FACULTAD DE DERECHO Y CIENCIAS SOCIALES

LA FIRMA ELECTRÓNICA EN EL ECUADOR: LOS ESTÁNDARES INTERNACIONALES DE FIRMA ELECTRÓNICA Y EL PRINCIPIO DE NEUTRALIDAD TECNOLÓGICA

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de Abogado de los Tribunales y Juzgados de la República

Profesor Guía

Dra. Jacqueline Guerrero

Autora

Maraile Francesca Bast Frixone

Año

2016

DECLARATORIA DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido, y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.”

_____

Jacqueline Guerrero
Doctora en Jurisprudencia
C.C. 2000027470

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

Maraile Francesca Bast Frixone

C.C.171290799-5

AGRADECIMIENTOS

Quisiera agradecer a la Universidad de las Américas por brindarme la educación necesaria para cumplir mi sueño.

A mi directora de tesis, Jacqueline Guerrero, por su paciencia, ayuda y apoyo a lo largo del desarrollo de este trabajo de titulación.

A mis padres, por su apoyo incondicional y por darme fuerzas en los momentos que más lo necesitaba.

DEDICATORIA

A mi papá, Jörn Bast, por siempre estar para mí con las palabras correctas de apoyo y aliento, por ayudarme a alcanzar mis metas y sueños y a mi mamá, Ana María Frixone, por ser mi apoyo incondicional, mi motor, sin ellos esto no hubiese sido posible. A mi hermano, Nicolás Bast, por enseñarme que ningún sueño es imposible. A mis abuelos, Ana María Astorga de Frixone y César Frixone, por todo su cariño y conocimientos impartidos. A María Amada Moreno, mi amiga y futura colega. A Felipe Ulloa, por su paciencia y ayuda y a mis amigos y familiares.

RESUMEN

Existe una clara tendencia a la desmaterialización, por las ventajas que ofrece el sistema. Sin embargo, estas ventajas pueden convertirse en un factor de riesgo, puesto que la mayoría de veces no existe la posibilidad de identificar al firmante y, sin el debido sistema, no se puede vincular la firma a una persona y por ende la voluntad de la misma al documento emitido. Además, por la amplitud de la red, la información es fácilmente accesible por terceros no autorizados. Entonces la protección de la información resulta imperativa a la hora de empezar a aplicar sistemas informáticos. Existen requisitos mínimos que debe cumplir un programa para lograrlo, estos son el de confidencialidad, autenticación, integridad y no repudio. La firma digital cumple con estos requerimientos.

Dentro de los países que tienen más desarrollado el tema de las firmas están Estados Unidos, España y Argentina. En sus respectivas legislaciones regulan a la firma digital, sin quitarle valor a otras firmas que usen distintos tipos de tecnología. En España se habla de firma electrónica reconocida que es la firma digital con otro nombre. Ecuador regula lo que se denomina como firma electrónica, que, como se demostrará, contradice el principio de neutralidad tecnológica, descrito y defendido por la Ley Modelo de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional.

Es por esto que la tesis que se desarrolla es que la firma digital es el equivalente funcional de la firma manuscrita, porque garantiza la identificación del firmante, se puede comprobar que el mensaje no ha sido alterado, el mensaje se vuelve confidencial por el sistema de criptografía asimétrico con el que cuenta la firma y además garantiza el no repudio de la firma y de lo firmado. Además, la firma electrónica si violenta el principio de neutralidad tecnológica, puesto que discrimina a los otros tipos de tecnología que puedan ser usados para la firma.

Conforme a la tesis se pretende proponer una reforma al cuerpo normativo ecuatoriano, para que este pueda satisfacer no solo los parámetros internacionales, sino también la realidad nacional y así fomentar el uso de la firma digital.

ABSTRACT

There’s a clear tendency to dematerialization, because of all the advantages that the system has to offer. This advantages can turn into a risk factor due to the fact that most of the times, without the right system, It’s impossible to identify the signer of the document and no way to link the signature to a person and thus to the will of that person to the document signed. Due to the amplitude of the network, the information contained in it is easily accessible for non-authorized third parties. This is why the protection of the information, is imperative. There are minimum requirements that an informatics program has to fulfill to guarantee the security of the information, these are: confidentiality, authentication, integrity and non-repudiation. The digital signature satisfies these requirements.

Within the countries that are more developed in this subject are the United States of America, Spain and Argentina. They regulate about the digital signature without detracting from the possibility of using others that use different types of technology. In Spain they regulate about the electronic recognized signature, it’s the same but with another name. Ecuador regulates what is known as an electronic signature, which contradicts the principle of technological neutrality, described and defended by the Model Law of the United Nations Commission for International Trade Law.

This is why the thesis that unfolds is that the digital signature is the functional equivalent of a handwritten signature, as it ensures the identification of the signer, it's possible to verify that the message has not been altered, the message becomes confidential by the usage of an asymmetric cryptography system which contains the signature and also ensures non-repudiation of the signature and the text signed with it. Additionally, electronic signatures violate the principle of technological neutrality, since it discriminates against other types of technology that can be used for signing.

In accordance with the thesis described, the intention of this paper is to propose a reform of the Ecuadorian regulatory body so that it can meet not only international standards but also the national reality and thus encourage the use of digital signature.

ÍNDICE

INTRODUCCIÓN

Desde el surgimiento de las nuevas tecnologías el Derecho ha debido dar respuesta a la problemática que surge por la incorporación de las TIC en todos los ámbitos del quehacer social, tales como: la conectividad entre personas, la aceleración de las transacciones, la seguridad de la información. Frente a esto último y en el campo de la informática se desarrolló la solución técnica conocida como firma digital, que por su importancia y trascendencia debió regularse jurídicamente.

Mediante este trabajo se pretendió determinar que la normativa que regula la firma electrónica en el Ecuador, específicamente en la Ley de Comercio electrónico y Firmas electrónicas y Mensajes de Datos, debe ser objeto de una actualización, para incorporar las tendencias actuales y los elementos de debate sobre las firmas electrónicas y las digitales, que se reflejan a nivel mundial. Comprendió los siguientes aspectos: la vulneración al principio de neutralidad tecnológica, la implementación del sistema PKI así como de la criptografía asimétrica y, por lo tanto, la actualización de la normativa.

En primera instancia se trataron temas generales que ayuden al lector a entender mejor el tema de la firma digital. Se determinó que la información es el principal objeto de protección dentro de la red y los requisitos de seguridad que se debe cumplir para protegerla. Además se presentó la problemática que existe entre la firma electrónica y la digital y como la referencia a lo electrónico contradice el principio de neutralidad tecnológica, por lo cual el término digital resulta ser la correcta en el momento de regular el tema.

El capítulo segundo se centró en el análisis de legislaciones relevantes extranjeras en lo que respecta al tema de firmas digitales. Entre las legislaciones analizadas se encuentra la argentina que tiene una ley específica sobre firmas digitales; la española que regula la firma electrónica avanzada reconocida, que es una firma digital con un nombre distinto y la Ley del Estado

de Utah, que también regula la firma digital y además es la primera norma jurídica sobre el tema.

En todas estas legislaciones se reconoce el uso de otros tipos de firmas, pero se regula específicamente la digital. También se analizó la Ley Modelo de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional. Así mismo se estudió el cuerpo normativo vigente sobre el tema en Ecuador, que a diferencia de los otros, regula la firma electrónica.

Adicionalmente, se analizaron los principios y estándares internacionales de la firma digital. La investigación, por tanto, se centró en demostrar que la normativa que regula la firma electrónica en Ecuador requiere una actualización. Por lo que se propone la aprobación de una nueva ley exclusivamente sobre firmas digitales, para que esta pueda satisfacer la realidad jurídica del país, pues luego de doce años de vigencia las disposiciones de las Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos resultan generales y no se adaptan a los escenarios jurídicos existentes, nacionales e internacionales, especialmente en el tema de firmas digitales, lo cual se evidenció en el capítulo tercero.

CAPÍTULO I

1. MECANISMOS DE SEGURIDAD DE LA INFORMACIÓN

1.1. ANTECEDENTES

Las nuevas formas de interactuar, a través de canales electrónicos, han creado una dependencia a los sistemas informáticos. Esta dependencia ha tenido como consecuencia una vulnerabilidad directa sobre los sistemas, ya sean de comunicaciones o informáticos que contienen información o sobre los cuales viaja la misma. Dicha vulnerabilidad se basa en la falta de seguridad física, característica obvia de los medios electrónicos, la falta de seguridad lógica y la falta de seguridad jurídica (Davara Rodríguez, 2008, p. 35-36). Miguel Ángel Davara Rodriguez sostiene que “todas las aparentes ventajas que entrañan el tratamiento informático, con la transferencia electrónica de datos y la llamada contratación electrónica, exigen unos presupuestos mínimos de seguridad física y lógica ya sea de equipos, ya sea de sistemas de comunicaciones, ya sea tratamiento de la información.” (2008, p. 36)

Jesús Costas Santos sostiene que la seguridad informática trata sobre la protección “de los recursos del sistema de información” (2010, p. 19), para que estos no sean utilizados de forma errónea o no autorizada. Explica que la seguridad informática consiste en “que el acceso a la información alli contenida, asi como su modificación, sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites autorizados” (Costas , 2010, p. 19)

Existe una clara tendencia hacia la interoperabilidad e interconectividad ofrecida por las redes. Debido a esto, la seguridad de la información se ha vuelto crucial en el desarrollo de la sociedad. (Bertolín, 2008, p. 2) Las redes brindan un sistema amplio de almacenamiento de información, así como envío y recepción de la misma; por lo que la seguridad de esta información y, por lo tanto, los mecanismos que la sustentan, se han vuelto un tema de suma importancia, especialmente para el Derecho.

Los mecanismos de seguridad de la información, al inicio de su desarrollo, eran utilizados únicamente para preservar la información del gobierno, en lo que a datos militares y diplomáticos se refiere. (Bertolín, 2008, p. 2) Esto, probablemente, se debe a que el internet tuvo sus inicios como un programa que formaba parte del Departamento de Defensa de los Estados Unidos, específicamente la Agencia de Proyectos de Investigación Avanzados de Defensa, conocido también como DARPA por sus siglas en inglés.

Debido al potencial que presentaba el uso de la red, se volvió una herramienta útil en campos como el comercio. Por esto, los mecanismos de seguridad de la información, que eran utilizados anteriormente para proteger información militar y diplomática, pasaron a ser requeridos en otros campos, como las transacciones bancarias, relaciones contractuales, entre otros actos que forman parte del comercio.

Por el cambio de enfoque de los mecanismos de seguridad, de ser una herramienta para preservar la información militar y diplomática, a una necesidad social, estos han pasado a ser un elemento esencial en cualquier tipo actividad, comercial o no, que implique el uso de la red y la preservación de la información en la misma. Además, debido al impacto que ha tenido el desarrollo y, por lo tanto, el empleo de las tecnologías de la información y comunicación o TIC, la seguridad de la información se ha vuelto un tema importante, como lo dice Bertolín:

> “a través de internet, está posibilitando almacenar, procesar o compartir información. En el actual entorno competitivo de la sociedad de la información y del conocimiento, la adecuada gestión de la seguridad de la información es de vital importancia para la supervivencia de una organización.” (2008, p. 2)

Cabe entonces mencionar que la protección de la información es fundamental, especialmente al tratarse de medios electrónicos, puesto que el almacenamiento de la misma en este soporte es infinito. Al existir un

almacenamiento tan masivo es crítica su protección porque, como se mencionó anteriormente, si un tercero llegase a tener acceso a la misma, esto podría conllevar un daño significativo para sus titulares y la sociedad en general.

Con el surgimiento de las nuevas tecnologías se han creado diversas formas jurídicas, tales como los actos que forman parte del comercio electrónico, que, a pesar de contar con el respaldo del principio de equivalencia funcional, requieren de un sistema distinto de protección de la información, esto es, para darle validez y seguridad al mismo. Al tratarse de un sistema tan amplio como lo es la red, deben existir ciertos mecanismos que garanticen la seguridad de la información que se está tratando por este medio.

1.2. REQUERIMIENTOS Y SOLUCIONES DE SEGURIDAD DE LA INFORMACIÓN

Costas advierte que a pesar de que todos los elementos de un sistema informático pueden ser atacados, llámese a estos hardware o software, resulta la información, el principal objeto de protección en lo que se refiere a la matería de técnicas de seguridad. Esto se debe a que la información es el componente más sensibles dentro de un sistema informático (2010, p. 21). Al ser la red tan amplía, puede llegar a albergar todo tipo de información y si no existieren técnicas de seguridad, esta quedaría vulnerable y a libre disposicion de terceros no autorizados y sobre todo no deseados.

Esta seguridad comprende cinco aspectos fundamentales, que son: la confidencialidad, la integridad, la disponibilidad, la autenticación y, por último, el no repudio. Si en algún momento, uno de los aspectos mencionados anteriormente, llegase a verse afectado, es muy probable que los otros también sean vulnerados y por esto debe funcionar en un conjunto para que pueda existir la denominada seguridad.

Costas especifica que estos servicios de seguridad mencionados dependen jerárquicamente de otros, si no existe el menor, no se puede aplicar el superior. Es por esto que:

> “la disponibilidad se convierte en el primer requisito de seguridad, cuando existe ésta, se puede disponer de la confidencialidad, que es imprescindible para conseguir integridad, para poder obtener autenticación es implrescindible la integridad y por último el no repudio sólo se obtiene si se produce previamente la autenticación.” (2010, p. 29)

Una vez que se logra llegar al último peldaño, que es el del no repudio, entonces se puede afirmar que existe la seguridad deseada, en lo que a datos e información concierne.

A continuación se realiza una descripción de los principales requerimientos de seguridad, en contraste con la solución técnica que permite solventar cada debilidad de seguridad.

1.2.1. DISPONIBILIDAD Y LA CONSERVACIÓN DE DATOS

Es la cualidad que posee un documento o mensaje para que la información contenida en él pueda ser de libre acceso con posterioridad, a fin de que pueda ser utilizada por las partes o usuarios autorizados, siempre que lo necesiten. Es decir, tener la seguridad de que se podrá acceder a un documento o mensaje, cuando las partes lo requieran, evitando su périda o bloqueo, por la razón que fuere, así sea por terceros malintencionados, caso fortuito, fuerza mayor o mala operación del sistema, explica Costas (2010, p. 27). Este requerimiento resulta indispensable al momento de tener la pretención de presentar un documento electrónico como prueba en un juicio.

Bertolín sostiene que este requisito “protege al sistema contra determinados problemas como los intentos deliberados o accidentales de realizar un borrado

no autorizado de datos, de causar cualquier tipo de denegación del servicio o de acceso a los datos y de los intentos de utilizar el sistema o los datos para propósitos no autorizados.” (2008, p. 3)

En la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, se establece que en el caso en el que se requiera que la información sea escrita, esta condición se verá satisfecha con un mensaje de datos, siempre y cuando la información sea accesible posteriormente(art. 6). En la misma ley se determina que todo mensaje de datos podrá ser conservado, mediante el archivo del mismo, pero para eso deberá cumplir con los siguientes requisitos:

> “a) Que la información que contenga sea accesible para su posterior consulta; b) Que sea conservado con el formato en el que se haya generado, enviado o recibido, o con algún formato que sea demostrable. Que reproduce con exactitud la información generada, enviada o recibida; c) Que se conserve todo dato que permita determinar el origen, el destino del mensaje, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado; y, d) que se garantice su integridad por el tiempo que se establezca en el reglamento a esta ley. Toda persona podrá cumplir con la conservación de mensajes de datos, usando los servicios de terceros, siempre que se cumplan las condiciones mencionadas en este artículo.” (Ley de Comercio electrónico, Firmas Electrónicas y Mensajes de Datos, art. 8)

En el Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, se complementa lo mencionado ya que establece que pueden existir terceros que estén encargados de la conservación de un mensaje de datos. Este servicio incluye el almacenamiento y custodia de los mismos. Toda la infraestructura que permita dicha conservación se denomina Registro Electrónico de Datos (art.9)

1.2.2. CONFIDENCIALIDAD Y CRIPTOGRAFÍA

Sobre la confidencialidad se podría decir que “Se trata de la cualidad que debe poseer un documento o archivo para que este sólo se entienda de manera comprensible o sea leido por la persona o sistema que esté autorizado.”

(Costas , 2010, p. 23) Es decir, un documento es confidencial cuando, únicamente, las partes intervinientes pueden tener acceso a su contenido, para que, de esta manera, un tercero no autorizado no pueda obtener la información contenida en el mismo. Es por esto que este elemento resulta imprescindible, como lo explica Lorenzetti, ya que al tratarse de un medio como lo es la red, se presentan riesgos importantes por parte de terceros. (2001, p. 81)

Entonces, cabe decir que, este requerimiento de seguridad resulta indispensable, especialmente en lo que se refiere a mensajes de datos. En la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos se define al mensaje de datos como:

> “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 ennumeración limite su definición, los siguientes: documentos electrónicos, registros electrónicos, correo electrónico, servicios web, telegrama, telex, fax e intercambio electrónico de datos” (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, disposición general novena).

La confidencialidad es una herramienta necesaria, especialmente en el campo del comercio electrónico. En esta área, normalmente, se maneja información delicada, como datos bancarios o simplemente una propuesta de negocio. Esto se convierte en información delicada, porque si un tercero no autorizado llegase a tener acceso a esta información, podría apropiarse de la propuesta de negocio o informar sobre la misma a la competencia directa. Sin embargo, el

empleo de documentos electrónicos en la actualidad, abarca prácticamente todos los ámbitos.

La solución ofrecida a este requerimiento es la criptografía; Fernández explica que “Etimologicamente el lenguaje críptico, equivalente a secreto o enigmático (cabe también su aplicación a un lenguaje profesional o técnico) deriva de dos palabras griegas kryptos, oculto y grafo, escritura que resulta suficientemente indicativo.” (2006, p. 82) Por lo cual se podría afirmar que la criptografía es un mecanismo de comunicación basado en la privacidad, ya que al encriptar un texto, este se vuelve ininteligible para terceros que no estén autorizados a leer el contenido del mismo. Es una forma de ocultar la informacion del mensaje y asegurarse de que solo personas autorizadas tengan acceso al contenido.

Las técnicas de cifrado, es decir, la criptografía es parte de la criptología, que es el área de conocimiento como ciencia, que a su vez también incluye el criptoanálisis. Ésta área se dedica al estudio de los métodos que se emplean para romper el cifrado de los textos, en el caso en el que no exista la o las claves, para, de esta manera, poder recuperar la información original. (Costas , 2010, p. 236)

El objeto de protección de la criptografía es la información original, la que se desea mantener oculta de terceros no autorizados, esta se denomina texto en claro o texto en plano. El proceso que se realiza para ocultar el mensaje o el documento, se llama cifrado y lo que hace es convertir el texto en claro en un galimatías ilegible que se denomina criptograma o mensaje cifrado. “Por lo general, la aplicación concreta del algoritmo de cifrado (también llamado cifra) se basa en la existencia de una clave” (Costas , 2010, p. 237) La clave es información secreta, que cuando se aplica al texto cifrado, deshace este proceso y así el texto se vuelve legible nuevamente. A este proceso se lo conoce como descifrado. A la final, lo que utiliza el usuario es un criptosistema, que se constituye por un conjunto de protocolos, algoritmos de cifrado, actuación de los usuarios y procesos de gestión de claves. Los protocolos criptográficos detallan la forma en la que se usan los algoritmos y las claves.

