UNIVERSIDAD ANDINA SIMÓN BOLÍVAR

SEDE, ECUADOR

ÁREA DE DERECHO

PROGRAMA DE MAESTRÍA

MENCIÓN EN DERECHO ECONÓMICO

FIRMAS ELECTRÓNICAS Y SU REGIMEN DE APLICACIÓN, ANÁLISIS DE LA NORMATIVA EN EL ECUADOR

Por:

Mario Tobar Estrella

Quito, 2006

Al presentar esta tesis como uno de los requisitos previos para la obtención del titulo de magíster de la Universidad Andina Simón Bolívar, Sede, Ecuador, autorizo al centro de información o a la biblioteca de la institución para que haga de esta tesis un documento disponible para su lectura según las normas de la universidad.

Se autoriza que se realice cualquier copia de esta tesis dentro de las regulaciones de la universidad, siempre y cuando esta reproducción no suponga una ganancia económica potencial.

Sin perjuicio de ejercer mi derecho de autor autorizo a la Universidad Andina Simón Bolívar, Sede, Ecuador, la publicación de esta tesis o parte de ella por una sola vez dentro de los treinta meses después de su aprobación.

Mario Tobar Estrella

3 de marzo de 2006

UNIVERSIDAD ANDINA SIMÓN BOLÍVAR

SEDE, ECUADOR

ÁREA DE DERECHO

PROGRAMA DE MAESTRÍA

MENCIÓN EN DERECHO ECONÓMICO

FIRMAS ELECTRÓNICAS Y SU REGIMEN DE APLICACIÓN, ANÁLISIS DE LA NORMATIVA EN EL ECUADOR

Por: Mario Tobar Estrella

Tutor: Dr. José Luis Barzallo

Quito, 3 de marzo del 2006

RESUMEN

La presente tesis se ocupa del análisis de la normativa vigente en el Ecuador sobre la Firma Electrónica y su régimen de aplicación. Con el objeto de determinar la problemática actual en la estructura de la normativa en el tratamiento de la Firma Electrónica y, si se encuentra acorde con la normativa internacional.

En esta investigación se analiza la Firma Electrónica, teniendo como referencia la firma digital; se examina también la criptografía, rama de las matemáticas, que utilizando fórmulas o algoritmos transforma mensajes ininteligibles a su forma original, siendo la criptografía asimétrica la empleada para crear firmas digitales a través de la utilización de claves. Para su funcionamiento la Firma Electrónica necesita la utilización de los denominados certificados de Firma Electrónica, y la intervención de una tercera parte de confianza o conocida como entidad de certificación. Finalmente tenemos el estudio de los organismos encargados de la promoción, difusión de los servicios electrónicos, de regulación y control de las entidades de certificación.

Lo anteriormente expresado se desarrolla en tres capítulos. El capítulo primero sobre La Firma Electrónica. El capítulo segundo que trata sobre el certificado de Firma Electrónica y entidades de certificación de información. El capítulo tercero relativo a los organismos como el COMEXI, CONATEL y la Superintendencia de Telecomunicaciones.

INDICE

INTRODUCCION

Con el presente trabajo pretendo analizar la normativa ecuatoriana referente a la Firma Electrónica y su régimen de aplicación; con lo que se analizará la problemática actual en la estructura de esta normativa y si se encuentra acorde con la normativa internacional, ya que ésta, siendo parte del comercio electrónico, su tratamiento ha trascendido las fronteras físicas.

Este trabajo se desarrolla en tres capítulos a la luz de la doctrina, documentos, y normativas emitidas por países como España, Argentina, y del Ecuador en tanto objeto de nuestro análisis y, de organismos como la Unión Europea y la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional -CNUDMI-, conocida por sus siglas en ingles como -UNCITRAL-.

En el primer capítulo se analiza la Firma Electrónica, en un inicio partiendo de definiciones técnicas como las de criptográfía, claves públicas y privadas, hasta el análisis de la firma digital y la Firma Electrónica; considerándose también de importancia entre otros temas el recuento y análisis de la normativa internacional sobre Firma Electrónica, y el tratamiento de la Firma Electrónica como instrumento público con los efectos que esto acarrea. Lo anterior con la finalidad de determinar si la normativa ecuatoriana concibe a la Firma Electrónica o a la firma digital; si su régimen de aplicación presenta algún inconveniente en su desarrollo y si se encuentra acorde a la normativa internacional existente.

El segundo capítulo contiene el análisis de los certificados de Firma Electrónica y de las entidades de certificación de información o terceras partes de confianza, que en el caso del Ecuador se denominan Entidades de Certificación de Información; por su importancia en este segundo capítulo, se considerara también el período de validez del certificado de Firma Electrónica, que involucra la duración, extinción, suspensión y revocatoria del mismo. Lo descrito con la finalidad de determinar de que se tratan estos certificados y entidades de certificación en la normativa internacional, y como se encuentran concebidos en la normativa ecuatoriana.

El tercer y último capítulo de esta investigación, desarrolla el estudio de los organismos encargados de la promoción, difusión de los servicios electrónicos, de regulación y control de las entidades de certificación, así como de sus funciones, claro está, sin dejar de revisar la normativa internacional sobre el tema. Estos organismos respectivamente son: El Consejo de Comercio Exterior e Inversiones (COMEXI), el Consejo Nacional de Telecomunicaciones (CONATEL) y la Superintendencia de Telecomunicaciones. De esta manera procuramos establecer si estos organismos se encuentran desarrollando sus funciones y si cuentan con la reglamentación necesaria y apta para ello.

Siendo la Firma Electrónica un tema de muy reciente aparición en el ámbito nacional, aspiro que este trabajo de investigación aporte al conocimiento y desarrollo de la Firma Electrónica en el Ecuador, ya que actualmente en el mundo globalizado en el que vivimos, con el avance de las tecnologías de la

información el comercio electrónico se ha convertido en una de las herramientas más importantes en la economía mundial, las transacciones comerciales por su rapidez se las hace utilizando el tan en boga internet, por esto deberíamos revisar y actualizar nuestra normativa para no apartarnos del contexto comercial internacional de esta era.

Capítulo I

Firma Electrónica

La Firma Electrónica es una de las herramientas que permite que se haga efectivo el comercio electrónico, que en un sentido amplio es toda transacción realizada a través de redes electrónicas de información conocidas en la actualidad como el Internet, es así como también se concibe en la normativa internacional y en la normativa ecuatoriana.

Estas redes abiertas, como lo es el internet; son redes en las cuales confluyen una gran cantidad de personas con la posibilidad de interceptar con diversas finalidades las transacciones electrónicas o lo que se ha denominado el tráfico electrónico, generando riesgos e incertidumbres en las rutinas comerciales, que desde el punto de vista jurídico crean dudas sobre la validez y la eficacia de las transacciones electrónicas, es así, como en gran medida las Firmas Electrónicas dan seguridad a dichos negocios.

El sistema comercial sustentado en papel se encuentra viviendo la transición a un comercio electrónico de documentos y Firmas Electrónicas, que deben ofrecer a sus usuarios la misma seguridad jurídica del sistema comercial respaldado en papel. Es así, como en el transcurso de este capítulo, trataremos de demostrar si es correcto que la legislación del Ecuador norme como Firma Electrónica, o firma digital; además, y en desarrollo de lo anterior, se determinará, sí nuestra normativa sobre el tema y su régimen de

aplicación se encuentran acordes a la normativa internacional. Para el cual en un inicio se analizara a manera de antecedente los aspectos técnicos relacionados.

Antecedentes

1. Terminología y conceptos técnicos

1.1 La criptografía

Son los especialistas o programadores en sistemas, los indicados para tratar este tipo de conceptos y mecanismos, sin embargo, introduciremos el tema en lo que interesa al estudio de la Firma Electrónica. El Diccionario de la Real Academia Española define la criptografía como: *"Arte de escribir con clave secreta o de un modo enigmático."*[1]; se dice también, *"que la criptografía es la ciencia que se ocupa de transformar mensajes en formas aparentemente ininteligibles y devolverlos a su forma original".*[2] De otra parte la etimología del término *cripto* en griego significa *oculto*. Por lo cual podemos concluir de lo anteriormente expuesto: que la criptografía en un significado amplio es aquella que utilizando fórmulas o algoritmos, transforma mensajes en forma aparentemente ininteligibles a su forma original.

[1] Real Academia Española, *Diccionario de la Lengua Española*, Madrid, 2001, 2da ed., p. 462.
[2] Apol L. Martínez, *Comercio Electrónico, Firma digital y Autoridades de Certificación*, Madrid, Ediciones Civitas, 2001, p .45.

Referente al tema principal de la tesis, es necesario indicar que la firma digital viene a constituirse en una especie de Firma Electrónica, al respecto Oliver Hance expresa: *"La criptografía también puede emplearse para crear firmas digitales, para autenticar mensajes electrónicos y para verificar su integridad (esto es: los mensajes se recibieron en la misma forma en que se enviaron y provienen de la fuente indicada), lo que en el contexto de los negocios electrónicos resulta de vital importancia."*[3]. Además, para el desarrollo de este trabajo, es menester tener presente a los siguientes tipos de criptografía, la simétrica de una sola clave, y la asimétrica o de clave pública, que se maneja con dos claves diferentes pero matemáticamente relacionadas entre sí, lo anterior en base a grandes números producidos utilizando una serie de fórmulas matemáticas aplicadas a números primos, sin embargo, la criptografía de clave pública no necesariamente podría utilizar algoritmos basados en números primos, sino también criptosistemas de curvas elípticas, Mauricio Devoto al respecto expresa: "*En la actualidad se están utilizando o desarrollando otras técnicas matemáticas, como los criptosistemas de curvas elípticas, que se suelen describir como sistemas que ofrecen un alto grado de seguridad mediante el empleo de longitudes de clave notablemente reducidas."*[4], es así, como estas nuevas técnicas ofrecen más seguridad a las claves y por ende a la firma digital.

La criptografía *simétrica* como explica Miguel Dávara es aquella en la que*: "se utiliza la misma clave para cifrar que para descifrar los datos, con lo que ambas partes, emisor y receptor, deben conocer la clave (uno para cifrar y*

[3] Oliver Hance, *Leyes y Negocios en Internet*, México, Mc Graw - Hill., 1997, p. 180.
[4] Mauricio Devoto, *Comercio Electrónico y Firma Digital*, Buenos Aires, Editorial La Ley S.A. 2001, p. 169.

otro para descifrar), teniendo que basar sus relaciones en cuestiones de total y absoluta confianza, ya que, para que exista seguridad, la clave debe permanecer secreta y uno debe confiar en que el otro no la da a conocer a nadie y viceversa."[5], como se explica, las dos partes u operadores comparten una clave secreta por medio de la cual es posible cifrar y descifrar el mensaje.

La criptografía *asimétrica* en cambio, se basa en que cada uno de los operadores tiene dos claves; una privada que sólo él conoce, y una pública que conocen o pueden conocer todos los que intervienen en el tráfico electrónico -clave que incluso puede constar en un directorio público-, para comprender mejor lo anotado, citemos a Rafael Mateu De Ros que al respecto explica: *"Cuando el operador A quiere enviar un mensaje electrónico aplica al mismo su clave privada y el mensaje así cifrado se envía a B, que al recibir el mensaje le aplica la clave pública de A para obtener el mensaje descifrado."*[6]. Este último sistema tiene la ventaja de generar confidencialidad en el envió de mensajes a través de canales inseguros como son las redes abiertas –Internet-, así como también, permite crear las firmas digitales, dotando a los mensajes de datos de autenticidad, integridad y no rechazo de origen, que son las condiciones básicas de las firmas digitales.

[5] Miguel Dávara A., *Firma Electrónica y Autoridades de Certificación: El Notario Electrónico*, en: Problemática Jurídica en Torno al Fenómeno de Internet, Madrid – España, Lerko Print S.A., p. 421.
[6] Rafael Mateu de Ros, *Derecho de Internet, Comercio Electrónico y Firma Digital*, Navarra, Editorial Arazandi, S.A., 1ra ed., 2000, p. 182.

Por el momento y de la manera como se concibe a la Firma Electrónica en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Registro Oficial No. 557, de 17 de abril del 2002), debemos tener presente a la criptografía asimétrica, que como veremos mas adelante, cumple un papel importante en nuestra normativa, sin embargo podrían presentarse a futuro nuevas especies de Firma Electrónica para lo cual el artículo 10 del Reglamento a la Ley contempla la neutralidad tecnológica.

1.2 Claves públicas y claves privadas

Habiendo hecho alusión a la criptografía, queda claro que para su función de cifrado y descifrado hace uso de claves, y que estas pueden ser públicas y privadas, particularmente en la criptografía asimétrica que es con la que se construye la firma digital. En relación a las claves Mauricio Devoto las describe como: *"Las claves complementarias utilizadas para las firmas digitales se denominan ´claves privadas`, que se utiliza para firmar digitalmente, mediante un dispositivo de creación de firma digital en un criptosistema asimétrico seguro, y la "clave pública", que de ordinario conocen más personas y se utiliza para que el tercero que actúa confiando en el certificado pueda verificar la firma digital"*[7]. La clave pública es aquella que es conocida tanto por el emisor como por el receptor, es decir, por las dos partes implicadas en la transacción, lo cual no es garantía para la integridad y autenticidad del mensaje. Mientras que la clave privada es exclusivamente conocida por el emisor, lo cual sí garantiza su integridad y

[7] Mauricio Devoto, *op. cit.*, p. 169.

autenticidad, tanto como la identidad de su autor. Desde este momento podemos entender la importancia de la relación criptografía asimétrica /Firma Electrónica.

Es importante mencionar, que las claves públicas son una combinación de letras, números o combinaciones de estos, es decir, que una clave puede ser incluso nuestro nombre, para que sea fácil de identificar y ser conocido por los usuarios; mientras que la clave privada es una extensa e intrincada combinación de símbolos gráficos de difícil memorización, este tipo de clave puede estar plasmada en un soporte magnético, al que se le puede agregar un PIN o un número de identificación personal -esta clave puede incluirse en una tarjeta magnética como la de los cajeros de los bancos-, al respecto se presenta el siguiente comentario: *"Las claves no son otra cosa que una combinación de letras y números, es decir, un conjunto de bits, que a su vez constituyen un conjunto de ceros y unos. La creación de una firma digital implica combinar los caracteres que conforman la clave privada del usuario con los caracteres del documento o información al que se desea firmar."*[8]

Para concluir el presente tema, debemos subrayar que las claves públicas y privadas son técnicas utilizadas en la criptografía asimétrica, que es con la que se crea la firma digital o también llamada de clave pública, mecanismo de autenticación que en la actualidad se constituye como el más seguro dentro de lo que es la Firma Electrónica, siendo también contemplado en las

[8] *Ibíd,* p. 205.

normativas existentes en el tema, incluida la Ley de Comercio Electrónico del Ecuador.

2. Diferencias entre la Firma Electrónica y la firma digital

2.1 Firma Electrónica

Por Firma Electrónica se entiende: "*Es un mecanismo electrónico mediante el cual se añaden ciertos códigos a un archivo electrónico para asegurarlo."*[9], de aquí, que las transacciones electrónicas deben garantizar a los usuarios principalmente seguridad y confianza, características que son propias de las firmas manuscritas y a las que deben responder las Firmas Electrónicas. Sobre éstas no hay un criterio único de denominación, es así como en las normativas existentes sobre el tema se habla de Firma Electrónica, firma digital y firma electrónica avanzada; consideramos al igual que Mauricio Devoto que acertado es definirla de la siguiente forma: "*El término Firma Electrónica sería un término genérico y tecnológicamente neutro, y haría referencia al universo de métodos por los que se podría "firmar" un documento electrónico. Estas firmas podrían tomar diversas formas y ser creadas por medio de diferentes tecnologías. Serían firmas electrónicas por ejemplo, el nombre de una persona colocada al final de un correo electrónico, la imagen digitalizada de una firma manuscrita agregada a un documento electrónico, un código secreto o PIN, un identificador basado en*

[9] *El ABZ de las Firmas Electrónicas*, www.corpece.org.ec/informante/index.htm, 28/3/02.

un mecanismo biométrico, y, finalmente, una firma digital creada por medio del uso de criptografía de clave pública."[10]

La Firma Electrónica como se encuentra definida en la mayor parte de las normativas del mundo es un término genérico, por lo cual también se contempla dentro de éstas a la firma digital, así cuando se define la Firma Electrónica se hace en un sentido de neutralidad tecnológica, que permite anticiparse al avance de la tecnología donde podrían presentarse otro tipo de firmas que no sean la firma digital o de clave pública.

2.2 Firma digital

Asimilar en un inicio lo que es una firma digital no es fácil para una persona sin bases en el tema, ante esto Juan Carlos Riofrío comenta: *"Si la definición de ´firma` de por sí envuelve muchas complicaciones, la de ´firma digital` todavía mas"*[11], la firma digital es aquella que se basa en el uso de la criptografía asimétrica que es una especie de Firma Electrónica caracterizada por agregar elementos de seguridad que la Firma Electrónica no posee, esto lo corrobora José Manuel Villar al expresar: "*ello es así porque la firma digital cumple, en relación con los documentos electrónicos, las principales funciones que se atribuyen a la firma manuscrita sobre un documento en papel; a saber, permite identificar al autor del escrito –*

[10] Mauricio Devoto, *op. cit* p. 166.
[11] Juan Carlos Riofrío Martínez-Villalba, *Garantías en las Comunicaciones Electrónicas en países sin Ley Especial*, en Revista de Derecho Informático (REDI), No. 038.

autenticación- y constatar que el mensaje no ha sido alterado después de su firma -integridad-" [12]

Otra característica de la firma digital es que da lugar al no rechazo o no repudio, es decir, que las partes que intervienen no pueden negar su actuación y, finalmente es garantía de confidencialidad; esto se traduce en ciertos servicios que están contemplados en las normativas sobre el tema y que protegen los datos al acceso de terceros no autorizados, pero desde ya podemos decir que específicamente se refiere al certificado de Firma Electrónica y entidades de certificación que se encuentran regulados en la Ley de Comercio Electrónico ecuatoriana y que desarrollaremos en el segundo capítulo.

Además, se debe indicar que en normativas como de la Unión Europea y de los Estados Unidos de Norteamérica, las Firmas Electrónicas tienen otra concepción en cuanto a su clasificación, concibiéndolas como Firmas Electrónicas y firmas electrónicas avanzadas, a lo anterior el español Leopoldo González Echenique comenta: "*Al fin y al cabo, la firma avanzada es aquella que confiere seguridad y certeza en la integridad, autenticidad u autoría del mensaje. No es más que aquella Firma Electrónica cuya eficacia ha sido comprobada por la autoridad competente y por la entidad técnica dedicada a esas actividades."*[13]. En relación a las Firmas Electrónicas

[12] José Manuel Villar, *Una aproximación a la Firma Electrónica*, en Rafael Mateu De Ros, *Derecho de Internet, Contratación Electrónica y Firma Digital*, Navarra, Editorial Aranzadi, S.A., 2001, p. 170.

[13] Leopoldo González – Echenique Castellanos de Ubao, *Estudio de la Directiva y del Real Decreto-Ley de 17 de septiembre de 1999 sobre Firma Electrónica,* en: Mateu De Ros, Rafael, Derecho de Internet, Contratación Electrónica y Firma Digital, S.A., Navarra, Editorial Aranzadi, 2001, p. 222.

avanzadas, consideramos que éstas son equiparables a la firma digital, además se puede decir que a pesar de que ciertas normativas la conciben así, indirectamente mantienen vigentes a las firmas electrónicas, aduciendo una neutralidad tecnológica, y argumentando que con el avance de la tecnología podrían presentarse otro tipo de Firmas Electrónicas que garanticen más seguridad que la firma digital.

Después de analizar la Firma Electrónica y la digital, consideramos prudente mencionar la distinción que entre los dos tipos de firma hace Ricardo Lorenzetti: "*La gran diferencia estriba en que cuando se utilice la firma digital, se aplican presunciones juris tantum sobre la identidad del firmante y la identidad del documento que suscriba.*"[14]. Para concluir, podemos decir que la mayor parte de autores coinciden en que la firma digital basada en la criptografía asimétrica, por el momento constituye el sistema más seguro y un paso fundamental para el comercio electrónico.

2.3 Concepto de Firma Electrónica en la legislación del Ecuador

Consideramos importante iniciar señalando lo que la Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos en el artículo 13, referente a la Firma Electrónica determina: "*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*

[14] Ricardo L. Lorenzetti, *Comercio Electrónico*, Buenos Aires, Ediciones Abeledo - Perrot, 2001, p. 8.

firma aprueba y reconoce la información contenida en el mensaje de datos."[15]

En concordancia con lo anterior el Reglamento a la Ley en el artículo 10, determina:

> *"Elementos de la Infraestructura de Firma Electrónica.- La Firma Electrónica es aceptada bajo el principio de neutralidad tecnológica. Las disposiciones contenidas en la Ley 67 y el presente Reglamento no restringen la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la infraestructura de llave pública, ni afecta los pactos que acuerden las partes sobre validez y eficacia jurídica de la Firma Electrónica conforme a lo establecido en la Ley y el presente Reglamento."*[16]

De los artículos citados se desprenden dos cosas, a saber: La *primera*, que la normativa ecuatoriana habla de Firma Electrónica, y como está redactada la definición, confiere seguridad y certeza en la integridad y autenticidad del mensaje, características de la firma digital y, la *segunda*, que se habla de neutralidad tecnológica, que a criterio de José Luis Barzallo se la interpretaría como: "*Siguiendo con la teoría de la neutralidad tecnológica propugnada por la UNCITRAL, tenemos que se ha interpretado tal teoría por la no definición de estándares tecnológicos en las legislaciones internas, ya*

---

[15] *Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos*, Registro Oficial Suplemento No. 557, de 17 Abril del 2002.

[16] *Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*, Registro Oficial Suplemento No. 735, de 31 de diciembre del 2002.

que con el avance de la tecnología, la ley puede quedar obsoleta en cuestión de meses."[17], situación última que responde a la necesidad de que la Ley tenga vigencia en el tiempo a pesar de los cambios tecnológicos.

En este momento es conveniente mencionar que en normativas sobre Firma Electrónica como la española y de la Comunidad Europea dan lugar a que se clasifique como Firma Electrónica y firma electrónica avanzada, pero lo expresado tiene una razón a criterio de Leopoldo González Echenique, que sostiene:

> *"La única explicación plausible al mantenimiento de esas dos modalidades legales de firma, primero por el legislador español y luego por el comunitario, sería la de dejar abierta la posibilidad de utilizar posibles nuevas técnicas creadas por la ingeniería informática que concedan a la Firma Electrónica simple mayor grado de fiabilidad que el ofrecido en el estado actual de los sistemas de creación y verificación superando la encriptación de clave doble y sustituyéndola por dispositivos de creación y verificación que alcancen mayor seguridad."*[18]

Remitiéndonos a la concepción de la Firma Electrónica contenida en la normativa ecuatoriana, ésta nos da a entender que dicho instrumento identifica a su titular (autenticidad), y de éste con el mensaje de datos (integridad), y que el titular de la firma aprueba y reconoce la información

[17] José Luis Barzallo, *Artículo: Los Terceros de Confianza en el Comercio Electrónico*, en Revista de Derecho Informático No. 033.

[18] Leopoldo González-Echenique Castellanos de Ubao, *op. cit.,* pp. 266 y 267.

contenida en el mensaje de datos (no repudio), así, Juan Carlos Riofrío comenta el no repudio: *"Si la autenticidad prueba quien es el autor de un documento y cual es su destinatario, el "no repudio" prueba que el autor envió la comunicación y que el destinatario la recibió".*[19], en otras palabras, la Firma Electrónica cumpliría las principales funciones que se atribuyen a la firma manuscrita sobre un documento en papel.

En cuanto a la confidencialidad, entendida ésta como la seguridad (no accesible) que un mensaje debe tener frente a terceros, en la legislación ecuatoriana, el Reglamento a la Ley no restringe la autonomía privada para el uso de otras Firmas Electrónicas generadas fuera de la infraestructura de llave pública (neutralidad tecnológica), así también estaría permitiendo el uso de firmas basadas en el sistema de criptografía simétrico que como ya se ha indicado no permite se presente la confidencialidad sin embargo, aquí cumplen un papel muy importante las entidades de certificación de información.

