónica. Así lo manifiesta Alfredo Reyes Krafft cuando expone que "la misión fundamental de los certificados es permitir la comprobación de que la clave pública de un usuario, cuyo conocimiento es imprescindible para autenticar su firma electrónica, pertenece realmente a ese usuario, ya que así lo hace constar en el certificado una autoridad que da fe de aquello." (Reyes, 2002, P.271)

En fin podemos decir que los certificados de firma electrónica tienen como finalidad brindar seguridad a las partes que intervienen en el intercambio de información mediante el uso de los mensajes de datos, permitiendo establecer fehacientemente la identidad de la contraparte, e impidiendo que ésta pueda usar una clave falsa.

Los certificados de firma electrónica son otorgados a las personas por las entidades de certificación de información. En el caso de nuestro país como ya lo habíamos manifestado, por ser el Banco Central la única entidad de certificación acreditada por el Consejo Nacional de Telecomunicaciones, es quien tiene la facultad de emitir los certificados de firma electrónica dentro de nuestro territorio patrio.

Las entidades de certificación tienen la facultad de otorgar y suspender los certificados de firma electrónica a las personas, además son las responsables de la autenticidad de estos certificados. Reyes (2002) indica que una de las características fundamentales que debe tener una entidad de certificación es que ésta debe gozar de una gran confianza por parte de la comunidad.

Los certificados de firma electrónica reúnen información personal del titular de la firma electrónica. Obviamente entre estos datos se encuentra la clave pública del firmante. Con estos datos el receptor o destinatario de un mensaje de datos que se encuentre firmado electrónicamente, podrá verificar plenamente la identidad del firmante, y de esta forma el certificado de firma electrónica estaría cumpliendo con su objetivo.

3.3 Utilidad.

Como bien lo manifiesta Díaz (2008) los certificados de una firma electrónica constituyen una "identidad digital." Al constituir una identidad digital el certificado de firma electrónica posee ciertas utilidades, las mismas que a continuación las enunciaremos:

- El certificado de firma electrónica sirve para identificar al titular de una firma electrónica, cuando éste ha firmado electrónicamente un mensaje de datos. Con el certificado de firma electrónica el receptor de un mensaje de datos, que puede ser desde el receptor de un simple *e-mail* hasta el de un mensaje de gran importancia mediante el cual se pretenda concretar un negocio, puede establecer a plenitud la identidad del autor de dicho mensaje de datos; y no solo permite identificar al autor del mensaje de datos, que además es el titular de la firma electrónica que consta en dicho mensaje, sino que los certificados de firma electrónica garantizan que se cumpla uno de los principios más importantes que regulan a la firma electrónica, esto es, el principio de no repudio. Este principio garantiza que aquella persona que ha emitido una firma electrónica en un mensaje de datos, no podrá negar su autoría respecto del mismo; y precisamente mediante el certificado de firma electrónica, es que este principio puede hacerse efectivo; pues el certificado de firma electrónica posee datos que permiten identificar al titular de la firma, por lo que una vez que se conozca la identidad del firmante, este tendrá que aceptar inevitablemente que es el autor del mensaje de datos, y en consecuencia deberá hacerse cargo de las declaraciones que haya realizado en dicho mensaje.
- Cuando nos referíamos al tema de la criptografía asimétrica veíamos que esta se basaba en la coexistencia de un par de claves, una pública y otra privada, cabe recalcar que estas dos claves le correspondían a la misma persona. Como ya lo manifestamos en su momento, la clave pública es aquella que está destinada a ser divulgada, con el fin de que el público en general tenga conocimiento de la misma; mientras que la clave privada únicamente es conocida por el titular de la firma electrónica. Los certificados de firma

electrónica representan una forma eficaz de hacer que la sociedad conozca la clave pública del titular de una firma electrónica.

