PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE JURISPRUDENCIA

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL

TÍTULO DE ABOGADA

"EL CONTRATO ELECTRÓNICO COMO CONTRATO A DISTANCIA"

MARÍA ALEJANDRA ZAMBRANO TORRES

DIRECTOR: DOCTOR VÍCTOR CEVALLOS VÁSQUEZ

QUITO, 2014

RESUMEN

El presente trabajo tiene como objetivo evidenciar la importancia que ha cobrado el contrato electrónico, en el contexto de la nueva era de la sociedad de la información. Dicha modalidad de contrato incorpora variables al contrato a distancia tradicional como son las técnicas o medios de comunicación electrónicos, el soporte electrónico que lo contiene y la constante circulación de información. El objetivo principal planteado en esta investigación, es lograr determinar si en Ecuador, la normativa vigente protege a las transacciones comerciales electrónicas ante las inseguridades técnicas propias de las redes abiertas.

Para satisfacer estos objetivos, se han desarrollado tres capítulos, los cuales obedecen a una metodología esencialmente descriptiva y explicativa, pretendiendo observar lo ocurrido alrededor del contrato electrónico durante los últimos diez años, específicamente, desde la expedición de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos. De manera general, se aplicó también el método deductivo, pues, se ha partido de datos generales aceptados como válidos, para a partir de ellos, llegar a conclusiones particulares.

Los problemas detectados durante el desarrollo de esta investigación fueron: que las técnicas o medios de comunicación utilizados en contratación electrónica, tanto en su etapa de formación como en su perfeccionamiento, implican riesgos que no se presentaban con los medios de comunicación tradicionales, tales como, la falta de certeza sobre la identidad de los intervinientes, sobre el lugar en el que dicen encontrarse, falta de seguridad sobre la seriedad de la propuesta y contraofertas y, fundamentalmente, falta de seguridad respecto a la confidencialidad con la que será tratada la información circulante.

A pesar de ello, el ordenamiento jurídico prevé la existencia de mecanismos técnico – jurídicos que permiten salvar las dificultades antes referidas, a través de los servicios de certificación a cargo de las entidades de certificación.

De igual manera, se logró determinar que en cuanto a la exigibilidad del cumplimiento del contrato electrónico así como la determinación de responsabilidades, el ordenamiento ecuatoriano resulta insuficiente, pues la normativa comercial y civil no desarrolla supuestos de hecho relacionados al contrato electrónico, ni mucho menos ofrece respuestas ágiles, que se compadezcan con la finalidad del contrato electrónico. Situación similar ocurre en materia penal en cuanto a la dificultad para demostrar la existencia del delito y, luego, para la determinación de responsabilidades.

Como conclusión, se puede afirmar que la legislación ecuatoriana vigente en materia de comercio electrónico, protege parcialmente a los usuarios de Internet que quisieran intervenir en contratación electrónica, señalando que las soluciones a esta situación no se las debe esperar únicamente por el camino de reformas o mayor desarrollo normativo, sino que se requiere también de políticas públicas que incentiven el uso de medios electrónicos, así como también, de una mayor participación de la sociedad civil.

PALABRAS CLAVE: contrato electrónico – sociedad de la información – servicios de certificación – entidades de certificación.

AGRADECIMIENTOS

A la Pontificia Universidad Católica del Ecuador por brindarme la oportunidad de alcanzar mi titulación de tercer nivel de la mano de los valores jesuitas.

A todos quienes forman parte de la Facultad de Jurisprudencia, en especial, al doctor Santiago Guarderas Izquierdo, Decano de la Facultad, así como, al personal administrativo que colabora en Secretaría, quienes siempre estuvieron prestos a colaborar amablemente durante todo mi proceso de estudios.

Finalmente, agradezco sobremanera al doctor Víctor Cevallos Vásquez, director de esta tesis de investigación, quien página a página, fue guiando este proyecto hasta alcanzar su exitosa culminación.

Dedicatoria

A mis padres y hermanos, por su amor y apoyo incondicional. Ustedes son el pilar de mi vida.