3. Normativa internacional sobre Firma Electrónica

El desarrollo del comercio electrónico ha generado una serie de incertidumbres en lo técnico y en lo legal; en lo técnico se están utilizando sistemas o mecanismos (criptografía – firma digital), que si bien han solucionado los inconvenientes, desde el punto de vista jurídico las leyes y normativas internacionales existentes incluida la del Ecuador, siguen

[19] Juan Carlos Riofrío Martínez-Villalba, *op. cit.,* No. 038.

presentando inconsistencias, al respecto Apol Lonia Martínez comenta: *"La alternativa entre la existencia o inexistencia de regulación en materia de firma digital y autoridades de certificación, nos lleva a inclinarnos por la prevalecía, en principio, de la autonomía de la voluntad, pero sin excluir la existencia de legislación al respecto que establezca un mínimo legal imperativo, que debe respetarse."*[20]

De esto se deriva que hayan surgido diversas iniciativas sobre el tema de la Firma Electrónica, de distinto ámbito de aplicación, sobre el cual varios países como España y Estados Unidos de Norteamérica han emitido leyes sobre la materia, y han surgido iniciativas de organismos o comunidades internacionales como la Unión Europea, así como de grupos u asociaciones, y proyectos de Ley y acuerdos orientados a establecer lineamientos sobre la materia. Contribuyendo todas estas a la elaboración de normativas en el tema.

En el párrafo anterior se mencionaron algunas iniciativas legislativas en materia de Firma Electrónica, en lo referido a los ámbitos de aplicación, a criterio de la última autora citada, la especificidad de éstos no determina su regulación, en el sentido en que:

> *"En caso de optarse por una regulación específica de las firmas digitales, ésta puede enfocarse de distintas formas. a) puede perseguir solamente la eliminación de formalismos (p. ej., equiparando expresamente la firma digital a la firma manuscrita allí*

[20] Apol L. Martínez, *op. cit.,* p. 96.

donde esta sea exigida, caso, como veremos, de la Ley francesa); b) puede ser una regulación de la firma digital y las autoridades de certificación de forma completa y total, estableciendo sus derechos, deberes y responsabilidades (caso de la Ley de Utah); c) puede ser una regulación legal sólo a nivel de principios que necesitará de un posterior desarrollo reglamentario (caso de Italia y Alemania)."[21]

Esto resulta necesario señalarlo a manera de antecedente para entender el tema de la regulación de la firma digital.

En cuanto a mecanismos de autenticación de Firma Electrónica y digital la experiencia internacional habla de tres modelos, a saber: un *primer* modelo minimalista que tiende a la utilización de Firmas Electrónicas de forma genérica; un *segundo* modelo que es más específico y que legisla sobre firmas digitales basadas en la criptografía de clave pública; y, un *tercero*, que contempla los dos anteriores, para lo cual creemos oportuno citar el comentario que al respecto realiza Mauricio Devoto, así: *"Algunos consideran que la bondad de este modelo radica en que asegura la neutralidad al reconocer distintos mecanismos de autenticación, mientras crea un entorno legal predecible y mejor definido al incorporar provisiones referidas a una tecnología en particular."*[22]. La normativa ecuatoriana sobre Firma Electrónica a nuestro criterio se inscribe dentro de este tercer modelo, puesto que en el artículo 13 de la Ley de Comercio Electrónico se define la Firma Electrónica conteniendo características de una firma digital y en el artículo 10 del Reglamento a la Ley se recoge la neutralidad tecnológica.

[21] *Ibíd*, p. 96.
[22] Mauricio Devoto, *op. cit.*, pp. 195 - 196.

De lo anterior cabe señalar, que gran cantidad de países han desarrollado su normativa sobre el comercio electrónico y en particular sobre la Firma Electrónica, en base a estudios de peritos en la materia, pero en países latinoamericanos como el Ecuador al parecer no se ha legislado de esta manera, concordando lo expresado con lo que al respecto sostiene el mismo Mauricio Devoto: *"La sensación que me queda, confirmada por comentarios de especialistas de los Estados Unidos y Europa, es que nuestros proyectos se caracterizan, por la falta de debate, por la falta de grupos interdisciplinarios, por celos sectoriales. Pocos se preguntan acerca de las características del mundo en que se realizan las actividades o mecanismos a regular."*[23]; seguidamente revisaremos como concibe la normativa internacional a la Firma Electrónica (firma digital/neutralidad tecnológica).

3.1 Legislación en los Estados Unidos de Norteamérica

En los Estados Unidos fue el Estado de Utah quien adoptó una Ley de Firma Electrónica (la Utah Digital Signatur Act) aprobada en el año de 1995 y modificada en marzo de 1996 y en el 2000, al respecto Mauricio Devoto expresa: *"ha sido la primera Ley en el mundo en sistematizar y conferirle validez jurídica a un mecanismo de autenticación – en este caso, un mecanismo en particular: la firma digital -. Basada en la digital Signaturas Guidelines, de la ABA, regula la firma digital basada en la criptografía de clave pública y la infraestructura requerida para su funcionamiento*."[24].

[23] *Ibid*., p. 189.
[24] *Ibid*., p. 197.

Dentro de éste mecanismo no solo se encontraban los Estados Unidos, sino también otros países que practican el Common Law. [25]

Finalmente en el año 2000, ante la necesidad de una ley que abarque todas las iniciativas surgidas en cuanto a Firma Electrónica en los Estados Unidos, se aprobó la Federal Electronic Signaturas in Global and Nacional Commerce Act (Federal E-Sign Act), Ley de aplicación en el ámbito federal, es importante señalar también que esta ley ha recibido críticas en el sentido que se define ampliamente a la Firma Electrónica, y que no es una ley de firma digital, es así como lo corrobora el mismo Mauricio Devoto al decir: *"Debe tenerse en cuenta que no es una es una ley de ´firma digital`, como se ha publicitado en los medios. Confiere validez jurídica a la ´firma electrónica`, definiéndola como ´…un sonido, símbolo o proceso electrónico adjunto o lógicamente asociado a un contrato u otro registro y ejecutado o adoptado por una persona con la intención de firmar el registro.`"*[26], sin embargo de todo lo expresado, a nuestro criterio, el documento estudiado es de gran ayuda para el afianzamiento de la Firma Electrónica como tal, tanto en los estados Unidos de Norteamérica como a nivel internacional.

3.2 Legislación en Europa

Al igual que en el caso de la normativa de los Estados Unidos de Norteamérica, los países europeos han presentado una gran variedad de decisiones legislativas sobre Firma Electrónica, para las que se tiene

[25] Modelo específico que regula a la firma digital en base a la criptografía de clave pública adoptado también en países como Australia, Canadá, Reino Unido y Nueva Zelanda.
[26] Mauricio Devoto, *op. cit.*, p. 201.

presente como parámetro principal, la Directiva 1999/93/CE, del Parlamento Europeo y del Consejo, de fecha 13 de diciembre de 1999. Directiva que en materia de Firma Electrónica determina una normativa común para la Unión Europea; el contenido y decisiones de esta Directiva tienen el carácter obligatorio para los países miembros, al respecto es importante citar el comentario que sobre las directivas realizan Araceli Mangas Martín y Diego Liñán Nogueras, así: "*En efecto, una directiva es una norma que impone una obligación de resultados para los Estados destinatarios que debe ser alcanzado al vencimiento del plazo; una directiva correctamente ejecutada en plazo no genera por sí misma derechos y obligaciones para los particulares sino a través de la norma de transposición o aplicación adoptada por el estado miembro.*"[27]

Lo importante de lo anterior, es el señalar la obligatoriedad de la decisión de la Directiva sobre Firma Electrónica, es así como en Europa las normativas anteriores a ésta debieron adaptarse, y las que se emitieron posteriormente la incorporaron. Las relaciones del Derecho Comunitario y el Derecho interno de los países de la Unión Europea parten de la autonomía del ordenamiento comunitario, además, de la atribución de competencias y de la colaboración de los dos ordenamientos que se integran, para de esta manera integrarse al derecho que se aplica a cada miembro.

Para el análisis de la normativa emitida por los países europeos, en primera instancia revisaremos los casos anteriores a la Directiva 1999/93/CE. En el

[27] Araceli Mangas Martín y Diego Liñán Nogueras, *Los principios del derecho comunitario en sus relaciones con los ordenamientos internos, en Instituciones y derecho de la Unión Europea*, segunda edición, Madrid, McGrawn-Hill, 1999, p. 303.

caso de Alemania, se emite la Ley alemana de firma digital, aprobada el 13 de junio de 1997, cuya finalidad fue otorgar una infraestructura segura para el uso de las firmas digitales; a través de ésta se regula la firma digital y las autoridades de certificación. En el caso de Italia, es el primer país de Europa en emitir un Reglamento en materia de firma digital, determinando básicamente conceptos de firma digital, claves asimétricas y certificado; igualmente Portugal, con el Decreto Ley número 290-D/99, del 2 de agosto del mismo año, que contiene la firma digital, destacando como finalidad el regular la validez, eficacia y valor probatorio de los documentos electrónicos de la firma digital.

Dentro de los países que emitieron normativas relacionadas con las firmas electrónicas antes de la Directiva 1999/93/CE se encuentra también España, caso que merece un análisis detenido, ya que consideramos a esta normativa como un marco de referencia para la normativa internacional de Firma Electrónica ya que España apenas dos meses antes de la Directiva 1999/93/CE, el 17 de septiembre de 1999 aprueba el Real Decreto (Ley 14/1999), en el que en el numeral 1 del artículo 1, se determina la finalidad de este instrumento, que es la regulación del uso de la Firma Electrónica. [28]

Lo interesante de observar es que con la publicación del Real Decreto Ley, se ocasiona un cambio definitivo en la legislación de firmas digitales, así también coincide Mauricio Devoto al comentar sobre el Real Decreto: *"... rompe en Europa la tendencia de legislar sobre firmas digitales y recoge la*

[28] Artículo 1. Ámbito de aplicación. 1. del *Real decreto-ley* regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación. Las normas sobre esta actividad son de aplicación a los prestadores de servicios establecidos en España.

tendencia que ya venía desarrollándose en los Estados Unidos desde la "Utah Act" y la "UNCITRAL Model Law", finalmente plasmada en la Directiva de la Unión Europea aprobada en diciembre de 1999."[29], en definitiva se empieza a dar la transformación de tratamiento a la normativa sobre firma digital a Firma Electrónica, ya no se legisla específicamente sobre firma digital o de clave pública, el Decreto Ley con su artículo primero se adelantó en cuanto al tratamiento de las Firmas Electrónicas a la Directiva 1999/93/CE, la cual también en su artículo primero determinará como finalidad principalmente facilitar el uso de la Firma Electrónica en la Comunidad Europea.

Entre los países que han aprobado su normativa posterior a la Directiva 1999/93/CE, se encuentra Francia con la Ley No 2000-230 expedida el 13 de marzo del 2000, que regula principalmente el valor probatorio de la Firma Electrónica. Esto confirma el cambio de forma de legislar a partir de la emisión de la Directiva de la Unión Europea.

3.3 Legislación en la Unión Europea

Como antecedente a la Directiva 1999/93/CE, tenemos la comunicación de las comunidades europeas al Consejo del Parlamento Europeo, al comité económico y social y al comité de las regiones, garantizando la seguridad y confianza en las comunicaciones electrónicas. Este marco europeo para las firmas digitales y la encriptación COM (97) 503, fue presentada el 8 de

[29] Mauricio Devoto, *op. cit.*, p. 200.

octubre de 1997, con la cual se pretendía crear un marco común para el desarrollo del comercio electrónico y para las firmas digitales que asegurara el funcionamiento del mercado interno, mismo que debía aplicarse en la Unión Europea a más tardar hasta el año 2000.

Los antecedentes a la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, terminan concretándose en ésta el 13 de diciembre de 1999, siendo lo principal la determinación de un marco comunitario para la Firma Electrónica, es así como especialmente en el inciso primero del artículo 1[30], de la Directiva se plantea como finalidad principal facilitar el uso de la Firma Electrónica y su reconocimiento legal, establece además, un marco común para determinados servicios de certificación. Es importante señalar que esta Directiva no habla solamente de Firmas Electrónicas, pues de conformidad con el considerando contenido en el numeral (8) de la Directiva[31], se pretende tener una posición tecnológica abierta, criterio que comparte Apol Lonia Martínez cuando sobre el tema comenta:

> *"Por ello, pretende, en concreto, contribuir al uso y reconocimiento legal de las firmas electrónicas en general (y no sólo de las firmas digitales en particular, pues se quiere adoptar una posición tecnológicamente abierta) dentro de la Unión Europea, y establecer un marco común para determinados servicios de certificación disponibles para el público a fin*

[30] Artículo 1. Ámbito de Aplicación 1. La presente Directiva tiene por finalidad facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico. La presente Directiva crea un marco jurídico para la firma electrónica y para determinados servicios de certificación con el fin de garantizar el funcionamiento del mercado interior.

[31] (8) Los rápidos avances tecnológicos y la dimensión mundial de Internet hacen necesario un planteamiento abierto a diferentes tecnologías y servicios de autenticación electrónica de datos.

de asegurar el correcto funcionamiento del mercado interno en el campo de las firmas electrónicas."[32]

Es importante señalar que la Unión Europea tiene como base al Derecho Comunitario Europeo, mismo que es propio y autónomo, ya que los Estados miembros han cedido voluntariamente en ciertos campos el ejercicio de su soberanía, y que no son sólo aquellas relativas a materias técnicas concretas, sino respecto a funciones que corresponden al ámbito esencial de la propia existencia en tanto Estado, lo anterior tiene relación con la tan debatida supranacionalidad, consideramos importante lo que al respecto pronuncia José Manuel Sobrino, así:

"En resumen, integración y supranacionalidad en sentido de supraestatalidad, son expresiones cercanas pero no sinónimas. Puesto que la integración no exige la renuncia por parte de los Estados miembros a su soberanía, solamente precisa que éstos, en virtud de dicha soberanía, cedan voluntariamente el ejercicio de la misma a la organización de que se trate. Supranacionalidad en tanto supraestatalidad, significaría, en cambio, que estamos más allá de una mera cesión del ejercicio de la soberanía, y que aparecen nuevos entes internacionales por encima de los Estados dotados de soberanía"[33].

Sin embargo de lo expresado, lo cual tiende más a un análisis de la naturaleza jurídica de la unión Europea dentro de su proceso de integración,

[32] Apol L. Martínez, *op. cit.*, pp. 122 y 123.
[33] José Manuel Sobrino, *El derecho de Integración: Marco Conceptual y Experiencias Regionales*, en Integración y Supranacionalidad, Soberanía y Derecho Comunitario en los Países Andinos, Lima, 2001, p. 45

lo que nos interesa para nuestro estudio es que en la Unión Europea con la Directiva 1999/99/CE, se determinó una normativa común, aplicable a los Estados Miembros, que es la que tiene relación con la Firma Electrónica.

La Unión Europea es uno de los procesos más importantes de integración, pero la Comunidad Andina en nuestro hemisferio tampoco deja de serlo, ésta cada vez se desarrolla institucional y jurídicamente, puesto que ha creado órganos e instituciones comunitarios (Secretaría General), órganos intergubernamentales (Consejo de Cancilleres) y un sistema de solución de diferencias (Tribunal Andino de Justicia). El ordenamiento jurídico de la Comunidad Andina de Naciones tiene sus pilares en dos principios fundamentales: el principio de aplicación directa y el principio de preeminencia del ordenamiento jurídico[34], de lo dos principios expresados, el que nos interesa para nuestro estudio es el segundo, puesto que nos permite colegir que cuando se quiera aplicar normas legales en actos jurídicos contemplados en el derecho de la integración, es obligatorio remitirse a la norma comunitaria, la que prevalece sobre la norma interna.

A lo anterior y con relación a la supranacionalidad, Víctor Manuel Rico expresa: *"En el nivel en el que nos encontramos en la CAN, cuando hablamos de supranacionalidad, estamos hablando básicamente de eso, de transferencias nacionales hacia órganos intergubernamentales como el Consejo de Cancilleres y la Comisión o hacia órganos comunitarios como la*

[34] El principio de aplicación directa se entiende como la capacidad jurídica de la norma comunitaria para generar derechos y obligaciones que los ciudadanos de cada país puedan exigir de los tribunales nacionales.
El principio de la preeminencia del ordenamiento jurídico, conlleva la virtud que tiene el ordenamiento comunitario de ser imperativo, y de primar sobre una norma de derecho interno.

Secretaría General."[35]*,* luego de este análisis, y en base a la investigación de la normativa de la CAN, podemos decir que no existe normativa emitida por ésta que tenga relación con la Firma Electrónica, por ende la normativa que nos rige es la contemplada en la ley de Comercio Electrónico y sus reglamentos.

En definitiva, en la Unión Europea el uso de la Firma Electrónica se consolidó con la Directiva 1999/93/CE, ya que como se analizó en el marco del derecho de la integración europea, las directivas prevalecen sobre las normas internas, es por esto, que para las normativas anteriores a la Directiva 1999/99/CE fue obligatoria la adaptación a esta última y para las normativas emitidas con posterioridad tuvieron que acogerla; mientras que en la Comunidad Andina, no se ha emitido norma alguna relacionada con la Firma Electrónica, por lo que se encuentra en vigencia la ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

3.4 El Proyecto de Ley Modelo para las Firmas Electrónicas de la UNCITRAL

Luego de varios proyectos e informes presentados por el grupo de trabajo conformado para debatir sobre comercio electrónico en la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional -CNUDMI-UNCITRAL- éste en su trigésimo séptimo período de sesiones celebrado en Viena del 18 al 29 de septiembre del 2000, aprobó el Proyecto de Ley

[35] Víctor Manuel Rico Frontaura, *El Derecho de la Integración en la Comunidad Andina*, en Integración y supranacionalidad. Soberanía y derecho Comunitario en los Países Andinos, Lima, 2001, p. 78.

Modelo para las Firmas Electrónicas, éste instrumento ha colaborado como base y punto de partida para las leyes que sobre Firma Electrónica se han emitido en el mundo, así también para las que se están elaborando y reformando; esta Ley no es una imposición u obligación para los países u organizaciones, como su título lo indica es un modelo, que pretende guiar la unificación de la normativa existente sobre Firma Electrónica, es así, como en el numeral segundo de la parte introductoria de esta Ley se considera: *"Recomienda que todos los Estados consideren de manera favorable la Ley Modelo cuando promulguen o revisen sus leyes, habida cuenta de la necesidad de que el derecho aplicable a los métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel sea uniforme"*[36]

Dentro de este proyecto se concibe un régimen uniforme sobre las cuestiones de la firma digital y de las entidades de certificación adoptando el criterio de la neutralidad tecnológica, dejándose abierto el tema de las firmas electrónicas a otras técnicas de autenticación; se establece además dentro de este instrumento, en lo que se refiere a sus efectos jurídicos igual validez legal tanto para los mensajes escritos como para los mensajes digitales; a lo anterior, consideramos el criterio de Mauricio Devoto que hace la siguiente aclaración: *"Sin perjuicio de lo expuesto, debe tenerse en cuenta que se trata de una Ley marco (framework law) que no contemplan todas las regulaciones que puedan resultar necesarias para implementar aquellas técnicas en los estados que la adopten. Por tal motivo los estados pueden*

[36] *Ley Modelo de la ULCITRAL sobre Comercio Electrónico*, CENUDMI – ULCITRAL, 28 de mayo al 14 de junio de 1996.

dictar la regulación que consideren conveniente para cumplimentar los procedimientos adoptados."[37], con lo anterior vemos que esta Ley deja lugar a que el Estado intervenga en la creación de la reglamentación correspondiente.

En definitiva la Ley Modelo de -CNUDMI-UNCITRAL-, es una base de legislación integral en materia de comercio electrónico, ya que define los principios y procedimientos básicos a aplicarse respecto de la Firma Electrónica. Lo que se pretende es la armonización y la unificación del Derecho Mercantil Internacional, transacciones que se realizan actualmente a través del comercio electrónico, la finalidad de la Ley Modelo es la de ofrecer al legislador nacional un marco jurídico que permita un desarrollo más seguro del comercio electrónico.

3.5 Legislación ecuatoriana

Como es de conocimiento general, el 23 de mayo de 1969 se suscribió la Convención de Viena sobre Derecho de los Tratados, la cual ha sido suscrita pero no ratificada por el Ecuador, sin embargo, nuestro país se caracteriza por el respeto al Derecho Internacional; es así como en la Constitución Política vigente, en los numerales 3,4 y 5 del artículo 4 se determina: *"3. Declara que el derecho internacional es norma de conducta de los estados en sus relaciones recíprocas y promueve la solución de las controversias por métodos jurídicos y pacíficos. 4. Propicia el desarrollo de la comunidad*

[37] Mauricio Devoto, *op. cit.*, p. 198.

internacional, la estabilidad y el fortalecimiento de sus organismos. 5. propugna la integración, de manera especial la andina y latinoamericana."[38], de lo anterior podemos destacar el hecho de tener la base constitucional para ser parte de la Comunidad Andina de Naciones, habilitándole a suscribir tratados en los que puede ceder ciertas atribuciones soberanas a los organismos comunitarios.

Lo anterior también nos acerca a la supranacionalidad, tema muy debatido desde hace mucho tiempo atrás, Cesar Montaño Galarza respecto de ésta dice:

> *"En lo tocante a la supranacionalidad, diremos que se expresa de dos maneras: como la transferencia de soberanía con la consecuente delegación de competencias desde los estados que se integran hacia el apartado comunitario; y, mediante la conformación de órganos e instituciones comunitarios autónomos, cuya característica distintiva consiste en la toma de decisiones o en la expedición de fallos que son aceptados en los territorios de los PM, debido a su preeminencia y aplicabilidad directa e inmediata."*[39]

Lo importante de recalcar, es que en el derecho comunitario, tenemos en relación a la Firma Electrónica la Directiva 1999/93/CE, que prevalece sobre la normativa interna de los países miembros; mientras que en la Comunidad Andina no se conoce de norma alguna relacionada con la Firma Electrónica,

---

[38] *Constitución Política de la República del Ecuador*, Gaceta Constitucional, de julio de 1998.

[39] Cesar Montaño Galarza, *Constitución del Ecuador e Integración Andina*, artículo inédito, Quito, 2002, p. 10.

por lo que nuestro país se rige internamente por su Ley, misma que se la concibe en base a los principios y procedimientos contenidos en la Ley Modelo, insistiendo en el hecho de que dicho cuerpo normativo no nos ha sido impuesto.

Otro aspecto que no podemos dejar de mencionar es el que tiene que ver con la globalización, que involucra el acortamiento de distancias entre los países, debido en su mayor parte a los adelantos tecnológicos en las comunicaciones. En la relación economía - derecho, nuestros países latinoamericanos han experimentado en estos últimos siglos una transición de tipo económico, por lo cual también se ha experimentado diferentes modelos estatales, pasando por el modelo liberal, el intervencionista hasta llegar al estado moderno de corte neoliberal, así, nuestra actual Constitución en el artículo 244, concibe a una economía social de mercado, impulsando mercados competitivos y libre competencia[40]; a lo anterior, Cesar Montaño manifiesta: *"La globalización económica que se expresa en lo comercial, financiero, productivo y tecnológico, también es presentada como paradigma vital que debe ser asumido por los países menos desarrollados, demostrando como fieles feligreses claras señales de apertura comercial, inversiones sin restricciones y abstracción del estado de sus funciones económicas como orientador, regulador y promotor del crecimiento económico y del bienestar social, so pena de perder el tren del desarrollo."*[41]

[40] Dentro del sistema de economía social de mercado al Estado le corresponderá: 3. Promover el desarrollo de actividades y mercados competitivos. Impulsar la libre competencia y sancionar, conforme a la ley, las prácticas monopólicas y otras que la impidan y distorsionen.
[41] Cesar Montaño Galarza, *Documento Visión General del Derecho Económico,* p. 5.

Hemos dicho que cada vez más en el mundo globalizado se relacionan el derecho con la economía, especialmente con la evolución de los avances tecnológicos, como es el Internet que actualmente da lugar al comercio electrónico, del cual la Firma Electrónica hace parte, esto nos hace pensar que nos encontramos ante un orden jurídico nuevo, en construcción, comentario que corrobora Jorge Witker, al decir: *"En síntesis, el derecho en la economía internacional de mercado libre, sufre cambios conceptuales profundos que alteran las bases mismas de lo que se conoce como derecho nacional o interno. La revolución del conocimiento y los vertiginosos adelantos técnico-científicos (nuevos materiales, la biotecnología, la informatización de la vida diaria y las relaciones multilenguas,etc.), preparan un nuevo derecho que recién esta generación comienza a vislumbrar."*[42], lo anterior, podríamos decir que se traduce en la relación que existiría entre comercio electrónico y Derecho Económico, el cual de conformidad a nuestra realidad, y a criterio de Cesar Montaño podría concebirse como: *"El derecho económico es el conjunto de normas jurídicas de corte público, con efectos en el ámbito nacional, internacional o supranacional, que sirve en un régimen de economía mixta o socializada (marco institucional), para regular y orientar las actividades del sistema económico (objeto), de las personas físicas, jurídicas y demás sujetos económicos (sujeto), para la consecución de las metas y objetivos de la vida económica nacional y para consolidar la democracia económica (finalidad o sentido) expresada en un sostenido desarrollo económico y social."*[43]

[42] Jorge Witker, *El Derecho Económico en los Sistemas Económicos del siglo XX*, en: Introducción al derecho Económico, Tercera Edición, Editorial Harda, Mexico, 1997, p. 33.