- Los certificados de firma electrónica pueden servir también de identificación ante un acceso restringido. Hasta el momento la forma tradicional de ingresar a un espacio restringido se verifica digitando el *username* y el *password*, es decir digitando el nombre de usuario y la contraseña, como por ejemplo cuando deseamos ingresar a nuestra cuenta de correo electrónico. Pero en la actualidad, debido a los riesgos que representa esta forma tradicional de ingresar a sitios restringidos, se está desarrollando otra forma de identificación, en virtud de la cual se permitirá el acceso a estos sitios mediante la verificación de los datos contenidos en un certificado digital.
- Los certificados de firma digital son utilizados también para firmar *software.* De esta manera se está garantizando a la persona natural o jurídica que va a utilizar el *software* que éste es el original y que no ha sido modificado, además de indicar quien es el creador del software; razones por las que es muy escasa la posibilidad de que dicho *software* posea algún tipo de virus, ya que de existir dicho virus, sería el propio creador del *software* quien se responsabilice por los daños que pudiera provocar aquel virus, pues el *software* ya fue firmado por él, y no puede negar su autoría en virtud del principio de no repudio.
- Uno de los principales motivos por los que las relaciones telemáticas no logran aún un desarrollo total, es el hecho de que las personas tienen temor a la inseguridad que este tipo de relaciones pudieran entrañar. Es por eso que los certificados de firma electrónica buscan brindar seguridad a las partes que intervienen en este tipo de relaciones. Pues el temor de las partes muchas de las veces se debe al hecho de no saber exactamente con quien están comunicándose, pero si las partes deciden firmar electrónicamente sus mensajes de datos, y adjuntan el respectivo certificado de firma electrónica, ya no existirá más esa incertidumbre respecto de la identidad de la contraparte.

3.4 Requisitos.

Los certificados de firma electrónica deben cumplir con ciertos requisitos para poder ser válidos, estos requisitos los establece la Ley de Comercio Electrónico en su artículo veinte y dos, que a continuación lo cito textualmente:

> "Art. 22. Requisitos del certificado de firma electrónica.- El Certificado de firma electrónica para ser considerado válido contendrá los siguientes requisitos:
>
> a) Identificación de la entidad de certificación de información;
> b) Domicilio legal de la entidad de certificación de información;
> c) Los datos del titular del certificado que permitan su ubicación e identificación;
> d) El método de verificación de la firma del titular del certificado;
> e) Las fechas de emisión y expiración del certificado;
> f) El número único de serie que identifica el certificado;
> g) La firma electrónica de la entidad de certificación de información;
> h) Las limitaciones o restricciones para los usos del certificado; e,
> i) Los demás señalados en esta ley y los reglamentos. "

Como podemos apreciar en esta disposición, los dos primeros requisitos que debe cumplir un certificado de firma electrónica para poder ser válido se refieren a las entidades de certificación; pues como ya dijimos, sobre estas entidades recae toda la fiabilidad que la sociedad pueda tener respecto del proceso de firma electrónica, ya que estas entidades dan fe del hecho de que una clave pública corresponde a determinada persona, y además que los datos que aparecen en el certificado de firma electrónica efectivamente corresponden al firmante, por lo que en base a esta garantía, las personas pueden confiar en que no están siendo engañadas por la contraparte. Es por esto que este artículo exige además en su literal "g" que los certificados de firma electrónica cuenten con la firma electrónica de la entidad de certificación de información, para brindar aún más confianza.

Para que un certificado de firma electrónica tenga validez, la Ley de comercio electrónico exige además que éste contenga los datos que permitan identificar y ubicar al firmante. Pues si decimos que el certificado de firma electrónica es un

mensaje de datos que permite verificar el vínculo existente entre el firmante y su firma electrónica, es obvio que el certificado deberá contener los datos que permitan determinar la identidad del firmante; más aún si tenemos en cuenta que el principio de no repudio rige a la firma electrónica, principio en virtud del cual el titular de una determinada firma electrónica no puede negar su vinculación con la firma electrónica; por lo que será necesario identificar plenamente al titular de dicha firma para poder ubicarlo y que así se haga cargo de las obligaciones adquiridas mediante el mensaje que contiene su firma. Por estas razones resulta del todo lógico que la ley exija que estos datos consten en el certificado.