Existen dos tipos de criptografía, la simétrica y la asimétrica. La primera es aquella en la que se utiliza una única clave para cifrar y descifrar mensajes. Para esto es necesario que las partes hayan establecido previamente cual será la clave que utilizarán en el intercambio de información. Lo más importante resulta ser la clave, versus el algoritmo que se emplea en conjunto con la misma para cifrar el mensaje, o por lo menos así se manejaría un buen sistema de cifrado. Aunque pareciere obvio, resulta entonces primordial que la clave que se utilice debe presentar una alta dificultad al momento de intentar adivinar, esto se logra mediante un abanico amplio de claves posibles. (Costas , 2010, p. 239)

En este sistema de criptografía lo complicado no recae sobre la seguridad del mismo, como lo expresa Costas, sino sobre el intercambio de claves. Esto se debe a que si se llegase a interceptar el envío, entonces el sistema quedaría vulnerable puesto que terceros no autorizados tendrían conocimiento de la clave. No existe un canal de comunicación lo suficientemente seguro como para garantizar que un tercero no hubiere podido acceder. (2010, p. 240)

En el sistema de criptografía de clave asimétrica cada usuario tiene en su posesión un par de claves que resultan ser complementarias, una privada y una pública. La privada solo la conoce el propietario, es decir que no la puede conocer otra persona, mientras que la pública deberá ser y será conocida por todos los usuarios. La clave pública del receptor es la que cifra el mensaje y la clave privada del mismo es la que lo descifra. A la final, con este sistema se logra evitar el inconveniente de envío de clave como en el sistema asimétrico y de esta manera se garantiza la confidencialidad y la integridad del mensaje enviado(Costas, 2010, p. 242). El tema de la autenticación y no repudio se tratará más adelante al hablar de la firma digital.

1.2.3. AUTENTICACIÓN

La autenticación “es la situación en la cual se puede verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice”

(Costas, 2010, p. 28). Este escenario se produce cuando el emisor de un mensaje o documento, puede probar de alguna forma, que en efecto es quien dice ser y que es el real emisor del documento o mensaje en cuestión. Una vez que se logra dicha autenticación, el emisor se considera como un usuario autorizado.

Cotidianamente, la autenticación se produce mediante un login que también se conoce como usuario y una contraseña o password (Costas , 2010, p. 28). A modo de resumen, la autenticación resulta ser la capacidad de determinar la autoría y emisión del mensaje o documento. Este requerimiento de seguridad se encuentra ligado íntimamente con el de confidencialidad, pero sobre todo con el de integridad.

Una de las soluciones que se encontró para la correcta autentificación son los medios biométricos. “Definimos a la **Biometría** como *la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos.* [cursivas y negrillas en el original]” (Costas , 2010, p. 55) El mismo autor añade que, la tecnología utilizada en la Biometría “realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas.” (2010, p. 55)

En este tipo de medios, la identificación recae en la comparación de las particularidades físicas de las personas. Para esto se crea un patrón conocido que se guarda en una base de datos y así cada vez que se identifique la característica o particularidad, esta permite el acceso necesitado. (Costas , 2010, p. 56)

Entre los beneficios de la utilización de este sistema se encuentran la optimización de los recursos de administración puesto que solo se necesita la instalación y mantenimiento de los equipos, mientras que al utilizar una tarjeta o una clave, esta se puede perder. De esta misma manera cabe mencionar que las características biometricas de cada persona son intransferibles y así se evita el acceso de personas no deseadas. (Costas , 2010, p. 56)

Los sistemas biométricos más conocidos son: el lector de huellas digitales, de iris y el de emisión de calor. Este último se basa en la medición del calor corporal de la persona, dibujando así un mapa de los valores que muestre el medidor de calor. (Costas, 2010, p. 56) Adicionalemnte existen otras soluciones para el tema de la autenticación, como lo son los usuarios y las claves, las tarjetas magnéticas y, de manera obiva, la firma digital.

1.2.4. INTEGRIDAD, NO REPUDIO Y FIRMA DIGITAL

Se dice que un documento cuenta con integridad cuando no ha sido alterado y permite la comprobación de que el mismo no ha sido manipulado de ninguna manera. A través de la correcta implementación de este requerimiento, es decir, una vez que se compruebe que el mensaje o documento no ha sido alterado de ninguna manera, se puede proceder a la autenticación del mismo. Si primero se hiciere la autenticación y resultare que el mensaje o documento se ha manipulado, entonces la identificación del emisor resulta irrelevante. Es por esto que la confidencialidad es primordial, porque es el primer paso para poder asegurar la integridad del mensaje.

Sobre la diferencia entre la autenticación y el no repudio de un mensaje de datos, Costas explica que el no repudio “es un servicio de seguridad estrechamente relacionado con la autenticación y permite probar la participacion de las partes en una comunicación. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de no repudio se produce frente a un tercero” (2010, p. 28).

En otras palabras, la autenticación se produce entre las partes que participen en el envío y recepción del mensaje o el documento, mientras que el no repudio se aplica en el caso en el que exista un conflicto con respecto a la identificación del emisor y su vinculación con el contenido ante un tercero que resolverá dicho conflicto. Costas sostiene que la autenticación recae sobre el

autor del documento y su destinatario, mientras que el no repudio prueba el envío y la recepción del mismo (2010, p. 29).

El no repudio es un tipo de garantía sobre la identidad del emisor y su vinculación al contenido, en el que dicha parte no puede negar su participación. Por este principio se presume que el emisor es quien dice ser y que el envío del mensaje o el documento fue voluntario. Esto se produce cuando el receptor recibe una prueba suficiente de que el emisor es en efecto el emisor legítimo del mensaje. En caso de que se iniciare un juicio al respecto, la prueba recaería sobre el emisor y no el receptor debido al no repudio.

Existen dos posibilidades de no repudio, la primera, explicada en el anterior párrafo, que recae sobre el emisor y se denomina no repudio en origen y la segunda que recae sobre el receptor, no repudio en destino. Esta última explica que el receptor no puede negar la recpeción del mensaje o el documento, debido a que el emisor tiene pruebas de la recepcion del mismo. El servicio de no repudio en destino, descarta la posibilidad de que el receptor niegue la recepeción del mensaje o documento y así su vinculación al mismo. Si llegase a existir un desacuerdo sobre la recepción, entonces la prueba recaería sobre el receptor, bajo este precepto de seguridad mencionado. (Costas , 2010, p. 29)

La solución brindada a estos requerimientos es la firma digital, que, como se verá a continuación, es el mecanismo idóneo para asegurar la integridad del mensaje y el requerimiento de no repudio. Al ser la firma digital el equivalente de la firma manuscrita, adquiere las mismas garantías que esta y esto quiere decir que si una parte firma digitalmente, no puede negarlo. Al firmar se entiende que la parte está de acuerdo con el contenido y que recibió y envió la información. Es un tipo de presunción que también se encuentra en la firma manuscrita.

Devoto afirma que la verificación de la firma digital no solo ayuda con la identificación del mensaje, sino con la comprobación de la integridad del

mismo. El proceso de esta verificación consiste en que el emisor prepara un digesto del mensaje, que es un resumen del mismo, mediante la utilización de un algoritmo de control seguro. Este resumen también es enviado al receptor, el cual al recibir el mensaje completo debe realizar otro digesto del mismo mensaje. Acto seguido se comparan los dos resúmenes y si coinciden a la perfección, entonces se asegura que el mensaje no ha sido alterado y así se cumple con el requerimiento de integridad. Entonces, con el programa de verificación se aseguran dos cosas, la primera, que el emisor es quien dice ser y que utilizó su clave privada para firmar el documento por lo que se presume que el documento no ha sido alterado. (2001, p. 170-171)

1.3. FIRMA DIGITAL

La firma es un mecanismo idóneo de protección de los mensajes de datos. El uso de dicha firma es esencial en cualquier ámbito en que se empleen documentos electrónicos, puesto que provee de veracidad, autenticidad, confidencialidad y no repudio al mensaje de datos.

Al ser la red tan amplia e impersonal es necesario contar con un mecanismo de identificación seguro y es por estas razones que la firma digital adquiere la importancia que posee.

1.3.1. ANTECEDENTES

El origen de la firma digital se remonta a una oferta tecnológica por parte de Diffie y Hellman, en la que se proponía acercar la forma social de operar de la firma manuscrita a lo que se denominó como el trabajo en redes(Formentín Zayas, 2013, p. 106). Diffie y Hellman desarrollaron una técnica que se llamo “acuerdo de distribución de claves”, mediante la cual dos partes que no hubieren tenido comunicación previa puedan llegar a un acuerdo sobre una clave asimétrica. Esto se logró mediante la empleación de un algoritmo en el cual se utiliza una función unidireccional con trampa, que a cada valor de “x” le otorga un valor de “y”. Entonces, al saber el valor de cualquiera de las dos

variables se puede saber la otra, pero resulta difícil para un tercero que no conozca ninguno de los valores (Formentín Zayas, 2013, p. 106).

Existió, después, un importante progreso en el tema; en 1976 Diffie y Hellman descubren lo que se llamaría la criptografía de clave pública, marcando un precedente para la firma digital. Posteriormente, en 1977, Ron Rivest, Adi Shamir y Len Adleman crean el sistema criptográfico de clave pública que, en la actualidad sirve para firmar y cifrar digitalmente un documento; éste método se denomina RSA, por las siglas de los creadores. (Formentín Zayas, 2013, p. 106).

1.3.2. DEFINICIÓN

Conforme al principio de equivalencia funcional, la firma digital produce los mismos efectos que la firma manuscrita, entendida ésta última como: “el vocablo firma proviene del latín “firmare” que significa afirmar, dar fuerza, y el vocablo autógrafa significa grabar o escribir por si mismo, se aplica a un escrito realizado por la mano del propio autor de los signos o trazos sin que para ello se acuda a ningún tipo de medio mecánico” (Nieves, 2009, p. 76). Al ser la firma digital el equivalente de la firma manuscrita, se le podrían aplicar las mismas características señaladas por el autor.

Complementando, Jesús Ignacio Fernández Domingo explica que la firma “es un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje.” (2006, p. 37-38) Para el mismo autor es necesario que la firma cumpla con ciertos requisitos para que pueda ser considerada como el equivalente de la firma manuscrita, como serían el poder vincular el mensaje de datos al firmante, esto lo denomina como identidad; la integridad, es decir, que exista la certeza de que el mensaje no fue alterado; la no repudiación, que en otras palabras explica que el firmante no puede negar su firma ni el vínculo existente con el mensaje de datos y la confidencialidad, explicada como la seguridad de que el mensaje no pueda ser

leído por terceros no autorizados. Este último requisito no es esencial, pero si accesorio conforme al autor. (Domingo, 2006, p. 38)

Siguiendo la misma línea de pensamiento, la Ley Modelo de la Comisión de Naciones Unidas para el Derecho Mercantil Internacional, en su artículo 7, ennumera asimismo las características que debe reunir la firma, y establece como tales, la posible identificacion de la persona y el vínculo aprobatorio que esta tiene con el mensaje de datos y la fiabilidad del método empleado para la creacion de la firma. (Ley Modelo CNUDMI, art. 7)

La firma digital "está basada en los sistemas de criptografía de clave pública (PKI – Public Key Infrastructure)" (Costas , 2010, p. 253). Es ésta firma la que se utiliza generalmente y que se almacena en soportes de *hardware* y *software*, mientras que la firma electrónica es almacenada en soportes de *hardware* (Costas , 2010, p. 253). El *hardware* está compuesto por todos los elementos fisicos que posee un sistema informático, como por ejemplo el CPU y los medios secundarios de almacenamiento que vendrían a ser las memory flash o los CD-ROM, entre otros. Por otro lado, el *software* es lo que hace que el *hardware* funcione, son el conjunto de programas lógicos, como serían sistemas operativos, aplicaciones, entre otros. (Costas , 2010, p. 30)

A modo de resumen, la firma digital es un conjunto de datos ordenados lógicamente que sirve para vincular a una persona al contenido del mensaje de datos y asegurar la identidad del mismo, siempre y cuando esta cumpla con los requisitos antes mencionados, utilizando el sistema de criptografía asimétrica. Es por esto que se logra realmente llegar a una equivalencia funcional óptima con la firma manuscrita, debido a que se cumplen con los requisitos preestablecidos para otorgar efectos y seguridad jurídica a las mismas.

1.3.3. PROCESO DE FIRMA DIGITAL

Debido a que la criptografía asimétrica asegura la confidencialidad y la integridad, pero no la autenticación y el no repudio, se utiliza la firma digital

para estos fines. Como lo explica Costas, el emisor decide escribir un mensaje al receptor, pero para que este compruebe la identidad del emisor, este debe firmarlo. Para esto el emisor resume el mensaje, mediante lo que se denomina una función hash. Para Devoto:

> "esta función consiste en un proceso matemático, basado en un algoritmo que crea una representación digital o forma comprimida del mensaje, a menudo conocida con el nombre de "digesto de mensaje" o "huella digital" del mensaje, en forma de un "valor control" o "resultado control" de una longitud estándar que suele ser mucho menor que la del mensaje, pero que es no obstante esencialmente única al mismo." (Devoto, 2001, p. 169-170)

En otras palabras, es una función que permite resumir un texto, mediante algoritmos en una representación alfanumérica y así se puede comprobar que el texto recibido es el mismo que el enviado.

Después de haber utilizado la función hash, se procede a cifrar el resultado con su clave privada, para, de esta manera, obtener su firma digital. Se procede a enviar el mensaje firmado al receptor, quien descifra el resumen utilizando la clave pública del emisor; aplica la función hash al mismo mensaje y si los resúmenes coinciden, entonces el receptor puede estar seguro de que en efecto fue el emisor quien envío el mensaje. Adicionalmente, el mensaje que se envía se cifra con la clave pública del emisor para que el mismo lo descifre con su clave privada. De esta manera se asegura la confidencialidad, la integridad, la autenticación y el no repudio.

1.3.4. INFRAESTRUCTURA DE CLAVE PÚBLICA

Existen varios elementos dentro del proceso de intercambio de información y especialmente en el ámbito del comercio electrónico, que hacen que los usuarios desconfíen, especialmente en lo que se refiere a firmas digitales. Entre estos elementos se encuentran, por ejemplo, la posibilidad de que las

partes no tengan una relación de confianza puesto que han realizado pocas o ninguna transacción entre ellas, o el hecho de que el sistema de clave pública utilizado en las firmas digitales sea altamente matemático lo que puede tener como resultado la desconfianza de los usuarios en el sistema.

Es por esto que una de las soluciones otorgada a este problema de desconfianza es la utilización de uno o más terceros de confianza. Estos terceros de confianza, que se denominan generalmente proveedor o prestador de servicios de certificación o autoridad certificante, sirven para ayudar a vincular a una persona o firmante a una clave pública determinada, conforme a lo que explica Devoto y prosigue diciendo que cuando dichas entidades son organizadas jerárquicamente, se denomina insfraestructura de clave pública o PKI, como sucede en algunos países.

El prestador de servicios de certificación vincula el par de claves proveido a un usuario mediante un certificado. En este registro constan la clave pública y el nombre del usuario y así se confirma que el sujeto dueño de la clave pública posee la clave privada respectiva y de esta manera se confirma la entidad del firmante. (Devoto, 2001, p. 171)

Entre las garantías que ofrece una infraestructura de clave pública se encuentran las siguientes:

> “1) gestión de las claves criptográficas utilizadas para las firmas digitales; 2) certificación de que una clave pública corresponde a una clave privada; 3) provisión de claves a usuarios finales; 4) establecimiento de los privilegios que tendrán los diversos usuarios de un sistema; 5) publicación de un directorio seguro de certificados o claves públicas; 6) administración de contraseñas personales[…] que permitan identificar al usuario con información de identificación personal singular o que permitan generar y almacenar claves privadas individuales; 7) comprobación de la identificación de los usuarios finales y prestación de servicios a estos; 8) prestación de servicios de repudio

> negativo; 9) prestación de servicios de marcado cronológico; 10) gestión de las claves de codificación utilizadas con fines de confidencialidad en los casos en que esté autorizado el empleo de esta técnica.” (Devoto, 2001, p. 172)

Entonces, un sistema PKI contribuye a fortalecer la confianza entre las partes y certificar la entidad del firmante.

La forma de organización de una infraestructura de clave pública depende de cada Estado, ya que se toman en cuenta distintas cuestiones técnicas o de orden público. En algunos países el modelo utilizado se basa primero en una entidad que certifica la tecnología y prácticas, al resto de entidades que están autorizadas a emitir certificados o claves; las segundas son entidades que certifican que las claves públicas y privadas se corresponden la una a la otra; en tercer lugar se encuentran las entidades que reciben las solicitudes de los usuarios para la obtención de una clave pública y privada o certificados que tengan que ver con el uso de las mismas. (Devoto, 2001, p. 172)

En Ecuador, la emisión de firmas electrónicas se considera un servicio electrónico regulado, por lo que la infraestructura PKI involucra la participación del Estado, a través de la Agencia de Regulación y Control de las Telecomunicaciones (antes CONATEL), para acreditar a las entidades de certificación de información, que son las únicas autorizadas para emitir firmas electrónicas.

1.3.5. PROBLEMÁTICA: LO ELECTRÓNICO VS. LO DIGITAL

El artículo 13 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos ecuatoriana define a la firma electrónica como:

> “Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje

> de datos e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos."(Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 13)

Existen varios autores que sostienen que la firma electrónica es una expresión genérica. Explican que resulta ser un concepto indefinido y amplio visto del punto de vista de la tecnología como lo explica Costas (2010, p. 253). En el mismo sentido, Miguel Ángel Moreno, dice que la firma electrónica no obedece a una determinada técnica y por esto resulta ser un término más genérico (2002, p. 156).