[43] Cesar Montaño Galarza, *op. cit.* p. 11.

Como podemos colegir existe una relación comercio electrónico y Derecho Económico, en el Ecuador se ha normado al comercio electrónico y a la Firma Electrónica aspirando generalizar la utilización de servicios de redes de información e Internet, con la finalidad principal de desarrollar el comercio, es así como en el cuarto considerando de la Ley de Comercio Electrónico se expresa: *"Que a través del servicio de redes electrónicas, incluida la Internet se establecen relaciones económicas y de comercio, y se realizan actos y contratos de carácter civil y mercantil que es necesario normarlos, regularlos y controlarlos, mediante la expedición de una Ley especializada sobre la materia."*[44]*;* en relación a lo anterior, en el Ecuador el artículo 1, de la Ley de Comercio Electrónico determina: *"Objeto de la Ley.- Esta Ley regula los mensajes de datos, la Firma Electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas."*[45]

Ahora bien, según el objeto contenido en la Ley Comercio Electrónico, la Firma Electrónica fue elaborada en base a la Ley Modelo de la UNCITRAL, adoptando también el criterio de la neutralidad tecnológica, consideramos a manera de complemento y para una mejor comprensión del tema tratado traer a colación lo que al respecto comenta Mauricio Devoto:

> *"Originalmente el Grupo de Trabajo en Comercio Electrónico comenzó estudiando y concentrándose en las firmas digitales basadas en*

[44] Ley de comercio Electrónico, *op. cit.*
[45] Ley de Comercio Electrónico, *op. cit*.

criptografía de clave pública, reconociéndolas como el mecanismo de autenticación más conocido, desarrollado y probado, Sin perjuicio de no haber surgido otro mecanismo o tecnología que la superara, fue abriéndose paso la corriente de "neutralidad tecnológica", recogida en la Ley Modelo.[46]

En lo que se refiere a la normativa nacional, sobre la Firma Electrónica y su régimen de aplicación, ésta se encuentra normada principalmente en los siguientes instrumentos legales: Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos, publicada en el suplemento del Registro Oficial No. 557, del 17 de abril del 2002; el Reglamento General a la Ley de Comercio Electrónico, mediante Decreto Ejecutivo No. 3496, publicado en el Registro Oficial No. 735 de 31 de diciembre del 2002; Reformas al Reglamento General, expedidas a través del Decreto Ejecutivo No. 908, publicado en el Registro Oficial No. 168, de 19 de diciembre del 2005 y, El Reglamento para la Acreditación, Registro y Regulación de Entidades Habilitadas para prestar Servicios de Certificación, Información y Servicios Relacionados, Resolución No. 584-23 – CONATEL, publicado en el Registro Oficial No. 196, de 23 de octubre del 2003.

4. Período de validez de la Firma Electrónica en el Ecuador

4.1 Duración de la Firma Electrónica

[46]Mauricio Devoto, *op. cit.*, p. 202.

En referencia a la duración de la Firma Electrónica, la Ley de Comercio Electrónico en el artículo 18, determina: *"Las firmas electrónicas tendrán duración indefinida. Podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el Reglamento a esta Ley señale."*[47]. La Firma Electrónica en la legislación del Ecuador, tiene un período de validez indefinido o indeterminado, en otras palabras, durarían hasta la muerte del titular; esto es correcto, ya que la Firma Electrónica de la manera como está concebida en la normativa ecuatoriana tiene los mismos efectos jurídicos que la firma manuscrita, sin embargo, de conformidad con la Ley de Comercio Electrónico puede extinguirse.

Dentro del artículo citado se habla de revocación, anulación o suspensión de las Firmas Electrónicas, que a criterio del ecuatoriano Efraín Torres Cháves se las puede concebir como: *"Revocar, es dejar sin efecto una declaración de voluntad o un acto jurídico en que unilateralmente se tenga tal potestad. Anular es levantar la validez y quitarle todo valor a un acto o contrato. Suspensión, es detención de un acto, interrupción de un oficio o beneficio, es una sanción administrativa donde se le priva a alguien de las operaciones."*[48], revisando también el Reglamento a esta Ley, no encontramos nada al respecto de la revocación, anulación y suspensión de la Firma Electrónica. Lo expresado no se debe confundir con la extinción, suspensión y revocación del certificado de Firma Electrónica, artículos 24, 25 y 26 de la Ley de Comercio Electrónico y artículo 13 del Reglamento a la Ley.

[47] Ley de Comercio Electrónico, *op. cit.*
[48] Efraín Torres Cháves, *Breves Comentarios a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*, Quito, Corporación de Estudios y Publicaciones, 2002, p. 32.

4.2 Extinción de la Firma Electrónica

En el artículo 19, la Ley de Comercio Electrónico contempla las causas por las que la Firma Electrónica se extingue, que significaría también la terminación de la responsabilidad del titular y de éste con la Firma Electrónica, sin embargo, en el inciso final del artículo, se aclara que la extinción de la Firma Electrónica no exime a su titular de las obligaciones que contrajo antes de la extinción y que hayan sido derivadas de su uso. Las causas de la extinción son:

a) Voluntad de su titular; ésta causa se puede presentar siempre y cuando el titular comunique de tal decisión a la entidad de certificación, lo cual por el momento traería consigo, el hecho de dejar sin efecto el certificado de Firma Electrónica.

b) Fallecimiento o incapacidad de su titular; en caso de fallecimiento, la extinción se hará efectiva con la partida de defunción, pudiéndose también presentar el caso de muerte presunta, para lo cual será necesaria la declaración judicial; el caso de incapacidad del titular de la firma, tiene concordancia con lo determinado en el Código Civil, por lo cual habría que determinar el hecho de la incapacidad, si es absoluta o relativa.

c) Disolución o liquidación de la persona jurídica, titular de la firma. El aspecto más importante de este literal, es que se reconoce a la persona

jurídica como titular de una Firma Electrónica; además, en materia societaria, previa la disolución o liquidación de una compañía, ésta debe ser considerada por la Junta de Accionistas, y aprobada por resolución de la Superintendencia de Compañías, para finalmente ser inscrita en el Registro Mercantil, solo en ese instante surte efectos, este procedimiento toma tiempo por lo cual mientras tanto la Firma Electrónica estaría vigente. Debe reformarse la Ley en este sentido, haciendo referencia a la Ley de Compañías.

d) Por causa judicialmente declarada; ésta, comentada por Efraín Torres Cháves vendría a ser: *"no es otra que la expresada en la Ley y a petición de parte, en materia de infracciones informáticas o administrativas, el juez podrá – según sus facultades legales – de oficio, dar por extinguida una Firma Electrónica. En esta circunstancia, el bien jurídico protegido es la propiedad del titular."*[49].

5. La Firma Electrónica como instrumento público en el Ecuador

En el transcurso de la historia, la fe pública siempre ha estado ligada al desarrollo del instrumento público notarial, este antecedente es considerable que se mencione, es así como la ecuatoriana Katia Murrieta comenta: *"En el mundo de la legislación existen dos sistemas, el escrito, de origen latino, conocido comúnmente como romano-germánico y el consuetudinario de origen anglosajón. Nuestra legislación pertenece al primero y la forma*

[49] *Ibíd.,* p. 33.

notarial de otorgamiento de documentos y celebración de contratos es totalmente escrita"[50]*,* nuestra Ley de Comercio Electrónico en su artículo 51, determina: *"Instrumentos públicos electrónicos.- Se reconoce la validez jurídica de los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmados electrónicamente. Dichos instrumentos públicos electrónicos deberán observar los requisitos, formalidades y solemnidades exigidos por la Ley y demás normas aplicables."*[51], en concordancia con lo citado, la Ley Notarial del Ecuador en su artículo 6[52], determina que los notarios son los funcionarios investidos de fe pública para autorizar a requerimiento de parte, los actos, contratos y documentos determinados por la Ley.

La evolución de los medios electrónicos es tan rápida, que actualmente nos invaden en nuestros quehaceres diarios, sin dejar de estar presentes en el campo del derecho; el tema que nos ocupa hace referencia a lo que se podría llamar instrumento público electrónico, mismo que se está imponiendo rápidamente en el mundo de la contratación por ser mas funcional y práctico en relación con el que podríamos denominar clásico, es así, como la celebración de un contrato a través de un instrumento público electrónico es simple y rápido, siempre y cuando también se respeten las formalidades legales contempladas en nuestras leyes, ya que todo

[50] Katia Murrieta Wong, *Presente y Futuro de la Contratación Electrónica a Distancia y Comentarios a la Ley de Comercio Electrónico Ecuatoriana*, en Xavier Castro, Libro Homenaje al Dr. Héctor Romero Parducci, Guayaquil, Edino, 2000, p. 103.
[51] Ley de Comercio Electrónico, *op. cit*
[52] Art. 6. Notarios son los funcionarios investidos de fe pública para autorizar, a requerimiento de parte, los actos, contratos y documentos determinados en las leyes.
Para juzgarlos penalmente por sus actos oficiales gozarán de fuero de corte.

instrumento público debe reunir requisitos que le son exigibles por ser esenciales para su validez.

Una de esas formalidades y que creemos la más importante es la intervención de un notario; para lo cual consideramos la existencia de un instrumento público notarial informático, ante esto el Notario Honorario español Antonio Rodríguez Adrados, al hacer la presentación del libro Instrumento Público Electrónico de Eugenio Alberto Gaete, expresa:

> *"Por todo ello me parece que el verdadero camino es el emprendido por GAETE en esta tesis doctoral; hay que partir de nuestro sistema de derecho, y construir en él un instrumento público notarial informático, un documento que sea al mismo tiempo documento informático y escritura pública notarial; de manera que según las necesidades de los diversos sectores del tráfico jurídico y la rogación de los otorgantes, la escritura pudiera otorgarse y autorizarse en papel o informáticamente."*[53]

Para que se cumpla lo anterior, pensamos necesario designar al Notario como autoridad certificadora y dando fe de las actuaciones informáticas, ya que de lo contrario no se podría contar como instrumento electrónico público; este es un criterio que compartimos y puede ser considerado para una reforma de nuestra normativa específicamente del Código de Procedimiento Civil.

5.1 Medio de Prueba

[53] Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, Editorial Bosh S.A., Baecelona, 2000, p. 15.

Partimos el análisis de este tema comentando que la normativa internacional sobre Firma Electrónica, concibe que la Firma Electrónica (firma digital – Firma Electrónica avanzada), cumple la función propia de la firma manuscrita; esta firma avala la autoría e integridad del mensaje de datos o instrumento electrónico, por lo que se considera también constituye medio de prueba; la autora María Luisa Domínguez referente al tema comenta la Directiva 1999/93/CE de la siguiente forma: *"el artículo 5, de la Directiva reconoce a la Firma Electrónica avanzada que reúna los requisitos anteriormente descritos, el mismo valor jurídico que la manuscrita y servirá como medio de prueba en los procedimientos judiciales.* [54], lo citado guarda concordancia con lo que Carmen Ordoño expresa: *"La Firma Electrónica viene a cumplir la función propia de la firma manuscrita. De manera, que al igual que ésta, constituye un instrumento o sistema de autenticación, que va a aportar eficacia a los documentos informáticos."*[55], en definitiva la normativa internacional al equiparar las funciones de la firma manuscrita a la firma digital, tiene como consecuencia la determinación de esta última como medio de prueba.

La Firma Electrónica como medio de prueba, también se concibe en el artículo 14, de nuestra Ley, que determina: *"Efectos de la Firma Electrónica.- La Firma Electrónica tendrá igual validez y se le reconocerán los mismos*

[54] María Luisa Domínguez Gragera, *Normativa Aplicable a la Firma Electrónica (Directiva 99/93/CE y Real Decreto-Ley 14/1999)*, en Javier Cremades, *Régimen Jurídico de Internet*, Las Rozas-Madrid, La Ley-Actualidad, 2002, p. 1346.

[55] Carmen Ordoño Artés, *El Avance Tecnológico y los Nuevos Medios de Prueba en la Ley de Enjuiciamiento Civil*, en Javier Cremades, *Régimen Jurídico de Internet*, Las Rozas-Madrid, La Ley-Actualidad, 2002, p. 508.

efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio."[56]; a su vez y en cuanto al reconocimiento extraprocesal de firmas y rubricas, Efraín Torres Cháves expresa: *"La vigencia en esta Ley, probablemente carece de un requisito formal para efectos procesales o extraprocesales, esto es, el reconocimiento de firma y rúbrica que se lo hace ante un Notario, o Juez."*[57]

Dentro de este contexto, también se encuentra el artículo 52, de la Ley de Comercio Electrónico, que determina*: "Medios de prueba.- Los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, emitidos de conformidad con esta Ley, cualquiera sea su procedencia o generación, serán considerados medios de prueba. Para su valoración y efectos legales se observará lo dispuesto en el Código de Procedimiento Civil."*[58]; ahora bien, el Código de Procedimiento Civil, en el artículo 198[59], contempla los casos o actos en los que un instrumento privado hace igual fe que uno público, son cuatro los casos, pero el de nuestro interés el primero, que sostiene que un instrumento privado hace tanta fe como un público, sí el que lo hizo o mandó hacer lo reconoce como suyo ante cualquier juez civil, o en escritura pública, sin embargo, a lo anterior existe una critica de la ecuatoriana Katia Murrieta, que consideramos es meritorio anotarla, quien sostiene: *"Dicho sea de paso, el*

[56] Ley de Comercio Electrónico, *op. cit*.
[57] Efraín, Torres Cháves, *op. cit* , p. 28.
[58] Ley de Comercio Electrónico *op. cit.*
[59] Artículo 198, dice: el instrumento privado en que una persona se obligue a dar, hacer o no hacer alguna cosa, o en que confiesa haberla recibido o estar satisfecha de alguna obligación, hace tanta fe como un instrumento público en los casos siguientes, siempre que la Ley no prevenga la solemnidad del instrumento público: 1º.- Si el que hizo o mandó hacer lo reconoce como suyo ante cualquier juez civil, o en escritura pública.

documento cuya firma es reconocida ante notario conforme a la Ley notarial, no tiene esta calidad probatoria, puesto que cuando se reformó dicha Ley no modificamos el CPC de modo expreso. Distinto es cuando el documento es firmado ante dicho fedatario público."[60]

Los notarios en la legislación del Ecuador tienen la facultad de certificar la autenticidad de las firmas puestas en los documentos privados, para esto, deben estar presentes los firmantes, dejando claro que esta certificación no convierte al instrumento privado en público, pero en cuanto a la certificación en particular, se trata de un instrumento público y por ende haría plena fe en juicio. Lo mencionado en este párrafo sobre certificación notarial de firmas, no hay que confundirlo con la verificación válida de una firma digital, es así como en relación a lo último, Mauricio Devoto expresa: *"asegura que la ´firma` ha sido creada con la clave privada correspondiente a la clave pública utilizada para verificar la firma, pero no asegura que haya sido el propio titular del par de claves que haya creado la firma."*[61]

La conclusión de este tema es que en nuestra normativa por el momento cualquier otro sistema de certificación de firmas que no sea la certificación ante notario autorizado carecería de plena fe, por esto, considero valioso el aporte que respecto a nuestra normativa sostiene Katia Murrieta, así: *"Debe reformarse la legislación civil de modo que se admita el documento informático como medio de prueba, cuando haya sido producido con la intervención de un Notario (al efecto, debería reformarse el título XXI del*

[60] Katia Murrieta Wong, *op. cit.*, p. 118.
[61] Mauricio Devoto, *op.cit.*, pp. 212 y 213.

Libro IV del Código Civil, de las obligaciones en general y de los contratos, de la prueba de las obligaciones y la sección séptima del título I del Libro 2º del Código de Procedimiento Civil, de las pruebas).”[62], de llegarse a presentar la reforma propuesta, debería también considerarse el argumento de Eugenio Gaete respecto de considerar la creación de un instrumento público notarial informático.

5.2 Presunción, práctica y valoración de la prueba

Para el estudio del presente título iniciaremos señalando lo que al respecto determina la Ley de Comercio Electrónico sobre estos temas y posteriormente analizaremos el principio de la equivalencia funcional. La *presunción* de una Firma Electrónica se encuentra contenida en el artículo 53, de nuestra Ley nacional: *“Presunción.- 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.”*[63], lo citado guarda concordancia con lo que se conoce como la verificación válida de la firma digital, lo que no se debe confundir con la certificación notarial de firmas, en la que se encuentra presente el notario haciendo que la firma certificada por éste haga plena fe.

[62] Katia Murrieta Wong, *op. cit.*, p. 132.

[63] Ley de Comercio Electrónico, *op. cit.*.

El artículo 54, de la Ley de Comercio Electrónico que se refiere a *la práctica de la prueba,* determina que se procederá de conformidad con lo previsto en el Código de Procedimiento Civil, (Sección Séptima, Título I, del Libro Segundo) y en base a las siguientes normas:

> *"a) Al presentar un mensaje de datos dentro de un proceso judicial en los juzgados o tribunales del país, se deberá adjuntar el soporte informático y la trascripción en papel del documento electrónico, así como los elementos necesarios para su lectura y verificación, cuando sean requeridos; b) En el caso de impugnación del certificado o de la Firma Electrónica por cualesquiera de las partes, el juez o tribunal, a petición de parte, ordenará a la entidad de certificación de información correspondiente, remitir a ese despacho los certificados de Firma Electrónica y documentos en los que se basó la solicitud del firmante, debidamente certificados; c) El facsímile, será admitido como medio de prueba, siempre y cuando haya sido enviado y recibido como mensaje de datos, mantenga su integridad, se conserve y cumpla con las exigencias contempladas en esta Ley."*[64]

El último inciso del artículo 54, determina que en el caso de que una de las partes niegue la validez del mensaje de datos, se deberá probar conforme Ley, que éste adolece de algún vicio o que no puede ser reconocido como técnicamente seguro el procedimiento de seguridad, incluido los datos de creación y, los medios utilizados para verificar la firma. Los vicios que puede adolecer el consentimiento son: el error, la fuerza y el dolo, y se encuentran

[64] Ley de Comercio Electrónico, *op. cit*.

determinados en el artículo 1494[65], y siguientes del Código Civil, sin embargo, y como se ha señalado, la Firma Electrónica en los mensajes de datos forma parte del todo, así también lo determina el artículo 16, de la Ley de Comercio Electrónico[66], al decir que la Firma Electrónica debe enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste, por lo que, sí se dice que la firma es técnicamente segura, no se puede tampoco dudar del mensaje, y por ende tampoco se podría alegar invalidez fundamentado en este argumento.

La *valoración de la prueba* se encuentra normada principalmente en el inciso primero del artículo 55, de la Ley de Comercio Electrónico[67] y se basa fundamentalmente en la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó el mensaje si fuese el caso; además, la valoración se someterá al libre criterio judicial. Consideramos que lo último expresado no constituye garantía dentro de un proceso, ya que es un aspecto bastante técnico y necesariamente debe ponerse en consideración de peritos en la materia, como así también lo señala el último artículo mencionado, Juan Carlos Riofrío al respecto de la valoración hace el siguiente comentario: *"La sana crítica aplicada a la*

[65] Artículo. 1494.- los vicios de que puede adolecer el consentimiento son: error, fuerza y dolo.

[66] Artículo 16.- La firma electrónica en un mensaje de datos.- Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste. Se presumirá legalmente que el mensaje de datos firmado electrónicamente conlleva la voluntad del emisor, quien se someterá al cumplimiento de las obligaciones contenidas en dicho mensaje de datos, de acuerdo a lo determinado en la Ley.

[67] Art. 55.- Valoración de la prueba.- La prueba será valorada bajo los principios determinados en la ley y tomando en cuenta la seguridad y fiabilidad de los medios con los cuales se la envió, recibió, verificó, almacenó o comprobó si fuese el caso, sin perjuicio de que dicha valoración se efectué con el empleo de otros métodos que aconsejen la técnica y la tecnología. En todo caso la valoración de la prueba se someterá al libre criterio judicial, según las circunstancias en que hayan sido producidos.

valoración de la prueba informática es quizá el mejor sistema en la mayoría de los casos, excepto en aquellos en donde la Ley exige expresamente la firma quirografaria, eso sí, siempre y cuando nuestros jueces tengan, efectivamente, una ´sana crítica`".[68]

Una vez revisados los artículos referentes a la *presunción, práctica y valoración de la prueba* y sin dejar de mencionar que en el Reglamento a la Ley de Comercio Electrónico no se expresa nada al respecto, consideramos importante señalar en este punto al llamado *principio de la equivalencia funcional*, y que para entenderlo mejor citaremos a Rafael Illescas Ortiz, que dice: *"El significado de la regla de la equivalencia funcional puede formularse de la siguiente manera: la función jurídica que cumple la instrumentación escrita y autógrafa respecto de todo acto jurídico –o su expresión oral- la cumple igualmente la instrumentación electrónica a través de un mensaje de datos, con independencia del contenido, extensión, alcance y finalidad del acto así instrumentado."*[69], en palabras mas sencillas se equipara: la validez del documento electrónico y la Firma Electrónica con el documento que tiene como soporte el papel y la firma manuscrita. La equivalencia funcional implica también el principio de no discriminación, a lo que Mariliana Rico Carrillo dice: *"La equivalencia funcional implica aplicar a los mensajes de datos un principio de no discriminación respecto de las declaraciones de voluntad, independientemente de la forma en que hayan sido expresadas, en este sentido, los efectos jurídicos deseados por el emisor de la declaración*

[68] Juan Carlos Riofrío Martínez-Villalba, *op. cit.*, No. 038.

[69] Rafael Illescas Ortiz, Tema de debate: *El Comercio Electrónico: fundamentos de Derecho y el principio de equivalencia funcional*, www.uc3m.es/uc3m/inst/FL/boletin/español/pdfdebate/td562.pdf

deben producirse con independencia del soporte en papel o electrónico donde conste la declaración."[70]

Tanto la Ley Modelo de la CNUDMI en su artículo 5[71], como la Guía para la incorporación al derecho interno de la Ley Modelo de la misma Ley[72], enuncian el principio de equivalencia funcional. En nuestra Ley de Comercio Electrónico, en el artículo 2, con el título de Reconocimiento jurídico de los mensajes de datos, también se contempla al principio analizado, así: *"Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento."*[73]. En definitiva y como lo hemos analizado, nuestra normativa sobre comercio electrónico y Firma Electrónica concibe al principio de equivalencia funcional, otorgando igual valor jurídico al contenido de un mensaje de datos y Firma Electrónica, como al contenido de un documento tradicional y firma manuscrita.

6. Requisitos de la Firma Electrónica

[70] Mariliana Rico Carrillo, *Artículo: Validez y regulación legal del documento y contratación electrónica,* en: Revista de Derecho Informático NO. 019, de febrero del 2000, edita Alfa – Redi, http://www.alfa-redi.org/rdi-articulo.shtml?=422-30k

[71] Artículo 5. Reconocimiento jurídico de los mensajes de datos. 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.

[72] La Ley Modelo sigue un nuevo criterio, denominado a veces ´criterio del equivalente funcional`, basado en un análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito consignado sobre papel con miras a determinar la manera de satisfacer sus objetivos y funciones con técnicas del llamado comercio electrónico.

[73] Ley de Comercio Electrónico, *op. cit*.

El artículo 15, de la Ley de Comercio Electrónico determina cinco requisitos para que la Firma Electrónica sea válida, con fines analíticos los dividiré en dos partes, así:

En la *primera parte* tenemos el literal a) del artículo citado que expresa: *"Ser individual y estar vinculada exclusivamente a su titular",* la Firma Electrónica es individual, a causa de estar necesariamente vinculada al titular - efecto de la firma -.

En la *segunda parte* se encuentran los literales b), c), d) y e) del artículo 15 de la Ley, en los que se expresa:

> *"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 pertenece."*[74]

Compartimos el criterio de Efraín Torres Cháves en el sentido de que los citados literales se resumen en un único requisito, puesto que se refieren a: *"la comprobación y verificación de la legalidad de la Firma Electrónica, por medio del certificado conferido por la entidad correspondiente, quien a través de una clave digital absoluta propiedad del titular, y por tanto, secreta, quien*

[74] Ley de Comercio Electrónico, *op. cit*.

es el único responsable de su utilización."[75]*,* los requisitos planteados tienen un sentido lógico pero se sigue manteniendo una falta de reglamentación, tal es así, que en el literal b) se remite a la Ley y reglamentos; instrumentos que una vez analizados, no mencionan nada al respecto de los requisitos de la Firma Electrónica, observándose un vacío legal.