Otro de los datos que la Ley de Comercio Electrónico exige que conste en el certificado de firma electrónica se refiere a la fecha de emisión y de expiración del certificado de firma electrónica. Esta es una exigencia que vale la pena tenerla en cuenta; pues como ya lo veremos más adelante, el Reglamento a la Ley de comercio electrónico establece un plazo dentro del cual el certificado de firma electrónica tiene validez, fuera de ese plazo el certificado de firma electrónica no tiene ningún valor, por lo que debe ser renovado ante la entidad de certificación de información que emitió este certificado. Por lo anotado es que concluimos en que los datos referentes tanto a la fecha de emisión como a la fecha de expiración del certificado de firma electrónica, son de vital importancia dentro del desarrollo de las relaciones telemáticas, en las cuales el derecho busca brindar seguridad, la cual no existiría si es que se usara certificados expirados en las distintas transacciones.

3.5 Duración y extinción.

El Reglamento a la Ley de Comercio Electrónico establece en su artículo once la duración que tiene un certificado de firma electrónica, al manifestar que ésta dependerá de lo que hayan acordado contractualmente el titular de la firma electrónica con la entidad de certificación de información, que como sabemos son los entes que se hayan facultados para otorgar los certificados de firma electrónica a los titulares de las firmas electrónicas.

La regla que acabamos de anotar en el párrafo anterior podríamos considerarla como una regla general, pues bien puede darse el caso de que no exista ningún acuerdo

entre el titular de la firma electrónica y la entidad de certificación de información, y para este caso el mismo Reglamento a la Ley de Comercio Electrónico se encarga de establecer que el certificado de firma electrónica tendrá una duración de dos años.

Pero la duración del certificado de firma electrónica puede extenderse aún más de los dos años que señala el Reglamento a la Ley de Comercio Electrónico. Esto sucede cuando el titular de la firma electrónica desempeña una función pública o privada que deba durar más de dos años.

En cuanto a la extinción de los certificados de firma electrónica, la Ley de Comercio Electrónico establece las siguientes causales: en primer lugar la solicitud por parte del titular del certificado, la segunda causa por la que los certificados de firma electrónica se extinguen se refiere a la extinción de la firma electrónica, y como última causal tenemos la expiración del plazo de validez del certificado de firma electrónica.

Creo pertinente referirme a las tres causales que establece le Ley de Comercio Electrónico para la extinción de los certificados de firma electrónica. En cuanto a la primera causal, es decir por voluntad del titular del certificado, creo que no hay mucho que comentar, pues esta causal faculta al titular de un certificado de firma electrónica para acudir a la entidad de certificación de información a expresar su voluntad de extinguir el certificado proveído por esta entidad. Puede darse este caso por ejemplo cuando la clave privada del titular de la firma electrónica ha sido divulgada, y para que no se dé un uso indebido a su certificado de firma electrónica decide extinguirlo.

La segunda causal para la extinción de un certificado de firma electrónica se presenta cuando se produce una de las causas por las que se extingue la firma electrónica. Como ya lo habíamos revisado en el segundo capítulo de este trabajo, las causales para la extinción de una firma electrónica son: la voluntad del titular de la firma electrónica, la muerte o incapacidad del titular de la firma electrónica, la disolución o liquidación de la persona jurídica titular de la firma electrónica, y finalmente por una causa judicialmente declarada. Si se extingue una firma electrónica debe extinguirse como consecuencia lógica su certificado, por eso es que la ley contempla la extinción

de la firma electrónica como causal para la extinción del certificado de firma electrónica, pues como habíamos mencionado ya, el certificado de una firma electrónica tiene como finalidad confirmar el vínculo que existe entre una determinada firma electrónica y su titular, pero si no existe firma electrónica, el certificado no tiene razón de ser.

La tercera y última causal para la extinción de un certificado de firma electrónica se refiere a la duración que tiene el certificado de firma electrónica. Como ya habíamos anotado, el certificado durará el tiempo que hayan acordado contractualmente la entidad de certificación de información y el titular de la firma electrónica, en caso de no existir acuerdo el certificado tendrá una validez de dos años, los mismos que se pueden prolongar, en atención al cargo que desempeñe el titular del certificado, vencidos estos plazos el certificado de firma electrónica se extingue.