Rubio, Rodríguez y Muñoz afirman que "el concepto de firma electrónica engloba un conjunto de mecanismos técnicos a través de los cuales se pretende conseguir jurídicamente una equivalencia funcional en mayor o menor grado con la firma manuscrita" (2004, pág. 17). Es decir, la firma electrónica es lo mismo que la firma manuscrita, pero ésta debe cumplir con ciertos requisitos para cumplir con las funciones con las que cumple la firma manuscrita.
Sobre los requisitos y funcionalidad de la firma electrónica, Ana Yasmín Torres afirma que:

> "mediante la firma electrónica se le permite al receptor de unos datos transmitidos por medios electrónicos (documento electrónico) verificar su origen (autenticación) y comprobar que están completos y no han sufrido alteración (integridad). Es decir, se acredita la autoría (genuidad) y la integridad del contenido (autenticidad) del documento electrónico." (Torres, 2012, p. 67)

El Dr. Santiago Acurio del Pino sostiene que entre la firma electrónica y la firma digital existe una relación género especie; al hablar sobre firma digital se hace referencia a una firma electrónica basada en una infraestructura de clave pública. Considera que "nuestra ley tiene que siempre ir por la generalidad, porque va a regular lo que está ahorita a lo que puede venir. Entonces por el principio de neutralidad tecnológica, la ley ecuatoriana hace referencia a la

firma electrónica, porque puede ser que después de algún tiempo cambie la tecnología para generar la firma y automáticamente esa ley quedaría en desuso.” Adicionalmente sostiene que la ley no debería ser actualizada, puesto que, bajo su punto de vista, esta debe ser general. (Acurio, comunicación personal, 24 de febrero de 2016).

Por su parte el Dr. José Luis Barzallo, uno de los redactores de la ley que regula la firma electrónica en el Ecuador, explica que en el borrador de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos se diseñó un concepto de firma electrónica, sin embargo, explica que en el proyecto de ley existía un artículo referente a la firma digital, pero fue sustituido por uno que trata sobre empresas unipersonales. Describe que en las disposiciones de la Ley se puede observar que se habla sobre la no discriminación a otros tipos de firma electrónica y que, bajo este pensamiento, la firma digital era aceptada en la ley. Pero al eliminar este artículo se creó un vacío en la misma. (Barzallo, comunicación personal, 25 de febrero de 2016)

Devoto explica que existe cierto sector de la comunidad jurídica, así como una parte de la legislación extranjera que sostiene que entre la firma electrónica y la firma digital no existe más que una relación género-especie, siendo la electrónica el genérico y lo digital lo específico (2001, p. 165-166). Sin embargo, el autor procede a aclarar que en realidad los especialistas sostienen que esta no es la posición correcta con respecto al tema de firmas.

> “Aunque es cierto que cuando la firma digital se encuentra momentáneamente almacenada en la memoria volátil de una PC (“RAM”) los dígitos de una firma digital consisten en magnitudes eléctricas, también es cierto que cuando se encuentra almacenada en el disco duro (magnético) de la PC consiste en campos magnéticos, cuando se encuentra perdurablemente almacenada en un CD-ROM consiste en agujeros perforados en la capa de aluminio del CD y cuando es transmitida por una fibra óptica de telecomunicaciones consiste en fotones.” (Devoto, 2001, p. 166)

Es decir que, así como la firma digital consiste en magnitudes eléctricas, existen otros tipos de tecnologías que también son aplicables, como lo son la mecánica, magnética, óptica, entre otras. Entonces cabría decir que al hablar de firma electrónica se estarían discriminando los tipos de tecnología mencionados, puesto que se encasilla a la firma a un solo tipo de tecnología que es la eléctrica y es por esto que nacería una contradicción al principio de neutralidad tecnológica, el cual se tratará adelante. Este criterio determinó que la ley Argentina distinga la firma digital de la firma electrónica.

Por otro lado, el uso de la firma digital brinda mayor seguridad a las partes involucradas, puesto que como se vio anteriormente, la firma digital está basada en un sistema de criptografía de clave pública y es por esto que resulta el mecanismo idóneo al momento de intercambiar mensajes de datos o información, asegurándose que terceros no autorizados no puedan acceder al mismo. Incluso, en la Ley 25.506, de Argentina, se establece que la firma electrónica es el "conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, *que carezca de alguno de los requisitos legales para ser considerada firma digital.* [cursivas añadidas]" (Ley 25.506, art. 5)

Adicionalmente, como lo explica Formentín, sobre la diferencia entre la firma electrónica y la digital, esta recae:

> "en el alcance que ofrece cada reglamentación y en el mecanismo de seguridad que se utilice para garantizar sus características. En este sentido, si se parte del hecho de avalar la integridad, autenticidad e identidad de un mensaje, el término firma electrónica (a excepción del Ecuador) se utiliza para regular las formas de firmas que no se enmarcan dentro del sistema de criptografía asimétrico, y el término firma digital para aquellas formas que sí cumplen con los parámetros que implica la utilización de este criptosistema." (Formentín Zayas, 2013, p. 111)

Por lo mencionado anteriormente, y a modo de resumen, cabe decir que, a pesar de que existan numerosas obras y algunas legislaciones que sostengan la relación género-especie de la firma electrónica y la digital, al referirse a lo electrónico se trata un tipo de tecnología específico. Esto quiere decir que se extingue la posibilidad de abarcar otras tecnologías existentes o venideras, como los ejemplos mencionados con anterioridad. Lo electrónico es discriminatorio y los países miembros de las Naciones Unidas, que utilicen la Ley Modelo de la CNUDMI como ejemplo, en donde se especifica el principio de neutralidad tecnológica, no deben legislar sobre la firma electrónica, porque se contradice con los estándares internacionales preestablecidos.

CAPÍTULO II

2. REGULACIÓN JURÍDICA DE LA FIRMA DIGITAL

2.1. NECESIDAD DE REGULACIÓN

Devoto afirma que:

> "el desarrollo de las TIC impactará en todos los órdenes de la vida, alcanzando a todas las personas, exigiendo el desarrollo de nuevas estrategias a nivel país y nuevas estrategias para las empresas, la adquisición de nuevos conocimientos para nuevos tipos de trabajos, exigiendo el replanteo de muchas profesiones y actividades." (Devoto, 2001, p. 6-7)

Es decir que conforme se desarrollen las TIC deben desarrollarse otros ámbitos de la vida como: el trabajo, los estudios, las estrategias de un país y de las empresas, así como las regulaciones que permiten crear una base para las mismas. La revolución digital permite que las empresas locales participen a nivel mundial en actividades de comercio, esto les otorga un posicionamiento internacional, por lo cual, a parte de que se genera un mayor rango de actividades, la producción crece. La distancia va perdiendo importancia, mientras que la accesibilidad, confidencialidad e identificación de los participantes se vuelven más importantes.

Por otro lado, el desarrollo de las TIC puede conllevar al desempleo, a la atrofia de la mente y a la invasión a la privacidad como lo explica Devoto (2001, p. 9). Para que todo funcione correctamente debe existir, no solo el desarrollo de la tecnología, sino también una legsilación que ayude a controlar, supervisar y regular las actividades correspondientes. Para esto, sin embargo, lo fundamental resulta ser el conocimiento "saber elegir y combinar los mejores ingredientes, adecuándolos al cliente y su circunstancia." (Devoto, 2001, p. 11)

No es idoneo pensar que las TIC solamente brindan herramientas que se deben adaptar a lo ya conocido, puesto que a veces son las actividades mismas las que cambian y no solo las herramientas utilizadas. Es por esto que si el enfoque recae únicamente en lo tecnológico, resulta peligroso, pues es en realidad una estrategía la que se debe seguir. Se debe apuntar a la mayor armonización posible, teniendo todos los elementos en consideración. Por ende, la regulación de las actividades también debería ser considerado parte de la estrategia que se persigue y una muy importante.

En la Ley Modelo sobre Comercio Electrónico de la CNUDMI se menciona que una de las razones para la creación de esta ley fue que el número de transacciones realizadas por medios electrónicos, en el ámbito del comercio internacional, había crecido sustancialmente. Adicionalmente, se indica que todos los países, especialmente aquellos en desarrollo, mostraban un gran interés en el desarrollo y progreso amplio del derecho mercantil internacional. En el año 1985 se emitió la recomendación aprobada por la Comisión que, al igual que la resolución 40/71 del mismo año, establece que, cuando así lo requieran, los países deberán adoptar medidas para brindar seguridad jurídica al procesamiento automático de datos, dentro del comercio internacional (Ley Modelo CNUDMI, p. 1).

Como se establece en el primer capítulo, la firma digital cumple con los requerimientos de seguridad necesarios. Y al ser la firma en general el método utilizado para vincular a la persona con un texto y por lo tanto para manifestar la voluntad de obligarse conforme a lo que se establezca, resulta indispensable la creación de un método equivalente para el comercio electrónico, que como se ha mencionado, ha adquirido cada vez mayor fuerza. Al hablar de firma y de cómo esta sirve para garantizar la autoría, las personas, usualmente, se hacen la idea de la firma manuscrita, pero con las nuevas tecnologías y los nuevos modos de transaccionar electrónicamente resulta obvio que la firma manuscrita no puede utilizarse en este ámbito. Es por esto, que se crea el equivalente funcional de la firma manuscrita, que es la firma digital. (Formentín Zayas, 2013, p. 105-106)

La firma digital ha sido producto de una evolución tecnológica constante. Sin embargo, cabe recalcar, que la evolución no ha sido únicamente en el ámbito tecnológico, sino, también en el jurídico, pues al crear un tipo de firma equivalente a la manuscrita, se deben crear las regulaciones pertinentes para la misma. Especialmente al tratarse de un elemento que forma parte de una red tan amplia como lo es el comercio electrónico.

Lo primero fue establecer los conceptos de una firma digital, pues, al variar la legislación en cada país, aquellos también varían, aunque sea en forma mínima. Lo que resulta importante es que el aporte que otorgan los conceptos es la conexión que existe entre la voluntad de la persona y la firma, así como del firmante con la misma. Esto se debe a que en la firma manuscrita es fácil identificar al firmante, puesto que se conforma de rasgos únicos, pero la firma digital se compone de dígitos y bits, por lo cual no existe un trazo único que identifique al firmante (Formentín, 2013, p. 106-108). Está claro que las partes pueden acordar distintos tipos de identificación de las mismas para sus transacciones, pero “la falta de generalidad de esta norma y la inseguridad jurídica que sugiere el uso de medios no contemplados por la ley obstaculiza el desarollo de esta nueva tecnología”. (Formentín Zayas, 2013, p. 108)

2.2. PRIMERAS INICIATIVAS DE REGULACIÓN

Existe una importante actividad en lo que respecta a la regulación del tema de las nuevas tecnologías, especialmente sobre el problema de la autenticidad y no repudio, que son otros requerimientos de seguridad con los que cumple la firma digital. Las primeras regulaciones que sirvieron de modelo para las posteriores son: la Ley del Estado de Utah y la Ley Modelo de la CNUDMI (Formentín Zayas, 2013, p. 112-114). Mientras que la Ley Modelo, por ser un modelo, contiene disposiciones muy generales para que pueda ser aplicada por los Estados miembros de la ONU, la Ley de Utah es más específica y trata varios temas más a fondo, como se verá posteriormente.

Al tratarse la red de un sistema tan amplio de comunicación, especialmente en lo que se refiere a comercio electrónico, se generan varias dudas por los medios utilizados en el mismo. Los problemas que se plantean son a los que se refieren los requerimientos de seguridad, que, como se demostró, se solucionan con el uso de la firma digital, al dotar de confidencialidad al mensaje de datos, brindar un sistema efectivo de identificación, ayudar a confirmar la integridad del mensaje y asegurar el no repudio del mismo (Formentín Zayas, 2013, p. 112).

Sin embargo, aunque existan herramientas técnicas para solucionar estos inconvenientes, en el ámbito jurídico todavía existen vacíos, como lo explica Formentín Zayas (2013, p. 112). Estos vacíos generan incertidumbre y dudas sobre “la validez y eficacia de las transacciones electrónicas” (Formentín Zayas, 2013, p. 112), es por esto que la regulación jurídica de la firma digital resulta crucial, especialmente para su aplicación en el comercio electrónico.

2.2.1. LA LEY DE UTAH

En lo que se refiere a la regulación de la firma digital en el derecho interno, Estados Unidos es pionero en el tema y aunque se rijan bajo leyes estatales no unificadas, se pueden extraer ideas básicas de todas, como lo son “la voluntariedad del sistema, la equivalencia del documento electrónico y el escrito convencional y la equivalencia de la firma electrónica con la firma escrita.” (Formentín Zayas, 2013, p. 114) La primera ley aprobada en Estados Unidos fue la Ley del Estado de Utah. Esta ley no solo sirvió como precedente para otros estados del país, sino también sirvio como ejemplo para Alemanía, Francia, Argentina y posteriormente la Unión Europea (Formentín Zayas, 2013, p. 114).

Cabe mencionar que la ley en cuestión va conforme a las normas de la American Bar Association (ABA). Esta asociación, cuenta con un comite llamado Information Security Committee of the Electronic Commerce Division, Section of Science and Technology, que fue responsable de emitir la Guía para

la Firma Digital. Esta guía no fue hecha como ley, si no como un texto de asistencia para la redacción o interpretación de leyes (American Bar Association, 1996, p. 23). Debido a que la Ley de Utah fue corregida en 1996, tomando en cuenta las normas establecidas en la guía mencionada, se tratará los dos textos en conjunto.

Es en el título 46 de la Ley de Firma Digital de UTAH en el que se tratan los aspectos relativos a la firma digital y empieza por establecer los objetivos del capítulo, mencionando entre ellos que se pretende facilitar las transacciones comerciales, brindando medios electrónicos seguros para asi reducir al mínimo la falsificación de firmas digitales y el fraude en la utilización de los mismos. La falsificación de una firma digital se da cuando una persona ajena a la firma la utiliza o cuando la persona que consta en el certificado de la firma no es real (Ley de Firma Digital de UTAH, art.102,103).

Como referencia de los objetivos mencionados están los principios de interpretación dados por las normas ABA. Estos establecen que las disposiciones deberán ser interpretadas conforme a la situación y con lo que se pueda llegar a considerar sensato dentro de las mismas. Dentro de los comentarios de las normas, se determina que razonable o sensato se entiende por encontrar términos generales para aplicarlos a momentos específicos, y, así, evitar daños o la evasión de responsabilidades (American Bar Association, 1996, p. 76).

Dentro de las definiciones que ofrece la Ley de Utah, se describe a la firma digital como un método que permite transformar el mensaje, usando un sistema asimétrico de criptografía. Esto debe permitir al receptor determinar si la clave privada del emisor, empleada para cifrar el mensaje, corresponde a la clave pública, que se utiliza para descifrar el mensaje y también poder establecer que no se han producido cambios al mensaje enviado (Ley de Firma Digital de UTAH, art.103). Estas dos características de la firma electrónica se mencionan también en la Ley Modelo de CNUDMI, en la legislación argentina, española y ecuatoriana.

En lo que se refiere a los requisitos que debe cumplir la firma digital para que sirva como equivalente funcional de la firma manuscrita, se menciona dentro de esta Ley los siguientes: si la firma se puede verificar mediante un certificado, si existe la voluntad del firmante de hacerlo y si el receptor desconoce que el firmante ha infringido una de las obligaciones respecto de la firma o si el emisor no tiene la clave privada de la firma, porque no está legalmente autorizado a tenerla (Ley de Firma Digital de UTAH, art.103). Estos requisitos no restan validez a otro tipo de firmas reguladas por otras leyes, siempre y cuando exista la voluntad de las partes intervinientes de contratar entre ellos. (American Bar Association, 1996, pág. 108) En caso de que la firma utilizada no fuere confiable, el receptor asume la responsabilidad en caso de continuar con la actividad para la que decidió emplearla, en caso de que no decidiere continuar, debe notificar de manera inmediata al emisor, para que este pueda tomar las medidas necesarias requeridas por el caso (Ley de Firma Digital de UTAH, art.402).

Las normas de la ABA establecen factores para determinar si una firma es confiable o no. Entre estos factores se dice que importan los hechos que conozca la parte interesada sobre la otra parte, la información brindada en el certificado de firma digital o que hayan sido incorporados por referencia. Los hechos que pueda conocer la parte involucrada también se refiere a los antecedentes que existen entre las partes, esto también se establece como factor y adicionalmente se señala la confianza que se puede llegar a tener en la otra parte, dejando a un lado la firma digital. Otro factor determinante es el valor o importancia que pueda tener el mensaje firmado digitalmente y, finalmente, el sistema utilizado para el intercambio de mensajes también influye como factor al momento de determinar la validez de una firma digital (American Bar Association, 1996, p. 112-113).

En la Ley de Utah se establece que la firma digital es necesaria para otorgarle validez a un mensaje, de tal manera que surta los mismos efectos que un documento físico. Sin embargo, para que esto sea posible, el mensaje debe ser firmado en su totalidad y la firma debe ser verificada mediante un certificado

otorgado por una entidad certificadora autorizada. Puede resultar inecesario, pero es importante mencionar que la firma digital debe ser emitida dentro del plazo de vigencia del certificado (Ley de Firma Digital de UTAH, art.401).

La firma digital otorga validez a un documento, porque tiene efectos jurídicos como la firma manuscrita y puede ser utilizada como prueba. Adicionalmente, mediante el uso de una firma se puede entender que las partes actuarán con la mínima prudencia posible en sus transacciones, por las obligaciones que acarrea la firma, es decir, por los efectos jurídicos de la misma, por lo cual se entiende que las partes entienden lo que firman. Pero, la razón más importante de todas, es que mediante la firma se asegura que en la transacción existe la voluntad de los participantes (Ley de Firma Digital de UTAH, art.403).

Sobre los requerimientos de seguridad explicados en el capítulo primero, en las normas ABA se menciona la autenticación y se la define como un proceso utilizado para asegurar la identidad de una persona o la integridad de una información determinada. La firma digital brinda autenticación, puesto que al tener la clave pública que desencripta el mensaje enviado y encriptado con la clave privada del emisor, se asegura que en efecto fue el emisor quien firmó digitalmente el documento (American Bar Association, 1996, p. 33,53).

Siguiendo la misma línea de pensamiento, la integridad de un mensaje se da cuando se asegura que no han existido cambios en el documento, desde el momento que se envió hasta que se recibió. La firma digital sirve para corroborar la integridad de un mensaje, puesto que cualquier alteración significaría un cambio en el resumen resultante de la función Hash (American Bar Association, 1996, p. 42). Adicionalmente, en las normas ABA se menciona el requermiento de no repudio, que extingue la posibilidad de negar el envío y la recepción de un mensaje (American Bar Association, 1996, p. 54).

Sobre los certificados de firma digital, la ley de Utah establece que si este es emitido por una entidad certificadora autorizada, sirve como reconocimiento de una firma digital autenticada y la otorga de una clave pública correspondiente.

Para que el certificado cumpla con estas características la firma debe poder ser verificable y el documento debe ser firmado en el plazo en el cual el certificado se encuentre vigente (Ley de Firma Digital de UTAH, art.103).

Para que una entidad certificadora pueda emitir un certificado se deben cumplir ciertas disposiciones. Empezando por la solicitud expresa del suscriptor, la cual debe estar firmada por el mismo. Además, la entidad debe asegurarse de que el solicitante es la persona a nombre de quien se emitirá el certificado, o si quien solicita está debidamente autorizado por el suscriptor para hacerlo, que la información dada por el certificado es fidedigna, que el solicitante posee la clave privada correspondiente a la pública que se mostraría en el certificado y que la clave privada pueda usarse para la creación de la firma así como la pública para verificación de la privada. Estos requisitos resultan irrenunciables para ambas partes. En caso de que la emisión del certificado resultare deficiente, este se podrá revocar o suspender (Ley de Firma Digital de UTAH, art.302).