Lo requerido en los literales citados, tiene relación con la integridad, autenticidad, confidencialidad y no repudio, cualidades que brindan las Firmas Electrónicas (firma digital – Firma Electrónica avanzada), mismas que se traducen en las Firmas Electrónicas y entidades de certificación de información contenidas en la normativa internacional y en la normativa nacional.

Finalmente, al expresarse también dentro del inciso primero, del artículo 15, de la Ley, que por acuerdo de las partes pueden establecerse otros requisitos, podría presentar problemas por ser una norma abierta que plantea muchos interrogantes e incertidumbres de competencia del legislador y que debió dejarse debidamente expresado en el desarrollo de la Ley. Ante tal situación podemos interpretar que son el titular de la firma y el representante de la entidad de certificación de información los que podrán establecer voluntariamente otros requisitos, siempre y cuando no estén en contra de la Ley y no afecten a terceros o usuarios y, tendrían que estar relacionados directamente con la finalidad de la firma.

[75] Efraín Torres Cháves, *Breves*, *op. cit*., p. 29.

7. Funciones y efectos de la Firma Electrónica

Las funciones de la Firma Electrónica son las mismas funciones que se les acredita a las firmas sobre el papel, que son identificar a la persona que firma, garantizar la participación personal de esa persona en el acto de firmar, y finalmente, asociar a la persona que firma con el contenido del documento que firma. En nuestra normativa sobre Firma Electrónica no se habla específicamente del tema, pero se podría decir que analizado el contexto de la normativa, la Firma Electrónica en el Ecuador se legislo con las funciones mencionadas.

En cuanto a *los efectos* de la Firma Electrónica, la Ley de Comercio Electrónico en el artículo 14, reconoce los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos además, que será admitida como prueba en juicio. Sin embargo, existe una contradicción con el artículo 52, de la misma Ley, puesto que este solo expresa que la Firma Electrónica puede ser considerado como medio de prueba, esta observación es comentada por Efraín Torres Cháves en el siguiente sentido: *"En este caso, dada la complejidad del asunto y reciente intromisión en el campo electrónico, el artículo 14, es disposición especial, pues se refiere exclusivamente a la Firma Electrónica, por tanto será admitida como prueba y valorada como tal, siempre que cumpla con los requisitos que posteriormente se analizarán."*[76]*;* compartimos de lo citado, ya que es suficiente con que el artículo 14, determine a la Firma Electrónica como medio de prueba, lo otro es complementario, pero para mantener una

[76] *Ibíd.,* p. 28.

coherencia dentro del texto de la Ley, el legislador debe expresar el mismo sentido en los dos artículos, esto es que la Firma Electrónica sea admitida como prueba en juicio.

En definitiva los efectos de la Firma Electrónica en la Ley ecuatoriana de Comercio Electrónico son los mismos efectos jurídicos que tiene una firma manuscrita, en relación con los datos consignados en documentos físicos y, será admitida como prueba en juicio, esto se mantiene en coherencia con la normativa internacional.

8. Obligaciones del titular de la Firma Electrónica

La Ley de Comercio Electrónico del Ecuador y el Reglamento a esta Ley, contienen normas que hacen referencia a estas obligaciones, el artículo 17, de la Ley, determina que el titular de la Firma Electrónica tiene las siguientes obligaciones:

> *"a) Cumplir con las obligaciones derivadas del uso de la Firma Electrónica;*
>
> *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;*
>
> *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;*
>
> *d) Verificar la exactitud de sus declaraciones;*

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;

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

g) Las demás señaladas en la Ley y sus Reglamentos."[77]

Lo importante de las obligaciones enumeradas, es que estas se encuentran enmarcadas dentro de los esquemas que plantea la normativa internacional sobre Firma Electrónica, y se resumen básicamente en dos puntos:

El Primero, consiste en la responsabilidad del titular sobre el uso autorizado de la firma, y del que no ha sido autorizado, siempre y cuando actúe de buena fe. Lo expresado tiene relación con el hecho de que el certificado de firma vincula a ésta con el titular, que a su ves tiene concordancia con el literal *h)* del artículo 22, de la Ley de Comercio Electrónico, donde se determinan los requisitos del certificado de Firma Electrónica, tales como señalar las limitaciones para el uso del certificado de la firma, ya que si hubo uso indebido del objeto de la firma, éste será responsabilidad de la entidad de certificación que será sancionada de acuerdo a la Ley.

[77] Ley de Comercio Electrónico, *op. cit*.

El Segundo, tiene relación con la seguridad de la firma, así, es obligación del titular de la firma, de existir algún inconveniente con ésta comunicar a la entidad de certificación de información y a los usuarios de la misma, debiendo también suspender inmediatamente cualquier tipo de transacción. La Ley de Comercio Electrónico remite a su Reglamento, en este caso hay concordancia con el inciso primero, del artículo 19, de este último, pero no facilita su comprensión para la aplicación, ya que no se determina nada al respecto de las obligaciones del titular de la Firma Electrónica, a no ser de las obligaciones citadas anteriormente en el artículo 17, de la Ley; más bien se determina que se deberán considerar también como obligaciones, las previstas en las Leyes por el empleo de la firma manuscrita.

El inciso segundo del artículo 19, del Reglamento a la Ley[78], contempla que la Superintendencia de Telecomunicaciones, desarrollará los mecanismos, políticas y procedimientos para auditar técnicamente la actividad de las entidades bajo su control. Se complementa lo dicho con el análisis que se realiza en el título 3.2 del capítulo tercero, es por esto que considerar el contenido del artículo 19, no guarda concordancia con el tema de las obligaciones del titular de la Firma Electrónica, ya que en el segundo inciso de este artículo trata de las auditorias técnicas a las entidades de certificación, interpretando esta situación como un desfase dentro de la normativa nacional que deberá ser corregido o reformado.

[78] El órgano que ejerce las funciones de control prevista en la Ley 67, desarrollará los mecanismos, políticas y procedimientos para auditar técnicamente la actividad de las entidades bajo su control.

Capítulo II

Certificados de Firma Electrónica y entidades de certificación de información

En el desarrollo de este tema, es fundamental tener presente a la criptografía, especialmente la asimétrica, que utiliza las claves públicas y las claves privadas para la firma digital; que en ciertas normativas como en la Comunidad Europea se traduce o se equipara a lo que es la firma electrónica avanzada.

La criptografía asimétrica o de clave pública como se la denomina, y las firmas digitales proveen seguridad al comercio electrónico, pero para que esto funcione es necesario la utilización de los denominados certificados de Firma Electrónica, que asocian la clave pública a una persona determinada, y que deben ser emitidos por las entidades de certificación de información. Constituyéndose en un componente de gran utilidad para que esas tecnologías sean aplicables.

En el desarrollo de éste capítulo se tratarán estos temas, revisando la normativa del Ecuador, su reglamentación, así también refiriéndonos a la normativa internacional.

1 Certificado de Firma Electrónica

1.1 Concepto y Clases de Certificados

Como parte del sistema de la Firma Electrónica tenemos al certificado de ésta, definiéndole Angel García como: "*la certificación electrónica que vincula unos datos de verificación de firma a un signatario y confirma su identidad."*[79], Xavier Rivas en complemento a lo citado expresa que el certificado es: *"Documento digital que identifica a la autoridad certificadora que lo ha emitido, identifica al firmante del mensaje o transacción, contiene la clave pública del firmante, y contiene a su vez la firma digital de la autoridad certificadora que lo ha emitido."*[80]

Los certificados son emitidos por una entidad de certificación, que como parte de su labor identifica a las partes, así lo conciben también Aranzazu Calvo-Sotelo y Manuel Lobo cuando expresan: *"El empleo de la Firma Electrónica basada en un sistema de clave pública o asimétrica tiene su punto débil en la identificación de las partes. Este punto débil ha sido solventado mediante la expedición, por terceros de confianza (prestadores de servicios de certificación), de certificados que garantizan la distribución segura de claves públicas o datos de verificación de firma y que vinculan, de forma indisoluble, el par de claves (pública y privada) a una persona determinada."*[81]. El artículo 20, de la Ley de Comercio Electrónico ecuatoriana define al certificado de Firma Electrónica como: *"el mensaje de*

[79] Angel García Vidal, *La Regulación Jurídica de la Firma Electrónica*, en José Antonio Segade, *Comercio Electrónico en Internet*, *Madrid*, Ediciones Sociales y Jurídicas S.A., 2001, p. 360.
[80] Xavier Rivas, www.onnet.es/06041002.htm
[81] Aranzazu Calvo-Sotelo y Manuel C. Lobo, *La Firma Electrónica*, en Javier Cremades, *Régimen Jurídico de Internet*, Las Rozas-Madrid, La Ley-Actualidad, 2002, p. 1397.

datos que certifica la vinculación de una Firma Electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad"[82]*.* De todo lo anterior se desprende que un certificado es un mensaje de datos que confirma la vinculación firma/persona, pero no se determina al tipo de persona, que de acuerdo a nuestras leyes pueden ser naturales o jurídicas; también, que la emisión de un certificado se lo hace a través de un proceso de comprobación, del que la normativa ecuatoriana carece y que habrá que reglamentarlo. Los artículos 20, y 21 de la Ley de Comercio Electrónico[83] son concordantes, ya que este último se refiere al uso del certificado, que se emplea para acreditar la identidad del titular de una Firma Electrónica.

Además el artículo 20, de la Ley, guarda concordancia con la definición de la disposición general novena de la Ley que expresa: *"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."*[84]*,* esto último una vez más confirma la existencia en la normativa nacional de la concepción de neutralidad tecnológica, que se ha señalado en la definición de la Firma Electrónica,

[82] Ley de Comercio Electrónico, *op. cit.*
[83] Art 21.- Uso del certificado de firma electrónica**.-** El certificado de firma electrónica se empleará para certificar la identidad del titular de una firma electrónica y para otros usos, de acuerdo a esta Ley y su reglamento.
[84] Ley de Comercio Electrónico, *op. cit*.

dejando a futuro la posibilidad de que puedan existir otros tipos de Firmas Electrónicas.

Analizada la normativa ecuatoriana referente a la definición de certificado de Firma Electrónica, se concluye que su tratamiento se encuentra acorde a la normativa internacional, vincula una clave pública con una persona determinada, pero hace falta reglamentar el procedimiento de comprobación que confirma la identidad del titular del certificado, así la normativa internacional ha establecido un procedimiento para la generación y emisión de los certificados. En el título siguiente se propone un modelo de procedimiento de comprobación.

1.2 Generación y emisión del certificado

Criticábamos que todo trámite de expedición de certificados necesita de un procedimiento del que carece la legislación del Ecuador sobre Firma Electrónica, es por esto que a continuación me permito ilustrar un mecanismo que ayudaría a la aplicación para la expedición de certificados en la legislación, aclarando antes, que en la normativa internacional cada entidad de certificación tiene sus propias políticas al respecto. El procedimiento tendría las siguientes fases:

a) Solicitud y registro del solicitante.- Este trámite necesariamente debe iniciar con una solicitud de emisión de certificado, punto de partida y del que depende todo lo subsiguiente, Mauricio Devoto en referencia a este paso

comenta: *"La solicitud de un certificado de clave pública para firmar digitalmente constituye el punto de partida en la relación usuario-certificador de clave pública. Recordemos que el certificado de clave pública es el documento digital firmado digitalmente por un certificador de clave pública, que asocia una clave pública con su suscriptor durante el período de vigencia del certificado."*[85]. La solicitud o aplicación contiene inmerso el consentimiento del suscriptor, hecho que debe darse con la firma manuscrita del mismo. El registro se confirmaría y, registraría al solicitante cuando entregue cierta información adicional, misma que registra y que incluso puede ser incluida en el certificado dependiendo de la finalidad de este.

b) Comprobación de la solicitud.- Esta es una fase muy importante, ya que de esta depende el buen funcionamiento del sistema de certificados, como también, las responsabilidades que se generan para la autoridad de certificación, en otras palabras, la solicitud y el registro son datos mínimos que deben ser confirmados, Apol Lonia Martínez los concibe como: "*Elementos mínimos que se derivan de la propia función y finalidad del certificado, y que han sido recogidos como tales en las diversas regulaciones que se han realizado sobre la materia."*[86]

Insistimos en el hecho de que estos requisitos deben ser comprobados obligatoriamente, como lo es la autenticación del sujeto, que es confirmar la identidad del solicitante y que corresponda a la clave pública contenida en el certificado; esta identidad se comprueba con el uso de técnicas de

[85] Mauricio Devoto, *op. cit*., p. 210.
[86] Apol L. Marínez, *op. cit.*, p.179.

confirmación que pueden cambiar en función de una política determinada de certificados o de una clase de certificados, como son: la presencia del solicitante, documentos acreditativos, confirmación de datos personales por una tercera parte; esta verificación es de tal importancia que ha sido exigida en las diferentes regulaciones sobre la materia, también sería la razón de que sea considerado en la normativa ecuatoriana; otro elemento sujeto a verificación obligatoria tiene relación con la posesión legítima de una clave privada apta y válida con la correspondiente clave pública, que en síntesis comprueba que el solicitante tenga la clave privada correspondiente a la clave pública del sujeto del certificado.

c) Firma y emisión del certificado. Confirmado que la información entregada por el solicitante es real, la entidad certificadora firma digitalmente el certificado utilizando la clave privada de la que es titular; tras un razonamiento lógico cuando se emita un certificado por una autoridad de certificación, ésta genera el certificado y la firma digital del mismo, garantizándose de esta manera la autenticidad del documento y la integridad de su contenido -certificado de Firma Electrónica-, además, el certificado debe contener otros requisitos que se requerirán de acuerdo a la normativa del país.

d) El envío de una copia del certificado y aceptación del mismo por parte del solicitante. Esto corresponde a una fase que se presenta como consecuencia de los anteriores literales, donde la entidad de certificación envía una copia del certificado al suscriptor, que lo debe revisar y si esta de

acuerdo a sus intereses, aceptarlo. Esta es una fase que depende del certificador.

e) Publicación y archivo del certificado. La publicación puede ser catalogada como un servicio que presta la entidad de certificación en un directorio de certificados, también, la publicación implicaría indirectamente que el suscriptor ha aceptado el certificado y su contenido; una copia del certificado debe ser archivada, por ejemplo a futuro en caso de pérdida. En definitiva, la publicación es importante porque de esta manera los usuarios pueden verificar la Firma Electrónica, además de otra información relacionada como suspensiones o revocatorias.

Para concluir, debemos insistir en el hecho de que cada entidad de certificación fija sus políticas referentes a la generación y emisión de los certificados, pero es importante que en la normativa del Ecuador se contemple un procedimiento para tal efecto, ya que de esta manera se está garantizando las actuaciones del titular del certificado de Firma Electrónica y de la entidad de certificación que debe estar supervisado por la Superintendencia de Telecomunicaciones en calidad de ente de control.

1.3 Requisitos del Certificado de Firma Electrónica

En concordancia con lo manifestado en el literal b) del título anterior, la Ley de Comercio Electrónico del Ecuador en el artículo 22, determina cuáles son

los requisitos mínimos obligatorios del certificado de Firma Electrónica para ser considerado válido, y son:

a) Identificación de la entidad de certificación de información; que vendría a ser el nombre o razón social de la entidad, incluso correo electrónico y de ser el caso página web.

b) Domicilio legal de la entidad de certificación de información; esto estaría contemplado dentro del literal anterior.

c) Los datos del titular del certificado que permitan su ubicación e identificación; en otras normativas como la española se dice signatario; datos que pueden ser nombres y apellidos, si se actúa en representación, deberá acreditar poder; cabe señalar que estos datos sólo se utilizarán para los fines pertinentes al certificado, cave señalar que siendo también un requisito importante, no debe ser muy detallado, como ha sido recomendado por la UNCITRAL, y así también lo comenta Apol Lonia Martínez:

> *"En este punto, la UNCITRAL recomienda que las especificaciones exigidas sean las menos posibles, y que, en todo caso, hay que evitar requisitos como la fecha de nacimiento de las personas físicas, que pueden interferir en la esfera de la protección de datos personales. Por ello, bastará recabar los datos mínimos imprescindibles para identificar de cualquier manera al titular del certificado (persona física o jurídica) y a la entidad certificadora (firma digital de esta)."*[87]

[87] *Ibíd.,* p. 197.

d) El método de verificación de la firma del titular del certificado; lo anterior guarda concordancia con la normativa que se aplique.

e) Las fechas de emisión y expiración del certificado; en este literal sólo se habla de fechas, no de horas, a nuestro criterio debería insertarse la hora, puesto que en el sistema de los computadores y de las redes de información siempre esta presente esta información, además en el comercio electrónico el horario de trabajo no existe. Cuando en la legislación española se habla de certificados reconocidos, el artículo 12, en el literal a) del Real Decreto-Ley sobre Firma Electrónica[88], obliga a los prestadores de servicios de certificación que expidan este tipo de certificados el indicar la fecha y la hora en las que se expidió o se dejó sin efecto un certificado.

f) El número único de serie que identifica el certificado; número que puede ser el referente dentro del listado de certificados revocados y que no se repite dentro de una misma entidad de certificación.

g) La Firma Electrónica de la entidad de certificación de información; así, en el caso de la normativa española en lo que respecta a certificados reconocidos se exige la Firma Electrónica avanzada, que es la firma digital.

h) Las limitaciones o restricciones para los usos del certificado. Los objetivos para los cuales se emitió el certificado imponen ciertas limitaciones de responsabilidades a la entidad de certificación y el valor de las transacciones

[88] *Real Decreto-Ley 14/1999*, de 17 de septiembre, sobre Firma Electrónica.

para las que el certificado es apto; esto último guarda concordancia con lo expresado en el artículo 31, de la Ley de Comercio Electrónico, que en la parte pertinente obliga a que tenga un límite de uso el certificado[89], y el importe de las transacciones que deben constar como cláusulas en los contratos con los usuarios. Los límites hacen referencia a que el certificado debe contener claramente las limitaciones del uso de la Firma Electrónica, ya que esto implicaría responsabilidades para las partes por el uso dado y no autorizado, debido a que debe constar por acuerdo de las partes en una cláusula determinada por Ley.

i) Los demás señalados en esta Ley y los Reglamentos; revisada la documentación, nada dice al respecto la normativa del país respecto de este punto, por lo que se necesita emisión de nuevos reglamentos que normen estos vacíos legales, es así como Ángel García Vidal comentando el real Decreto Ley dice:

> *"Los prestadores de servicios de certificación que emitan certificados reconocidos han de cumplir unas obligaciones específicas enumeradas en el art. 12 del RDLFE. De ellas cabe destacar la obligación de indicar la fecha y la hora en las que se expidió o se dejo sin efecto un certificado; la de tomar medidas contra la falsificación de certificados o la de disponer de recursos económicos suficientes para afrontar el riesgo de responsabilidad por daños y perjuicios."*[90]

[89] Serán también responsables por el uso indebido del certificado de firma electrónica acreditado, cuando éstas no hayan consignado en dichos certificados, de forma clara, el límite de su uso y el importe de las transacciones válidas que pueda realizar.
[90] Ángel García, *op. cit.,* p. 363.

Del análisis hecho en relación con la normativa española se desprende que nuestro certificado ante tal normativa no sería un certificado reconocido, no cumpliría todos los requisitos para serlo, nuestra Ley de Comercio Electrónico define y establece los requisitos como certificado de Firma Electrónica, pero no como certificado reconocido como lo contempla la otra normativa, situación que debe ser aclarada en el sentido de definir cuáles son los certificados reconocidos y cuáles pueden ser considerados simplemente como certificados.

2. Período de validez del certificado

2.1 Duración del certificado de Firma Electrónica

Todos los certificados de Firma Electrónica tienen un período de validez, la razón de esto es porque en un sistema bien tratado de emisión de certificados el juego de claves (públicas y privadas) también debería tener una vida limitada. Apol Lonia Martínez a lo anterior comenta: *"La duración del período de validez del certificado es una cuestión política de la autoridad de certificación y que implica y afecta a los diversos sujetos intervinientes."*[91]; en este aspecto la legislación española distingue dos situaciones en el período de validez de los certificados, así: el de períodos operacionales o tiempos de validez para los certificados de suscriptores como destinatarios finales y para los certificados de las entidades de certificación; para los primeros, los períodos van de uno a tres años, mientras que para los

[91] Apol L. Marínez, *op. cit.*, p. 213.

segundos los períodos son más largos debido a que los cambios de clave son más críticos.

En la Ley de Comercio Electrónico del Ecuador, la duración del certificado de Firma Electrónica se encuentra contenido en el artículo 23[92], éste artículo contempla dos situaciones: *la primera,* nos da a entender un acuerdo contractual para el período de validez entre el titular de la Firma Electrónica y la entidad de certificación, es decir, en este caso quedaría al libre albedrío de las partes, lo cual no sería tan seguro para el sistema y de paso para los usuarios, ya que no sería un régimen uniforme; *la segunda* situación, se presenta de una forma determinante, y es que cuando no se llega a un acuerdo, el plazo de validez de los certificados de Firma Electrónica será el establecido por el Reglamento a esta Ley; esto es un plazo de dos años como máximo.

Si recurrimos al Reglamento a la Ley, específicamente al artículo 11, éste hace alusión a que de no existir acuerdo entre las partes el certificado de Firma Electrónica se emitirá con una validez de dos años a partir de su expedición, pero hace una excepción al tratarse de certificados emitidos con relación al ejercicio de cargos públicos o privados, es en estos casos en donde la duración podría ser superior a dos años, sin que exceda el tiempo de duración del cargo o por prórroga de acuerdo a la Ley. Aquí valdría hacer una observación, y es que de ser el caso y extenderse por esta situación el plazo de duración, una nueva especie de Firma Electrónica, producto del

[92] Art.- La duración del certificado de firma electrónica.- Salvo acuerdo contractual, el plazo de validez de los certificados de firma electrónica será el establecido en el reglamento a esta ley.

avance tecnológico y de la neutralidad tecnológica se encontraría en la imposibilidad de actualizarse o quedarse sin efecto, es por esto, que se hace necesario reglamentar la duración en una norma de un solo sentido que determine un solo plazo fijo para los certificados, salvando el hecho de una nueva tecnología.

2.2 Extinción del certificado de Firma Electrónica

El artículo 24, de la Ley de Comercio Electrónico se refiere a la extinción de la Firma Electrónica, por asuntos de análisis se le dividirá en dos partes: *en la primera,* estarían contenidas las causas por las cuales se extingue el certificado de Firma Electrónica; y, *en la segunda*, que corresponde al segundo inciso del artículo, que norma el hecho o momento de la extinción:

Las causas para la extinción del certificado son:

a) Solicitud de su titular; compartimos el criterio de Efraín Torres Cháves que al respecto argumenta: *"requisito que debe constar en un Reglamento, pues es norma de aplicación (la solicitud)"*[93]

b) Extinción de la Firma Electrónica de conformidad con lo establecido en el artículo 19, de esta Ley; esto es, voluntad de su titular, fallecimiento o incapacidad de su titular, disolución o liquidación de la persona jurídica y por causa judicialmente declarada.

[93] Efraín Torres Cháves , *op. cit.*, p. 36.

c) Expiración del plazo de validez del certificado de Firma Electrónica; es una causal demasiado entendible, así también lo argumenta Apol Lonia Martínez cuando dice: *"En cualquier caso, finalizado el período de vida del certificado, cabe entender que cesan también las obligaciones y responsabilidades de la autoridad y del suscriptor."*[94], el vínculo entre la clave pública y el sujeto del certificado no sería ya válido, y por tanto, no debe confiarse en el certificado.

El segundo inciso del artículo 24, de la Ley[95], regula el momento en que se extingue el certificado, haciéndose efectivo este hecho desde la comunicación a la entidad de certificación de información, excepto en el caso de fallecimiento del titular de la Firma Electrónica en cuyo caso se extingue a partir de que acaece el fallecimiento; habría que determinar que tipo de comunicación, que podría ser un mensaje de datos o de acuerdo a derecho conforme al proceso de emisión. Expresa también el inciso que estamos analizando que cuando se trata de personas secuestradas o desaparecidas, se extingue a partir de que se denuncia ante las autoridades competentes tal secuestro o desaparición, y finalmente se contempla que la extinción del certificado de Firma Electrónica no exime a su titular de las obligaciones contraídas previamente a la extinción y que se hayan derivado de su uso.

2.3 Suspensión del certificado de Firma Electrónica

[94] Apol L. Martínez, *op. cit.*, p.216.