Debemos anotar que las obligaciones que hayan nacido como consecuencia del uso del certificado de la firma electrónica deben ser cumplidas sin perjuicio de la extinción del certificado de la firma electrónica. Además es preciso anotar que la extinción del certificado de firma electrónica se perfecciona en el momento en que se comunica de este hecho a la entidad de certificación de información. En el caso de la muerte del titular de la firma electrónica, la extinción del certificado de firma electrónica se perfecciona en el momento mismo de la muerte.

La Ley de comercio electrónico en su artículo veinte y cuatro manifiesta que en caso de secuestro o desaparición del titular de un certificado de firma electrónica, la extinción del mismo se verifica en el momento en que se efectúe la respectiva denuncia ante las autoridades competentes. A pesar de que este mismo artículo establece en sus tres literales las causales de extinción de los certificados de firma electrónica, dentro de los cuales no se contempla ni el caso del secuestro ni la desaparición del titular del certificado, debemos entender que estas dos posibilidades también constituyen causas para la extinción de un certificado de firma electrónica, pues considero que lo que existe es un error en la redacción del artículo veinte y cuatro, pues debió agregarse un cuarto literal en el que se hagan constar al secuestro o desaparición del titular del certificado como causa de extinción del certificado.

3.6 Suspensión y revocatoria.

Nos compete ahora referirnos a la suspensión de los certificados de firma electrónica; para ello es preciso hacer una diferenciación entre la suspensión y la extinción de los certificados de firma electrónica, pues existen diferencias substanciales entre estas dos figuras, ya que la extinción supone que el certificado de firma electrónica ya no podrá ser utilizado por quien era su titular, es decir la extinción del certificado de firma electrónica implica el cese definitivo de las funciones que el certificado de firma electrónica está llamado a brindar; mientras que la suspensión implica un cese temporal de las funciones que cumple el certificado de firma electrónica.

Una vez que hemos efectuado la respectiva diferenciación entre la suspensión y la extinción de los certificados de firma electrónica, creo pertinente citar las causales por las que los certificados de firma electrónica son suspendidos: en primer lugar tenemos que los certificados de firma electrónica pueden ser suspendidos por disposición del Consejo Nacional de Telecomunicaciones, la segunda causal por la que se suspenden los certificados de firma electrónica se verifica cuando la entidad de certificación de información logra comprobar que existe falsedad en los datos que han sido consignados por parte del titular del certificado de firma electrónica; finalmente, se suspenden los certificados de firma electrónica cuando existe incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular del certificado de firma electrónica.

La suspensión del certificado de firma electrónica dispuesta por la entidad de certificación de información debe ser notificada inmediatamente tanto al titular del certificado de firma electrónica como a la entidad de control, es decir al Consejo Nacional de Telecomunicaciones, además deben estar claramente explicadas las causas por las que se procedió a suspender el certificado de firma electrónica.

Cuando las causas por las que se procedió a suspender el certificado de firma electrónica se desvanecen, o cuando existe resolución por parte del Consejo Nacional de Telecomunicaciones; la entidad de certificación de información debe levantar la suspensión del certificado de firma electrónica y además debe habilitarlo de forma inmediata.

Una vez que nos hemos referido al tema de la suspensión de los certificados de firma electrónica, nos corresponde referirnos a la revocatoria de los mismos. A diferencia de la extinción y de la suspensión de los certificados de firma electrónica, la revocatoria se produce por hechos que tienen que ver única y exclusivamente con la entidad de certificación de información, por lo que el organismo competente para declarar la revocatoria de los certificados de firma electrónica es el Consejo Nacional de Telecomunicaciones. Existen dos causales por las que el Consejo Nacional De Telecomunicaciones puede revocar un certificado de firma electrónica.

La primera causal se refiere al cese de las actividades de la entidad de certificación de información. Es de importancia anotar, respecto de esta causal, que únicamente se puede revocar el certificado de firma electrónica cuando no exista otra entidad de certificación de información que asuma los certificados que fueron otorgados por la entidad que está cesando en sus actividades. Para que se produzca la cesión de los certificados a otra entidad de certificación de información se debe contar con el consentimiento expreso del titular del certificado. La entidad de certificación de información que esta cesando en sus actividades debe notificar este particular a sus usuarios con por lo menos noventa días de anticipación.