Siempre y cuando el certificado sea emitido por una entidad acreditada, se garantizará que el mismo no contiene información falsa, que el certificado cumple con todas las disposiciones legales necesarias y que las funciones específicas no han sido excedidas. Al ser estas garantías mínimas con las que cumple el certificado, no se pueden limitar y la entidad no se puede deslindar de las mismas(Ley de Firma Digital de UTAH, art.302-303). Adicionalmente la entidad está obligada a suspender o revocar un certificado si existiese peligro y a notificar al titular de la firma sobre cualquier situación que pueda afectar la validez o seguridad del certificado(Ley de Firma Digital de UTAH, art.303). Sobre lo que certifica la entidad ante terceros que confíen razonablemente en el contenido del mismo, se dice que la información que contiene el certificado es válida, que dicha información es completa, que existió la voluntad del suscriptor al solicitarlo y que por ende acepta el mismo y su contenido y que se ha cumplido con todas las disposiciones legales referentes al tema(Ley de Firma Digital de UTAH, art.303).

Sobre lo que garantiza el suscriptor sobre la aceptación de terceros del certificado es que él posee la clave privada que corresponde a la pública mencionada en el certificado, que toda la información que contiene el certificado es válida y veraz y que toda la información que no se contempla en el certificado, pero que fue dada por el suscriptor a la entidad para la emisión del mismo es verídica. En caso de que un reperesentante del suscriptor hubiere solicitado la emisión del certificado a nombre del mismo, este garantiza que posee la debida y legal autorización para hacerlo. Además se establece que el representante posee el mandato para firmar digitalmente a nombre del suscriptor. En caso de que a quien representa tuviere alguna limitación para firmar, se estableceran los resguardos necesarios para prevenir un exceso de las disposiciones del mandato otorgado (Ley de Firma Digital de UTAH, art.304).

En la Ley de Utah también se regula sobre el control de la clave privada. Se establece que es el suscriptor quien tiene la obligación de mantener la seguridad de la clave, siempre y cuando este acepte el certificado emitido por una entidad certificadora autorizada. Esto se da, en parte, porque la clave es propiedad del suscriptor, como lo establece la disposición 305 de la ley mencionada. La persona que obtenga la clave sin estar autorizado legalmente sera civilmente responsable por apropiación ilícita(Ley de Firma Digital de UTAH, art.306).

A parte, en la ley, se menciona el límite de confianza. El límite de confianza es aquel que se establece en el certificado y explica que se podrá confiar razonablemente en el contenido del mismo, siempre y cuando el monto de la transacción no exceda el límite plasmado en este, en cuyo caso la confianza no es razonable. La entidad certificadora no se hará responsable si la transacción excedere dicho límite. Esta última disposición será aplicable en el caso en que se hubiere originado una pérdida por un dato falso contenido en el certificado. De la misma manera se establecen límites de responsabilidad para las entidades de certificación. Los límites mencionados exoneran a la entidad de responsabilidad, en caso de que el uso de una firma falsa por parte de un

suscriptor hubiese causado pérdidas, siempre y cuando la entidad hubiere cumplido con todas las disposiciones legales a las que esta sujeta(Ley de Firma Digital de UTAH, art.309).

A modo de conclusión, la Ley del Estado de Utah fue una ley pionera en lo que se refiere a comercio electrónico. Muchas legislaciones la usaron como modelo a seguir y sirvió para marcar precedentes dentro de esta rama de derecho. Por lo cual se resalta inclusive el avanze tecnológico norteamericano y al ser este un país pionero en lo que a eso se refiere resultaría natural intentar adaptar sus disposiciones o por lo menos analizarlas. Finalmente, y como punto clave, cabe recalcar que en esta ley se reconoce a la firma digital como equivalente funcional de la manuscrita (Ley de Firma Digital de UTAH, art.401).

2.2.2. LEY MODELO DE CNUDMI

En la resolucion 2205 (XXI) de la Asamblea General de las Naciones Unidas, el 17 de diciembre de 1966, se estableció que se conformaría la Comisión de las Naciones Unidas para el Desarrollo Mercantil Internacional y se le encargó fomentar la armonización y unificación del derecho mercantil internacional. En 1984 se inició el proceso de elaboración de la Ley Modelo con el examen realizado por el secretario general de la ONU sobre un informe, llamado “Aspectos jurídicos del proceso automático de datos”. (Moreno, 2002, p. 11)
La mencionada comisión redactó la Ley Modelo sobre el Comercio Electrónico al observar que el número de las transacciones comerciales realizadas por vías electrónicas iba aumentando. Como lo menciona Horacio Férnandez Delpech, la “ley modelo fue una respuesta frente a las aplicaciones de las nuevas tecnologías a las relaciones comerciales, ofreciendo a los diferentes Estados un texto armónico y completo para la regulación de este tipo de actividades comerciales” (2001, p. 277).

Dicha ley fue aprobada el 16 de diciembre de 1996, en la 85va. sesión plenaria de la CNUDMI. La finalidad de esta ley fue ofrecer a los países una guía para la elaboración de sus legislaciones respectivas que trataren sobre ese tema. Así

mismo, dicha comisión redactó y aprobo la guía para la correcta aplicación de la Ley Modelo.

En la Ley Modelo y en la Guía de la misma, se establecen directrices generales para que los países miembros puedan adaptar su legislacion conforme a las disposiciones establecidas de base por la Ley y Guía mencionadas. En su artículo tercero establece que “Las cuestiones relativas a materias que se rijan por la presente Ley y que no esten expresamente resueltas en ella serán dirimidas de conformidad con los principios generales en que ella se inspira.” (Ley Modelo CNUDMI, art.3) Para lograr un cierto tipo de armonización es necesario contar con principios generales que puedan regular cualquier tipo de inquietud o de oscuridad legal y es por esto que en esta Ley se crean los principios de equivalencia funcional y el principio de neutralidad tecnológica.

Existen adicionalmente otros principios, como el de protección a la privacidad, libertad de comercio, libertad de información y autodeterminación, entre otros. Todos los principios mencionados serán tratados posteriormente.

En el artículo 7 de la Ley Modelo de la CNUDMI se establecen los requisitos que debe cumplir la firma en relación a un mensaje de datos; el primero trata sobre la identificación y vinculación del firmante con el texto, es decir que se debe poder identificar a la persona de manera precisa y además debe poder vincular al emisor con el texto, de manera en la que se entienda que está de acuerdo con lo enviado. El segundo requisito explica que el método debe ser fiable para todas las circunstancias del caso. Estos dos requisitos son cumplidos por la firma digital, al proveer confidencialidad, integridad, autenticación, el requisito de no repudio y disponibilidad (Ley Modelo CNUDMI, art.7). Pero, debido a la generalidad que caracteriza a la Ley Modelo, con este artículo incluso una firma escaneada podría tener validez, todo dependería del acuerdo al que lleguen las partes.

Sin embargo, en la Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico se recomienda a los Estados miembros que desarrollen equivalentes funcionales para los tipos de firmas manuscritas ya existentes (Ley Modelo CNUDMI, art.7). Adicionalmente se establecen ciertos factores que pueden tenerse en cuenta para determinar si el método seleccionado es el indicado:

> "1) la perfección técnica del equipo utilizado por cada una de las partes; 2) la naturaleza de su actividad comercial; 3) la frecuencia de sus relaciones comerciales; 4) el tipo y magnitud de la operación; 5) la función de los requisitos de firma con arreglo a la norma legal o reglamentaria aplicable; 6) la capacidad de los sistemas de comunicación; 7) la observancia de los procedimientos de autenticación establecidos por intermediarios; 8) la gama de procedimientos de autenticación que ofrecen los intermediarios; 9) la observancia de los usos y prácticas comerciales; 10) la existencia de mecanismos de aseguramiento contra el riesgo de mensajes no autorizados; 11) la importancia y el valor de la información contenida en el mensaje de datos; 12) la disponibilidad de otros métodos de identificación y el costo de su aplicación; 13) el grado de aceptación o no aceptación del método de identificación en la industria o esfera pertinente, tanto en el momento cuando se acordó el método como cuando se comunicó el mensaje de datos; y 14) cualquier otro factor pertinente." (Ley Modelo CNUDMI, art.7)

Por todo lo mencionado hasta este momento es pertinente señalar que la firma digital puede solventar muchos, sino todos los factores mencionados, asegurando la identificación y la vinculación al mensaje de datos por parte del emisor. Además resulta importante resaltar que en la Ley Modelo no se utiliza el término "electrónica" para describir a la firma.

2.3. NORMATIVA INTERNACIONAL DESTACADA

2.3.1. REGULACIÓN DE LA FIRMA DIGITAL EN ARGENTINA

Resulta importante empezar explicando que en Argentina la firma digital y la firma electrónica no son lo mismo, a pesar de que se reconoce el empleo a los dos tipos de firmas (Ley 25.506, art.1). La firma electrónica es aquella que no cumple con todos los requisitos necesarios para ser considerada firma digital, conforme lo establece el artículo 5 de la Ley 25.506, promulgada el 11 de diciembre de 2001. Por otro lado, a la firma digital se la define como el "resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control." (Ley 25.506, art. 2). Adicionalmente este artículo enumera alguno de los requisitos que debe cumplir una firma digital. Debe poder ser verificada por terceros y esta verificación debe constar sobre la identidad del firmante y la integridad del mensaje de datos, haciendo posible la identificación de cualquier tipo de alteración al mensaje de datos posterior a la firma (Ley 25.506, art.2).

En el artículo tercero de la Ley mencionada se trata el principio de equivalencia funcional, al decir que la exigencia de requerir una firma manuscrita se podrá cumplir con el uso de una firma digital (Ley 25.506, art.3). Sin embargo, en el artículo posterior se mencionan excepciones a esta disposición y por esto lo mencionado no será aplicable:

> "a) A las disposiciones por causa de muerte;
> b) A los actos jurídicos del derecho de familia;
> c) A los actos personalísimos en general;
> d) A los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes." (Ley 25.506, art.4)

Para complementar lo mencionado, en el artículo 9 de la Ley se enumeran los requisitos que debe reunir la firma digital para ser considerada válida. Primero, la firma digital debe ser creada en el periodo de vigencia que tenga el certificado digital emitido. Este certificado debe ser emitido por una entidad certificadora licenciada, como lo dice el requisito tercero. Mientras que el segundo trata sobre la verificación de los datos plasmados en el certificado y que estos vayan conforme a los datos presentados por el titular y su firma, siempre y cuando el procedimiento de verificación sea el adecuado (Ley 25.506, art.9).

Dos atribuciones adicionales que se le da a la firma digital en la Ley argentina son: cuando un documento esté firmado digitalmente o se encuentre reproducido de uno que si se encuentra firmado, será considerado como documento original y de esta manera obtiene un valor probatorio (Ley 25.506, art.11). La otra atribución trata sobre la conservación, que está ligado con el requerimiento de seguridad de la disponibilidad. Cuando se requiera la conservación de algún tipo de documento físico, el documento digital permitirá cumplir esta disposición siempre y cuando esté firmado digitalmente y se pueda acceder al mismo posteriormente. Además de estar disponible, debe ser posible verificar la hora de creación, el destino y origen del mensaje, así como el momento de envío o recepción (Ley 25.506, art.12).

En el artículo 7 se establece un principio que resulta importante, especialmente para apoyar el requerimiento de seguridad denominado no repudio, y es el principio de presunción de autoría. Esto quiere decir que se presume que el firmante es el dueño legítimo de la firma digital y por esto se respalda el requerimiento de no repudio de la misma, a menos que exista prueba en contrario, situación en la cual se entiende que la carga probatoria recae sobre quien niega la validez de la firma, es decir, el dueño de la misma (Ley 25.506, art.7).

Además se complementa esto con la presunción redactada en el artículo 10 que explica que “Cuando un documento digital sea enviado en forma automática por un dispositivo programado y lleve la firma digital del remitente se presumirá, salvo prueba en contrario, que el documento firmado proviene del remitente.” (Ley 25.506, art.10)

Es decir, que en caso de que exista un programa de respuesta automática y esta conteste un mensaje de datos enviado, entonces se presumirá que proviene del remitente del mensaje, siempre y cuando esté firmado digitalmente.

Además, se menciona también la presunción de integridad de un mensaje. Esta presunción revela que en caso de que un mensaje haya sido verificado así como la firma digital, entonces se presume que el mensaje no ha sufrido alteraciones desde que se firmó (Ley 25.506, art.8).

Sobre los certificados de firmas, la ley argentina contiene disposiciones que hablan sobre el plazo de los mismos, el reconocimiento de los certificados emitidos en el extranjero y los requisitos que deben cumplir. Es importante mencionar que antes de enumerar los datos mínimos que deben contener los certificados, se establece que deberán cumplirse aquellos requisitos que vayan conforme a los estándares internacionales y deben ser emitidos por una entidad de certificación licenciada. Los datos que debe contener un certificado son aquellos que permitan la correcta identificación del firmante y toda la información relevante del mismo, así como el plazo de vigencia (Ley 25.506, art.14).

En la legislación argentina se crea una Comisión Asesora para la infraestructura de firma digital, que tiene como función emitir recomendaciones sobre:

> “a) Estándares tecnológicos;
> b) Sistema de registro de toda la información relativa a la emisión de certificados digitales;
> c) Requisitos mínimos de información que se debe suministrar a los potenciales titulares de certificados digitales de los términos de las políticas de certificación;
> d) Metodología y requerimiento del resguardo físico de la información;
> e) Otros que le sean requeridos por la autoridad de aplicación.” (Ley 25.506, art.36)

Así lo explica el artículo 36 de la Ley 25.506. Además, esta comisión tiene el deber de consultar con los usuarios, las cámaras de comercio, entre otros, sobre los temas referentes a la firma digital y hará saber los resultados de dichas consultas a la autoridad encargada de la aplicación (Ley 25.506, art.35).
En conclusión, como se mencionó anteriormente, la legislación argentina, en lo que se refiere a comercio electrónico, utilizó como modelo la Ley del Estado de Utah analizada previamente. Y, como se dijo, en esa ley se reconoce a la firma digital como el equivalente funcional de la firma manuscrita. Es por esto que resulta lógico entender que dentro de la legislación argentina también se reconozca a la firma digital como equivalente funcional y la firma electrónica es aquella que no cumple con los requisitos necesarios para ser considerada como digital.

2.3.2. REGULACIÓN DE LA FIRMA EN ESPAÑA

En España se aprobó la Ley 59/2003 de Firma Electrónica el 19 de diciembre del 2003. Esta Ley tiene como antecedente el Real Decreto Ley 14/1999, aprobado el 17 de septiembre de 1999. Sin embargo, después de su ratificación por el Congreso de los Diputados, se acordó que a este real Decreto se lo tramite como una Ley modelo para un posterior perfeccionamiento de su texto. La Ley 59/2003 incorpora algunas novedades tecnológicas que no contempla el Real Decreto mencionado (disposiciones generales).

La legislación española describe tres tipos de firma: la electrónica, la electrónica avanzada y la electrónica reconocida. La primera es la concepción dada por la Ley Modelo de la CNUDMI, mientras que la segunda es aquella que permite la identificación del firmante al igual que la comprobación de que no ha existido alteración al mensaje de datos, así como lo logra hacer la firma digital y por último está la firma electrónica reconocida. La única diferencia entre la avanzada y la reconocida es que esta última cuenta con un certificado reconocido y es generada por un sistema considerado como seguro. Es esta última firma la que se considera como equivalente funcional de la firma manuscrita, puesto que brinda todas las seguridades necesarias para serlo. Sin embargo, no se le quitará efectos jurídicos a una firma electrónica con respecto al mensaje de datos en el que fue usada, solo porque no cumpla con todos los requisitos necesarios para ser considerada una firma electrónica reconocida (Ley 59/2003, art.3).

En esta legislación, al igual que en la argentina y en la ecuatoriana, como se verá posteriormente, el sistema idóneo para otorgar validez a la firma es el certificado otorgado por una entidad certificadora de información. Sin embargo, en lo que se diferencia esta legislación de las otras mencionadas, es que en esta se reconoce el certificado electrónico, que es un mensaje de datos firmado electrónicamente por una entidad certificadora en el cual se presentan los datos que vinculan al firmante con su respectiva firma, y el certificado electrónico reconocido (Ley 59/2003, art.6). Este último es aquel que es emitido por una entidad certificadora que cumple con todos los requisitos que se establecen en la ley, especialmente en los temas que traten sobre la autenticación, las condiciones establecidas por las partes y, por último, a las garantías que brinda la entidad y su fiabilidad. El contenido de estos es el mismo establecido en la legislación ecuatoriana, que se tratará más adelante.

En el artículo 24 de la Ley 59/2003 se trata el tema de los dispositivos usados para la creación de la firma electrónica, este dispositivo es un programa o sistema informático que se usa para aplicar los datos de la firma. Se determina que los datos de creación de la firma son únicos y son códigos o claves

privadas que forman parte del sistema criptográfico, que se usan para la creación de la misma. En el inciso tercero del mismo artículo se discute sobre las garantías con las que debe cumplir un dispositivo seguro de creación de firma, que son:

> "a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.
> b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.
> c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.
> d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma." (Ley 59/2003, art.24)

Adicionalmente, así como se regula el dispositivo de creación de la firma, también se regula el dispositivo de verificación de la misma en el artículo siguiente. Los datos que se utilizan para verificar la firma electrónica son códigos o claves públicas. Este dispositivo, al igual que el otro, es un programa o sistema informático que sirve para aplicar los datos descritos con anterioridad. Entre las garantías que debe cumplir un sistema de verificación de firma electrónica se encuentran: la fiabilidad de la verificación, que, aparte de todo, se verifique también el certificado, en lo que se refiere a la autenticidad y validez del mismo, que también exista la posibilidad de verificar la integridad del mensaje, que se pueda mostrar la identidad del firmante, entre otros más técnicos (Ley 59/2003, art.25).

Resulta interesante mencionar que en la legislación española se integra la firma electrónica avanzada a un documento de identidad que se llama documento nacional de identidad o DNI. Este documento acredita de forma electrónica la identidad del titular. Con este documento se pueden firmar

documentos tanto públicos como privados. Con este documento se acredita la identidad y todos los datos personales del titular y firmante así como la integridad de los documentos que se firmen utilizando este medio (Ley 59/2003, art.15).

Finalmente, la firma electrónica avanzada es el equivalente funcional para la firma manuscrita, conforme a lo establecido en la legislación española. La firma electrónica avanzada sirve para identificar al firmante, otorgarle autenticidad e integridad al mensaje y asegurar el no repudio del mismo. Se podría decir entonces, que la firma electrónica avanzada cumple la misma función y brinda la misma seguridad que la firma digital, la única diferencia recae en el nombre otorgado a estas.