ÍNDICE

INTRODUCCIÓN **8**

CAPÍTULO I **14**

1. El Contrato electrónico como contrato a distancia **14**

1.1. Antecedentes 14

1.2 Contrato electrónico 14

1.2.1 Contrato a distancia y/o entre ausentes 16

1.3 Seguridad de las redes: aspectos técnicos e informáticos 18

a) Criptografía 19

b) Función Hash 21

c) Firma electrónica 21

d) Sellado de tiempo 24

1.4. Entidades de certificación.- Mecanismos que protegen las fases de formación del contrato: oferta, aceptación y formación del consentimiento 25

1.5 Formación y terminación del contrato 29

1.5.1 Fase precontractual 29

1.5.1.1 Propuesta: oferta o policitación 29

1.5.1.1.1 Contenido de la propuesta 31

1.5.2 Aceptación 34

1.5.3 Formación del consentimiento 35

1.6 Terminación del contrato 37

1.6.1 Desistimiento 37

1.6.2 Resolución del contrato 38

CAPÍTULO II **41**

2. Responsabilidad en la contratación electrónica **41**

2.1 La Responsabilidad civil 42

2.1.1 Responsabilidad extracontractual por daño informático 45
2.1.1.1 Contenidos ilícitos o nocivos 46
2.1.1.2 Daños a los sistemas informáticos: programas dañinos 48
2.1.1.3 Daños a los sistemas de información: derecho a la intimidad 52
2.1.2 Responsabilidad contractual 58
2.1.2.1 Cláusulas abusivas: cláusulas exonerativas o limitativas de responsabilidad 58
2.2 Responsabilidad penal 60
2.2.1 La información como bien jurídico: carácter económico y privacidad de la información 61
2.2.2 Delitos informáticos 65
a) Acceso ilegítimo a sistemas de información 66
b) Daño o sabotaje informático 68

CAPÍTULO III **70**

3. Seguridad jurídica en el comercio electrónico **70**

3.1 Análisis de la Ley de Comercio Electrónico, Firma Electrónica y Mensajes de Datos ecuatoriana, en el ámbito de la contratación 72
3.1.1 Sanciones penales y administrativas 80
3.2 El comercio electrónico en la Comunidad Andina 86
3.3 Normativa expedida por la Comunidad Europea sobre comercio Electrónico 95

CONCLUSIONES **102**
RECOMENDACIONES **110**
BIBLIOGRAFÍA **113**

INTRODUCCIÓN

Debido a la globalización, los mercados se expanden de maneras nunca antes imaginadas, ampliando la capacidad de ofertas de proveedores a potenciales clientes.

A su vez, el desarrollo tecnológico de las últimas décadas, ha posibilitado la aparición de nuevos medios de información y de comunicación que han configurado la llamada *sociedad de la información*, proceso que se ha desarrollado de la mano de una creciente evolución del sector de las telecomunicaciones, donde se ha creado toda una gama de servicios telemáticos con vastas posibilidades de interconexión[1].

La capacidad que tenemos hoy en día para acceder a la información, a través del Internet, es un proceso únicamente comparable con la aparición de la imprenta, lo cual nos evidencia que estamos ante una nueva revolución de la información y comunicación.

La expansión y desarrollo de la telemática genera múltiples usos, entre los cuales se encuentra el comercio por medios electrónicos.

Esta nueva alternativa de ejercer comercio incorpora elementos que permiten agilizar el proceso comercial logrando reducir costos y tiempos. Sin embargo, también presenta numerosos desafíos para los cuales es necesario proponer soluciones adecuadas que garanticen a las partes intervinientes, la protección de sus derechos, tal y como si se tratara de una transacción comercial tradicional.

De allí la importancia y actualidad del presente tema, pues la aparición de la naciente sociedad de la información, nos obliga a replantear principios tradicionales de la contratación, por ejemplo en lo relacionado a la participación en igualdad de condiciones de los intervinientes

[1] La infraestructura de la sociedad de la información tiene como base lo que se conoce como redes de telecomunicaciones, concepto que abarca medios de transmisión, medios de recepción, tipos de contenidos que se transmiten y objetivos que impulsan a los actores a la transmisión.

en una contratación electrónica dentro del mercado. Si bien es cierto que en Internet prolifera la interactividad y la libertad contractual, ello no implica que el legislador deba despreocuparse en la creación de medidas de protección apropiadas.