[95] La extinción del certificado de firma electrónica se producirá desde el momento de su comunicación a la entidad de certificación de información, excepto en el caso de fallecimiento del titular de la firma electrónica, en cuyo caso se extingue a partir de que acaece el fallecimiento. Tratándose de personas secuestradas o desaparecidas, se extingue a partir de que se denuncie ante las autoridades competentes tal secuestro o desaparición. La extinción del certificado de firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

Al emitirse el certificado el suscriptor estima que lo va a utilizar por el tiempo de validez para el cual se emitió, pero se pueden presentar circunstancias que dejen sin validez a dichos instrumentos antes de cumplir el período operacional para el cual se lo emitió, es así como al respecto Mauricio Devoto comenta: *"Si la clave privada ha quedado ´en entredicho`, por ejemplo si el tenedor de la clave ha perdido el control de ésta, el certificado puede dejar de ser fiable y la entidad certificadora (a petición del tenedor o aún sin el consentimiento de éste, según las circunstancias), puede suspender (interrumpir temporalmente el período operacional) o revocar (invalidar de forma permanente) el certificado."*[96]

La suspensión de un certificado se traduce en hacer al certificado no operativo; inoperatividad que es temporal y reversible, por lo que ninguno de los usuarios puede fundamentarse en el contenido de tal, suspensión que incluye e involucra también a la clave pública y privada del suscriptor, de esta manera lo concibe también Apol Lonia Martínez que sostiene: *"Pues, si la principal función del certificado es unir el suscriptor a la clave pública, e indirectamente a la clave privada, utilizada para las firmas digitales, el certificado revocado o suspendido deja de cumplir esa función: no garantiza ya que es el titular de la clave privada"*[97]

La Ley de Comercio Electrónico del Ecuador no define la suspensión del certificado de Firma Electrónica, indicando únicamente en el artículo 25, las

[96] Mauricio Devoto, *op. cit.*, p. 147.
[97] Apol L. Martínez, *op. cit.*, p. 218.

causas por las que la entidad de certificación de información podrá suspender temporalmente el certificado, estas causas son:

> *"a) Que sea dispuesto por el CONATEL, de conformidad con lo previsto en esta Ley;*
>
> *b) Se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado; y,*
>
> *c) Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la Firma Electrónica.*[98]"

El mencionado literal a), tiene concordancia con el literal b) del artículo 37, de la misma Ley[99] en el que se determina que el CONATEL en su calidad de organismo de autorización, registro y regulación de las entidades de certificación podrá suspender los certificados cuando los hayan emitido, sin haber cumplido las formalidades legales, previo informe motivado de la Superintendencia de Telecomunicaciones.

Otro punto importante de analizar es el hecho que en el inciso segundo del mismo artículo 25 de la Ley[100], se previene la situación de que una vez ocurrida la suspensión de un certificado de Firma Electrónica, es necesaria la inmediata *notificación* por parte de la entidad de certificación al titular del certificado y al organismo de control, que de conformidad con el artículo 14,

[98] Ley de Comercio Electrónico, *op. cit*.
[99] b) Revocar o suspender los certificados de firma electrónica, cuando la entidad de certificación acreditada los emita con inobservancia de las formalidades legales, previo informe motivado de la Superintendencia de Telecomunicaciones.
[100] La suspensión temporal dispuesta por la entidad de certificación de información deberá ser inmediatamente notificada al titular del certificado y al organismo de control, dicha notificación deberá señalar las causas de la suspensión.

del Reglamento a la Ley, se realizará a la dirección electrónica y a la dirección física que hubiere señalado en el contrato, debiéndose también señalar las causas de la suspensión. Una vez justificada la causa la entidad de certificación inmediatamente debe levantar la suspensión, así también, en el caso de que exista resolución del CONATEL.

En concordancia con lo anteriormente expresado, del inciso primero del artículo 27 de la Ley[101], se desprende que la suspensión hace que el certificado deje de cumplir su función, así con relación a su titular surte efectos desde el momento de su comunicación o notificación y, respecto de terceros desde el momento de su publicación, de éste último tema Apol Lonia Martínez comenta: *"Por ello la autoridad de certificación debe inmediatamente dar publicidad al hecho de la revocación o suspensión para que pueda ser conocida por la comunidad de usuarios, y/o, en su caso, notificarlo a las personas que lo soliciten o es sabido que han recibido una firma digital verificable por referencia a un certificado no fiable"*[102]

La publicación de conformidad con el artículo 15, del Reglamento a al Ley, deberá efectuarse en la forma que se establece en éste instrumento, y por cualquiera de los siguientes medios: a) obligatoriamente en las páginas WEB determinadas por el "CONATEL" y de la entidad certificadora; b) Mediante un aviso al acceder al certificado de Firma Electrónica desde el hipervínculo de

[101] Art. 27.- Tanto la suspensión temporal, como la revocatoria, surtirán efectos desde el momento de su comunicación con relación a su titular; y, respecto de terceros, desde el momento de su publicación que deberá efectuarse en la forma que se establezca en el respectivo reglamento, y no eximen al titular del certificado de firma electrónica, de las obligaciones previamente contraídas derivadas de su uso.

[102] Apol L. Marínez, *op. cit.,* p. 220.

verificación; y, c) Opcionalmente, de creerse conveniente en uno de los medios de comunicación. Importante de aclarar en este párrafo es que antes constaba el CONELEC, institución no idónea para cumplir con la función del literal a), es por esto, que mediante el Decreto Ejecutivo No. 908, de 19 de diciembre del 2005 se introducen reformas al Reglamento General a la Ley de Comercio Electrónico, así el literal a) del artículo 15 es reformado por el literal b), del artículo 1, del Decreto en el siguiente sentido: *"donde se lee "CONELEC", dirá "CONATEL"*[103]*,* lo anterior es lo correcto, ya que el Consejo Nacional de Telecomunicaciones en calidad de organismo de autorización, registro y regulación es el debe realizar dicha función.

Finalmente debemos señalar que en la Ley de Comercio Electrónico la suspensión y revocación del certificado de Firma Electrónica, en cuanto a la notificación y publicación, guardan concordancia con el artículo 27, de la Ley antes mencionado, y todos los anteriores, con los artículos 14 y 15, del Reglamento a la Ley (reformado); en cuanto al tiempo de la notificación de suspensión al titular, según el Reglamento debe ser inmediata, no es claro lo referente a la publicación, la cual por toda la inseguridad del tema debe ser también inmediata. Este tema de la suspensión, de la forma como esta tratado en la normativa ecuatoriana, observamos que guarda relación con la normativa internacional sobre el tema.

2.4 Revocatoria del certificado de Firma Electrónica

[103] *Reformas al Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos,* Decreto Ejecutivo No. 908, Registro Oficial No. 168, de 19 de diciembre del 2005.

Al igual que el tema de la suspensión, la Ley del Comercio Electrónico del Ecuador no define lo que es una revocatoria del certificado de Firma Electrónica, de acuerdo al Diccionario de Derecho Usual de Guillermo Cabanellas revocar es: *"Dejar sin efecto una declaración de voluntad o un acto jurídico en el que unilateralmente se tenga tal potestad; como testamento, mandato, donación (por ciertas causas) y otros."*[104], sin embargo, ya hemos indicado que el principal rol del certificado es unir el suscriptor a la clave pública e indirectamente a la clave privada utilizadas para las firmas digitales. La revocación en cambio destruye la capacidad de firma digital del suscriptor basada en el par de claves al que va referido ese certificado revocado de clave pública.

Arturo Ribagorda respecto de la revocación sostiene: *"Aunque la revocación de certificados sea la manera usual de abortar el período de validez de uno de ellos, bajo ciertas circunstancias …"*[105], lo importante de destacar de la cita anterior, es que nos da a entender que la revocatoria viene siendo una invalidez anticipada del certificado. En el artículo 26, de la Ley de Comercio Electrónico únicamente se previenen las causas por las que un certificado de Firma Electrónica puede ser revocado; revocatoria que en calidad de organismo de autorización, registro y regulación la realiza el CONATEL; esta facultad, guarda concordancia con el literal b) del artículo 37[106], de la misma

[104] Guillermo Cabanellas, *Diccionario de Derecho Usual*, Buenos Aires, Editorial Heliasta S.R.L., 1997, 25a ed., p. 228.
[105] Arturo Ribagorda Garnacho, *Sistema de Certificación: la Firma y el Certificado Digital*, en Cremades Javier, *Régimen Jurídico de Internet*, Las Rozas-Madrid, La Ley-Actualidad, 2002, p. 1331.
[106] b) Revocar o suspender los certificados de firma electrónica, cuando la entidad de certificación acreditada los emita con inobservancia de las formalidades legales, previo informe motivado de la Superintendencia de Telecomunicaciones.

Ley que fue analizada cuando se trato el tema de la suspensión del certificado. Las causas de revocación son:

> *"a) Cuando la entidad de certificación de información cese en sus actividades y los certificados vigentes no sean asumidos por otra entidad de certificación; y,*
> *b) Cuando se produzca la quiebra técnica de la entidad de certificación judicialmente declarada."*[107]

En referencia a las citadas causas de revocación, en el caso de la *cesación de una persona jurídica y cesión de los certificados*, los incisos segundo y tercero del artículo 13 del Reglamento a la Ley[108], determinan que ésta debe ser notificada a los usuarios, organismos de regulación y control con noventa días de anticipación, y para poder realizar la cesión de los certificados, se debe contar con la autorización expresa del titular del certificado.

La *quiebra técnica* se encuentra descrita en la disposición general novena de la Ley de Comercio Electrónico, que expresa: *"Es la imposibilidad temporal o permanente de la entidad de certificación de información, que impide garantizar el cumplimiento de las obligaciones establecidas en esta Ley y su Reglamento.".*[109]*.* No se trata de la quiebra establecida en la normativa societaria, se la debe tomar en el sentido de una desactualización

[107] Ley de Comercio Electrónico, *op. cit.*
[108] En caso de que las actividades de certificación vayan a cesar, la entidad de certificación deberá notificar con por lo menos noventa días de anticipación a los usuarios de los certificados de firma electrónica y a los organismos de regulación de control sobre la terminación de sus actividades.
La cesión de certificados de firma electrónica de una entidad de certificación a otra, contará con la autorización expresa del titular del certificado.
[109] Ley de Comercio Electrónico, *op. cit.*

tecnológica de la entidad de certificación, lo que implica también una carencia de seguridad para los usuarios, este tema lo resume Efraín Torres Cháves así: *"La Ley prevé la seguridad de sus ciudadanos, al tener conocimiento de un caos operacional, que puede resultar en perjuicios a los afiliados o clientes, por tanto, este procedimiento debe ser declarado por orden del juez del domicilio de la entidad expresando cuáles fueron las circunstancias que motivaron declarar tal quiebra, y si fue a petición de parte o de oficio."*[110]

Las causas contenidas en el artículo 26, de la Ley nacional son muy concretas comparadas con la mayor parte de normativas sobre el tema, que a diferencia de la española, ésta determina más causas, como las siguientes: pérdida, robo, modificación de la clave privada del sujeto del certificado, solicitud discrecional por parte del suscriptor, incumplimiento de una obligación de la declaración de práctica de certificación, etc; sin embargo, en concordancia con esto último, la disposición general sexta de la Ley determina que el CONATEL tomará las medidas necesarias con la finalidad de que no se afecten los derechos del titular del certificado o de terceros cuando se produzca la revocatoria del certificado por causa no atribuible al titular del mismo.

Consideramos importante el comentar el hecho que previo a la revocatoria de un certificado se generan hechos subsecuentes, Apol Lonia Martínez también lo concibe: *"La invalidez anticipada de un certificado por revocación*

[110] Efraín Torres Cháves, *op. cit.,* p. 38.

del mismo implica el desarrollo temporal de una serie de hechos y acciones, desde la puesta en peligro, es su caso de la clave privada (causa fundamental de revocación), hasta el conocimiento por parte de terceros del hecho de la revocación."[111]*.* La normativa ecuatoriana no regula estos acontecimientos, sin embargo, podríamos resumirlos de la siguiente manera: *en primer lugar* se presenta el hecho que exige la revocación del certificado; *lo segundo* es el conocimiento del peligro y petición de revocación realizada por persona autorizada, para lo cual la mayor parte de legislaciones consideran como legítimos solicitantes al suscriptor, la autoridad de certificación o terceros con la debida autorización; *como tercer paso* se presenta la confirmación de la validez de la solicitud de revocación de un suscriptor, aquí se decide si un certificado a de revocarse o no; y, *lo cuarto* es la publicación y/o comunicación de la revocación; aspecto importante, ya que de esta manera los usuarios del certificado quedan prevenidos de tal situación.

Finalmente, en concordancia con el artículo 26, de la Ley, el inciso primero del artículo 13, del Reglamento a la Ley[112], en lo principal determina que una vez producida la revocación se debe desactivar el enlace que informa sobre el certificado. La notificación por parte de la entidad de certificación al titular del certificado, así como también a la publicación de la revocación, al igual que la suspensión guarda concordancia con el artículo 27 de la Ley y se lo

[111] Apol L. Martínez, *op. cit.,* p. 220.
[112] Revocación del certificado de firma electrónica.- Establecidas las circunstancias determinadas en la Ley 67, se producirá la revocación, que tendrá también como consecuencia la respectiva publicación y la desactivación del enlace que informa sobre el certificado.

hará de acuerdo a lo expresado en los artículos 14 y 15 (reformado), del Reglamento.

2.5 Lista de revocación y suspensión de los certificados de Firma Electrónica

Estas listas son los mecanismos más idóneos para hacer conocer a terceros los certificados que se encuentran revocados y suspendidos, compartimos la manera de concebir a estas listas por parte de Apol Lonia Martínez, así:

> *"El método más común para dar publicidad, de forma general, a la revocación consiste en la publicación por parte de la autoridad de certificación de una lista de certificados revocados (Certificate Revocation List -CRL- y, descriptiva y significativamente, lista negra), definida en el Standard X.509, como una lista sellada temporalmente de certificados revocados que ha sido firmada digitalmente por una autoridad de certificación y hecha accesible a los usuarios de los certificados."*[113]

Método publicitario que se lo llama también método PULL de distribución, en complemento a lo expresado, Arturo Ribagorda manifiesta: *"Esta es una estructura de datos firmada normalmente por la AC conteniendo, en esencia, los números de los certificados revocados, la fecha y la hora de la revocación, y la fecha y hora de publicación de la lista."*[114].

[113] Apol L. *op. cit.*, pp. 232-233.
[114] Arturo Ribagorda Garnacho, *op. cit*., pp. 129 y 130.

En nuestra normativa el artículo 12, del Reglamento a la Ley de Comercio Electrónico, determina: *"Las entidades de certificación de información proporcionarán mecanismos automáticos de acceso a listas de certificados revocados o suspendidos de acuerdo al artículo 26 de la Ley 67. Cuando la verificación de la validez de los certificados de Firma Electrónica no pueda ser posible realizar en tiempo real, la entidad de certificación de información comunicará de este hecho tanto al emisor como al receptor del mensaje de datos. Los períodos de actualización de las listas de los certificados suspendidos, revocados o no vigentes por cualquier causa se establecerán contractualmente."*[115]. Como se puede discernir, nuestra normativa no fija un tiempo para actualizar las listas (días, horas, semanas, etc.), más bien da la potestad a las partes, para que sean éstas las que determinen, se trata de una norma abierta que en el caso que las partes no prevean el tiempo de acuerdo a la finalidad del certificado, se podrían presentar serios problemas como los que describe Apol Lonia Martínez:

> *"El problema está en determinar la adecuada periodicidad: si las listas son muy próximas, el tercero usuario tiene la carga de consultar listas continuamente, mientras que si son muy lejanas, se puede acumular un número muy elevado de certificados revocados pero no publicados todavía, respecto de los que, mientras tanto, existe el riesgo de que sean utilizados (con el problema de la atribución de responsabilidad durante ese período)"*[116]

[115] Reglamento a la Ley de Comercio Electrónico, *op. cit.*
[116] Apol L. Marínez, *op. cit.*, pp. 233 y 234.

Existen otros mecanismos además del anteriormente descrito, como las listas de revocación por difusión (el método PUSH), donde la autoridad de certificación esta obligada a distribuir las listas de revocación para los sistemas de usuarios a medida que se van incluyendo en la lista las nuevas revocaciones; también tenemos a la revocación inmediata (real-time revocation u on- line status checking), en este sistema de revocación se obliga al tercero usuario del certificado a obtener información de la entidad certificadora. Como lo afirma Apol Lonia Martínez, la forma de comunicar la revocación dependerá de diferentes factores, así: *"La naturaleza y el tipo de servicios de comunicación de la revocación dependerá de las necesidades del cliente en función del tipo de certificado, del riesgo que la autoridad esté dispuesta a asumir, y, en última instancia, de lo específicamente pactado al respecto."*[117]

En definitiva en el Ecuador en referencia a estas listas de certificados revocados y suspendidos la normativa se inclina por el método general, que exige datos básicos, pero que no plantea un tiempo definido para la publicación de estas listas, pero será el legislador el encargado en base a un estudio técnico sobre estos sistemas quien realice las reformas del caso.

3. Entidad de certificación

3.1 Concepto

[117] *Ibíd.,* p. 239.

Se ha señalado que la firma digital con la criptografía asimétrica soluciona la necesidad jurídica de autenticación, integridad y no rechazo de origen del mensaje electrónico, pero se necesita de la intervención de una tercera parte de confianza, que en otras normativas se la conoce como autoridad de certificación o prestadora de servicios de certificación. El principal objetivo de estas entidades es asegurar el vínculo entre la clave pública y el titular de la clave privada, al respecto Aranzazu Calvo-Sotelo y Manuel Lobo comentan: *"En una transacción on line resulta imprescindible garantizar que tanto el emisor o remitente como el receptor o destinatario son quienes dicen ser, es decir, se trata de garantizar la autenticación de las partes."*[118]

Que la finalidad de la entidad de certificación sea asegurar el vínculo entre la clave pública y el titular de la clave privada generando fiabilidad y confiabilidad en el sistema de generación de certificados, no debe confundirse con el objeto social de la entidad de certificación de información que sería la emisión del certificado de Firma Electrónica y la prestación de servicios relativos a esta.

En el caso ecuatoriano, la Ley de Comercio Electrónico en el artículo 29, hace referencia a las entidades de certificación de información, así: *"Son 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*

[118] Aranzazu Calvo-Sotelo y Manuel C. Lobo, *op. cit*., p. 1392.

Presidente de la República."[119], sin embargo de lo citado nos acogemos al criterio de Fabrizio Peralta Díaz que argumenta*: "Nuestra Ley de Comercio Electrónico no define a las entidades de certificación de información, pues, siguiendo conceptos recogidos por otras legislaciones y autores, simplemente se limita a señalar quienes pueden ejercer estas actividades y cuáles son sus funciones."*[120]

En este tema la Ley de Comercio Electrónico presenta una contradicción al hablar de entidades de certificación de información y entidades de certificación de información acreditadas, para entenderlo mejor, es necesario hacer un recuento del proceso de aprobación de esta Ley. Es así como en el Acta No. 160, de 7 de Febrero del 2002, que contiene el proyecto de ley para segundo debate, las entidades de certificación constaban de la siguiente manera:

> *"Artículo 29 Entidades de Certificación de Información.- Son las personas jurídicas que emiten un certificado de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica.*
>
> *Artículo 30 Entidades de Certificación Acreditadas.- Son las personas jurídicas acreditadas ante el Consejo Nacional de Telecomunicaciones para emitir certificados electrónicos y otros servicios relacionados con la*

[119] Ley de Comercio Electrónico *op. cit.*
[120] Fabrizio Peralta Díaz, *Comercio Electrónico, Firmas Electrónicas y Entidades de Certificación*, en Javier Castro, Libro Homenaje al Dr. Hector Romero Parducci, Guayaquil, Edino, 2000. p. 142.

firma electrónica, para lo cual deben cumplir con los requisitos determinados en esta ley y sus reglamentos."[121]

Sin embargo en el Acta No. 164, de 19 de Febrero del 2002, que contiene la continuación del segundo debate del Proyecto de Ley de Comercio Electrónico, consta que se aprueba el artículo 29, en la parte pertinente con el siguiente texto: "*Entidades de Certificación de Información.- Son las personas jurídicas constituidas como compañías, bajo alguna de las especies contempladas en la Ley de Compañías y esta ley, que emiten certificados de firma electrónicas."*[122]*.* Posteriormente se produce un veto en el que el Presidente de la República argumenta: *"En el artículo 29, no se encuentra fundamento para excluir a las cámaras de comercio, fundaciones, corporaciones, o empresas unipersonales. Por esa parte el artículo 30 bien puede ser integrado con el 29 por lo que se propone el siguiente artículo que unifica el 29 y 30."*[123]

La redacción propuesta en el veto es la que consta en el artículo 29 de la Ley, y al que se allanaron los legisladores. Ahora bien, en el Congreso Nacional el debate se enfocó en el tipo de persona jurídica y que consideramos pudo haber quedado redactado como consta del Acta No. 164; el ejecutivo y el legislativo debió aprobar a las entidades de certificación como costa del Acta No. 160, como entidades de certificación de información

[121] Acta No. 160 de 7 de febrero del 2002, Segundo Debate del Proyecto de *Ley de Comercio Electrónico, Firmase Electrónicas y Mensajes de Datos*, PL No. 21-315.

[122] Acta No. 164, de 19 de febrero del 2002, Segundo Debate del Proyecto de *Ley de comercio electrónico, firmas electrónicas y mensajes de datos*, PL No. 21-315.

[123] *Veto Presidencial*: oficio No. T 1862-DAJ-2002-5312, de 14 de marzo del 2002.

y entidades de certificación de información acreditadas. De la forma como ahora se define en la Ley a estas entidades se desprende una contradicción, puesto que en el transcurso de ésta se hablan de los dos tipos de entidades, que como se podrá entender complican por ejemplo el articulado que hace relación a las funciones del Consejo Nacional de Telecomunicaciones; también consideramos que en ningún momento se emite una definición funcional o descriptiva de entidad de certificación de información.

3.2 Naturaleza de las entidades de certificación

En referencia al tema, existen diversos criterios que se conciben en las normativas vigentes, a lo cual es menester citar lo que manifiesta Mauricio Devoto:

> *"Las entidades certificadoras podrán ser entidades públicas o privadas, en algunos países, por razones de orden público, se prevé que solo las entidades públicas estén autorizadas para actuar como entidades certificadoras. En otros países, se considera que los servicios de certificación deben quedar abiertos a la competencia del sector privado. Independientemente de que las entidades certificadoras sean públicas o privadas y de que deban obtener una autorización, normalmente existe mas de una entidad certificadora en el PKI"*[124]

[124] Mauricio Devoto, *op. cit.*, p. 174.

Lo citado permite observar de forma clara que estas entidades pueden ser públicas o privadas, físicas o jurídicas[125]. Las entidades públicas pueden desempeñar diversos papeles, ya sea como autoridad de certificación, certificando a las otras entidades de certificación comerciales, o ya sea para actuar en las relaciones administración - administrados. Las privadas pueden desempeñar este servicio para terceros como parte de su objeto principal o para su organización interna.

Las entidades de certificación pueden crearse libremente o con licencia pública, lo que le proporciona un valor agregado siempre y cuando cumpla con ciertos requisitos. Lo que se denomina licencia en otras legislaciones, en la ecuatoriana se define como título habilitante, el cual se encuentra contenido en el artículo 11, del Reglamento para la Acreditación, que expresa:

> *"La acreditación para la prestación de servicios de certificación de información y servicios relacionados por parte de entidades de certificación de información o entidades de registro de información se obtendrá a través de un título habilitante que será el permiso y registro de operación, otorgado por la Secretaría Nacional de Telecomunicaciones, SENATEL, previa autorización del Consejo Nacional de Telecomunicaciones, CONATEL."*[126]

[125] Por personas físicas, entenderíamos que son las personas naturales, que tampoco son las empresas unipersonales que contempla la Ley de Comercio Electrónico ecuatoriana, que en nuestro derecho societario no existen; las jurídicas se encuentran plenamente determinadas en la ley.

[126] *Reglamento para la Acreditación, Registro y Regulación de las Entidades Habilitadas para prestar Servicios de Certificación Información y Servicios Relacionados*, Resolución No. 584-23-CONATEL, publicada en el Registro Oficial No. 196, de 23 de octubre de 2003.