2.4. REGULACIÓN DE LA FIRMA ELECTRÓNICA EN EL ECUADOR.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos fue aprobada el mes de abril del año 2002 y publicada en el Registro Oficial el 17 del mismo mes y año. Está conformada por consideraciones, 5 títulos que tratan los temas pertinentes al comercio electrónico y disposiciones generales. En las consideraciones de la misma se menciona que el uso de redes electrónicas ha adquirido un rol importante en el comercio y que este campo, llamado comercio electrónico, resulta de vital importancia para el desarrollo económico tanto del sector público como privado (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, consideraciones). Mediante el uso de redes electrónicas en el comercio, por el tipo de relaciones que se crea entre los usuarios, se realizan actos jurídicos, tanto mercantiles como civiles, que generan la necesidad de una regulación.

Debido a que el comercio electrónico cuenta con un carácter internacional, resulta pertinente que el país cuente con una normativa que otorgue las herramientas jurídicas necesarias para su correcta participación en el mismo. Adicionalmente, se menciona la necesidad de “impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de

diferentes medios electrónicos" (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, consideraciones), así como la generalización del uso "de servicios de redes de información e Internet, de modo que éstos se conviertan en un medio para el desarrollo del comercio, la educación y la cultura" (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, consideraciones).

2.4.1. LA FIRMA ELECTRÓNICA

En el título segundo de la Ley se trata específicamente el tema de firmas electrónicas y es por esto que en el artículo 13 se define a la firma electrónica como "los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos." (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 13) Cabe decir, entonces, que se reconocen y cumplen con los dos requisitos básicos enumerados en la Ley Modelo de la CNUDMI, que son la identificación del firmante y la vinculación y aceptación del mismo al contenido mensaje de datos. No solo se cumple con los requisitos de la ley, sino también con algunos de los requerimientos de la seguridad de la información mencionados en el capítulo primero. Estos son la autenticidad y el requerimiento de no repudio, al asegurar la identidad del firmante se asegura el primero y al vincular al mismo con el contenido del mensaje de datos, el segundo.

En el artículo 7 de la Ley se consagra un principio general que es el de información original. Se establece que un mensaje de datos se considera original si es conservado íntegramente (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 7) y en Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, en el artículo 6 se explica que la integridad de un Mensaje de Datos resulta de que el mismo se encuentre firmado electrónicamente (Reglamento a Ley de Comercio

Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 7). Es decir, la integridad, que es otro requerimiento de seguridad, se garantiza mediante el uso de una firma electrónica, conforme a la legislación ecuatoriana. Se considera que un mensaje ha conservado su integridad si su contenido no ha sido alterado y se mantiene completo.

El artículo 14 hace referencia al principio de equivalencia funcional, mencionado también en la Ley Modelo, al expresar que la firma electrónica tendrá los mismos efectos que la firma manuscrita, incluso jurídicamente. Es decir, se podrá presentar como prueba en un juicio. Sin embargo, en este artículo se especifica que "se le reconocerán los efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos." (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 14)

Por otro lado, la disposición general cuarta establece que "No se admitirá ninguna exclusión restricción o limitación al uso de cualquier método para crear o tratar un mensaje de datos o firma electrónica, siempre que se cumplan los requisitos señalados en la presente Ley y su reglamento." (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, disposición general cuarta) Esto hace alusión al principio de neutralidad tecnológica, pero lo limita al especificar que el uso de cualquier método de creación o tratado de la firma debe ser conforme a la base legal ecuatoriana. En el reglamento a la ley se menciona el principio de neutralidad tecnológica, en su artículo 10 al decir que la firma electrónica está aceptada dentro del mismo (Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 10). Además, en el mismo artículo, se enumeran principios y elementos que respaldan a la firma, estos son:

> "a) No discriminación a cualquier tipo de firma electrónica, así como a sus medios de verificación o tecnología empleada;
> b) Prácticas de certificación basadas en estándares internacionales o compatibles a los empleados internacionalmente;

> c) El soporte lógico o conjunto de instrucciones para los equipos de cómputo y comunicaciones, los elementos físicos y demás componentes adecuados al uso de las firmas electrónicas, a las prácticas de certificación y a las condiciones de seguridad adicionales, comprendidas en los estándares señalados en el literal b);
> d) Sistema de gestión que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad, transparencia y no-discriminación en la prestación de sus servicios; y,
> e) Organismos de promoción y difusión de los servicios electrónicos, y de regulación y control de las entidades de certificación.” (Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 10)

En el inciso a) se menciona que no se discriminará a cualquier tipo de firma electrónica, sin embargo, como se trató en el primer capítulo, al hablar de electrónico se discriminan otros tipos de tecnología y por ende, esta disposición legal es contraria al principio de neutralidad tecnológica. Sobre este punto se hablará en el siguiente capítulo.

El artículo 15, establece los requisitos que deben ser cumplidos por la firma para que sea válida. Entre estos se encuentran la vinculación entre el firmante y la firma, la garantía de identificación del mismo, que se asegure que los datos con los que se creó la firma estuvieron en total control de quien solicitó la firma y que el método que se usó para la creación de la misma sea totalmente confiable, seguro e inalterable, y, finalmente, que la firma este bajo control absoluto del firmante autorizado (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 15).

Enseguida se menciona que, además, en los casos en los que la firma esté vinculada a un mensaje de datos, deberá enviarse como parte lógica del mismo (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 16). El plazo de vigencia de una firma electrónica es indefinido y, sin embargo,

puede ser revocada, suspendida o anulada. La extinción de la misma puede darse por voluntad del titular, por muerte del mismo o disolución de la persona jurídica a quien pertenece o por orden de un Juez (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 18).

En el artículo 17 se mencionan las obligaciones del titular de la firma, que apoyan los requisitos previamente descritos. Estas son:

> "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." (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 17)

Cabe mencionar que la extinción de la firma no conlleva la extinción de las obligaciones contraídas previamente por el titular de la misma.

En lo que respecta a las firmas electrónicas, la legislación ecuatoriana es bastante generalizada e incluso existe cierta contradicción en lo que se refiere al principio de neutralidad tecnológica, como se explicó.

2.4.2. CERTIFICADOS DE FIRMA ELECTRÓNICA

El capítulo segundo del mismo título trata sobre los certificados de firma electrónica, que, en el artículo 20, se define como “el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.” (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 20) Es decir, que mediante este mensaje de datos se confirma y comprueba la identidad del firmante y se vincula a la firma con el mismo. Esto es respaldado por el Reglamento de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, en su artículo séptimo al explicar que la concordancia entre el firmante y la firma se verificará revisando los datos consignados en el certificado, salvo acuerdo contrario de las partes (Reglamento General a Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 7). Cabe recalcar que la vinculación que se brinda es únicamente la del firmante con la firma y no con el contenido del mensaje de datos firmado y por el cual se solicita un certificado.

Adicionalmente, en el mismo artículo del Reglamento mencionado se establece que en caso de que hubiere algún tipo de peligro con respecto a la firma, el certificado o el mensaje de datos, el emisor deberá notificar inmediatamente al receptor, para que este pueda tomar las medidas que considere necesarias. Sin embargo esto solo surtirá efecto si no se han realizado transacciones comerciales (Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 7).

Para que el certificado goce de validez, este debe contener la identificación, el domicilio y los datos de ubicación del autor de la firma, así como el método con el cual se pueda verificar la firma. Adicionalmente debe contener el plazo de validez, la firma electrónica de la entidad que emitió el certificado, el número de serie que identifica al certificado y las limitaciones del mismo. El plazo de vigencia del certificado, salvo acuerdo contractual entre las partes, se establece

en el Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y es de 2 años conforme al artículo 11.

A parte de la extinción por vencimiento del certificado, del plazo existen otras dos razones, que son por voluntad del solicitante o por extinción de la firma electrónica. La extinción se da desde la notificación a la entidad de certificación, excepto en caso de la muerte, secuestro o desaparición del titular, en ese caso será desde el momento de la muerte o la denuncia del secuestro o desaparición del mismo (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 24).

Por otro lado, la suspensión del certificado se puede dar cuando exista falsedad en los datos del firmante, un incumplimiento del contrato entre la entidad certificadora y el titular de la firma o cuando así lo dicte la Agencia de Regulación y Control de las Telecomunicaciones, antes Consejo Nacional de Telecomunicaciones. En el primer caso, la entidad deberá notificar inmediatamente al titular de la firma y revocar la suspensión una vez que se hubiere arreglado el problema o por resolución del ARCOTEL. En ambos casos la reactivación del servicio debe ser inmediata (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 26).

Para la revocación del certificado existen únicamente dos causas. La primera es en el caso en el que la entidad de certificación cese sus actividades y no exista otra que las absorba, en cuyo caso se deberá notificar con 90 días de anticipación antes del cese de las actividades; y, la segunda es en el caso de que se presente una quiebra técnica de la entidad de certificación respaldada judicialmente. En ambos casos la revocación será otorgada por la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), mientras que la suspensión es otorgada por la entidad de certificación. (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 26)

La revocación y suspensión generan efectos inmediatamente, desde su respectiva notificación. En caso de revocación, suspensión y extinción de los

certificados surtirá efectos para terceros desde su publicación, que conforme al artículo 15 del Reglamento se hará en la página electrónica determinada por ARCOTEL, la página web de la entidad certificadora y mediante un aviso que aparecerá cuando se intentare acceder al certificado mediante su respectivo hipervínculo. (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 27)

En el artículo 28 se establece que, para que exista un reconocimiento de los certificados y las firmas emitidas internacionalmente, las firmas y los certificados deben cumplir con lo estipulado en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su reglamento. Asimismo, se establece que todos los tratados y convenios internacionales suscritos buscarán la armonización en los temas tratados en esta ley, que incluye la firma electrónica y la firma electrónica (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, art. 28).

Conforme al Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, se determina que se debe crear el Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados(art. inumerado primero). Además se atribuye al CONATEL la emisión de su respectivo reglamento. En la Resolución 479-20-CONATEL-2008 se determina que dicho registro tiene como objetivo:

> “Art. 1.- La inscripción de los actos administrativos contenidos en las resoluciones emitidas por el CONATEL por las cuales se autoriza la Acreditación como Entidad de Certificación de Información y Servicios Relacionados. Art. 2.- La inscripción de terceros vinculados contractualmente con una Entidad de Certificación de Información y Servicios Relacionados Acreditados y las modificaciones posteriores que se introduzcan en dichos contratos.” (arts. 1-2)

Además, se establece como objetivo las marginaciones de “las características técnicas de operación o prestación de servicios”(art. 3), las de cancelación o suspensión, extinción, reformas o derogatorias de la Acreditación y registro de Entidades de Certificación de Información y Servicios Relacionados Acreditada y Terceros Vinculados (art. 4-5), las de “revocatorias o suspensiones de certificados de firma electrónica, cuando la Entidad de Certificación de Información y Servicios Relacionados Acreditada los emita” (art. 6) y como objetivo final establece que debe “garantizar transparencia y acceso oportuno a la información de carácter público, con sujeción a la legislación aplicable” (art. 7).

En el artículo único de la resolución 481-20-CONATEL-2008 se acredita al Banco Central del Ecuador como entidad de certificación (Resolución 481-20-CONATEL-2008, art. único). Adicionalmente, el entonces, CONATEL, ahora ARCOTEL, determina que el valor que se deberá pagar para la acreditación de una entidad de certificación es de veinte y dos mil DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA (Resolución 480-CONATEL-2008, art. 1).

A diferencia de las otras legislaciones analizadas, en Ecuador es la firma electrónica la que se encuentra regulada. Esto se debe a que la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos se basa íntegramente en la Ley Modelo de la CNUDMI, que tenía como objeto establecer bases mínimas para que exista una homogenización a nivel internacional, sin perjuicio de que los Estados podían modificarla para su aplicación interna. Es por esto que sus disposiciones resultan generales e incluso de contradicen algunas con otras, como por ejemplo al hablar de neutralidad tecnológica, puesto que en un artículo se reconoce y en el otro se limita.

CAPÍTULO 3

3. PRINCIPIOS Y ESTÁNDARES INTERNACIONALES DE LA FIRMA DIGITAL

3.1. PRINCIPIOS DE LA FIRMA DIGITAL.

Ricardo Lorenzetti explica que:

> *"*los principios son muy usados […] por el legislador para legislar […] No sólo son perennes frente al devenir del tiempo, sino que su importancia se acrecienta cada vez más. Ante el evidente desprestigio de la ley derivado de la superproducción legislativa, […] ante la multiplicidad de ordenamientos que conviven en el contexto de la globalización del mundo, se postula cada vez más una tarea de simplificación basada en principios" (2001, p. 47).

Para Lorenzetti un principio "es un enunciado amplio que permite solucionar un problema y orienta un comportamiento […] se trata de normas prima facie" (, 2001, p.47), lo cual quiere decir que dichas normas son flexibles y se pueden cambiar o completar, por no tener una terminación acabada. Es decir, son normas de aplicación general, no específica, que pretenden brindar un soporte al momento de solucionar un problema o dictar un comportamiento. Son bases que permiten simplificar la labor del legislador así como el fruto de la misma que son las leyes.

Así lo respalda Torres al decir que:

> "Los principios generales del derecho son los enunciados normativos más generales que, sin haber sido integrados al ordenamiento jurídico en virtud de procedimientos formales, forman parte de él, porque le sirven de fundamento a otros enunciados normativos particulares o

> recogen de manera abstracta el contenido de un grupo de ellos.” (Torres, 2012, p. 4)

Por contar con esta característica de ser generales, es que funcionan como una herramienta para la homogenización de las legislaciones de distintos países. Resultan entonces, no sólo normas generales, sino también guías para la elaboración de leyes y que estas puedan ser reconocidas por otros Estados, para que de esta forma no exista una contradicción mayor entre las mismas.

La firma digital, cuenta con distintos principios creados para la facilitación de la interpretación, la homogenización y la aplicación de normas que traten sobre este tema. Entre estos principios se encuentran el de equivalencia funcional y el de neutralidad tecnológica. Estos principios fueron plasmados en la Ley Modelo de la CNUDMI sobre Comercio Electrónico y en la Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico.

La ley modelo, como se mencionó con anterioridad, es aquella en la cual los países pertenecientes a las Naciones Unidas deben basar su legislación interna sobre el tema en cuestión, para, de esta manera, poder intentar homogenizar las distintas legislaciones. Por lo cual, los principios que se encuentran establecidos en la mencionada ley deben ser respetados y aplicados por los países miembros. Es por esto que resultan ser de vital importancia para la creación o reforma de leyes.

3.1.1. EQUIVALENCIA FUNCIONAL

El principio de equivalencia funcional es aquel mediante el cual los medios electrónicos adquieren la misma validez que los medios o documentos que cuentan con un soporte de papel. Torres explica que este principio “se considera la piedra angular del comercio electrónico; de él se derivan las disposiciones fundamentales que regulan esta nueva actividad mercantil.” (Torres, 2012, p. 7) Es un criterio “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 las modernas técnicas del llamado comercio electrónico" (Fernández, 2001, p. 280).

Es decir, que se otorga el mismo valor al mensaje de datos equivalente al documento escrito, lo mismo sucede con la firma digital.

El artículo 5 de la Ley Modelo de la Comisión de las Naciones Unidas para el Desarrollo Mercantil Internacional hace una referencia a dicho principio, al establecer que "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" (Ley Modelo CNUDMI, art. 5). Sin embargo, dichos mensajes de datos deben cumplir con los requisitos de forma de un documento con soporte en papel como lo son: la fiabilidad, inalterabilidad, rastreabilidad, la posibilidad de una posterior consulta del mismo, la autenticación del mismo a través de la firma, la legibilidad, entre otros, como se menciona en la guía de la Ley Modelo de la CNUMDI. (pág. 21 párrafo 16 y 17)

Siguiendo esta línea de pensamiento, el Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, establece en su artículo tercero que "Cumplidos los requisitos de accesibilidad, el mensaje de datos tiene iguales efectos jurídicos que los documentos que constan por escrito." (art.3) En el mismo artículo se determinan dos requisitos para que un documento se entienda como accesible en su posteridad, estos son:

> "a) ha sido generada y puede ser almacenada en un lenguaje electrónico/informático y formato entendibles por las partes involucradas en el intercambio de información y sus respectivos sistemas informáticos de procesamiento de la información, pudiéndose recuperar su contenido y el de los remitidos o anexos correspondientes en cualquier momento empleando los mecanismos previstos y reconocidos para el efecto; y,

> b) se puede recuperar o se puede acceder a la información empleando los mecanismos provistos al momento de recibido y almacenarlo, y que deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo.” (Reglamento General a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2002, art. 3)

El principio mencionado debe ser “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” (Guía para la incorporación al derecho interno de la Ley Modelo CNUDMI sobre Comercio Electrónico, 1996, párrafo 16) y de esta manera evitar a los gobiernos la continua transformación de sus leyes en base a los avances técnicos futuros, conforme a la Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre el Comercio Electrónico. Es por esto que, como lo explica Fernández Delpech, la Ley Modelo hace una recomendación a los Estados miembros al fomentar una legislación flexible sobre las distintas tecnologías. (Fernández, 2001, p. 280)

En la Guía para la incorporación al derecho interno de la Ley Modelo CNUDMI sobre Comercio Electrónico, se menciona que la Ley Modelo reconoce el hecho que el principal problema para el desarrollo interno de medios modernos de comunicación son “los requisitos legales que prescriben en el empleo de la documentación tradicional con soporte de papel” (p. 20, párrafo 15). Es por esto que el principio de equivalencia funcional resulta ser uno de los principios más importantes del comercio electrónico, puesto que facilita la aplicación y el desarrollo del comercio electrónico, al brindar una herramienta que permite adaptar la legislación existente a los instrumentos electrónicos necesarios en el ámbito del comercio electrónico.

Al ser la legislación un elemento que evoluciona conforme a las necesidades del ser humano, resulta evidente afirmar que variará con el paso del tiempo, sin mencionar el hecho de que al intentar homogenizar las legislaciones de los países miembros de la Organización de las Naciones Unidas, el mecanismo predilecto para lograrlo es otorgar bases fundamentales, en las cuales los países miembros deberán basar sus legislaciones. Esto se debe a que los países miembros cuentan con legislaciones internas, que van respaldadas por la soberanía de cada Estado. Entonces, estas bases resultan en principios, entre esos el principio que permite, como se mencionó anteriormente, que los Estados miembros no tengan que actualizar todas sus leyes. Es una regla general, que facilita la aplicación de las normas de comercio electrónico.