La otra causal por la que se revocan los certificados de firma electrónica es la quiebra técnica judicialmente declarada de la entidad de certificación de información.

Cuando un certificado de firma electrónica es revocado o suspendido o se extingue, este hecho debe ser comunicado de forma inmediata al que fuera titular del certificado de firma electrónica. Esta notificación debe hacerse a la dirección electrónica y a la dirección física que haya señalado el titular del certificado, al celebrar el contrato de prestación de servicios con la entidad de certificación de información.

Tanto la suspensión como la revocatoria de los certificados de firma electrónica, surten efectos desde el momento de su comunicación, esto con relación al titular del certificado, y con relación a terceros, surten efectos desde el momento de la publicación de la revocatoria o de la suspensión del certificado de firma electrónica. En cuanto a la publicación de la suspensión o revocatoria del certificado de firma

electrónica tenemos que anotar que el Reglamento a la Ley de Comercio Electrónico faculta para que se publique por cualquiera de los siguientes medios:

> "a) Siempre en la página electrónica determinada por el CONATEL en la que se reporta la situación y la validez de los certificados, así como en la página WEB de la entidad certificadora; y,
> b) Mediante un aviso al acceder al certificado de firma electrónica desde el hipervínculo de verificación, sea que éste forme parte de la firma electrónica, que conste en un directorio electrónico o por cualquier procedimiento por el cual se consulta los datos del certificado de firma electrónica.
>
> Opcionalmente, en caso de que la entidad certificadora o la entidad de registro relacionada crean conveniente, se podrá hacer la publicación en uno de los medios de comunicación pública"

Es preciso anotar que ni la revocatoria ni la suspensión del certificado de firma electrónica eximen de responsabilidad al titular del certificado de firma electrónica respecto de las obligaciones contraídas como consecuencia del uso del certificado de firma electrónica; por ende estas obligaciones deben ser cumplidas.

La entidad de certificación de información es responsable por los perjuicios que ocasionaren tanto la ausencia como el retardo de comunicación o de publicación respecto de la suspensión o revocatoria de los certificados de firma electrónica.

3.7 Reconocimiento internacional.

Nos incumbe ahora tratar el tema del reconocimiento internacional de los certificados de firma electrónica; para ello es de indiscutible importancia recurrir tanto a la Ley de Comercio electrónico como a su reglamento, además nos referiremos a las disposiciones que contiene la Ley Modelo de la Comisión de la Naciones Unidas para el Derecho Mercantil Internacional sobre firmas electrónicas. Estos cuerpos legales contienen las normas que regulan la aplicación de los certificados de firma electrónica en territorio extranjero.

En primer lugar, nos vamos a referir al artículo dieciséis del Reglamento a la Ley de Comercio Electrónico. Esta disposición manifiesta que los certificados de firma electrónica otorgados fuera del territorio ecuatoriano tendrán valor legal en el Ecuador, siempre que hayan sido revalidados ante el Consejo Nacional de Telecomunicaciones; este organismo tiene el deber de verificar tanto el grado de fiabilidad del certificado de firma electrónica como la solvencia técnica de la entidad que lo otorgó.

De igual manera la Ley de Comercio Electrónico en su artículo veinte y ocho manifiesta que los certificados de firma electrónica emitidos por entidades de certificación extranjeras tendrán el mismo valor legal que tienen los certificados de firma electrónica otorgados por entidades de certificación ecuatorianas, siempre que estos certificados cumplan con los requisitos que establece la Ley de Comercio Electrónico, y tengan además un grado de fiabilidad equivalente a los certificados de firma electrónica emitidos en el Ecuador.

Según lo que hemos manifestado, podemos decir que es posible que aquellos certificados de firma electrónica, que no han sido otorgados en el Ecuador, pueden tener el mismo valor legal y surtir los mismos efectos jurídicos, que los certificados de firma electrónica otorgados por entidades de certificación de información ecuatorianas.