En la legislación nacional el artículo 29, de la Ley de Comercio Electrónico habla que las entidades de certificación de información podrán ser empresas unipersonales o personas jurídicas, y en el Reglamento a esta Ley no se norma nada al respecto, como complemento al comentario anterior, Fabrizio Peralta dice: *"Además, el citado cuerpo legal normativo no fue del todo claro para explicar si estas entidades son de naturaleza pública o privada, ya que tan solo menciona que sus servicios pueden ser ofrecidos por empresas unipersonales o personas jurídicas. De por sí el concepto personas jurídicas, sin mas calificativos, deja la puerta abierta para admitir varias posibilidades."*[127]. En lo referente a las empresas unipersonales, es importante de señalar que al inicio de esta investigación no se encontraban normadas en nuestro ordenamiento jurídico, pero en el Registro Oficial No. 196, de 26 de enero del 2006, se publica la Ley de Empresas Unipersonales de Responsabilidad Limitada, que en su artículo 1 determina: *"Toda persona natural con capacidad legal para realizar actos de comercio, podrá desarrollar por intermedio de una empresa unipersonal de responsabilidad limitada cualquier actividad económica que no estuviere prohibida por la Ley, limitando su responsabilidad civil por las operaciones de la misma al monto del capital que hubiere destinado para ello."*[128]; sobre el mismo punto y por el poco tiempo de vigencia de la Ley, consideramos que es muy pronto para realizar comentarios mas detallados, sin embargo, podemos atrevernos a decir, que estas empresas de acuerdo al artículo 29 de la Ley de Comercio

[127] Fabrizio Peralta Díaz, *op. cit.*, pp. 142 y 143.
[128] *Ley de Empresas Unipersonales de Responsabilidad Limitada,* Registro Oficial No. 196, de 26 de enero del 2006.

Electrónico[129] tendrían como objeto principalmente emitir certificados de Firma Electrónica, los cuales certifican la vinculación de una Firma Electrónica con una persona determinada.

En cuanto a las personas jurídicas el Código Civil, en el inciso primero del artículo 583, determina: *"Se llama persona jurídica a una persona ficticia, capaz, de ejercer derechos y contraer obligaciones civiles, y de ser representada judicial y extrajudicialmente."*[130], a lo manifestado, en el literal a) del artículo 30, de la Ley de Comercio Electrónico se obliga a que las entidades de certificación estén legalmente constituidas, lo que implicaría aprobación de la Superintendencia de Compañías en el caso de las compañías, y adicionalmente estar registradas en el CONATEL.

De todo lo dicho, se asume que la normativa en el Ecuador acepta como entidades de certificación a las personas jurídicas públicas y privadas, y ahora también pueden ser las empresas unipersonales, esto gracias a la nueva Ley de Empresas Unipersonales de Responsabilidad Limitada.

Además, se debe dejar señalado que el artículo 9, del Reglamento para la Acreditación, en la parte pertinente expresa: *"De acuerdo a lo que establece la Ley de Comercio Electrónico y su Reglamento, se dispone la implementación de un sistema de acreditación voluntario para las entidades*

[129] Art. 29.- Entidades de certificación de información**.-** Son 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.

[130] *Código Civil*, Ley No. 47, Registro Oficial No. 223, de 26 julio de 1997.

de certificación de información en la emisión de firmas electrónicas y certificados de firma electrónica …"[131]*,* el citado artículo tiene relación con el artículo 12, del Reglamento citado donde se refiere al título habilitante. Lo anterior plantea que la acreditación de las entidades de certificación en la legislación ecuatoriana puede ser voluntaria, las cuales al hacerlo serán calificadas como acreditadas, y contarán con su respectivo título habilitante, esto de acuerdo al artículo 53, de la Ley produce la presunción de que la Firma Electrónica reúne los requisitos de ley, pertenece al signatario y por ende que los datos de esta no han sido alterados desde su emisión.

3.3 Requisitos para ser entidad de certificación

Los requisitos se traducen en ciertas características mínimas de orden técnico, personal y financiero que deben cumplir las entidades de certificación, características que dan confianza y seguridad en la organización de las actividades de tales entes, en otras palabras son los requisitos mínimos que debe reunir la infraestructura requerida para proveer los servicios de certificación de información; este tema guarda estrecha relación con el título siguiente que analiza las obligaciones y responsabilidades de las mencionadas entidades, sin embargo, seguidamente describiremos a estos requisitos.

Requisitos técnicos, que se traducen en la utilización por parte de estas entidades de sistemas y productos fiables que no puedan ser vulnerados,

[131] Reglamento para la Acreditación, *op. cit.*

que estén protegidos contra toda alteración, con los cuales se pueda proceder inmediatamente a la suspensión y revocatoria de los certificados, sistemas que involucran también el dar aviso de forma efectiva que una firma tiene riesgo de uso indebido; *requisitos de personal*, estos deben ser idóneos y técnicos en la materia, esto significa que la entidad debe utilizar personal cualificado y con experiencia; *requisitos financieros*, que involucran dos situaciones, tanto para el desempeño de las funciones así como para garantizar su trabajo en caso de presentarse problemas en los cuales la responsabilidad corra a cargo de ellas, incluso deberían ofertarse seguros, requisito de gran importancia, ya que ayudaría a que las entidades de certificación sean cotizadas por los suscriptores y por los usuarios, utilizándose para el resarcimiento de daños y perjuicios ocasionados.

En la normativa ecuatoriana estos requisitos se encuentran determinados básicamente en los literales a), b), d) y e) del artículo 21 del Reglamento para la Acreditación[132], así el literal a) hace relación al requisito de personal, los literales b) y e) a lo técnico y del literal c) se deduce lo financiero. Lo anterior demuestra que nuestra normativa en el tema de los requisitos se encuentra acorde con la internacional, otorgando confianza y seguridad a las

[132] a) Identificación y generales de ley del solicitante, socios y representantes con los certificados y documentos que demuestren tal condición y el cumplimiento de los requisitos exigidos en las leyes y reglamentos para desempeñarse como tales, incluidos pero no limitados a: nombramientos, contratos de prestación de servicios, certificados de antecedentes penales, certificados profesionales, y certificados legales en general de acuerdo al tipo de servicio a prestar. El CONATEL podrá requerir la presentación de documentos adicionales cuando considere que es necesario para garantizar la idoneidad de la solicitud;
b) Diagrama esquemático y descripción técnica detallada del sistema cuando sea del caso;
d) Documentos de soporte que confirmen el cumplimiento de los requisitos establecidos en la Ley de Comercio Electrónico y su reglamento de acuerdo a la autorización solicitada;
e) Documentos de soporte que confirmen que se disponen de medidas para evitar la falsificación de certificados, y, en el caso que el Proveedor de Servicios de Certificación intervenga en la generación de claves criptográficas privadas, se garantice la seguridad y confidencialidad durante el proceso de generación de dichas claves.

actuaciones de las entidades de certificación, como también a los usuarios de los certificados.

3.4 Obligaciones y responsabilidades de las entidades de certificación

El artículo 30, de la Ley de Comercio Electrónico enumera *las obligaciones* de las entidades de certificación de información, este es un tema de gran importancia a nivel internacional, al respecto Miguel Dávara sostiene lo siguiente: *"Entre las obligaciones que tienen los prestadores de servicios de certificación, destacaremos desde las de controlar en todo caso y en todo momento la fiabilidad del certificado, antes de otorgarle, identificando perfectamente a quien se le va a otorgar y, una vez otorgado, manteniendo un registro de certificados y poniendo a disposición del signatario los dispositivos de creación y de verificación de Firma Electrónica"*[133]

En el artículo señalado de la Ley se habla de entidades de certificación "acreditadas", lo que implica el cumplimiento de requisitos más exigentes, y que se deben cumplir antes de ser autorizadas y luego de ello, estos requisitos u obligaciones son:

a) Encontrarse legalmente constituidas, y estar registradas en el Consejo Nacional de Telecomunicaciones; al expresarse que deben estar constituidas legalmente se guardaría concordancia con la Ley de Compañías, dando de esta manera un añadido legal a estas entidades.

[133] Miguel A. Dávara, *op. cit.*, p. 425.

b) Demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios; esto significa que la entidad debe utilizar personal cualificado, con experiencia, utilizando sistemas y productos fiables que no puedan ser vulnerados, que estén protegidos contra toda alteración. En relación al tema de solvencia financiera, esta debe garantizar suficientes recursos para afrontar un posible riesgo de responsabilidad por daños y perjuicios, también para garantizar el desarrollo del negocio y evitar una quiebra tecnológica.

c) Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de información; esto se traduce en rapidez y seguridad en sus actividades previniendo falsificaciones de certificados. La confidencialidad tiene relación con los datos de creación de firma durante el proceso de creación que no deben ser almacenados ni copiados.

d) Mantener sistemas de respaldo de la información relativa a los certificados; lo que implica tener un registro, archivar toda la información y documentación que tenga conexión directa con los certificados; la información que consta de archivos debe estar en éstos por un tiempo determinado, nuestra normativa no contempla esta situación.

e) Proceder de forma inmediata a la suspensión o revocatoria de certificados electrónicos previo mandato de la Superintendencia de Telecomunicaciones, en los casos que se especifiquen en esta Ley; este punto tiene concordancia

con los artículos 25, 26 y 37, literal b) de la Ley de Comercio Electrónico ya estudiados.

f) Mantener una publicación del estado de los certificados electrónicos emitidos; consideramos que esta publicación debe mantenerse el mismo criterio para la publicación de la suspensión y revocación, que fue también ya analizado.

g) Proporcionar a los titulares de certificados de Firmas Electrónicas un medio efectivo y rápido para dar aviso de que una firma tiene riesgo de uso indebido.

h) Contar con una garantía de responsabilidad para cubrir daños y prejuicios, que se ocasionen por el incumplimiento de las obligaciones previstas en la presente Ley, y hasta por culpa leve en el desempeño de sus obligaciones. Cuando certifiquen límites sobre responsabilidades o valores económicos, esta garantía será al menos del 5% del monto total de las operaciones que garanticen sus certificados (tiene relación con los requisitos financieros).

Analizando lo anterior, Efraín Torres Cháves resume al daño de la siguiente manera: *"Daño es el detrimento, perjuicio o menoscabo que por acción de otro ser recibe en la persona o en los bienes, y este puede provenir de dolo, de culpa o de caso fortuito, según el grado de malicia, negligencia o casualidad entre el autor y el efecto."*[134]*;* en referencia a los perjuicios, el

[134] Efraín Torres Cháves, *op. cit.*, p. 47.

Código Civil en el artículo 1599, determina: *"La indemnización de perjuicios comprende el daño emergente y el lucro cesante, ya provenga de no haberse cumplido la obligación o de haberse cumplido imperfectamente, o de haberse retardado el cumplimiento …"*[135]

i) Las demás establecidas en esta Ley y los reglamentos; sobre lo anterior podemos comentar que en otras normativas se contemplan situaciones como el hecho de comunicar la finalización de las actividades, el solicitar la inscripción en el Registro de Prestadores de Servicios de Certificación, informar los criterios que se comprometen a seguir, entre otros.

En cuanto a *las responsabilidades*, estas se encuentran determinadas en el artículo 31, de la Ley de Comercio Electrónico y son básicamente dos: *la primera* se presenta, cuando por negligencia o por incumplir con las obligaciones determinadas en la Ley, donde las entidades de certificación son responsables hasta de culpa leve y responderán por los daños y perjuicios, incluso pueden ser sancionados de acuerdo a la Ley de Defensa del Consumidor; *la segunda* responsabilidad, se desprende del hecho de no consignarse en los certificados el límite de su uso y el importe de las transacciones válidas que pueda realizar. De presentarse los casos mencionados, la carga de la prueba le corresponderá a la entidad de certificación, lo cual compartimos con Efraín Torres Cháves cuyo criterio al respecto es: *"Esta norma de excepción procesal, es adecuada, ya que la entidad supone dentro del ámbito obligatorio la solvencia técnica, logística y*

[135] Código Civil, *op. cit.*

financiera y garantía de sus obligaciones."[136]*.* En el Reglamento a la Ley no se expresa nada al respecto de las responsabilidades, pero en el Reglamento para la Acreditación, el artículo 5, determina que será responsabilidad de estas entidades el emitir certificados únicos e induplicables, debiendo contener un identificador exclusivo que lo distinga de los demás.

De todo lo tratado anteriormente se considera que las entidades de certificación de información tienen que estar registradas en el CONATEL, lo cual vendría a traducirse en un esquema regulador mínimo que otorga confianza en las actuaciones de las entidades, debiendo también mencionarse como conclusión de este tema, que nuestra normativa se encuentra dentro de los esquemas de la normativa internacional.

3.5 Reconocimiento internacional de certificados de Firma Electrónica

En la Ley de Comercio Electrónico ecuatoriana, el reconocimiento internacional de certificados se encuentra básicamente contemplado en el artículo 28, mismo que tiene concordancias con artículos contenidos en el Reglamento a la Ley y el Reglamento para la Acreditación; seguidamente analizaremos los incisos mas importantes del mencionado artículo.

Previamente, en el tema motivo de análisis, debemos tener presente lo que el Código Civil, en el artículo 1505, expresa: *"Hay objeto ilícito en todo lo que*

[136] Efraín Torres Cháves, *op. cit.,* p. 48.

contraviene al Derecho Público…"[137]*,* sin embargo, en el inciso primero del artículo 28, se determina: *"Los certificados electrónicos emitidos por entidades de certificación extranjeras, que cumplieren con los requisitos señalados en esta Ley y presenten un grado de fiabilidad equivalente, tendrán el mismo valor legal que los certificados acreditados, expedidos en el Ecuador. El Consejo Nacional de Telecomunicaciones dictará el Reglamento correspondiente para la aplicación de este artículo."*[138]*,* lo anterior guarda concordancia con: el artículo 16, del Reglamento a la Ley[139] y el artículo 32, del Reglamento para la Acreditación[140]. Los últimos artículos, coinciden en expresar que estos certificados tendrán validez legal en el Ecuador una vez obtenida la revalidación, que deberá ser emitida por el CONELEC, quien deberá comprobar la fiabilidad de los certificados y la solvencia técnica de quien los emite, en caso de no ser convalidados tendrán el carácter de no acreditados.

Específicamente, en lo concerniente a que en el Reglamento a la Ley se citaba al CONELEC (Consejo Nacional de Electrificación) debemos hacer una aclaración, puesto que entre la Ley y el Reglamento se presentaba una inconsistencia; la primera como efectivamente sucede, determina que es el

---

[137] Código Civil, *op. cit.*
[138] Ley de Comercio Electrónico, *op. cit.*,
[139] Art. 16.- Reconocimiento Internacional de certificados de firma electrónica.- Los certificados de firma electrónica emitidos en el extranjero tendrán validez legal en Ecuador una vez obtenida la revalidación respectiva emitida por el CONATEL, él deberá comprobar el grado de fiabilidad de los certificados y la solvencia técnica de quien los emite.
[140] Art. 32.- La revalidación en el país de los certificados de firma electrónica emitidos en el extranjero les otorga la misma validez que a los certificados emitidos por entidades de certificación de información acreditadas en Ecuador.
Los certificados de firma electrónica emitidos en el extranjero y no revalidados en Ecuador, tienen el carácter de no acreditados.
Para revalidar un certificado de firma electrónica emitido en el extranjero, se deberá cumplir con los requisitos de acreditación y las exigencias de la ley y reglamentos ecuatorianos.

CONATEL quien autoriza, registra y regula a las entidades de certificación, mientras que en el segundo se expresaba que la revalidación se la hará ante el CONELEC. Consideramos que esto se debió a que previo a publicarse el Decreto Ejecutivo No. 3496 que contiene el Reglamento a la Ley, éste fue enviado por el CONATEL a la Presidencia de la República, en donde se cometió el error de hacer constar al CONELEC; así también, lo corrobora Carlos Vera Quintana al comentar: *"Se recibió un documento bastante completo y bueno por parte del CONATEL. La "asesoría Jurídica" de la presidencia, con total desconocimiento de causa, modifica el documento ocasionando errores de bulto, algunos de cuales incluyen cambiar el término "órgano regulador" por CONELEC."*[141], Esta situación ha quedado aclarada mediante las reformas al Reglamento a la Ley de Comercio Electrónico, así el literal c), del artículo 1 del Decreto Ejecutivo No. 908, de 19 de diciembre del 2005, mismo que expresa*: "En el artículo 16, donde se lee "CONELEC", dirá "CONATEL"*[142]; las reformas contenidas en el Decreto aludido y que se refieren principalmente al error de citar al CONELEC en el Reglamento a la Ley han sido de importancia para la aplicación de la Ley de Comercio Electrónico puesto que causaban graves confusiones.

En el inciso tercero del artículo 28 se expresa: *"Cuando las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas y certificados, se reconocerá que ese acuerdo es suficiente en derecho."*[143], en este punto la Ley respeta el acuerdo de las partes para establecer requisitos

[141] Carlos Vera Quintana, *Artículo Especializado: El Arte de Legislar*, http://www.corpece.org.ec, en: El Informante. No. 129.
[142] Reformas al Reglamento General a la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos, *op. cit.*
[143] Ley de Comercio Electrónico, *op. cit.*

que pueden estar o no acorde a los que requiere el Ecuador por lo que surte los mismos efectos legales.

El cuarto inciso, hace referencia a que todo convenio que celebre el Ecuador en lo que tiene que ver con el comercio electrónico y todo lo que esto implica, debe guardar armonía con las otras normas internacionales, en este caso se podría considerar a la Ley Modelo de la UNCITRAL.

3.6 Régimen de acreditación

En un inicio debemos comentar, que tanto la normativa de la Unión Europea (Directiva 1999/93/CE), como la normativa española (Real Decreto Ley 14/1999), en cuanto al régimen de acreditación advierten el hecho de que no se debe condicionar la prestación de servicios de certificación a una autorización previa, pero como consecuencia de esto, se establece un régimen voluntario de acreditación de los prestadores de servicios de certificación de Firma Electrónica que permite un apropiado nivel de seguridad y la protección de los derechos de los usuarios.

No sin antes hacer presente nuevamente el comentario realizado respecto de la mención que se hace del CONELEC en el Reglamento a la Ley, mismo que quedo expresado en el título anterior, debemos indicar que efectivamente, en referencia al régimen de acreditación, podríamos decir que la normativa ecuatoriana se encuentra en la misma línea de las citadas,

ya que del análisis del artículo 17, del Reglamento a la Ley[144], reformado por el literal d) del Decreto Ejecutivo No. 908, de 19 de diciembre del 2005 en el siguiente sentido: "En los tres incisos del artículo 17, donde se lee "CONELEC", dirá "CONATEL"[145], se infiere lo siguiente:

Primero, para que una entidad de certificación sea autorizada a operar directamente o a través de terceros en el Ecuador debe obligadamente registrarse en el CONATEL, registro que en el Real Decreto/Ley español, se establece en el Ministerio de Justicia, lo cual ha sido criticado aduciendo que rompe con la unidad de control administrativo que el sistema ha establecido en torno a la Secretaría de Estado de Telecomunicaciones. En concordancia con lo expresado, del artículo 6 del Reglamento para la Acreditación[146], se infiere que las entidades extranjeras de certificación de información podrán solicitar su registro, pero bajo la condición de que se encuentren acreditadas en el extranjero, lo cual no le otorga la calidad de entidad de certificación acreditada.

---

[144] Art. 17.- Régimen de acreditación de entidades de certificación de información.- Para obtener autorización de operar directamente o a través de terceros relacionados en Ecuador, las entidades de certificación de información deberán registrarse en el CONATEL.
Los certificados de firma electrónica emitidos por las entidades de certificación de información que, además de registrarse, se acrediten voluntariamente en el CONATEL, tienen carácter probatorio.
Las entidades que habiéndose registrado y obtenido autorización para operar, directamente o a través de terceros relacionados en Ecuador, no se acrediten en el CONATEL, tendrán la calidad de entidades de certificación de información no acreditadas y están obligadas a informar de esta condición a quienes soliciten o hagan uso de sus servicios, debiendo también, a solicitud de autoridad competente, probar la suficiencia técnica y fiabilidad de los certificados que emiten.

[145] Reformas al Reglamento General a la Ley de Comercio Electrónico. Firmas Electrónicas y Mensajes de Datos, *op. cit.*

[146] Art. 6.-Las entidades extranjeras de certificación de información, para emisión de firmas electrónicas y certificados de firma electrónica, no domiciliadas en Ecuador, podrán solicitar su registro en el país, previo a demostrar la acreditación o reconocimiento legal de los servicios prestados en el extranjero, a través de su apoderado en el Ecuador.
El registro no otorga la calidad de entidad de certificación acreditada en el país, por lo que se deberá hacer constar en el contrato con los usuarios e informar al público en la promoción o publicidad de tal calidad.

Segundo, las entidades de certificación de información, que además de registrarse, se acrediten voluntariamente en el CONATEL, tienen como consecuencia que los certificados que emitan, gozarán de carácter probatorio; pero la acreditación de estas entidades, de acuerdo al artículo 11, del Reglamento para la Acreditación se obtendrá a través de un título habilitante que será el permiso y registro de operación otorgado por la Secretaría Nacional de Telecomunicaciones -SENATEL-, previa autorización del CONATEL.

Tercero, que las entidades registradas pero no acreditadas, como se comprenderá tienen como consecuencia el actuar en calidad de no acreditadas, además, el deber de informar esta situación a quienes soliciten o hagan uso de sus servicios, debiendo probar la suficiencia técnica y la fiabilidad de los certificados que emiten; hemos dejado expresado sobre la seguridad que deben brindar las entidades de certificación, a lo cual debemos considerar la obligación de acreditarse, al respecto es interesante el comentario que Leopoldo González-Echenique hace sobre la normativa española: *"El resultado de todo ello es que, en rigor, para proveer de esta clase de servicios con una mínima fiabilidad frente al mercado es precisa la acreditación previa del prestador de servicios de certificación, de modo que, (de facto) o de manera indirecta, se ha impuesto un sistema de autorización reglada del ejercicio de la actividad."*[147].

[147] Leopoldo González y Echenique Castellanos de Ubao, *op. cit.*, p. 238.

De todo lo anterior podemos concluir, que existía una inconsistencia en el Reglamento a la Ley al contemplarse en éste al CONELEC como organismo de registro, siendo por ley el CONATEL, por lo cual se reformó el Reglamento mediante Decreto Ejecutivo No. 908, publicado en el Registro Oficial No. 168, de 19 de diciembre del 2005; además, que nuestra normativa contempla el registro y la acreditación voluntaria, pero también determina que las entidades de certificación acreditadas deberán poseer la autorización previa y registro en el CONATEL, proporcionando de esta manera un adecuado grado de seguridad de los derechos de los usuarios, tal es así que los certificados emitidos por las entidades acreditadas tienen carácter probatorio.

Capítulo III

Organismos de promoción y difusión de los servicios electrónicos, y de regulación y control de las entidades de certificación acreditadas

En el capítulo anterior se analizó lo relacionado con los certificados de Firma Electrónica emitidos por las entidades de certificación de información; entidades que por Ley deben ser reguladas y cumplir ciertas obligaciones, para lo cual se han determinado organismos encargados de velar por su cumplimiento. La Ley de Comercio Electrónico en el capítulo IV regula a los organismos de promoción y difusión de los servicios electrónicos, Consejo de Comercio Exterior e Inversiones -COMEXI-; los organismos de regulación, Consejo Nacional de Telecomunicaciones –CONATEL- y, los organismos de control; Superintendencia de Telecomunicaciones.

Las funciones de los organismos citados, con la excepción del COMEXI se traducen principalmente en un sistema de control y sanción para las entidades de certificación, insistimos en el hecho que al referirnos a la normativa internacional en el análisis de este capítulo, no se pretende hacer un estudio comparado con la normativa del Ecuador, lo que se busca es tener una referencia para hacer más comprensible el estudio de nuestra normativa.

Para que los organismos citados puedan ejercer sus funciones han tenido que emitir normativa complementaria; en la normativa española así se lo hizo, por esto, Aranzazu Calvo-Sotelo y Manuel Lobo en lo concerniente al tema

comenta el Real Decreto de la siguiente manera: *"el artículo 6, del Real Decreto-Ley 14/1999, trasponiendo la directiva, habilitó al Gobierno para establecer un sistema de acreditación de los prestadores de servicios de certificación de Firma Electrónica de carácter voluntario, con el objeto de lograr el adecuado grado de seguridad y proteger debidamente los derechos de los usuarios."*[148], de esta manera en la orden del 21 de Febrero de 2000, se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de Firma Electrónica.

En el caso de la normativa ecuatoriana, de los tres organismos determinados en la Ley, es el CONATEL, que fundamentado principalmente en el inciso primero, del artículo 37, de la Ley de Comercio Electrónico[149], mediante resolución expide el Reglamento para la Acreditación, Registro y Regulación de las Entidades Habilitadas para prestar servicios de Certificación de Información y Servicios Relacionados, en adelante Reglamento para la Acreditación, como se observará, los otros organismos no poseen una reglamentación al efecto.

1. Organismo de promoción y difusión en el Ecuador

1.1 Consejo de Comercio Exterior e Inversiones - COMEXI -

[148] Aranzazu Calvo-Sotelo y Manuel C. Lobo Coello, *op. cit.*, p. 1394.