Sin embargo, al formar parte de una organización en la cual se establece que los países miembros deberán suscribir todos los tratados existentes como requisito previo, al momento de legislar también se debe tomar en cuenta, como en este caso, la Ley Modelo de la CNUDMI. Entonces, se podría decir que crear un modelo de ley específico sería algo ineficaz. Por todo lo mencionado en este último párrafo cabe recalcar que el principio de equivalencia funcional es la base del éxito de la aplicación de la firma digital, puesto que con este principio se evita que el Estado tenga que cambiar cada una de sus legislaciones ya sean leyes o reglamentos y le da la posibilidad de simplemente adaptar lo ya redactado a la Ley a los nuevos medios digitales.

3.1.2. NEUTRALIDAD TECNOLÓGICA.

El principio de neutralidad tecnológica es aquel mediante el cual se asegura la no discriminación a otras tecnologías, ya sean existentes o nuevas, especialmente en lo que concierne a la legislación de temas como el comercio electrónico. A través de este principio se asegura que el Estado no imponga sus preferencias a favor o en contra de otras tecnologías. Es por esto que al momento de redactar una ley no se puede exigir el uso de un tipo de tecnología determinado para llevar a cabo lo enunciado por dicha ley.

Por lo mencionado, “la neutralidad tecnológica es una garantía de independencia, soberanía y construcción democrática de las infraestructuras informáticas.” (Torres, 2012, p. 133) Mediante este principio se logra garantizar que los medios electrónicos gocen de la independencia necesaria para su evolución. Esto se logra mediante la no vinculación de un tipo de tecnología a una situación determinada. Es por esto que el principio de neutralidad tecnológica es reconocido como uno de los pilares fundamentales del comercio electrónico. Torres afirma que:

> “La neutralidad tecnológica es un equilibrio que obliga a las empresas y a la administración a ser sensibles a la libertad de opción tecnológica, competitividad, calidad y permitir que los instrumentos menos eficientes sean sustituidos y reemplazados por opciones tencológicas más eficientes.” (Torres, 2012, p. 164)

Es por este principio que se logra progresar tecnológica y legalmente, en base a las necesidades del ser humano. Al crear un nuevo tipo de software o un nuevo tipo de tecnología que brinde seguridad en las transacciones, como lo hace la firma digital, es importante que exista la posibilidad de una mejora. Es así porque con el tiempo, la necesidad de un sistema más seguro resulta evidente. Conforme el ser humano genere nuevas necesidades, la tecnología y la ley deben responder y siempre se inclinará por el sistema informático que sea capaz de brindar más seguridad.

Para la evolución legal, como es conocido, debe existir primero la situación que genere la necesidad de una regulación. Al ser las necesidades igual de cambiantes que la tecnología, resulta pertinente no estancar una ley a un tipo determinado de tecnología. Especialmente porque en un tiempo podría quedar obsoleta, como la tecnología regulada en la misma. La elaboración de leyes es un proceso que requiere, en primer lugar, de un estudio y análisis adecuado y en segundo una delicada elaboración. Todo esto lleva tiempo y la tecnología evoluciona de forma acelerada, sin depender de las regulaciones que puedan ser necesarias para su correcto y debido funcionamiento.

Por esta razón los principios, especialmente uno fundamental como lo es el de neutralidad tecnológica, son sumamente importantes. Pues, con el uso adecuado de los mismos, se puede solventar situaciones que se presenten en un futuro, para las cuales no exista el cuerpo normativo adecuado, y de esta manera prevenir cualquier tipo de daños que esto pueda llegar a ocasionar. Por ende se puede suponer que, además de ser una garantía, es una forma eficaz para la mitigación de daños que se puedan generar a futuro.

Sin embargo, como lo explica Torres, neutralidad tecnológica no es sinónimo de igualitarismo tecnológico (Torres, 2012, p. 159). Esto quiere decir que, aunque la legislación de un Estado no se debe vincular a un tipo de tecnología determinado, existen distintos tipos de instrumentos tecnológicos que brindan distintos tipos de seguridad y, por consiguiente, validez jurídica. Es por esto que en un mismo ordenamiento se pueden reconocer distintos tipos de firma, como sucede en la legislación argentina con la firma digital y la electrónica, pero no todos generan el mismo resultado, especialmente en lo que a validez y seguridad se refiere.

En esos casos la decisión sobre el tipo de firma que se debe usar recae en la situación a la que se la desea aplicar. Mientras más seguridad requiera la transacción o el intercambio de información, resulta aconsejable emplear la firma que brinde más seguridad, que resulta ser la digital. No obstante las partes son libres de elegir el medio tecnológico que deseen emplear y es de esto de lo que básicamente trata el principio de neutralidad tecnológica con respecto a los usuarios. Esto se encuentra relacionado con el principio de libertad de comercio explicado con anterioridad. Las partes son las que deciden si el tipo de firma empleado en su transacción resulta suficiente para complacer sus necesidades.

El artículo 43 de la Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico establece una lista no exhaustiva de los principios generales en los que se basa la Ley modelo, entre los cuales se encuentran algunas menciones al principio de neutralidad

tecnológica, como lo es el numeral 2 que dice “validar las operaciones efectuadas por medio de las nuevas tecnologías de la información” (art. 43), 3) “fomentar y estimular la aplicación de nuevas tecnologías de la información” (art. 43) (y el numeral 5) que expresa que se deberán apoyar las prácticas comerciales nuevas, es decir que pueden existir prácticas comerciales en las cuales de deba emplear un tipo de tecnología distinto (art. 43) y por esto es que el principio de neutralidad tecnológica también se encuentra respaldado en este numeral.

El principio de neutralidad tecnológica no solo protege al usuario, sino también al sector privado dedicado al desarrollo de las tecnologías. Al estar esta parte del mercado en constante evolución resulta altamente rentable y esto es especialmente atractivo para el sector privado. Sin embargo, como en todo lo relacionado con el comercio debe existir igualdad de oportunidad en el mercado. Es aquí en donde este principio es fundamental para el país. Porque en el caso en que el Estado favoreciere a una tecnología determinada, se generaría una competencia desigual que podría desfavorecer a aquellos proveedores que presten el mismo servicio utilizando un tipo de tecnología distinto. Incluso, en un caso extremo, se podría llegar a crear un monopolio y esto perjudicaría, no solo al usuario, también tendría repercusiones en la economía del país. Esta es otra de las razones por las cuales resulta fundamental garantizar este principio.

Así mismo en la Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico, al hablar sobre las recomendaciones al momento de crear un equivalente funcional para los distintos tipos de firmas, aclara que “cualquier esfuerzo por elaborar reglas sobre las normas y procedimientos que deberían utilizarse como sustitutos en casos específicos de “firmas” podría crear el riesgo de vincular irremisiblemente el régimen de la Ley Modelo a una determinada etapa del desarrollo técnico” (art. 7, párrafo 55) y esto concuerda con el principio de neutralidad tecnológica puesto que se debe evitar relacionar la legislación con un tipo de tecnología

definido porque se vulneraría el principio de neutralidad tecnológica al no permitir que se puedan utilizar otras y nuevas tecnologías.

Rubio, Rodríguez y Muñoz, al hablar sobre el elemento tecnológico de la firma electrónica, sostienen que “uno de los fundamentos presentes a nivel general en las legislaciones sobre firma electrónica es la voluntad de evitar el compromiso con una determinada tecnología o procedimiento.” (Rubio, Rodríguez , & Muñoz, 2004, p. 31) Es decir, bajo este principio de neutralidad tecnológica, se entiende que existe un acuerdo entre los países miembros de la Organización de las Naciones Unidas de no vincular su legislación a ningun tipo de tecnología específica.

Lorenzetti, siguiendo la línea de pensamiento, afirma que:

> “el Estado debe ser neutral y no dictar normas discriminatorias en el sentido de limitar la participación de algún sujeto por el sólo hecho de que no utilice un instrumento escrito. Las partes son libres de adoptar entre ellas cualquier procedimiento de registro, de verificación de autoría, de firmas, y no deben sufrir limitaciones por ello” (Lorenzetti, 2001, p. 49)

De la misma manera el autor sostiene que “el Estado debe permitir que puedan probar judicialmente que su transacción es válida; debe evitarse la imposición de estándares o regulaciones, y se deben eliminar los obstáculos basados en los requerimientos de forma escrita” (Lorenzetti, 2001, p. 49)

A modo de resumen, este principio resulta fundamental puesto que, a parte de evitar favoritismos que acarreen privilegios económicos, si en algun momento se llegase a vincular la legislación a un tipo de tecnología determinado, la innovación también se vería perjudicada y por ende el sector privado, que resulta ser la matriz productiva de un país. Al limitar la productividad del sector privado limitando la capacidad de innovación o la motivaci´´on para la misma, se correría el riesgo de generar monopolios dentro del sistema y eso afectaría

no solo al gran empresario, pero sobre todo al mediano. Es entonces, por esto, que el principio de neutralidad tecnológica resulta tan importante y su aplicación es imperativa al momento de redactar una ley o un reglamento que trate sobre temas vinculados a este principio.

3.1.3. PRINCIPIOS DE COMERCIO ELECTRÓNICO APLICABLES A LA FIRMA DIGITAL.

Existen principios del comercio electrónico que son aplicables a la firma digital; Lorenzetti expone alguno de estos:

1. El de libertad de comercio, que, según el autor, "implica la autorregulación de las partes y con ello una mínima intervención estatal que se limita a lo necesario para el funcionamiento institucional del mercado." (Lorenzetti, 2001, p. 49) Bajo este principio se crea el concepto de que el contrato es ley para las partes. Esto quiere decir que lo que se acuerde en un contrato, tendrá fuerza de ley y sus disposiciones serán las que valgan, antes de lo estipulado en la ley, siempre y cuando no se incurra en un ilícito con las mismas. Es por esto que la mayoría de normas analizadas en el capítulo anterior, resultan ser complementarias, en el caso en el que no se hubiere estipulado en el contrato nada sobre la situación normada. Esto se aplica a la firma digital en tanto que las partes pueden determinar el tipo de firma que deseen usar y esto será lo que rija la relación entre las mismas.

2. El de la protección a la privacidad, que resulta importante en la red por la cantidad masiva de almacenamiento de información y el fácil acceso a la misma que esta ofrece. Al ser la privacidad un tema delicado y el tratamiento de la información, que constituye parte fundamental de la privacidad, aún más. Es por esto que el acceso a la información debe ser limitado o por lo menos debe existir un tipo de control que permita garantizar la protección a la privacidad de la persona y la información que la misma desee mantener confidencial (Lorenzetti, 2001, p. 50-51). La firma digital, al contar con un sistema de criptografía asimétrica, códifica el

mensaje, haciendo la información contenida en el mismo inaccesible para terceros no autorizados y así, protegiéndola.

3. El del carácter internacional, este principio se basa en la notable tendencia a la homogenizacion de las legislaciones (Lorenzetti, 2001, p. 52), especialmente evidenciable en la Ley Modelo de la CNUDMI. Bajo este principio es que los principios en general resultan aplicables y deben ser considerados por las legislaciones internas de cada país al momento de redactar y promulgar sus leyes. Este principio refuerza la idea de homogenizar las legislaciones y debido a clara tendencia que existe de utilizar y regular la firma digital, sería correcto hacer lo mismo en la ecuatoriana.

Adicionalmente, Torres, propone otro principio, el de “Inalterabilidad del derecho preexistente de obligaciones y contratos privados” (2012, p. 91) Este principio pretende evitar que la introducción del comercio electrónico no genere cambios en el derecho existente referente a comercio. Esto se debe a que los medios y soportes electrónicos son nuevas herramientas para la transmisión de voluntades, pero no las regulan de una forma diferente.

Este nuevo tipo de soporte no pretende alterar el significado jurídico de los actos comerciales o sus voluntades y es por esto que por el simple motivo de estar en soporte electrónico, no debería ser justificación para cambiar el derecho existente al momento sobre transacciones comerciales. El objetivo principal de este principio es que el hecho de que se necesiten nuevas normas para aplicar los aspectos electrónicos del comercio, no significa que se deban cambiar las regulaciones sobre las relaciones comerciales, a pesar del tipo de soporte en el que se encuentren. (Torres, 2012, p. 91)

Este principio tiene un fuerte lazo con el de equivalencia funcional, puesto que el de equivalencia resulta ser un método para aplicar el principio explicado en este párrafo. El principio de equivalencia funcional otorga a los mensajes de datos la misma validez que los documentos o firmas físicas. Entonces,

mediante esta herramienta se puede cumplir con el objetivo del principio mencionado con anterioridad. Al ser la firma digital el equivalente funcional de la firma manuscrita, se le debe otorgar los mismos efectos jurídicos.

La misma autora señala un principio que forma parte fundamental del comercio y del derecho en general y es el de buena fe (Torres, 2012, p. 167). Cabanellas explica este principio diciendo “Rectitud, honradez, hombría de bien, buen proceder. Creencia o persuasión personal de que aquel de quien se recibe una cosa, por título lucrativo u oneroso, es dueño legítimo de ella y puede transferir el dominio.” (Cabanellas, 1993, p. 42) Este principio exige a las partes involucradas a, no sólo tener la intención de cumplir con lo establecido en el contrato, si no también a hacerlo, para, de esta manera, lograr la finalidad u objetivo por el cual decidieron obligarse. Por estos motivos la actuación de las partes debe ser leal y honesta.

Al estar basado en un sistema tan amplio e inseguro como lo es la red, el comercio electrónico, y las transacciones que se realicen bajo esta denominación, debe tener como base fundamental el principio de buena fe. Esto resulta fundamental puesto que los usuarios desconfían de las redes por la inseguridad existente. La inseguridad se origina en la idea del fácil acceso que se tiene a la información y el hecho de que un tercero no autorizado pueda interceptar el mensaje de datos. Con los documentos físicos esta inseguridad queda prácticamente anulada y aunque exista el principio de equivalencia funcional, resulta complicado garantizar la seguridad de la información que se desea mantener como privada (Torres, 2012, p. 181-183).

En el comercio electrónico la confianza, a pesar de ser un tema delicado, resulta realmente importante, puesto que por las posibilidadaes que brinda el mismo, las partes pueden no conocerse y no haber formado una relación de confianza como sucede en el mundo físico del comercio. Entonces, para que el ámbito del comercio electrónico pueda florecer es necesario generar confianza en el sistema y una de las formas de hacerlo es, que el principio de buena fe sea imperativamente exigido, para que despues sea reconocido y aplicado en

su totalidad. (Torres, 2012, p. 185-186). Este principio resulta especialmente importante para la firma digital, pues es en este que basa la idea de la presunción de autoría de la firma.

3.2. ESTÁNDARES INTERNACIONALES

Los estándares internacionales son presentados como bases mínimas sobre las cuales se debe legislar internamente, especialmente si lo que se pretende es la homogenización. Esto resulta importante, especialmente en lo que concierne al comercio electrónico. Lo mencionado se debe a que mucho del mismo se lleva a cabo en canales internacionales, por lo cual, estas bases resultan útiles para el reconocimiento de la validez de las distintas legislaciones con las cuales se manejan las otras partes.

En la norma ISO/IEC 9796-2 se especifican algunos estándares internacionales sobre firma digital. Entre estos se encuentran los requerimientos de la firma digital y establece que:

> “a) The message M to be signed shall be a binary string of any length, possibly empty. b) The signature function uses a private signature key, while the verification function uses the corresponding public verification key. --Each signing entity shall use and keep secret its private signature key corresponding to its public verification key. --Each verifying entity should know the public verification key of the signing entity. c) Use of the signature schemes specified in this standard requires the selection of a collision-resistant hashfunction h. There shall be a binding between the signature mechanism and the hash-function in use. Without such a binding, an adversary might claim the use of a weak hash-function (and not the actual one) and thereby forge a signature.” (art3)

Esto quiere decir que el mensaje que se debe firmar debe ser un cordón binario de cualquier largo. Además la función utilizada para la firma debe usar una clave privada, mientras que la función de verificación utiliza la clave pública que

corresponde a la privada. Todos los firmantes deben usar y mantener en secreto su clave privada así como los que verifican deben conocer la clave pública que concuerde. Establece también que debe existir un vínculo entre el mecanismo que se utilice para la firma y la función hash que se utilice. (ISO 9796-2, art. 3)

Las organizaciones ISO, International Organization for Standarization, e IEC, International Electrotechnical Comission, son las encargadas de publicar normas que sirvan como un estándar reconocido de forma internacional, en lo que a las TIC se refiere.

Sobre la infraestructura de clave pública, esta norma establece que el sistema de clave pública consiste en tres partes, la primera es la generación de la clave, que consiste en crear dos claves, la privada para firmar y la pública para verificar. La segunda se trata de un método que sirva para generar una firma representativa de un mensaje y una clave privada y el tercero, que determina un método para recuperar el mensaje representativo de una firma y una clave pública de verificación (ISO/IEC 9796-2, anexo A).

Como se ha podido evidenciar a lo largo de este trabajo, existen varios estándares internacionales adicionales con los que debe cumplir una firma digital. En este sub-capítulo se procederá a desarrollar un tipo de resumen que reúna dichos estándares internacionales. El principal y más básico punto sobre el cual coinciden todas las legislaciones analizadas, especialmente por la Ley Modelo de la CNUDMI, y por lo tanto, es considerado como estándar internacional, es que la firma digital debe servir para identificar al firmante, así como vincularlo con el texto firmado. Esto se encuentra ligado a los requerimientos de seguridad como se verá a continuación.

Empezando por los aspectos más generales, con los que debe cumplir la firma digital, están los requisitos de seguridad, mencionados en el primer capítulo. Estos son: confidencialidad, autenticación, integridad y no repudio. Al ser la

firma digital una solución ofrecida para la seguridad de la información, esta debe cumplir con los requisitos mencionados.

La confidencialidad es básicamente una garantía de que un tercero no autorizado no pueda acceder a la información contenida en un mensaje de datos. Es un requisito de seguridad muy buscado por las partes, especialmente en las relaciones comerciales, por lo cual es esencial poder brindar un mecanismo que ayude a mantener la privacidad de un mensaje de datos. La confidencialidad es importante, no solo por la información que se maneja, principalmente en las transacciones comerciales, sino también por la facilidad que existe de acceder a la misma, de manera singular, en un sistema tan abierto como lo es la red.

Como se advirtió en el primer capítulo, la información que se maneja en las relaciones comerciales es delicada. Un mensaje de datos puede contener por ejemplo un plan de negocios, una idea para la innovación de algún producto, información sobre cuentas bancarias, instrucciones que debe seguir la otra parte, direcciones de los domicilios de los respectivos participantes, entre otros. Si este tipo de información fuere interceptada por un tercero no autorizado, podría representar un gran daño para los que participan de esta relación comercial. Podría perjudicar a las partes involucradas y llegar a representar un daño económico significativo.

Entonces, al tratarse de información que puede resultar delicada y al ser fácilmente accesible, la solución es encriptar el mensaje para que esta solo pueda ser accedida por las personas autorizadas. El sistema más confiable de criptografía es el asimétrico, es decir, el que se maneja con un par de claves para cada usuario, la pública y la privada, como se mencionó con anterioridad. Por lo cual, la firma digital, al contar con un sistema de criptografía asimétrico, resulta ser uno de los métodos más seguros y confiables para asegurar la confidencialidad de un mensaje. Cabe entonces asegurar que la firma digital es un medio idóneo para garantizar la confidencialidad tan solicitada para el manejo de información en la red.