Ecuador, tanto en la esfera pública como privada, no puede quedar excluido de estas nuevas posibilidades de comercio; estamos en la obligación de intervenir y participar de sus beneficios, pero para ello, desde el Derecho, debemos reinventar los principios de la contratación comercial. De lo contrario, las variables que surgen en el comercio electrónico podrían generar un desequilibrio económico o la indefensión de alguna de las partes, como por ejemplo ocurre ante la incertidumbre sobre la identidad de las partes contratantes, dificultad propia de los contratos electrónicos a distancia.

Al hablar de un contrato a distancia queremos decir que no existe la presencia física simultánea de las partes contratantes, quienes deberán formar y perfeccionar su consentimiento a través de técnicas o medios de comunicación, que en el caso de los contratos electrónicos implica medios de comunicación electrónicos.

Es por ello que consideramos fundamental volver a estudiar el contrato a distancia y realizar un nuevo análisis de él, pues las técnicas o medios de comunicación que la sociedad de la información permite, distan sobremanera de las técnicas de comunicación tradicionales que lo inspiraron en su nacimiento, como fueron el teléfono o el correo tradicional.

Adicionalmente a ello, el contrato electrónico presenta otra característica que también es incorporada por el avance de la tecnología: el contrato electrónico está contenido en un soporte electrónico, alejado de la corporalidad tradicional del papel.

Pero, como decíamos anteriormente, la sociedad de la información no sólo trae bondades, sino que también incorpora múltiples vulnerabilidades, de carácter técnico, para el comercio electrónico, y para el contrato electrónico en específico, que deben encontrar respuestas en los ordenamientos jurídicos, los cuales deberán proveer al contrato electrónico de la seguridad jurídica que permita incentivar la confianza y el uso de esta modalidad de contratación.

Es por ello que a partir de esta investigación, esperamos se logre apreciar la necesidad en la aplicación de mecanismos jurídicos que garanticen la seguridad en Internet. El beneficio que representa dicha implementación, será el aumento de la confianza en el uso del comercio electrónico, lo que fomentará la concreción de negocios por este medio, incorporándonos inmediatamente en la era de la globalización, con todas las ventajas económicas y sociales que ello representa.

Todo lo antes expuesto deja de manifiesto las razones que motivan esta investigación, la cual tiene como objetivo principal determinar si en Ecuador, la normativa vigente, protege a las transacciones comerciales electrónicas ante las inseguridades técnicas propias de las redes abiertas. Dicho de otro modo, establecer si nuestro ordenamiento jurídico es suficiente para proteger a los usuarios de Internet en sus contratos electrónicos, de manera que contribuya con la disminución de los márgenes de desconfianza que rodean a la interactividad propia del Internet, y en consecuencia, incentivar su utilización.

Para cumplir con tal objetivo, debemos lograr identificar los problemas que se presentan en los contratos electrónicos, en relación a su característica propia por ser contratos a distancia, para al final poder concluir si la normativa vigente brida seguridad jurídica suficiente a los usuarios, frente a los problemas identificados.

Pretendemos responder al objetivo señalado, a través del desarrollo de tres capítulos.

El Capítulo I del **Contrato electrónico como contrato a distancia** empieza acercándonos a las definiciones de contrato electrónico y en particular, a las características que lo convierte en un contrato a distancia. Desarrollaremos el tema respecto de cuáles son los aspectos técnicos que deben ser considerados para que las comunicaciones electrónicas sean seguras, así como los mecanismos técnicos previstos para tales efectos.

Nos referiremos también a las entidades de certificación, es decir, aquellos intermediarios reconocidos por las legislaciones mundiales, para brindar servicios destinados a proteger el

contrato electrónico, tanto en su formación, perfeccionamiento y en cuanto a su integridad en sí mismo.

Definiremos términos como: propuesta electrónica, aceptación electrónica, consentimiento electrónico, y finalmente, el desistimiento y la resolución del contrato electrónico como formas de terminación de los contratos.

Esta nueva terminología será producto de una adaptación de los conceptos clásicos a los nuevos elementos insertos por la sociedad de la información, es donde, el *medio electrónico* será el eje central alrededor del cual gire la construcción de tales definiciones.