Ahora bien, nos hemos referido ya a los certificados de firma electrónica otorgados en el extranjero, que como dijimos tienen valor en el Ecuador si cumplen los requisitos legales, y son revalidados ante el Consejo Nacional de Telecomunicaciones. Pero surge una interrogante: ¿Qué sucede con los certificados de firma electrónica otorgados en el Ecuador, pueden tener valor legal fuera de nuestro territorio patrio?

Dando respuesta a la interrogante antes planteada, podemos manifestar que los certificados de firma electrónica otorgados por entidades de certificación ecuatorianas si tienen valor fuera del Ecuador; pues la Ley Modelo de la CNUDMI sobre Firmas Electrónicas, en su artículo doce, manifiesta que en el momento de determinar los efectos jurídicos de un certificado de firma electrónica, no se debe

tener en cuenta ni el lugar en donde el certificado fue otorgado, ni el lugar en donde se encuentre establecida la entidad de certificación que otorgó el certificado de firma electrónica.

Para concluir vamos a decir que el lugar en donde se otorgó el certificado de firma electrónica no constituye un obstáculo para que el certificado pueda surtir los efectos que está llamado a surtir. Así lo establece el inciso segundo de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas al establecer que "Todo certificado expedido fuera [del Estado promulgante] producirá los mismos efectos jurídicos en [el Estado promulgante] que todo certificado expedido en [el Estado promulgante] si presenta un grado de fiabilidad sustancialmente equivalente."

3.8 Conclusiones.

Como ya manifestamos dentro de este capítulo, los certificados de firma electrónica son mensajes de datos que contienen la información que permite establecer la identidad de la persona que haya firmado el mensaje de datos al cual está asociado el certificado de firma electrónica. Estos certificados de firma electrónica son indispensables en el proceso de firma electrónica, pues si la firma electrónica permite establecer la identidad de la persona que la emite, esta necesita de un mecanismo en el cual consten los datos que permitan identificar a dicha persona, éste objetivo se cumple a través de los certificados de firma electrónica, y para que no quepa la menor duda respecto de la identidad del firmante, las denominadas entidades de certificación de información se encargan de dar fe respecto de la veracidad de los datos que identifican al titular de la firma electrónica.

Como manifestamos en este capítulo, las entidades de certificación de información son los entes que tienen la facultad de otorgar a los titulares de las firmas electrónicas su respectivo certificado. En el caso del Ecuador solo existe una entidad de certificación de información, el Banco Central del Ecuador. Con esto se evidencia la falta de promoción respecto del proceso de firma electrónica dentro de nuestro país.

Considero que los certificados de firma electrónica hacen aún más fiable a todo el proceso de firma electrónica, ya que a través de ellos las personas podemos establecer a

plenitud la identidad de la persona que ha firmado un mensaje de datos; además debemos tener en cuenta que los datos consignados en el certificado de firma electrónica están respaldados por una entidad de información, que da fe de la veracidad de los datos que aparecen en el certificado, y además de que estos datos pertenecen al firmante.

Por todo esto concluyo en que gracias a los certificados de firma electrónica, la firma electrónica puede cumplir con los objetivos que está llamada a cumplir, es decir identificar a las personas dentro de las operaciones telemáticas, y por consiguiente brindar la seguridad a la que tanto se aspira en estas operaciones.

Conclusiones.

La Ley modelo de la Comisión de las Naciones Unidas para el derecho mercantil internacional (CNUDMI) sobre comercio electrónico, se basa en el criterio del "equivalente funcional"; este criterio busca que todas aquellas funciones y objetivos que desempeña la información cuando está plasmada en el papel, sean satisfechos y desarrollados por las técnicas del comercio electrónico, es decir, este criterio pretende que la información constante en un soporte electrónico cumpla las mismas funciones que cumple la información cuando está plasmada en un papel.

En nuestro país, al momento de redactar las disposiciones de la Ley de Comercio Electrónico, se tuvo muy en cuenta el criterio del "equivalente funcional" establecido por la La Ley modelo de la Comisión de las Naciones Unidas para el derecho mercantil internacional (CNUDMI) sobre comercio electrónico.