[149] Art. 137.- Organismo de regulación, autorización y registro de las entidades de certificación acreditadas.- El Consejo Nacional de Telecomunicaciones "CONATEL", o la entidad que haga sus veces, será el organismo de autorización, registro y regulación de las entidades de certificación de información acreditadas.

Abordaremos el presente tema de manera directa con lo determinado en el artículo 36, de la Ley de Comercio Electrónico, donde se expresa: *"Para efectos de esta Ley, el Consejo de Comercio Exterior e Inversiones, "COMEXI", será el organismo de promoción y difusión de los servicios electrónicos, incluido el comercio electrónico, y el uso de las firmas electrónicas en la promoción de inversiones y comercio exterior."*[150]. La normativa internacional como la española mantiene un régimen de supervisión y sanción respecto de las entidades de certificación, pero dentro de dicho régimen no se contempla un organismo de este tipo, que cumpla las funciones de promoción y difusión de servicios electrónicos como ocurre en el caso ecuatoriano.

Lo anterior, a pesar de no afectar la actuación de los otros organismos, creemos no debería constar en la Ley de Comercio Electrónico, ya que incluso, y como se podrá observar, el COMEXI no mantiene ninguna conexión en cuanto a funciones con los otros organismos contemplados en el capítulo IV, de la Ley; tampoco, una vez investigado dispone de la reglamentación referente a la Firma Electrónica, necesaria para cumplir con su trabajo y peor aún existe oficina alguna dentro de este organismo encomendada a estas labores.

No cabe duda que en el país se necesita que se difunda este tema tan complejo de la Firma Electrónica, así el artículo citado mantiene concordancia con el segundo considerando de la misma Ley, al respecto de: *"Que es necesario impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos"*[151], probablemente el

[150] Ley de Comercio Electrónico, *op. cit.*
[151] *Ibíd*.

sentido que se quiere dar en este caso, es el de difundir los servicios electrónicos, el comercio electrónico y el uso de la Firma Electrónica con la finalidad de atraer inversiones, y sea utilizada en el desarrollo del comercio exterior. En este momento, podemos atrevernos a decir, no existen datos de que este organismo se encuentre desarrollando la finalidad mencionada, ya que una vez que se acudió a las oficinas del COMEXI, como se ha dicho, no se cuenta siquiera con personal que asuma responsabilidades.

2. Organismo de regulación, autorización y registro de las entidades de certificación acreditadas

2.1 Consejo Nacional de Telecomunicaciones - CONATEL -

La Firma Electrónica, los certificados y las entidades de certificación constituyen un mecanismo relacionado, a lo cual consideramos necesario una regulación por parte del Estado, así, en el inciso primero del artículo 37, de la Ley de Comercio Electrónico se expresa: *"El Consejo Nacional de Telecomunicaciones "CONATEL", o la entidad que haga sus veces, será el organismo de autorización, registro y regulación de las entidades de certificación de información acreditadas."*[152]*;* en base a lo expresado y para cumplir con sus funciones, el CONATEL resuelve expedir el Reglamento para la Acreditación.

[152] *Ibíd*

En concordancia con lo expresado en el último Reglamento citado, el artículo 36, Capítulo VI, sobre regulación y control determina*: "La operación de servicios de certificación de información está sujeta a las normas de regulación, control y supervisión, atribuidas al Consejo Nacional de Telecomunicaciones, la Secretaría Nacional de Telecomunicaciones y la Superintendencia de Telecomunicaciones, de conformidad con la potestad de dichos organismos establecidas en las leyes y reglamentos."*[153]*.* De lo anterior se concluye principalmente que el CONATEL, esta facultado para autorizar y aprobar a las entidades de certificación de información, previo a ser inscritas en el registro correspondiente, de esta manera también se entiende que esta institución regula a estas entidades dentro de los parámetros que le permite la Ley y los reglamentos.

Finalmente, es importante dejar también señalado, que el artículo 37 de la Ley, guarda concordancia con el artículo 17, del Reglamento, reformado por el literal d), del artículo 1 del Decreto Ejecutivo No. 908, publicado en el Registro Oficial No, 168, de 19 de diciembre de del 2005, artículo que determina que las entidades de certificación para obtener autorización de operar, deberán registrarse en el CONATEL, organismo que autoriza, registra y regula a estas entidades.

2.2 Funciones

[153] Reglamento para la Acreditación, *op. cit.*

El CONATEL dentro de sus funciones en calidad de organismo de autorización, de conformidad con el artículo 37 de la Ley de Comercio Electrónico también se encuentra facultado a lo siguiente:

a) Cancelar o suspender la autorización a las entidades de certificación acreditadas previo informe motivado de la Superintendencia de Telecomunicaciones; *cancelación* es sinónimo de revocación y además se constituye en definitivo; considero que en este punto la Ley de Comercio Electrónico no es clara, sin embargo, en el literal a) del artículo 30, de la misma Ley, se obliga a que las entidades de certificación acreditadas deben registrarse en el CONATEL. El incumplimiento de esto sería una de las causas para dicha revocatoria o suspensión.

b) Revocar o suspender los certificados de Firma Electrónica cuando la entidad de certificación acreditada los emita con inobservancia de las formalidades legales, previo informe motivado de la Superintendencia de Telecomunicaciones; a diferencia del literal anterior, aquí se hace referencia a la suspensión y revocatoria de los *certificados de Firma Electrónica*, lo anterior es concordante con lo determinado en el artículo 25, literales a), b) y c) de la Ley de Comercio Electrónico[154], así también, con el primer inciso del artículo 26

[154] Art. 25.- Suspensión del certificado de firma electrónica.- La entidad de certificación de información podrá suspender temporalmente el certificado de firma electrónica cuando:
a) Sea dispuesto por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta Ley;
b) Se compruebe por parte de la entidad de certificación de información, falsedad en los datos consignados por el titular del certificado; y,
c) Se produzca el incumplimiento del contrato celebrado entre la entidad de certificación de información y el titular de la firma electrónica

de la misma Ley[155]; sin embargo, en el artículo 25, parecería existir una contradicción entre lo determinado en el literal a) y los literales b) y c) respecto a quien suspende, si el CONATEL o la entidad de certificación, al respecto Efraín Torres Cháves comenta: *"Esta oscuridad prevista por el Legislador, ha obligado a consultar su espíritu de creación, concluyendo que el CONATEL es el órgano de última instancia para conocer de la suspensión temporal, mientras que la entidad de certificación de información, está facultada para suspender temporalmente el certificado de Firma Electrónica sólo en los casos del literal b) y c) del artículo 25 y que puede ser revisada por el CONATEL, confirmándola o negándola"*[156]

c) Las demás atribuidas en la Ley y en los Reglamentos; el literal señalado guarda concordancia con el inciso primero del artículo 11, del Reglamento para la Acreditación, que determina: *"La acreditación para la prestación de servicios de certificación de información y servicios relacionados por parte de las entidades de certificación de información o entidades de registro de información se obtendrá a través de un título habilitante que será el permiso y registro de operación otorgado por la Secretaría Nacional de Telecomunicaciones, -SENATEL-, previa autorización del CONATEL."*[157]*;* otra concordancia se presenta con el artículo 30, del Reglamento citado que expresa: *"El formato de los contratos que las entidades de certificación de información o las entidades*

[155] Art. 26.- Revocatoria del certificado de firma electrónica.- El certificado de firma electrónica podrá ser revocado por el Consejo Nacional de Telecomunicaciones, de conformidad con lo previsto en esta Ley.
[156] Efraín Torres Cháves, *op. cit.,* p. 53.
[157] Reglamento para la Acreditación, *op. cit.*

de registro de información suscriban con los consumidores o usuarios deberán ser aprobados por el CONATEL y no podrán modificarse sin su autorización."[158]

Del análisis de las funciones del CONATEL, podemos extraer que estas se encuentran contenidas en la Ley de Comercio Electrónico y reglamentos, normativa que ayuda a la labor del Consejo Nacional de Telecomunicaciones en calidad de organismo de regulación, control y supervisión de las entidades de certificación, así también a la Superintendencia de Telecomunicaciones, organismos motivo de estudio de este capítulo.

3. Organismo de control de las entidades de certificación de información acreditadas

3.1 Superintendencia de Telecomunicaciones

Hemos analizado el organismo encargado de la regulación de las entidades de certificación, ahora observaremos al organismo de control de tales entidades, mismo que a su vez, tiene la facultad de sancionar. Siguiendo como referencia a la normativa internacional sobre la materia, especialmente la española, en esta última, en el Título IV, del Decreto / Ley, se mantiene un régimen de supervisión y sanción respecto de las entidades de certificación, así lo comenta Leopoldo González-Echenique: *"Los instrumentos en torno a los cuales se ha construido el régimen de supervisión son dos: atribuyendo a un órgano administrativo potestades administrativas tendientes a hacer efectivo el*

[158] *Ibíd.*

régimen jurídico aplicable a los prestadores de servicios de certificación e imponiendo a estos últimos un deber genérico de colaboración con el primero."[159].

En la normativa española el órgano supervisor es el Ministerio de Ciencia y Tecnología, el cual a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de Información controla que las entidades de certificación que emiten certificados reconocidos, cumplan con las obligaciones que se les impuso y vigila a las que no emiten este tipo de certificado. En lo que se refiere a la colaboración, las entidades de certificación deben estar prestas a entregar a la Secretaría, todo tipo de información respecto de ellas.

En la normativa ecuatoriana el artículo 38, de la Ley, determina lo siguiente: *"Para efectos de esta Ley, la Superintendencia de Telecomunicaciones, será el organismo encargado del control de las entidades de certificación de información acreditadas."*[160], en esta parte de la Ley estamos hablando del organismo que tiene la potestad para ejercer el control sobre dichas entidades, y a nuestro criterio diría que también sobre las actividades de estas, por lo que la Superintendencia de Telecomunicaciones en el país es el organismo que ejerce el control de las entidades de certificación de información acreditadas.

3.2 Funciones

[159] Leopoldo González - Echenique Castellanos de Ubao, *op. cit.*, p. 250.
[160] Ley de Comercio Electrónico, *op. Cit.*

En el título anterior se dejó señalado que la Superintendencia de Telecomunicaciones es el organismo encargado de controlar a las entidades de certificación de información acreditadas, en concordancia con lo dicho, en el artículo 39, de la Ley de Comercio Electrónico se determinan las funciones que este tiene en el ejercicio de las atribuciones establecidas en dicha Ley; a continuación analizaremos cada una de estas, así:

a) Velar por la observancia de las disposiciones constitucionales, legales, sobre la promoción de la competencia y las prácticas comerciales restrictivas; competencia desleal y protección al consumidor, en los mercados atendidos por las entidades de certificación de información acreditadas; esto guarda concordancia con el artículo 244, de la Constitución[161], 248 y siguientes de la Ley de Propiedad Intelectual[162] y la Ley de Defensa del Consumidor[163]

b) Ejercer el control de las entidades de certificación de información acreditadas en el territorio nacional y velar por su eficiente funcionamiento; la actividad de control a estas entidades se encuentra determinada en el artículo 38, de la Ley de Comercio Electrónico; al expresarse territorio nacional se hace referencia a la territorialidad de la Ley, lo cual guarda concordancia con el artículo 15, del Reglamento para la Acreditación, así: "*El prestador de servicios*

[161] Art. 244.- Dentro del sistema de economía social de mercado al Estado le corresponderá: 3. Promover el desarrollo de actividades y mercados competitivos. Impulsar la libre competencia y sancionar, conforme a la ley, las prácticas monopólicas y otras que la impidan y distorsionen.

[162] Art. 284.- Se considera competencia desleal a todo hecho, acto o práctica contrario a los usos o costumbres honestos en el desarrollo de las actividades económicas.
La expresión actividades económicas, se entenderá en sentido amplio, que abarque incluso actividades de profesionales tales como abogados, médicos, ingenieros y otros campos en el ejercicio de cualquier profesión, arte u oficio.

[163] Art. 1, 2º inc. El objeto de esta Ley es normar las relaciones entre proveedores y consumidores promoviendo el conocimiento y protegiendo los derechos de los consumidores y procurando la equidad y la seguridad jurídica en las relaciones entre las partes.

deberá fijar un domicilio principal de operaciones dentro del territorio ecuatoriano y podrá establecer oficinas de verificación física de datos en los sitios autorizados. Cada sitio donde el prestador de servicios tenga presencia física deberá ser un sitio seguro; contará con control de acceso, resguardo de documentos y protección contra siniestros."

c) Realizar auditorias técnicas a las entidades de certificación de información acreditadas; este literal guarda relación con el inciso segundo del artículo 19, del Reglamento a la Ley[164], que determina que la Superintendencia de Telecomunicaciones desarrollará políticas y procedimientos para auditar técnicamente la actividad de las entidades bajo su control; con el literal c) del artículo 21, del Reglamento para la Acreditación, que trata sobre los requisitos de la solicitud de título habilitante, y que en la parte pertinente expresa que el CONATEL podrá realizar inspecciones o verificaciones a las instalaciones del solicitante cuando lo considere necesario.

d) Requerir de las entidades de certificación de información acreditadas, la información pertinente para el ejercicio de sus funciones.

e) Imponer de conformidad con la Ley sanciones administrativas a las entidades de certificación de información acreditadas, en caso de incumplimiento de las obligaciones derivadas de la prestación del servicio; lo anterior guarda concordancia con los artículos 40 y 41, de la Ley la Ley de

[164] El órgano que ejerce las funciones de control prevista en la Ley 67, desarrollará los mecanismos, políticas y procedimientos para auditar técnicamente la actividad de las entidades bajo su control.

Comercio Electrónico que corresponden a las infracciones administrativas y a las sanciones, lo que será analizado en los próximos títulos.

f) Emitir los informes motivados previstos en esta Ley; informes que son requisitos para revocar o suspender la autorización a las entidades de certificación acreditadas y para revocar o suspender los certificados de Firma Electrónica cuando la entidad de certificación acreditada los emita con inobservancia de las formalidades legales, al respecto de estos informes Efraín Torres Cháves sostiene: *"Cabe mencionar, respecto al informe motivado, como un análisis de la Superintendencia de Telecomunicaciones, que no es vinculante en grado procesal, sino únicamente a nivel administrativo. En todo caso, el nivel superior referente a la Función Judicial, estará a cargo del Tribunal de lo Contencioso Administrativo."*[165]

g) Disponer la suspensión de la prestación de servicios de certificación para impedir el cometimiento de una infracción; la Ley habla de suspensión de los certificados de Firma Electrónica, pero no de las entidades de certificación, ésta situación tiene que ser reglamentada por el legislador; y,

h) Las demás atribuidas en la Ley y en los reglamentos; el citado literal guarda concordancia con el inciso primero del artículo 10, del Reglamento para la Acreditación, en el que se determina que la Superintendencia de Telecomunicaciones verificará que el prestador de servicios de certificación se encuentre legalmente establecido y representado en el Ecuador.

[165] Efraín Torres Cháves, *op. cit.,* p. 57.

Hemos señalado, que en la normativa española los instrumentos en torno a los cuales se ha establecido el régimen de supervisión eran dos, el órgano administrativo de control y el deber de colaboración de los prestadores de servicios de certificación para con dicho organismo, a lo último expresado, Leopoldo González Echenique sostiene:

> *"Los prestadores de servicios de certificación tienen la obligación de facilitar a la Secretaría de Estado de Telecomunicaciones toda la información y los medios precisos para el ejercicio de sus funciones y la de permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate, referida siempre a datos que conciernan al prestador de servicios."*[166]

Si volvemos nuestra lectura, en los literales c) y d), del artículo motivo de este análisis se determinan como funciones de la Superintendencia de Telecomunicaciones realizar autorías técnicas a las entidades de certificación y también requerir la información pertinente de éstas para el ejercicio de sus funciones, lo que se encasillaría dentro del deber de colaboración que contempla la legislación española. En resumen, el régimen de supervisión en la normativa nacional se presenta con la Superintendencia de Telecomunicaciones como ente de control, y dentro de sus funciones con la presencia indirecta del deber de colaboración de las entidades de certificación como el de permitir las auditorias técnicas, encontrándonos de esta manera dentro del esquema de la normativa internacional sobre la materia.

[166] Leopoldo González - Echenique Castellanos de Ubao, *op. cit*., p. 251.

3.3 Infracciones administrativas

Las infracciones tienen relación con el tema de las obligaciones de las entidades de certificación de información acreditadas, lo cual ya se analizó con los artículos 30 y 31, de la Ley de Comercio Electrónico. En el Diccionario Usual de Guillermo Cabanellas, a la *Infracción* se la concibe como: *"trasgresión, quebrantamiento, violación, incumplimiento de ley, reglamento, convenio, tratado, contrato u orden. Denominación de todo lo punible; sea delito o falta. En lo civil. La infracción de lo obligatorio permite reclamar la ejecución forzosa; y, cuando no quepa lograrla, se traduce en un resarcimiento de daños y perjuicios."*[167]

Las infracciones vienen acompañadas de la sanción respectiva, En la normativa española, es importante el criterio que al respecto emite Leopoldo González- Echenique, autor español que conoce del tema tratado, así: *"Tal y como viene siendo norma en nuestro derecho público, cada vez más presente en todas nuestras facetas de actuación, la coerción y el cierre último del sistema suele venir de la mano de un completo y pormenorizado régimen de infracciones y sanciones. En el Decreto- Ley de Firma Electrónica, el último de sus Títulos - el quinto - contiene un pormenorizado detalle de las infracciones y sanciones aplicables a los prestadores de servicios de certificación. "*[168], es así como las infracciones de las normas reguladoras de la Firma Electrónica y los servicios de certificación en la legislación española se los clasifica en: muy graves, graves y leves.

[167] Guillermo Cabanellas, *op. cit.*, p. 412.
[168] Leopoldo González y Echenique Castellanos, *op. cit*., p. 251.

A diferencia de la legislación española, en el inciso primero del artículo 40, de la Ley de Comercio Electrónico ecuatoriana se establece: *"Infracciones Administrativas.- Para los efectos previstos en la presente Ley, las infracciones administrativas se clasifican en leves y graves."*[169], de esto podemos entender que existe en el tema de la clasificación de las infracciones una marcada diferencia entre las dos normativas, sin embargo como ya se ha dicho es un buen referente, ya que esta diferencia también tiene ingerencia en las sanciones que se estipulan para las infracciones, además nos permite observar que normativas como la española, en el tema de infracciones se encuentran más desarrolladas, mismas que pueden ayudar como referente para un estudio y posible reforma de nuestra normativa.

Infracciones administrativas graves

Los hechos que diferencian la clasificación entre la normativa española y la ecuatoriana en cuanto a los tipos de infracciones son: en la normativa española las entidades de certificación se las clasifica en reconocidas y no reconocidas, a cada cual se len han impuesto determinadas obligaciones, lo que se refleja también en el tipo de infracción y sanción; en nuestra Ley de Comercio Electrónico no se presenta esta clasificación de las entidades de certificación, se la eliminó, es por esto que solamente se determinan las entidades de certificación acreditadas.

[169] Ley de Comercio Electrónico, *op. cit.*

A lo anteriormente expresado y a manera de información, para entender mejor el tema nuevamente nos referiremos a la opinión de Leopoldo González Echenique, mismo que comenta la normativa española: *"El tipo infractor es paralelo al correlativo del apartado anterior que recoge como infracción grave la misma conducta si bien referida a los prestadores que expidan certificados reconocidos. La diferencia, por tanto, entre uno y otro tipo es subjetiva: La infracción muy grave es aplicable a los prestadores que expidan certificados reconocidos mientras que la grave afecta a los que emitan certificados simples o realicen alguna otra actividad relacionada con la Firma Electrónica."*[170]; también son factores determinantes de la clasificación a mas del incumplimiento de las obligaciones como tales, que ese incumplimiento cause daños graves a los usuarios o terceros; así como la afectación a la seguridad de los servicios de certificación.

En la normativa nacional las infracciones administrativas graves se determinan en el artículo 40, de la Ley de Comercio Electrónico y de conformidad con el Código Civil atraería responsabilidad por dolo y mala fe, principalmente a las entidades de certificación que incurran en tales situaciones, y son las siguientes:

1. Uso indebido del certificado de Firma Electrónica por omisiones imputables a la entidad de certificación de información acreditada; la infracción mencionada guarda concordancia con el literal g) del artículo 30, de la Ley que hace relación a la obligación de estas entidades en proporcionar a los titulares de los

[170] Leopoldo González y Echenique Castellanos, *op. cit*., p. 253.

certificados un medio efectivo para informar que una Firma Electrónica tiene riesgo de uso indebido.

2. Omitir comunicar al organismo de control la existencia de actividades presuntamente ilícitas realizada por el destinatario del servicio; se entendería que la entidad de certificación al presumir un acto ilícito del titular del certificado esta obligada a comunicar a la Superintendencia de Telecomunicaciones, para que esta a su ves, en base al literal g) del artículo 39, de la Ley disponga la suspensión del servicio de certificación y de esta manera se impida cometer una infracción.

3. Desacatar la petición del organismo de control de suspender la prestación de servicios de certificación para impedir el cometimiento de una infracción; el *desacato* según el Diccionario Usual de Guillermo Cabanellas es: *"faltar al respeto debido a la autoridad; y desacato falta de respeto en relación con los jefes o superiores."*[171]

4. El incumplimiento de las resoluciones dictadas por los Organismos de autorización registro y regulación, y de control; así por ejemplo con las resoluciones emitidas por el CONATEL relacionados con la revocación o suspensión de la autorización a las entidades de certificación acreditadas o para revocar o suspender los certificados de Firma Electrónica; también las resoluciones de la Superintendencia de Telecomunicaciones en las que se

[171] Guillermo Cabanellas, *op. cit.*, p. 161.

aplican las sanciones por el cometimiento de infracciones administrativas contenidas en la Ley de Comercio Electrónico.

5. No permitir u obstruir la realización de auditorias técnicas por parte del organismo de control; lo anterior guarda relación con el literal c) del artículo 39, de la Ley que dispone como función de la Superintendencia de Telecomunicaciones lo siguiente: *"Realizar auditorias técnicas a las entidades de certificación de información acreditadas."*[172], el tema de las auditorias técnicas en la práctica no es posible cumplir, ya que la normativa ecuatoriana sobre Firma Electrónica carece de un reglamento para el caso, así lo corrobora Carlos vera Quintana al expresar: "*Aún restan por elaborarse normas legales complementarias como: 2. El Reglamento de auditorias técnicas que debe elaborar el órgano de control*"[173].

Infracciones administrativas leves

La normativa española contempla las obligaciones que deben cumplir tanto las entidades de certificación que emiten certificados reconocidos, como las que emiten solamente certificados, es así como con contadas excepciones, las infracciones leves son motivo de infracción por las entidades de certificación que emiten certificados no reconocidos, además por representar un menor riesgo por parte de la entidad, Leopoldo González comenta: *"Nuevamente nos encontramos con tipos residuales, definidos negativamente, y que se*

[172] Ley de Comercio Electrónico, *op. cit.*
[173] Carlos Vera Quintana, *El Reglamento a la Ley de Comercio Electrónico del Ecuador*, en: El Informante. No. 129, http://www.corpece.org.ec.

caracterizan por representar un riesgo por parte del prestador que incurre en ellos menor que el que se sanciona en la correlativa infracción grave o muy grave."[174]*.* A continuación, realizaremos un análisis de las infracciones leves que están determinadas en el artículo 40, de la Ley de Comercio Electrónico, que son:

1. La demora en el cumplimiento de una instrucción o en la entrega de información requerida por el organismo de control; en primera instancia, debemos indicar, que este numeral tiene relación con el numeral 5, del mismo artículo 40, que se refiere a las infracciones graves. La diferencia se encuentra en que esta infracción habla de la demora, mientras en el otro numeral de la obstrucción a las labores de requerimiento de información y auditorias técnicas por parte del organismo de control.

De manera similar se pronuncia la legislación española, esto lo confirmamos con el criterio del último autor citado que dice: *"La única cuestión que puede suscitarse a la hora de aplicarse este tipo infractor se asocia con la identidad entre esta conducta y la constitutiva de una infracción grave de obstrucción, resistencia o negativa a la actividad inspectora de la Administración supervisora. No cabe duda que el alcance de la resistencia, negativa o obstrucción determinarán la gravedad de la infracción y, por tanto de la sanción a imponer."*[175]

[174] Leopoldo González y Echenique Castellanos, *op. cit*., p. 255.
[175] *Ibíd.*, p. 256.

2. Cualquier otro incumplimiento de las obligaciones impuestas por esta Ley y sus Reglamentos a las entidades de certificación acreditadas; esta infracción puede interpretarse en el sentido de que no se deja abierta la posibilidad de cometimiento de infracción alguna sin la sanción respectiva.