Como se manifestó, la red es un sistema abierto, del que cualquier que tenga acceso a la misma puede participar. Desde cualquier parte del mundo, si se tiene acceso a una computadora, el usuario puede utilizar los servicios que brinda esta herramienta. Sin que exista la posibilidad de verificar exactamente quien estaba usando el aparato que envió la información recibida, la identificación de las partes resulta otro requerimiento de seguridad igual de importante que la confidencialidad.

Es posible establecer desde dónde se envió la información a través de la dirección IP (Internet Protocol). Pero a través de este mecanismo no se puede garantizar que el emisor es en realidad quien dice ser. La dirección IP es un conjunto de números asignado a un equipo informático específico, que permite su identificación en la red debido a que este número es único e irrepetible. Es por esto, que mediante la dirección IP se puede saber cuál es el origen del mensaje de datos, pero no se puede garantizar la identidad del emisor.

Siguiendo esta línea de pensamiento, al ser la red tan amplia y ofrecer la posibilidad de entablar relaciones comerciales con personas en cualquier parte del mundo, sin la necesidad de conocerlas personalmente, al manejar información delicada, la confidencialidad no sirve de mucho si no se puede asegurar la identidad de la otra parte. Si no existiere la posibilidad de autenticación, el comercio electrónico no podría florecer. Este tipo de comercio requiere, más que en el mundo físico, de la confianza de las partes. La confianza es esencial para el uso del comercio electrónico.

Por ende, la autenticación es otro requisito de seguridad de vital cumplimiento, especialmente en lo que a transacciones electrónicas se refiere. La autenticación se da cuando el receptor puede verificar de manera segura y confiable, que el emisor es quien dice ser. Esto es crucial puesto que, generalmente, los mensajes correspondientes a las transacciones comerciales contienen instrucciones en forma de obligaciones que la otra parte debe cumplir, como por ejemplo, la transferencia de dinero, es decir el pago, a cambio de un servicio o producto. Si no se pudiere verificar la identidad del

emisor, un tercero no autorizado podría interferir y aprovecharse de esta situación, especialmente de forma económica.

La firma digital, a través de su sistema de criptografía asimétrica, permite identificar al emisor del mensaje. Esto se debe a que el firmante tiene la obligación de mantener su clave privada segura y además este posee el certificado de firma digital, emitido por una entidad certificadora, que verifica la identidad del mismo. El certificado de firma digital es un mensaje de datos que permite vincular la firma al firmante y así autentificar el mensaje enviado. Es prudente entonces recalcar que la firma digital es una vez más el método idóneo para el cumplimiento de este requisito.

Como se reconoció previamente, la red es un sistema abierto, que puede ser accedido por terceros si no se cuenta con la seguridad necesaria. Al ser accesible, puede ser modificada. Si el contenido puede ser susceptible de modificación, la autenticación y la confidencialidad no tendrían valor. El hecho de que un mensaje sea confidencial o que se pueda identificar al emisor, no representa garantía alguna de que el mensaje no ha sufrido alteraciones.

En una relación comercial, el contenido del mensaje es lo más importante, puesto que, como se mencionó anteriormente, puede contener datos bancarios, instrucciones u obligaciones. Es en donde se establece los elementos esenciales de dicha relación, como el objeto, el precio y la forma de pago, las condiciones, en si todo aquello que, al final, va a ser ley para las partes. La información que se transmite en el mensaje de datos es la base de la relación comercial, es lo que dictará el comportamiento de las partes en lo que concierne a dicha relación.

Al ser el contenido del mensaje, lo más importante, es el objeto sobre el cual recaen todos los requisitos de seguridad. La información es lo que se cuida, no solo el acceso, sino, la integridad de la información contenida en el mensaje. Por lo tanto, presentar un método que garantice la integridad del mensaje, del contenido del mismo, es de suma importancia.

Devoto, al hablar sobre la integridad, sostiene que:

> “Integridad significa que la información no carece de ninguna de sus partes, que no ha sido modificada. La integridad es una cualidad imprescindible para otorgarle efectos jurídicos a la información. La firma digital comprueba la integridad de la información que fuera firmada, en forma independiente al medio de su almacenamiento.” (Devoto, 2001, p. 177)

El requisito de integridad representa una garantía en la que se asegura que el mensaje recibido no ha sufrido alteraciones de ningún tipo. La solución que se asignó a esta garantía es la llamada función control o *Hash function*. Esta función se basa en un proceso matemático que crea un tipo de resumen del texto enviado. Este resumen está representado de forma digital. Entonces, el emisor, aparte de enviar el mensaje encriptado y por lo tanto firmado digitalmente, envía también este resumen o digesto del mensaje, el emisor desencripta el mensaje y aplica nuevamente la función control sobre el mismo. Después procede a comparar los dos resúmenes y si estos coinciden a la perfección, entonces esto quiere decir que el mensaje no ha sido alterado, que se conservó en su integridad. (Devoto, 2001, p. 169)

Al respecto, Devoto establece que:

> “Para firmar un documento o cualquier otro material de información, el firmante delimita primero en forma precisa el espacio de lo que se ha de firmar. Seguidamente, mediante la función control del programa informático del firmante se obtiene un digesto del mensaje único, a todos los fines prácticos, de la información que se firma. El programa del firmante transforma luego el digesto de mensaje en una firma digital utilizando la clave privada del firmante. La firma digital es, por lo tanto, exclusiva de la información firmada y de la clave privada utilizada para crearla.” (Devoto, 2001, p. 170)

Entonces, después de crear este resumen, el firmante, utilizando su clave privada, transforma este resumen en una firma digital mediante su respectivo programa. El emisor, recibe el mensaje y lo resume también para verificar su integridad. Entonces, la firma digital garantiza la integridad del mensaje y por lo tanto cumple con este requisito se seguridad de la información.

Como se establece claramente en los párrafos que mencionan el requerimiento de seguridad de la autenticación, la red ofrece un mundo en el cual se puede dar la situación en que las partes no tienen que conocerse personalmente para poder incursar en una relación del tipo comercial. Esto podría generar desconfianza en el sistema como se señaló y esto llevaría como consecuencia el estancamiento del comercio electrónico. Sin embargo, la firma digital brinda un mecanismo en el cual la autenticación está garantizada.

De la mano de la autenticación se encuentra el requerimiento de seguridad de no repudio. Mientras que la autenticación recae sobre las partes, se lleva a cabo por las mismas y sirve únicamente para ellas, el no repudio garantiza que, en caso de que exista un tipo de problema respecto de identificación del firmante o el emisor y su vinculación con el contenido del mensaje enviado, en el que un tercero deba resolver, este no podrá negar que la firma le pertenece y que, por ende, está vinculado con el contenido firmado. En caso de que lo negare, la carga de la prueba recae sobre el mismo, es decir, por este requerimiento se presume que el firmante es quien dice ser y está vinculado al mensaje.

Así mismo, y como punto a parte, bajo este requerimiento, el receptor no podrá negar haber recibido el mensaje. Este se denomina no repudio de destino. En este caso, si el receptor llegase a alegar que él no recibió el mensaje enviado por el receptor la carga de la prueba recae sobre el receptor. El mensaje se presume recibido.

La firma digital, en conjunto con el certificado de firma digital, al ser el método idóneo de autenticación del firmante, vincula a este al contenido del mensaje.

Si una persona está de acuerdo con el contenido del mensaje, procede a firmarlo y enviarlo. Una vez que se el mensaje se encuentra firmado y, siempre y cuando, este no haya sido alterado, aplica la garantía de no repudio.

Al ser la firma digital el equivalente funcional de la firma manuscrita, esta cuenta con las mismas garantías y entre estás se encuentra esta presunción, que garantiza el no repudio. La firma manuscrita vincula al firmante directamente con el documento firmado. Este no puede negar su autoría y mucho menos la aceptación del contenido. Por lo cual si la firma manuscrita sirve para autenticar y vincular al firmante, la firma digital también.

A modo de resumen, como se observó, la firma digital cumple con todos los requisitos de seguridad propuestos como estándares internacionales. Mediante la firma digital se encripta el mensaje, lo cual garantiza la confidencialidad. Además, mediante la firma y su certificado se puede autenticar el mensaje y, como se explicó, garantiza el no repudio. Finalmente, con el uso de la función hash, que forma parte de la firma digital, se garantiza que el mensaje no ha sido alterado y, por lo tanto su integridad.

Al inicio del capítulo se trató el tema de los principios del comercio electrónico en general. Debido a que la firma digital forma parte fundamental del comercio electrónico, existen algunos con directa aplicación a la misma. Entre estos se encuentra el de libertad de comercio, el del carácter internacional, el de buena fe, el de la inalterabilidad del derecho, las obligaciones y contratos preexistentes, el de equivalencia funcional y por último, el de neutralidad tecnológica.

La libertad de comercio proporciona a las partes un ambiente libre de regulaciones, en el cual estas pueden decidir sobre las disposiciones a las que se quieren obligar, siempre y cuando no recurran en ilícitos. Este principio es el que permite que el contrato sea ley para las partes y por ende, que la ley que regule el tema sea un apoyo secundario. Bajo este principio las partes pueden decidir, entre otras cosas, el tipo de firma que deseen utilizar.

Uno de los elementos esenciales para el correcto cumplimiento de este principio es que el Estado no debe vincular un tipo de tecnología determinada a una situación específica. Porque, aunque lo acordado por las partes sea ley para las mismas, estas deben contar con un apoyo legal suficiente para dicha situación. Por lo cual el Estado debe reconocer y no discriminar los distintos tipos de firma, ya sea electrónica o digital.

Debido a la meta trazada de homogenización de las legislaciones, el principio del carácter internacional resulta importante también. Puesto que es, por este principio y su meta, que los países deben redactar o modificar sus leyes conforme a los principios o estándares internacionales. Es por esto que los principios o estándares que afecten a la firma digital deben ser considerados para la elaboración de un cuerpo normativo correspondiente.

El de buena fe está ligado a las presunciones antes mencionadas. Es también por este principio que se logra establecer la presunción de autoría de una firma digital, así como la recepción del mensaje que da cabida al no repudio, sea de origen o destino. Se presume que en las relaciones comerciales existe la buena fe de cumplir con las obligaciones a las que se vinculó mediante la firma digital. Existe también la presunción de que se firmó el documento o mensaje de datos de buena fe y por ende el que firmó es quien dice ser. Es esta entonces la base de los requerimientos mencionados.

También existe el principio que Torres señaló como “Inalterabilidad del derecho preexistente de obligaciones y contratos privados” (Torres, 2012, p. 91). Este principio establece que no por el hecho de que el comercio electrónico se maneje en un soporte diferente debe alterarse el derecho de las obligaciones o los contratos privados. Entonces, no porque la firma digital esté en un soporte distinto que el de la manuscrita, significa que tiene menos valor o que las obligaciones contraidas mediante el uso de esta no son exigibles o válidas.

Este principio forma parte de uno de los principios fundamentales del comercio electrónico, que es el de equivalencia funcional. Dicho principio dota a los

mensajes de datos de las mismas caracterísitcas que su equivalente físico, sea este un documento o firma. Es mediante este principio que a la firma digital se le otorga la misma validez y los mismos efectos jurídicos que a la firma manuscrita. Es por este principio que el derecho que regula comercio electrónico ha evolucionado de la forma en la que lo ha hecho, puesto que gracias a este principio, los Estados no tuvieron que cambiar sus cuerpos normativos y se logró que las regulaciones no relanticen al comercio electrónico.

La firma manuscrita es el método predilecto de identificación y vinculación de una persona a un documento. La firma permite que las obligaciones contraidas en un contrato sean cumplidas, puesto que representa la voluntad del firmante. Es la expresión de la voluntad del mismo. La firma es esencial en el comercio porque sin voluntad el acto no es válido.

Aunque resulte redundante, los requisitos que la firma manuscrita debe cumplir son el de vinculación e identificación. Estos requisitos son cumplidos por la firma digital, como se comprobó con anterioridad. Sin embargo, debido a la complejidad del mundo virtual, la firma digital debe cumplir con los demás requisitos mencionados. Es por esto que existe una regulación a parte para el tema.

Para que se pueda satisfacer completamente los requisitos de la firma manuscrita y su objetivo, la firma digital debe contar con estándares distintos. Entonces, si se cumple con los requisitos, con el objeto de la firma manuscrita, si se logra identificar al firmante y vincularlo al texto, se le otorga la misma validez. La firma digital es el equivalente a la firma manuscrita porque es el método más seguro y confiable y además cumple con todos los requisitos y todas las condiciones expuestas.

Finalmente, otro principio fundamental del comercio electrónico, la neutralidad tecnológica o la no discriminación del medio tecnológico, también está vinculada con el principio de equivalencia funcional. Esto se debe a que bajo

estos dos principios no se podrá quitar validez a un mensaje de datos por el simple hecho de estar en soporte electrónico. Se podría decir entonces que no se discriminará el medio tecnológico.

Este principio reúne varias ideas sobre un mismo tema. Por un lado está aquella mediante la cual un tipo de tecnología debe permitir que, si se elabora un tipo de tecnología mejor este pueda ser usado. Por ejemplo, si se crea una computadora que tenga instalada un software determinado, este equipo debe permitir que en un futuro se pueda utilizar un software distinto que presente mejoras. Esto da espacio a la innovación y es mediante la innovación que el sector privado crece, debido a que, normalmente, la innovación se encuentra a cargo del mismo. Sin embargo, si el Estado vincula mediante su cuerpo normativo un tipo de tecnología determinado a un equipo o situación específica, así el equipo permita una mejora, el sector privado también se verá perjudicado.

Es en este pensamiento que se basa la tercera idea contenida en el principio de neutralidad tecnológica. El Estado no debe vincular un tipo de tecnología determinado a ningún tipo de situación. Se deben crear leyes en las que se permita el uso de todo tipo de tecnología que satisfaga las necesidades de dicha situación.

El término digital, y por lo tanto firma digital, engloba todos los tipos de tecnología, puesto que, como lo afirma Devoto:

> “Aunque es cierto que cuando la firma digital se encuentra momentáneamente almacenada en la memoria volátil de una PC (“RAM”) los dígitos de una firma digital consisten en magnitudes eléctricas, también es cierto que cuando se encuentra almacenada en el disco duro (magnético) de la PC consiste en campos magnéticos, cuando se encuentra perdurablemente almacenada en un CD-ROM consiste en agujeros perforados en la capa de aluminio del CD y cuando

> es transmitida por una fibra óptica de telecomunicaciones consiste en fotones.” (Devoto, 2001, p. 166)

Al hablar de firma electrónica, se vincula a esta a un tipo de tecnología determinado, aquella basada en magnitudes eléctricas. Sin embargo, como se evidenció existen otros tipos de tecnología, como la mecánica, eléctrica, magnética, óptica, entre otras. Cabe entonces decir que, al regular la firma electrónica como método idóneo de equivalente de la firma manuscrita, se estaría contradiciendo al principio de neutralidad tecnológica puesto que se vincula una situación a un tipo de tecnología determinada, discriminando los otros medios tecnológicos. Es por esto que la firma digital, al englobar los distintos tipos de tecnología, es verdaderamente neutral y es por esto que este debería ser el término utilizado en los cuerpos normativos. Porque, además de ser la única firma que cumple con todos los requisitos y los garantiza, no discrimina a otros tipos de tecnología.

3.3. PROPUESTA: ELEMENTOS PARA LA ACTUALIZACIÓN DE LA NORMATIVA ECUATORIANA

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos cuenta con disposiciones que pueden resultar ser demasiado básicas en lo que a firmas se refiere. Al analizar la Ley Modelo de la CNUDMI y la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y compararlas, se puede notar un parecido extremo, casi igual, entre estos cuerpos legales. La Comisión de las Naciones Unidas sobre el Desarrollo Mercantil Internacional redactó dicha Ley Modelo para que los Estados Miembros puedan usarla como guía y para que las disposiciones escritas en esta, sean acogidas por los mismos.

Sin embargo, el hecho de que este texto sea aplicable como modelo, no quiere decir que no se pueda añadir disposiciones que favorezcan e impulsen su uso. Tanto en Argentina como en España se crearon leyes que regulan la firma digital o en el caso de España la firma electrónica reconocida; en dichas leyes

existen disposiciones adicionales que permiten regular distintos aspectos que rodean a dichas firmas pero que, sin embargo, no fueron contemplados en la Ley Modelo.

Esto se debe a que la Ley Modelo es intencionalmente general respecto a los aspectos que regula, precisamente para que los Estados miembros puedan ajustar sus leyes a dicho texto y tengan cabida para regular otras situaciones que consideren necesarios. Los Estados deben llenar los vacíos que una Ley Modelo deja por el hecho de ser general.

Tanto en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, como en su reglamento se habla de la firma electrónica como el equivalente funcional de la firma manuscrita (art. 14). Sin embargo, como se evidenció, es la firma digital la que puede brindar todas las garantías necesarias para que los requerimientos de seguridad queden satisfechos. La firma electrónica discrimina otros tipos de tecnología y no cumple con todos los estándares internacionales descritos anteriormente.

El Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos se establece que no se discriminará a ningún tipo de firma electrónica (art. 10). Pero al referirse a lo electrónico se discrimina los otros tipos de tecnología y como se mencionó en este trabajo, la firma digital no es un tipo de firma electrónica. Estas firmas no tienen una relación género-especie, por lo tanto, al decir que se admiten todos los tipos de firma electrónica, se discriminaría a la firma digital, puesto que esta no es un tipo de firma electrónica. La firma digital se basa en otros tipos de tecnología.

Los requisitos que debe cumplir una firma electrónica dictados por la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos establecen que mediante la firma debe ser posible identificar y vincular al firmante con el texto. Que el método con el cual se creó sea confiable, seguro e inalterable, así como el de verificación. Que el firmante tenga control absoluto sobre los datos que se usaron para crear la firma, así como de la firma en sí (art. 15). Todos

estos requisitos son cumplidos por la firma digital y su método de creación y verificación es el más seguro, confiable e inalterable existente.

Debido a que el éxito del comercio electrónico está basado en la confianza de los usuarios, es imprescindible contar con una herramienta que brinda la mayor confianza posible. Una herramienta que garantice la confidencialidad, autoría, integridad y el no repudio de la información contenida en el mensaje y de la firma misma, en lo que a no repudio se refiere. Como se aclaró previamente, la firma digital es la solución que se brinda para cada uno de estos requerimientos.