Hemos mencionado en reiteradas oportunidades la importancia de contar con un ordenamiento jurídico completo que proteja a los usuarios del comercio electrónico, lo cual implica un régimen claro en cuanto al establecimiento y exigibilidad de responsabilidades, civiles y penales, para los infractores de dicho ordenamiento.

De esta apreciación surge el siguiente capítulo de la presente investigación, que se titula **Responsabilidad en la contratación electrónica**, e inicia el análisis llamando la atención del lector sobre la necesidad de no perder de vista a los elementos caracterizadores de este tipo de contrato: la técnica de comunicación a distancia empleada durante la negociación y proceso de formación como tal, así como, el soporte electrónico en el cual reposa el contrato. Y, añadirá un tercero elemento caracterizador de la contratación electrónica, fundamental a la hora de estudiar la responsabilidad por las conductas que se realizan a través de medios electrónicos: la constante circulación de información.

Una vez realizado este planteamiento, continuaremos con el estudio de la responsabilidad civil contractual y extracontractual, diferenciando entre sistema informático y sistemas de información, como objetos de protección susceptibles de daños por medios informáticos.

Abordaremos algunos supuestos generadores de responsabilidades, siempre en relación a las posibilidades abiertas por el comercio electrónico.

Luego, nos referiremos a la responsabilidad penal como consecuencia de las nuevas formas de criminalidad posibles a través de Internet. Mencionaremos únicamente aquellas nuevas conductas ilícitas, que lesionan bienes jurídicos expuestos en contratación electrónica. Para ello, hemos considerado que el principal bien jurídico lesionado a través de conductas tipificadas por la ley penal, que se encuentra expuesto en contratación electrónica, es la información, con su conexión evidente con el derecho a la intimidad y de propiedad.

Podemos percatarnos que este segundo capítulo considera vital la protección de la información, sea personal o económica. Se trata de un capítulo bastante doctrinario, que pretende desarrollar teóricamente supuestos de responsabilidad civil y penal; así como determinar los problemas que acontecen para el establecimiento de responsabilidades.

Finalmente, el Capítulo III surge como una confrontación entre lo que teóricamente se requiere frente a la realidad del ordenamiento jurídico vigente.

El Capítulo III de la **Seguridad jurídica en el comercio electrónico**, empieza con el análisis de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, promulgada por el legislador ecuatoriano en el año 2002, la cual parecería que aparece en respuesta al desafío que representa la tecnología y que trae consigo la modificación de los paradigmas sociales, culturales y económicos.

Esta primera parte, busca observar minuciosamente el contenido de esta ley, partiendo desde su parte considerativa, tratando de identificar si sus reglas se compadecen con su motivación y objetivos trazados.

En la segunda parte de este capítulo, revisaremos la normativa sobre comercio electrónico aprobada por los países de la CAN: Colombia, Perú y Bolivia, estableciendo sus similitudes y novedades respecto de la legislación ecuatoriana.

Y, por último, estudiaremos la normativa expedida por la Comunidad Europea, la más desarrollada en este tema, lo cual nos volverá evidente lo lejos que estamos de alcanzar niveles óptimos en cuanto a desarrollo normativo del comercio electrónico.

Concluye esta investigación, con los argumentos que buscan responder al objetivo planteado así como el sugerir posibles soluciones, jurídicas y fácticas, a los problemas identificados, que sean aplicables a la realidad y costumbres de nuestro país.

El crecimiento del Internet y del comercio electrónico está íntimamente vinculado al desarrollo y actualización del ordenamiento jurídico que confiera seguridad jurídica a los interesados en negociar electrónicamente. Elevar los niveles de confianza en los miembros de la sociedad de la información, es fundamental, y ello no se dará sin que exista un elevado nivel de protección, el cual debe estar recogido y garantizado a través de las respectivas reformas a la ley, de manera que los nuevos contextos comerciales no pongan en peligro los intereses de los intervinientes o participantes, es decir, que las nuevas formas de contratación que surgen a través de la Internet, gocen de protección similar a la que cuenta una contratación tradicional.

El Derecho debe dar respuestas a las interrogantes nacidas de la evolución de las nuevas tecnologías, constituyendo un desafío. Sobre este tema, Luis Parraguez señala que *"las perspectivas de evolución y enriquecimiento del derecho son tantas cuantas puedan imaginarse para el desenvolvimiento de la misma sociedad humana, ya que aquél no es sino un fiel seguidor superestructural de los pasos de ésta última"*[2].