3.3 Sanciones

Respecto de las sanciones, empezaremos citando lo contenido en el artículo 41, de la Ley de Comercio Electrónico:

> *"Art. 41.- Sanciones.- La Superintendencia de Telecomunicaciones, impondrá de oficio o a petición de parte, según la naturaleza y gravedad de la infracción, a las entidades de certificación de información acreditadas, a sus administradores y representantes legales, o a terceros que presten sus servicios, las siguientes sanciones:*
>
> *a) Amonestación escrita;*
>
> *b) Multa de quinientos a tres mil dólares de los Estados Unidos de Norteamérica;*
>
> *c) Suspensión temporal de hasta dos años de la autorización de funcionamiento de la entidad infractora, y multa de mil a tres mil dólares de los Estados Unidos de Norteamérica; y,*
>
> *d) Revocatoria definitiva de la autorización para operar como entidad de certificación acreditada y multa de dos mil a seis mil dólares de los Estados Unidos de Norteamérica."* [176]

[176] Ley de Comercio Electrónico, *op. cit.*

En concordancia con lo anterior el artículo 40, de la misma Ley, determina que las infracciones leves serán sancionadas de conformidad a los literales a) y b) citados, mientras que las infracciones graves se sancionarán en base a lo contenido en los literales c) y d). Como complemento a lo anterior, es meritorio dejar expresado lo que el autor ecuatoriano Efraín Torres Cháves comenta: *"Así como la resolución de un contrato, condena al deudor al cumplimiento forzoso del mismo y a la indemnización de daños y perjuicios, la infracción administrativa no exime al responsable –la entidad de certificación de información- de sus obligaciones con las autoridades y con sus clientes."*[177]

En la normativa española las sanciones para infracciones muy graves y graves, se basan principalmente en el criterio del beneficio resultante de la actividad en la que se ha cometido la infracción, para lo cual existen parámetros, es así como, el importe de la multa estará comprendido entre el tanto y el quíntuplo del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción, pero cuando no es posible aplicar este criterio, o de su aplicación resulta una cantidad inferior a las cantidades que se encuentran determinadas, no puede aplicarse como sanción una cantidad mayor a la determinada como tal, pero también a lo comentado existen críticas como la de Leopoldo González-Echenique, así: *"En cualquier caso siempre que se usa el concepto del beneficio, se deja la cuestión a expensas del rigor contable del infractor lo cual puede hacer inaplicable el criterio."*[178]*;* también se sanciona con la prohibición de actuación de la entidad de certificación durante un plazo máximo de dos años.

[177] Efraín Torres Cháves, *op. cit.*, p. 60.
[178] Leopoldo González y Echenique Castellanos, *op. cit.*, p. 256.

Las sanciones que corresponden a las infracciones leves en la normativa española se encuentran plenamente determinadas con un valor en dinero, existe un valor máximo aplicable a estas infracciones que constituye el parámetro de determinación en el tipo de infracciones, entre muy graves, graves y leves.

Hasta aquí, el régimen sancionador español tiene diferencias con el nuestro, por ser una normativa con criterios más detallados, pero también tiene similitudes, variando sólo en cuestiones de forma, manteniendo en el fondo el mismo criterio, contemplando reglas comunes para fijar la cuantía de las multas, así como para la gradación de las demás sanciones, debiéndose tomar en cuenta para sancionar lo siguiente: a) La gravedad de las infracciones cometidas y su reincidencia; b) El daño causado o el beneficio reportado al infractor y c) La repercusión social de las infracciones.

Este constituiría básicamente el régimen de sanción o sancionador en la normativa nacional, sin embargo, se debe reglamentar la forma de cálculo de las multas, no necesariamente como la normativa española, ya que como hemos visto presenta dificultades, sino en base a parámetros más ciertos como por ejemplo tener de base el salario mínimo vital.

Procedimiento para sancionar

Ya hemos expresado que toda infracción conlleva una sanción, para lo cual también se necesita de un proceso o procedimiento, en nuestra normativa el

artículo 43, de la Ley de Comercio Electrónico, determina: "*El procedimiento para sustanciar los procesos y establecer sanciones administrativas, será el determinado en la Ley Especial de Telecomunicaciones."*[179]. De esta manera el procedimiento se halla contenido en el artículo 30, y siguientes de la Ley Especial de Telecomunicaciones y se resume de la siguiente manera.

De conformidad con el artículo 30, de la Ley Especial de Telecomunicaciones, en primera instancia se debe notificar a la entidad de certificación de información acreditada, a sus administradores y representantes legales, o a terceros que presten sus servicios; esto se lo hace mediante una boleta en el domicilio civil o mercantil del infractor o por correo certificado, (en la actualidad y por el sistema debería también hacérselo por correo electrónico), si no es posible determinar el domicilio del infractor se lo hará mediante una publicación en el periódico del domicilio del infractor; una vez notificado, y de acuerdo al artículo 32 de la Ley motivo de análisis, tendrá el infractor el término de ocho días para hacer uso de su derecho a la defensa.

El artículo 30, de la Ley Especial de Telecomunicaciones determina: *"Corresponde al Superintendente de Telecomunicaciones juzgar al presunto infractor, graduando la aplicación de la sanción según las circunstancias, mediante resolución motivada y notificada al infractor."*[180], como se menciona es el Superintendente de Telecomunicaciones máxima autoridad del organismo de control, quien juzga y aplica la sanción en caso de comprobarse una

[179] Ley de Comercio Electrónico, *op. cit.*
[180] *Ley Especial de Telecomunicaciones*, Ley No. 4, publicada en Suplemento del Registro Oficial de 13 mayo del 2000.

infracción administrativa. El artículo citado guarda concordancia con el artículo 33, de la misma Ley, que se refiere a la resolución del Superintendente, la cual debe dictarse en el término de quince días contados a partir del vencimiento del término para contestar se haya o no recibido la contestación, resolución que deberá ser motivada, causando ejecutoria en la vía administrativa, pudiendo oponerse en la vía jurisdiccional ante el Tribunal de lo Contencioso Administrativo.

Finalmente como anexo al procedimiento cabe mencionar las medidas cautelares, para lo cual el artículo 42 de la Ley de Comercio Electrónico expresa: *"En los procedimientos instaurados por infracciones graves, se podrá solicitar a los órganos judiciales competentes, la adopción de las medidas cautelares previstas en la Ley que se estimen necesarias, para asegurar la eficacia de la resolución que definitivamente se dicte."*[181], las medidas cautelares como conocemos previenen un daño, pero para una mejor compresión del tema citaremos el criterio de Efraín Torres Cháves que ha sido un referente en el análisis de nuestra normativa, el sostiene: *"Las medidas cautelares son aquellas diligencias establecidas en la Ley y facultadas al arbitrio de los juzgadores, a fin de adoptar precauciones, prevenir o precaver un daño irreparable, por la omisión o cumplimiento de deberes y obligaciones."*[182]. Es así como el CONATEL o la Superintendencia de Telecomunicaciones solicitará a los órganos jurisdiccionales correspondientes la adopción de estas medidas, (secuestro, prohibición de enajenar, embargo y remate), contenidas en el Código de Procedimiento Civil.

[181] Ley de Comercio Electrónico, *op. cit.*
[182] Efraín Torres Cháves, *op. cit.,* p. 61.

Es importante resaltar la remisión de la Ley de Comercio Electrónico a la Ley Especial de Telecomunicaciones que actúa como norma supletoria, haciéndose efectivo el procedimiento para sustanciar los procesos y establecer las correspondientes sanciones a las infracciones administrativas; el procedimiento se encuentra establecido en nuestras leyes pero no se hace efectivo en la práctica, ya que no se conoce hasta el momento se haya producido un procedimiento de este tipo y esto como una consecuencia de la falta de funcionamiento de entidades de certificación de información.

CONCLUSIONES

Para el desarrollo del comercio electrónico y la firma electrónica a nivel internacional se ha emitido la normativa correspondiente para su tratamiento. En el caso del Ecuador se cuenta con la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, que regula principalmente la Firma Electrónica y los servicios de certificación, normativa que se la ha emitido siguiendo los principios y procedimientos básicos establecidos en la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional -CENUDMI-, conocida por sus siglas en ingles como -UNCITRAL-

.

Al igual que la normativa internacional, la Ley de Comercio Electrónico ecuatoriana contiene a la Firma Electrónica, es así como en relación con los documentos electrónicos cumple con las principales funciones atribuidas a la firma manuscrita, identifica al autor (autenticación) y verifica que el mensaje no haya sido alterado después de firmado (integridad); en complemento a lo expresado, el Reglamento a la Ley contiene la teoría de la neutralidad tecnológica respaldada por la UNCITRAL, que no restringe el uso de otras Firmas Electrónicas concebidas fuera de la infraestructura de clave pública, situación última para que la Ley tenga vigencia en el tiempo ante el cambio de la tecnología.

La Firma Electrónica al cumplir las funciones que se le atribuyen a la firma manuscrita, tiene la misma validez y se le reconocen los mismos efectos jurídicos que esta última, por lo que también debe ser admitida como prueba en

juicio, sin embargo vemos la necesidad de concebir en nuestra normativa civil un instrumento público notarial informático, documento que sería al mismo tiempo documento informático y escritura pública notarial; de manera que según las necesidades de los diversos sectores jurídicos, la escritura pudiera otorgarse y autorizarse en papel o por medios informáticos, por ende debería también declararse a los notarios como una especie de entidad de certificación.

El certificado de Firma Electrónica en la normativa internacional y en nuestra Ley de Comercio Electrónico es concebido como el mensaje de datos que certifica la vinculación de una Firma Electrónica con una persona determinada, pero tanto en esta Ley como en su Reglamento no se definen aspectos de trascendencia relacionados con éste y con el sistema, como el procedimiento de generación y emisión, la revocación, suspensión; además existen contradicciones como en el plazo de duración de éstos, ocasionándose problemas en su aplicación, considerando lo anterior como causas por las que en el país no se hayan emitido aún este tipo de documentos electrónicos.

Las entidades de certificación de información son consideradas por la doctrina europea como una tercera parte de confianza, ya que aseguran el vínculo entre la clave pública y el titular de la clave privada, pero nuestra normativa en ningún momento pronuncia una definición funcional o descriptiva del tema, sigue conceptos recogidos por otras legislaciones, limitándose solamente a señalar quiénes pueden ejercer estas actividades y cuáles son las funciones de estas entidades; en este mismo tema, casos como los requisitos para ser entidad de certificación y las listas de certificados revocados o suspendidos no

se encuentran reglamentados y existe un vacío legal referente a las entidades de certificación de información y las entidades de certificación de información acreditadas. Podemos concluir que en el país no funcionan entidades que cumplan el objetivo expresado.

Importante de concluir es el hecho de que la Ley de Comercio Electrónico sostiene, que las entidades de certificación de información podrán ser empresas unipersonales o personas jurídicas, pero al decir empresas unipersonales, se adelantó a la entrada en vigencia de la nueva Ley de Empresas Unipersonales de Responsabilidad Limitada, publicada recién en el Registro Oficial No. 196, de 26 de enero del 2006, por lo que es apresurado desarrollar comentarios al efecto, pero estas empresas tendrán como objeto emitir certificados de Firma Electrónica.

El Consejo de Comercio Exterior e Inversiones, -COMEXI-, es el encargado de la promoción y difusión de los servicios electrónicos, y uso de las Firmas Electrónicas, cabe señalar que no existe organismo similar en la normativa internacional, pero es insertado en nuestra normativa con la finalidad de atraer inversión y desarrollar el comercio exterior; objetivos que no se han podido cumplir por no tener reglamentada su función, además de no mantener conexión alguna con los otros organismos.

El Consejo Nacional de Telecomunicaciones -CONATEL-, organismo encargado de la regulación, autorización y registro de las entidades de certificación acreditadas, tiene plenamente determinadas sus funciones en la

Ley de Comercio Electrónico, este organismo se encuentra en actividad respecto de sus funciones, y para el cumplimiento de éstas ha expedido el Reglamento para la Acreditación, Registro y Regulación de Entidades habilitadas para prestar servicios de Certificación de Información y Servicios Relacionados, sin embargo se ha llegado a determinar que en nuestro país no existen entidades de certificación que se encuentren trabajando.

La Superintendencia de Telecomunicaciones en calidad de organismo de control de las entidades de certificación de información acreditadas, mantiene también un régimen sancionador respecto de estas entidades, de sus administradores y representantes legales, y de terceros que presten sus servicios. Observamos que sus funciones se encuentran detalladas en la Ley, pero se carece de una reglamentación que colabore a su aplicación, como lo sería el reglamento de auditorias técnicas; mientras que para sustanciar los procesos y establecer sanciones se remite a la Ley Especial de Telecomunicaciones.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos apegada a los lineamientos y principios de la Ley Modelo de la UNCITRAL norma a la Firma Electrónica, pero ésta última es una ley marco que no contempla todas las regulaciones para hacer efectivas estas instituciones en los países que la han acogido como el Ecuador; sin embargo de lo expresado, y a pesar del esfuerzo de organismos como el CONATEL nuestra normativa tiene vacíos legales y una reglamentación incompleta, lo que ha conducido en la práctica a que no se pueda hacer efectivo el uso de la Firma Electrónica.

BIBLIOGRAFIA

Diccionario de la Lengua Española, Real Academia Española, vigésima segunda edición, España, 2001.

Cabanellas Guillermo, *Diccionario de Derecho Usual*, vigésima quinta edición, Buenos Aires, Editorial Heliasta S.R.L., 1997.

Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, Preparación de las Futuras Negociaciones Comerciales Multilaterales: Asuntos e Investigaciones Necesarias desde una perspectiva del Desarrollo, Publicación de las Naciones Unidas, Nueva York y Ginebra, 1999.

Calvo-Sotelo Aránzazu y Lobo Coello Manuel C., *La Firma Electrónica*, en: Cremades Javier, Régimen Jurídico de Internet, Las Rozas-Madrid, La Ley – Actualidad, S.A., 2002.

Castro Muñoz Xavier, *Libro Homenaje al Dr. Hector Romero Parducci*, Ecuador, Edino, 2000.

Cremades Javier, *Régimen Jurídico de Internet*, Las Rozas-Madrid, La Ley – Actualidad, S.A., 2002.

Dávara Rodríguez Miguel Angel, *Firma Electrónica y Autoridades de Certificación: El Notario Electrónico*, en: Problemática Jurídica en Torno al Fenómeno de Internet, Madrid – España, Lerko Print S.A., 2000.

Devoto, Mauricio, *Comercio Electrónico y Firma Digital,* Buenos Aires, Editorial La Ley S.A., 2001.

Domínguez Gragera María Luisa, *Normativa Aplicable a la Firma Electrónica (Directiva 99/93/CE y Real Decreto-Ley 14/1999)*, en: Cremades Javier, Régimen Jurídico de Internet, Las Rozas-Madrid, La Ley-Actualidad, S.A., 2002.

Echebarría Sáenz Josefa A., *El Comercio Electrónico*, Madrid, Edisofer S.L., 2001.

Fernández Delpech Horacio, *Internet: Su Problemática Jurídica*, Buenos Aires-Argentina, Abeledo - Perrot, 2001.

Gaete González Eugenio Alberto, *Instrumento Público Electrónico*, Barcelona, Editorial Bosh S.A., 2000.

García Vidal Angel, *La Regulación Jurídica de la Firma Electrónica,* en: Gómez Segade, José Antonio, Comercio Electrónico en Internet, Madrid, Ediciones Sociales y Jurídicas S.A., 2001.

Gómez Segade José Antonio, *Comercio Electrónico en Internet*, Madrid, Ediciones Sociales y Jurídicas S.A., 2001.

González – Echenique Castellanos de Ubao Leopoldo, *Estudio de la Directiva y del Real Decreto-Ley de 17 de septiembre de 1999 sobre Firma Electrónica*, en: Mateu De Ros, Rafael, Derecho de Internet, Contratación Electrónica y Firma Digital, Navarra, Editorial Aranzadi, S.A., 2001.

Hance Oliver, *Leyes y Negocios en Internet*, Mc Grow – Hill Interamericana Editores S.A., México, impreso en México en LIBEMEX, 1997.

Lorenzetti Ricardo L., *Comercio Electrónico,* Buenos Aires-Argentina, Abeledo - Perrot, 2001.

Mangas Martín Araceli y Liñán Nogueras Diego, *Los principios del derecho comunitario en sus relaciones con los ordenamientos internos*, en: Instituciones y Derecho de la Unión Europea, segunda edición, Madrid, McGrawn-Hill, 1999,

Madrid Parra Agustín, *Ley Modelo de la CENUDMI / UNCITRAL para las Firmas Electrónicas*, en: Cremades, Javier, Régimen Jurídico de Internet, Las Rozas-Madrid, La Ley – Actualidad, S.A., 2002.

Martínez Nadal Apol Lonia, *Comercio Electrónico, Firma Digital y Autoridades de Certificación*, Universitat de les Illes Baleares, Madrid-España, Civitas Editiones, S. L., tercera edición, 2001.

Mateu De Ros Rafael, *Derecho de Internet, Contratación Electrónica y Firma Digital*, Navarra, Editorial Aranzadi, S.A., primera edición, 2000.

Montagud Castelló Enrique, *Eficacia Jurídica de la Firma Electrónica*, en: Mateu De Ros, Rafael, Derecho de Internet, Contratación Electrónica y Firma Digital, Navarra, Editorial Aranzadi, S.A., 2001.

Montaño Galarza Cesar, *Constitución del Ecuador e Integración Andina*, artículo inédito, Quito, 2002.

Montaño Galarza Cesar, *Documento Visión General del Derecho Económico.*

Murrieta Wong Katia, *Presente y Futuro de la Contratación Electrónica a Distancia y Comentarios a la Ley de Comercio Electrónico Ecuatoriana*, en: Castro Muñoz Xavier, Libro Homenaje al Dr. Héctor Romero Parducci, Ecuador, Edino, 2000.

Ordoño Artés Carmen, *El Avance Tecnológico y los Nuevos Medios de Prueba en la Ley de Enjuiciamiento Civil*, en: Cremades, Javier, Régimen Jurídico de Internet, Las Rozas-Madrid, La Ley – Actualidad, S.A., 2002.

Peralta Díaz Fabrizio, *Comercio Electrónico, Firmas Electrónicas y Entidades de Certificación*, en: Castro Muñoz, Javier, Libro Homenaje al Dr. Hector Romero Parducci, Guayaquil-Ecuador, Edino, 2000.

Rico Frontaura Víctor Manuel, *El Derecho de la Integración en la Comunidad Andina*, en: Integración y Supranacionalidad. Soberanía y Derecho Comunitario en los Países Andinos, Lima, 2001.

Ribagorda Garnacho Arturo, *Sistema de Certificación: la Firma y el Certificado Digital*, en: Cremades, Javier, en: Cremades, Javier, Régimen Jurídico de Internet, Las Rozas-Madrid, La Ley – Actualidad, S.A., 2002.

Sarra Andrea Viviana, *Comercio Electrónico y Derecho*, Buenos Aires, Editorial Astrea, 2000.

Sobrino Heredia José Manuel, *El derecho de Integración: Marco Conceptual y Experiencias Regionales,* en: Integración y Supranacionalidad, Soberanía y Derecho Comunitario en los Países Andinos, Lima, 2001.

Torres Cháves Efraín, *Breves Comentarios a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos*, Quito-Ecuador, Corporación de Estudios y Publicaciones, 2002.

Ureba Alberto Alonso y Alcocer Garau Guillermo, *La Firma Electrónica*, en: Mateu De Ros, Rafael, Derecho de Internet, Contratación Electrónica y Firma Digital, Navarra, Editorial Aranzadi, S.A., 2001.

Verón Víctor Alberto, *Nueva Empresa y Derecho Societario*, Buenos Aires, Editorial Astrea, 1996.

Villar José Manuel, *Una Aproximación a la Firma Electrónica*, en: Mateu De Ros, Rafael, Derecho de Internet, Contratación Electrónica y Firma Digital, Navarra, Editorial Aranzadi, S.A., 2001.

Witker Jorge, *El Derecho Económico en los Sistemas Económicos del siglo XX*, en: Introducción al derecho Económico, tercera edición, Editorial Harda, Mexico, 1997.

Códigos, Leyes y Reglamentos

Constitución Política de la República del Ecuador, Gaceta Constitucional, de julio de 1998.

Código Civil, Ley No. 47, Registro Oficial No. 223, de 26 de Julio de 1997.

Código de Procedimiento Civil, Ley No. 45, Registro Oficial No. 372, de 19 de Diciembre del 2001.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Ley No. 67, Registro Oficial No. 557-S, de 17 de abril del 2002.

Ley de Empresas Unipersonales de Responsabilidad Limitada, Ley No. 27, Registro Oficial No. 196, de 26 de enero del 2006.

Ley Especial de Telecomunicaciones, Ley No. 4, Registro Oficial No. --, de 13 de Mayo del 2000.

Ley Modelo de la ULCITRAL sobre Comercio Electrónico, CENUDMI – ULCITRAL, 28 de mayo al 14 de junio de 1996.

Ley Notarial, Ley No. 73, Registro Oficial No. 595, de 12 de Junio de 2002.

Ley Orgánica de Defensa del Consumidor, Ley No. 21, Registro Oficial No. 116, de 10 de Julio del 2000.

Ley de Propiedad Intelectual, Ley No. 83, Registro Oficial No. 320, de 19 de mayo de 1998.

Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, Decreto Ejecutivo No. 3496, Registro Oficial No. 735, de 31 de Diciembre del 2002.

Reformas al Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensaje de Datos, Decreto Ejecutivo No. 908, Decreto Ejecutivo No. 908, Registro Oficial No. 168, de 19 de diciembre del 2005.

Reglamento para la Acreditación, Registro y Regulación de las Entidades Habilitadas para prestar Servicios de Certificación Información y Servicios

Relacionados, Resolución No. 584-23 – CONATEL, Registro Oficial No. 196, de 23 de octubre del 2003.

Reglamento General a la Ley Orgánica de Defensa del Consumidor, Decreto Ejecutivo No. 1314, Registro Oficial No. 287, de 19 de Mayo del 2001.

Páginas y documentos Web

http://www.alfa-redi.org.

http://www.arrakis.es.

http://www.conatel.gov.ec.

http://www.corpece.org.ec.

http://www.comexi.org.

http://www.onnet.es.

http://www.uncitral.org.

http://www.sice.oas.org.

Barzallo José Luis, *Artículo: Los Terceros de Confianza en el Comercio Electrónico*, en: Revista de Derecho Informático No. 033, de Abril del 2001, edita Alfa – Redi, http://www.alfa-redi.com/rdi-articulo.shtml?x=662.

Barzallo José Luis, Boletín Informativo No. 87, http://www.corpece.org.ec, Corporación Ecuatoriana de Comercio Electrónico.

Illescas Ortiz Rafael, *tema de debate: El Comercio Electrónico: fundamentos de Derecho y el principio de equivalencia funcional*, www.uc3m.es/uc3m/inst/FL/boletin/español/pdfdebate/td562.pdf.

Irabien Chedraui José Fernando, *Artículo: El Reconocimiento de Certificados Digitales Extranjeros,* en: Revista de Derecho Informático No. 060, de julio del 2003, edita Alfa – Redi, http://www.alfa-redi.com/rdi-articulo.shtml?x=1313

Rico Carrillo Mariliana, *Artículo: Validez y regulación legal del documento y contratación electrónica*, en: Revista de Derecho Informático NO. 019, de febrero del 2000, edita Alfa – Redi, http://www.alfa-redi.org/rdi-articulo.shtml?=422-30k

Riofrío Martinez-Villalba Juan Carlos, *Garantías en las Comunicaciones Electrónicas en países sin Ley Especial,* en: Revista de Derecho Informático, No. 038, septiembre del 2001, edita Alfa-Redi, http://www.alfa-redi.com/miembro.shtml?x=777

Artículo: El ABZ de las Firmas Electrónicas, 28 de Marzo del 2002, en http:// www.corpece.org.ec/informante/index.htm

Vera Quintana Carlos, *Artículo: El Reglamento a la Ley de Comercio Electrónico del Ecuador*, en: El Informante. No. 129, http:// www.corpece.org.ec

Vera Quintana Carlos, *Artículo Especializado: El Arte de Legislar*, en: El Informante. No. 129, http://www.corpece.org.ec

Otros documentos

Acta No. 160, de 7 de Febrero del 2002, Segundo Debate del Proyecto de Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos, PL No. 21-315.

Acta No. 164, de 19 de Febrero del 2002, Segundo Debate del Proyecto de Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos, PL No. 21-315.

Acta No. 191, de 10 de Abril del 2002, Segundo Debate del Proyecto de Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos, PL No. 21-315.

Veto Presidencial al Proyecto de Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos, PL No. 21-315, Oficio No. T 1862-DAJ-2002-5312, de 14 de Marzo del 2002.