Así por ejemplo, la Ley de Comercio Electrónico permite que los mensajes de datos reemplacen a los documentos escritos y a los documentos originales, cuando la ley exija su presentación. De igual manera, en virtud del criterio del "equivalente funcional", la Ley de Comercio Electrónico reconoce que la firma electrónica surte los mismos efectos que surte la firma ológrafa en un documento escrito.

Este criterio procura eliminar todo obstáculo que pueda limitar el desarrollo de las relaciones telemáticas, permitiendo que los mensajes de datos y la firma electrónica, produzcan los mismos efectos que producen los documentos escritos y la firma escrita u ológrafa.

Como manifestamos en este trabajo, existen ciertos principios que se aplican a los mensajes de datos y a la firma electrónica, principios que buscan que estas dos figuras cumplan eficazmente con sus objetivos, los mismos que se concretan en brindar seguridad a las personas que intervienen en el intercambio de información mediante la vía telemática, además constituir medios de prueba eficaces para justificar la veracidad de la información, que haya sido generada o que esté siendo almacenada por un medio electrónico.

Uno de estos principios es el de no discriminación, que se aplica tanto para los mensajes de datos como para la firma electrónica; y establece que no se puede negar efectos jurídicos, validez o fuerza obligatoria a la información por el solo hecho de encontrarse en un mensaje de datos o a la firma por constar en un formato electrónico.

Por lo anotado en los párrafos anteriores, y por todos los aspectos que hemos analizado en este trabajo, respecto de los mensajes de datos, de la firma electrónica, y de los certificados de firma electrónica, hemos llegado a la conclusión de que estas herramientas, que nos brinda el Estado mediante la Ley de Comercio Electrónico, definitivamente ayudan a solventar en gran medida el problema de la inseguridad que se presenta en el intercambio de información mediante la vía telemática. Pues el hecho de que la Ley de Comercio Electrónico reconozca a los mensajes de datos igual valor jurídico y probatorio que el de los documentos escritos, es un gran avance; debido a que se puede utilizar a los mensajes de datos dentro de un juicio para justificar un determinado hecho, existiendo incluso la posibilidad de que existan mensajes de datos, que cumpliendo con ciertos requisitos legales, gocen del mismo valor del que gozan los instrumentos públicos.

La firma electrónica permite además que su titular sea identificado por el resto de las personas que participan en las relaciones telemáticas, eliminando así la incertidumbre que pudiera existir respecto de su identidad. Para otorgar aún más seguridad al proceso de firma electrónica, ésta es gobernada por principios como el de autenticidad y el de no repudio, principios que garantizan que la persona que haya emitido una firma electrónica en un determinado documento, cumplirá con las obligaciones que hayan nacido como consecuencia de las declaraciones contenidas en dicho documento.

Y para permitir que el proceso de firma electrónica cumpla con su función, es decir que el titular de la firma electrónica pueda ser plenamente identificado, tenemos que la Ley de Comercio Electrónico regula a los certificados de firma electrónica, otorgando la facultad de dar fe, a las entidades de certificación de información, de que los datos contenidos en su certificado pertenecen efectivamente al titular del certificado.

Todas estas figuras hacen que el intercambio de información que se realiza mediante los modernos sistemas de información, como por ejemplo el internet, sea cada vez más seguro. No vamos a aventurarnos a decir que estas herramientas brindan una seguridad absoluta en las relaciones telemáticas, pues la seguridad absoluta no existe ni en las relaciones físicas, es decir aquellas operaciones o transacciones que se efectúan necesariamente con la presencia física de las personas que intervienen en ellas; pero si reducen de una manera substancial la inseguridad que suele presentarse en las relaciones telemáticas.

En cuanto a la normativa legal que regula a los mensajes de datos, a la firma electrónica, y a los certificados de firma electrónica en nuestro país, me atrevo a decir que en términos generales es correcta; pues regula de una forma ordenada todos los aspectos referentes a estas tres figuras; y además al reconocer los principios planteados por la Ley modelo de la CNUDMI sobre comercio electrónico, la ley garantiza que estas tres figuras brindarán seguridad a las personas en el intercambio de datos por medio de los nuevos sistemas de información.