Sobre los requerimientos de seguridad, Devoto afirma que:

> “Existe acuerdo a nivel mundial de que la firma digital basada en la criptografía de clave pública constituye en la actualidad el único mecanismo que permite resolver las cuestiones planteadas. En este sentido, de coincide en forma casi unánime que el término firma digital debe reservarse para aquel mecanismo que se basa en la criptografía de clave pública. Al facilitar la autenticación a distancia entre partes que no necesariamente se conocen previamente, las firmas digitales constituyen el mecanismo esencial para proveer seguridad y desarrollar la confianza en las redes abiertas. Por ello constituye un elemento clave para el desarrollo del comercio electrónico en internet.” (Devoto, 2001, p. 161)

Siguiendo esta línea de pensamiento, la firma digital es entonces una de las herramientas idónea para promover la confianza necesaria en el comercio electrónico. Porque, además de cumplir con los estándares internacionales y brindar una solución efectiva a cada requerimiento de seguridad de la información, cumple con los mínimos requisitos establecidos, que son el de identificación y vinculación.

Como se logró evidenciar, el comercio electrónico ha tomado fuerza con el paso del tiempo y su evolución tanto tecnológica como legal es necesaria. Si la

evolución legal se ralentiza, entonces, por los nuevos medios tecnológicos que brindan nuevas posibilidades para las transacciones comerciales, la desconfianza aumentará y esto tendrá como consecuencia inevitable que este nuevo mundo que brinda eternas posibilidades para comerciar, quede desaprovechado.

Es por esto que es necesario contar con un cuerpo normativo que respalde y brinde tanto una guía como un apoyo para las nuevas situaciones que se generen. Y, lo que es aún más necesario, contar con un cuerpo normativo que vaya conforme a los estándares y principios internacionales. Sin violar ninguno de ellos como sucede ahora con el uso del término electrónico versus el principio de neutralidad tecnológica, principio adoptado y reconocido globalmente. Las leyes y los reglamentos deben evolucionar conforme a las necesidades de las personas y es por esto que existen elementos que deben ser actualizados.

Empezando por la actualización del término “electrónico” a “digital” respecto a las firmas. Al demostrarse que la firma electrónica es discriminatoria frente a otro tipo de tecnologías y al ser el Ecuador miembro de las Naciones Unidas, no puede violentar el principio de neutralidad tecnológica. En el Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos se reconoce expresamente este principio, pero al referirse a firmas electrónicas se lo desvalida.

Por otro lado, al ser la firma digital el tipo de firma que más seguridad brinda, debería ser promovida por el Estado. Los participantes del comercio electrónico deben poder contar con el debido respaldo por parte de las leyes por las cuales se rigen los actos de comercio que realizan. Si una persona que desea incursionar en el mundo virtual a través del comercio electrónico, debe poder guiarse con lineamientos que velen por su interés. Debe poder confiar en que las leyes que lo respaldan van conforme a los parámetros internacionales, para que las disposiciones que contengan puedan ser aceptadas por leyes de otros

países con los que pretende interactuar comercialmente a través de personas de ese Estado.

Si el cuerpo normativo ecuatoriano va en contra de un principio fundamental, reconocido a nivel mundial, entonces las disposiciones que formen parte de su contenido no pueden brindar un respaldo eficaz para las personas que este supuestamente debe amparar. Resulta crucial contar con un cuerpo normativo que cumpla con los estándares internacionales establecidos, para que, de este modo, la persona quede protegida y debidamente respaldada. Es por esto que la actualización de este elemento es necesaria.

La firma digital es una parte fundamental del comercio electrónico, puesto que mediante la utilización de la misma se pueden suplir todos los requerimientos de seguridad de la información, para así poder generar o mantener la confianza en el tan amplio campo de la red. Es por esto que una regulación que vaya acorde es necesaria. Un cuerpo normativo que regule todos los aspectos esenciales de la firma digital y no únicamente los básicos como lo hace la Ley actual. Es necesario que en este cuerpo legal se establezcan todos los aspectos referentes a la validez de la firma digital, así como las garantías que son cubiertas por la misma.

Claro está, como se expuso el tema de la no violación al principio de neutralidad tecnológica, se deben reconocer otros tipos de firma, como la electrónica, pero la digital debe ser la principal por la seguridad que esta brinda. Resulta prudente tomar en cuenta los avances hechos por otros países que han evolucionado más en este tema, como Argentina, para poder crear una base sólida en torno a la cual se actualizará el cuerpo normativo ecuatoriano. En la ley argentina, se considera que la firma electrónica es aquella que no cumple con todos los requisitos para ser considerada firma digital, sin embargo, en sus disposiciones, también se reconoce a la firma electrónica como herramienta válida. La diferencia radica en que se pretende brindar a las personas la mejor herramienta posible para el desarrollo del comercio electrónico, que es la firma digital.

Al ser la firma digital un elemento fundamental del comercio electrónico, como se mencionó, sería sensato darle la importancia que se merece al crear una ley que se base únicamente en este tema y los aspectos que este conlleva. La amplitud del estudio del tema, y por lo tanto del tema en si, respalda esta idea. La firma digital no debe ser tratada de manera básica porque la firma digital no es sencilla. Involucra un mecanismo complejo que debe ser regulado de acuerdo al mismo para, de esta manera, poder sacar el mayor provecho de esta tan útil herramienta. A modo de resumen, la propuesta de elementos de actualización de la normativa ecuatoriana se basa en la creación de una Ley de Firma Digital.

CONCLUSIONES

Debido a la vulnerabilidad que experimenta la información en un sistema tan amplio como lo es la red, es necesario contar con la protección necesaria a la misma. Para esto se han establecido parámetros o requerimientos de seguridad que son: la disponibilidad, confidencialidad, autenticación, integridad y no repudio.

La firma digital surge como una solución técnica que satisface todos los requerimientos de seguridad de la información, a excepción de la disponibilidad, puesto que para esto se necesita un programa de almacenamiento que en todo caso se complementa con el empleo de la firma digital.

Por la importancia de la aplicación técnica, se hizo necesario adoptar una regulación jurídica para el empleo de firmas electrónicas y firmas digitales. Sin embargo, existe un constante debate acerca de la pertinencia de emplear la referencia a las firmas electrónicas o a las firmas digitales.

Hay quienes sostienen que la firma digital es una especie de firma electrónica, y por otro lado se explica que lo electrónico es en realidad discriminante de otras tecnologías. Como se pudo evidenciar, la segunda hipótesis es en realidad la aplicable. Esto se debe a que al hablar de firma electrónica se discriminan otros tipos de tecnología como lo son la mecánica, magnética, óptica, entre otras, porque la firma electrónica se basa únicamente en impulsos eléctricos y este tipo de tecnología no engloba a las otras. Es por esto que al usar el término de firma electrónica se contradice al principio de neutralidad tecnológica.

Con el paso del tiempo se ha establecido una clara tendencia a regular sobre la firma digital, por todos los beneficios que esta conlleva. Es por esto que en la ley del estado de Utah, al igual que en Argentina se norma la firma digital. En la legislación española se habla sobre la firma electrónica avanzada que es el

equivalente de la firma digital, pues se reconoce que la firma electrónica no puede sustituir a la firma ológrafa.

En estas legislaciones se reconoce a los otros tipos de firma, pero se establece que la digital es el equivalente funcional preferido de la firma manuscrita por todas las seguridades que brinda su sistema.

En Ecuador, sin embargo, es la firma electrónica la que se encuentra regulada. Esto se debe a que la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos se basa íntegramente en la Ley Modelo de la CNUDMI, que tenía como objeto establecer bases mínimas para que exista una homogenización a nivel internacional, sin perjuicio de que los Estados podían modificarla para su aplicación interna.

Existen dos principios fundamentales aplicables a la firma digital que son el de neutralidad tecnológica y el de equivalencia funcional. El primero, se cumple por el hecho de que este tipo de firma no discrimina a los otros tipos de tecnología, a diferencia de la electrónica. El de equivalencia funcional otorga a la firma digital los mismos efectos jurídicos que la firma manuscrita por ser esta la que permite garantizar la identidad del firmante eficazmente. Como se pudo evidenciar en el tercer capítulo, la firma electrónica cumple con los estándares internacionales establecidos, con los requisitos de seguridad y con los principios mencionados.

Finalmente y por todo lo expuesto es que se propone la actualización de la normativa ecuatoriana. Además, por la importancia del tema y la cantidad de aspectos que se deben regular, se plantea la posibilidad de crear una norma independiente para la firma digital, como sucede en Argentina.

La firma digital no es únicamente una herramienta del comercio electrónico y por esto no debería estar directamente vinculado con este como se hace en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. La firma digital brinda la seguridad necesaria para que los usuarios puedan confiar

en su sistema y así expandir su uso y poder evolucionar en el tema. Entonces, al ser la tendencia la de desmaterializar los documentos y actos, al determinar todos los beneficios que conlleva el uso de la firma digital, es imperativo contar con un cuerpo normativo que vaya acorde a esto para así poder explotar su uso y obtener los máximos beneficios posibles.

En conclusión, la firma digital es el tipo de firma favorito para ser regulado, puesto que cumple con todos los requerimientos de seguridad, con los estándares internacionales y no contradice ningún principio como lo hace la firma electrónica.

RECOMENDACIONES

Se recomienda continuar con los estudios sobre el tema, puesto que en Ecuador no ha existido mayor avance en esta área. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos fue redactada en el año 2002 y desde su publicación no ha sido revisada, especialmente en lo que se refiere al tema de firmas electrónicas. Como se ha podido comprobar, por las investigaciones realizadas en el tema a lo largo del mundo, la firma electrónica no es el mecanismo idóneo que se pensaba, puesto que contradice un principio fundamental, que es el de neutralidad tecnológica.

Adicionalmente se recomienda, trabajar en un proyecto de ley que pueda ser presentado por la Universidad de las Américas. Como se mencionó, la ley con la que cuenta el Ecuador no cumple con las exigencias del mundo actual. Existe una necesidad de una actualización, en lo que se refiere a firmas digitales, para poder evolucionar en el tema y sacarle el mayor provecho posible. Este trabajo tiene como finalidad proponer una actualización a la normativa que regula la firma electrónica en el Ecuador y esa resulta la recomendación final.

REFERENCIAS

Acurio, S. D. (24 de febrero de 2016). La Firma Electrónica vs La firma Digital. (M. Bast, Entrevistador)

American Bar Association. (1996). *Digital Signatures Guidelines.* Chicago, Estados Unidos de América: American Bar Association.

Barzallo, J. L. (25 de febrero de 2016). Firmas Electrónicas vs Firmas Digitales. (M. Bast, Entrevistador)

Bertolín, J. A. (2008). *Seguridad de la información. Redes, informática y sistemas de información.* Madrid, España: Paraninfo.

Cabanellas, G. (1993). *Diccionario Jurídico Elemental.* Buenos Aires, Argentina: Heliasta.

Constitución de la República del Ecuador, Registro Oficial 449 de 20 de octubre de 2008 y Registro Oficial 490, Suplemento, de 13 de julio de 2011.

Costas , J. S. (2010). *Seguridad Informática.* Madrid, España: RA-MA.

Davara Rodríguez, M. (2008). *Manual de Derecho Informático.* Navarra, España: Aranzadi.

Devoto, M. (2001). *Comercio Electrónico y Firma Digital.* Buenos Aires, Argentina: LA LEY.

Decreto Ejecutivo 3496 [Reglamento General a la Ley de Comercio Electrónico, firmas Electrónicas y Mensajes de Datos]. (2002). Recuperado el 10 de Septiembre de 2015 de https://plataformamunicipal.ame.gob.ec/recursos/descarga/FacturacionElectronica/baseLegal/9.%20Reglamento%20a%20la%20Ley%20de%20Comercio%20Electr%C3%B3nico,%20Firmas%20Electr%C3%B3nicas%20y%20Mensajes%20de%20Datos.pdf

Fernández Domingo, J. I. (2006). *Derecho de las Nuevas Tecnologías. La Firma Electrónica (Aspectos de la Ley 59/2003, de 19 de diciembre.* Madrid, España: Reus.

Formentín Zayas, Y. M. (2013). LaFirma electrónica, su recepción legal. Especial referencia a la ausencia legislativa en Cuba. *IUS Revista del Instituto de Ciencias Jurídicas de Puebla, Mexico*, 104-120.

Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre Comercio Electrónico. (1996)

ISO/IEC 9796-2. (2002). *ISO/IEC 9796*-2. Recuperado el 15 de Enero de 2016 de http://www.sarm.am/docs/ISO_IEC_9796-2_2002(E)- Character_ PDF_document.pdf

Ley 25.506. Promulgada de Hecho: Diciembre 11 de 2001. Recuperado el 15 de Diciembre de 2015 de https://www.santafe.gov.ar/index.php/web/content/download/58246/283924/file/Ley%2025506.pdf

Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. (1996)

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Registro Oficial 557 de 17 de abril del 2002.

Lorenzetti, R. L. (2001). *Comercio Electrónico.* Buenos Aires, Argentina: Abeledo-Perrot Lexis-Nexis Argentina S.A.

Moreno, M. N. (2002). *DERECHO-e Derecho del Comercio Electrónico.* Madrid, España: Ediciones Jurídicas y Sociales S.A.

Nieves, R. E. (2009). *Derecho Informático. Los Documentos Electrónicos.* Quito, Ecuador: Carpol.

Resolución 479-20-CONATEL-2008. (2008). Recuperado el 18 de Octubre de 2015 de http://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/11/2008-CONATEL-GEN-20-479.pdf

Resolución 480-CONATEL-2008. (2008). Recuperado el 11 de Octubre de 2015 de http://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/11/2008-CONATEL-GEN-20-480.pdf

Resolución 481-20-CONATEL-2008. (2008). Recuperado el 21 de Octubre de 2015 de http://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/11/2008-CONATEL-GEN-20-481.pdf

Rubio, R. V., Rodríguez , C. S., & Muñoz, R. M. (2004). *La Firma Electrónica.* Barcelona, España: Ediciones Experiencia.

Torres, A. Y. (2012). *Principios Fundamentales del Comercio Electrónico.* Bogotá, Colombia: Temis.

ANEXOS

ANEXO 1.

Entrevista realizada al Dr. Jose Luis Barzallo, quien participó en la elaboración de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. El Doctor Barzallo trabaja en un estudio jurídico de nombre: Barzallo & Barzallo Peñaherrera

.

Entrevista Doctor Barzallo:

1. ¿Por qué nuestra ley hace referencia a la firma electrónica y no firma digital?

No creo, estoy convencido, porque cuando se preparaba el modelo, no el modelo, si no el borrado de ley de comercio electrónico que estaba a mi cargo, porque yo fui el redactor de la ley de comercio electrónico, ese fue el concepto que se diseñó. De hecho existía un artículo que era el 29, que estaba en la ley, que hablaba sobre la firma electrónica en general y acto seguido pasaba a hablar de la firma digital. De hecho si te fijas en la ley, en las disposiciones generales, cuarta y quinta si no estoy equivocado, habla sobre el uso de la firma electrónica y la no limitación a ningún tipo de tecnología a la firma electrónica y las otras figuras que encuentras en la ley. Entonces, ese es el razonamiento que tenía la ley. Desafortunadamente por mejor hacer o desconocimiento de los legisladores al momento de aprobar en bloque o por capítulos eliminaron ese artículo, increíblemente para meter un artículo relacionado con empresas unipersonales, que en ese momento lo estaban discutiendo en el congreso y mejorar la ley a criterio de ellos, pero en realidad lo que hicieron fue dejar un vacío. Que si nosotros lo interpretamos y lo vemos de acuerdo a las disposiciones generales, nos damos cuenta que ahí tendría lógica y tendría coherencia la redacción.

2. ¿Cree usted que la ley 67 debe actualizarse en lo que respecta a la firma electrónica y que aspectos deberían considerarse?

Hay algunos aspectos que deberían mejorarse en nuestra ley y creo que estos relacionados con la firma electrónica. Especialmente sobre el uso. Yo sería de

la idea de volver a crear, de volver a introducir la figura de la firma electrónica genérica a efectos de que nos permita tener la utilización o implementación de la firma electrónica alternativa en nuestra legislación, pero en el uso cotidiano poder implementar el uso de la firma electrónica alternativa basada en la firma electrónica genérica.

3. ¿Cree usted que debería existir una normativa independiente para regular la firma digital o electrónica o debe mantenerse dentro de la ley 67?

Tener una ley especializada podría ser. Muchos países optaron por esa opción. De los países que lo hicieron fue España que saco una ley de firma electrónica, ley de firma digital y al final lo que hicieron fue unificar todo en la ley de la sociedad de la información. Nosotros, por técnica legislativa, o porque en un momento determinado esa era la realidad legislativa que teníamos, lo hicimos en un solo cuerpo legal. Por el momento no veo que estorbe, no veo que afecte, no lo tomaría como un objetivo primordial para entrar a reforma. Realmente no lo veo como una necesidad, ni es problema ni afecta para nada. Podría quedarse tal y como está.

ANEXO 2

Entrevista realizada al Dr. Santiago Acurio del Pino, uno de los autores de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. El Dr. Acurio trabaja actualmente en la Corte Provincial de Justicia de Pichincha, en la sala única de lo penal.

1. ¿Por qué nuestra ley hace referencia a la firma electrónica y no firma digital?

Porque la firma electrónica es en este caso, es el género, la firma digital es una especie de firma electrónica. Entonces el tema de la firma digital, cuando tú hablas de firma digital, estás hablando de una firma electrónica basada en lo que se llama infraestructura de clave pública. Es una especia de firma electrónica. Entonces nuestra ley tiene que siempre ir por la generalidad, porque va a regular lo que está ahorita a lo que puede venir. Entonces por el principio de neutralidad tecnológica, la ley ecuatoriana hace referencia a la firma electrónica, porque puede ser que después de algún tiempo cambie la tecnología para generar la firma y automáticamente esa ley quedaría en desuso.

2. ¿Cree usted que la ley 67 debe actualizarse en lo que respecta a la firma electrónica y que aspectos deberían considerarse?

Más que actualizarse no, porque la ley es básicamente un tema genérico de la Ley Modelo de la Uncitral, entonces como es basada en una Ley Modelo, es una ley que, en este caso, ha pasado por una discusión internacional. Adoptamos la ley, la adoptó Colombia, también la adoptó Chile, la adoptó también México, entonces hay algunas legislaciones que han adoptado esto porque el comercio electrónico es un comercio tras-fronteras, entonces yo no le veo la necesidad de cambiar el tema de la firma electrónica.

3. ¿Cree usted que debería existir una normativa independiente para regular la firma digital o electrónica o debe mantenerse dentro de la Ley 67?

A mí me parce que está bien porque, si ósea en otros lugares, por ejemplo Estados Unidos si hay específicamente una ley de firma electrónica. En este caso la nuestra es ley de comercio electrónico, firmas electrónicas y mensajes de datos. Yo creo que no sería necesario que haya una ley, también por el tema de la dispersión normativa. Es preferible tener todo en un mismo código. De hecho la tendencia del legislativo es hacer eso, con el COIP, ahora con el Código General de Procesos es tener todo en un mismo cuerpo normativo. Yo no le veo necesidad de que haya otra, de que este independiente el tema del comercio electrónico de la firma electrónica.