Sin embargo, existe un problema en cuanto al reconocimiento internacional de los certificados de firma electrónica, pues a pesar de que existe una ley modelo dictada por la Comisión de las Naciones Unidas para el derecho mercantil internacional sobre comercio electrónico, los criterios de los países, respecto del reconocimiento internacional de los certificados de firma electrónica, no se encuentran unificados, tornando problemático el reconocimiento internacional de los certificados de firma electrónica.

Es por esta razón que no podemos manifestar que estas figuras concedan a las personas una seguridad absoluta en sus transacciones u operaciones telemáticas; pero sin embargo debemos tener presente que la ley permite a las personas acordar el uso de determinados tipos de firma electrónica o certificados, siendo válido y suficiente en derecho este acuerdo. Entonces, como podemos apreciar, la ley otorga posibilidades a las personas con las que la inseguridad que pudiera presentarse puede desaparecer; pero para que esto suceda debe haber un excelente trabajo de promoción respecto de estas posibilidades que nos otorga la ley.

Todo esto nos lleva a manifestar que el Estado debe preocuparse de realizar un trabajo de promoción eficaz respecto de la firma electrónica, de los certificados de firma electrónica y de los mensajes de datos, así como de sus aspectos más relevantes, haciendo énfasis en las utilidades y beneficios que estas figuras brindan, así como las posibilidades que nos otorga la ley para disminuir la inseguridad en las relaciones telemáticas.

Bibliografía.

CABANELLAS DE TORRES, Guillermo. (1998). Diccionario Jurídico Elemental.

Código Civil Ecuatoriano.

Código de Procedimiento Civil Ecuatoriano.

DEL PESO NAVARRO, Emilio. (2003). Servicios de la Sociedad de la Información: Comercio Electrónico y Protección de Datos. España. Editorial Díaz de Santos.

DÍAZ, Guillermo. (Febrero de 2008). La Firma Electrónica y los Servicios de Certificación. Revista de Derecho Informático R.E.D.I. Edición No. 115. Fecha de acceso al documento: 22 de marzo de 2010. http://www.alfa-redi.org/miembro.shtml?x=10133

Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999.

GALENDE DÍAZ, Juan Carlos. (1995) Criptografía: Historia de la Escritura Cifrada. España. Editorial Complutense. Primera Edición.

GARCÍA MÁS, Francisco Javier. (2004). Comercio y Firma Electrónicos. España. Editorial Lex Nova. Segunda edición.

HERRMANN FERNÁNDEZ, Patricia. (2007). Comercio Electrónico. Ecuador. Universidad Técnica Particular de Loja.

HOCSMAN, Heriberto Simón. (2005). Negocios en Internet. Argentina. Editorial Astrea.

Ley 527 del 18 de agosto de 1999 de la República de Colombia.

Ley de Comercio Electrónico Mensajes de Datos y Firmas Electrónicas.

Reglamento a la Ley de Comercio Electrónico Mensajes de Datos y Firmas Electrónicas.

Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.

Ley Orgánica de Defensa al Consumidor.

Ley sobre el uso de medios electrónicos y firma electrónica para el Estado de Guanajuato y sus municipios

MARIMÓN, Santiago. (1999). La Sanidad en la Sociedad de la Información. España. Editorial Díaz de Santos.

NIEVES GALARZA, Ricardo. (2009). Los Documentos Electrónicos. Ecuador. Ediciones Carpol. Primera edición.

PEGUERA POCH, Miquel; AGUSTINOY GUILAYN, Albert, y otros. (2005) Derecho y Nuevas Tecnologías. España, Editorial UOC. Primera edición en español.

REYES KRAFFT, Alfredo. (2002). La Firma Electrónica y las Entidades de Certificación. Tesis doctoral. México. Universidad Panamericana.

RINCÓN CÁRDENAS, Erick. (2006). Manual de Derecho de Comercio Electrónico y de Internet. Colombia. Centro Editorial Universidad del Rosario. Primera edición.

YÁNEZ NARVÁEZ, Pablo (1999) Introducción al Estudio del Derecho Informático e Informática Jurídica. Ecuador. Escuela Politécnica Javeriana del Ecuador.