Esperamos que el contenido de la presente disertación logre responder algunas de las inquietudes que este interesantísimo tema genera, y pueda contribuir al desarrollo del pensamiento jurídico en el campo del Derecho Mercantil.

[2] PARRAGUEZ RUIZ, Luis, Manual de Derecho Civil Ecuatoriano, Libro IV, Teoría General de las Obligaciones, Volumen 1, Impreso en Talleres Gráficos UTPL, Loja, 2000.

CAPÍTULO I

1. El contrato electrónico como contrato a distancia

1.1 Antecedentes

Un contrato, en términos generales, es un acto jurídico bilateral que crea obligaciones, y, por lo tanto, *supone dos partes que han dado su consentimiento*[3].

Según el artículo 1481 del Código Civil ecuatoriano[4] el contrato es un acto por el cual una parte se obliga para con otra a dar, hacer o no hacer alguna cosa.

1.2 Contrato electrónico

Antes de iniciar el análisis del contrato electrónico como contrato a distancia, es necesario realizar ciertas precisiones:

En primer lugar, el contrato electrónico es una especie o modalidad de contrato. Esta afirmación, bastante obvia, implica consecuencias jurídicas importantes ya que extiende los efectos jurídicos del contrato tradicional a aquél[5].

Sin embargo, la sociedad de la información incorpora a la práctica contractual nuevos elementos que le dan un matiz interesante, siendo el principal de ellos, el soporte que lo contiene y a través del cual se produce la *transmisión de voluntades negociales*[6].

---

[3] Arturo Valencia Zea, Álvaro Ortiz Monsalve, Derecho Civil: de las Obligaciones, Bogotá, Editorial Temis, Décima Edición, 2010, p. 57.
[4] Corporación de Estudios y Publicaciones, Código Civil, Quito, 2001.
[5] En relación a los principios de la libertad contractual, consensualidad, etc., principios que encuentran su límite en las nociones de orden público y buenas costumbres. Por otro lado, el contrato electrónico comparte presupuestos de validez con el contrato tradicional, es decir, requiere de capacidad, consentimiento libre de vicios, objeto y causa lícita.

Tecnológicamente hablando, soporte electrónico es el medio inmaterial que contiene la información codificada o digitalizada[7], y que puede transmitirse por equipos electrónicos interconectados a su vez a redes abiertas de comunicación como es el Internet.

Desde el punto de vista jurídico y siguiendo a ORTEGA DÍAZ, el soporte electrónico implica: en primer lugar, la ausencia de papel y firma manuscrita; y, en segunda lugar, que la formación del documento – contrato – se dará mediante algún instrumento informático o electrónico[8].

En cuanto a la primera implicación, el contrato electrónico está contenido en un documento electrónico o mensaje de datos, el cual goza de plena validez jurídica conforme el artículo 2 de la Ley de Comercio Electrónico; y, que permite sea firmado también electrónicamente.

Respecto a la formación del contrato por medio de instrumentos informáticos, esto significa que la expresión de consentimiento entre las partes contratantes, en origen y en destino, se realiza, igualmente, por vía electrónica[9].

La posibilidad de utilizar un soporte de esta naturaleza confiere al contrato electrónico una de sus principales características, que es la distancia física que existe entre las partes negociales al momento de contratar.

---

[6] Andrea Burgos Puyo, El Consumidor y los Contratos en Internet, Bogotá, Universidad Externado de Colombia, 2000, p. 61.

[7] La digitalización es la base de la informática y de los modernos sistemas de telecomunicaciones. Este proceso consiste en convertir en números cualquier tipo de información: textos, sonidos, imágenes. Para ello se utiliza un código binario (unos y ceros) que pueden representar cualquier tipo de información.

[8] Juan Francisco Ortega Díaz, Contratación, Notarios y Firma Electrónica, Bogotá, Editorial Temis, 2010, p. 60.

[9] La legislación comunitaria europea define como *vía electrónica* al "servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la comprensión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, medios ópticos o cualquier otro medio electrómagnético".

Para concluir, podemos decir que *contrato electrónico es aquél que existe en función de un soporte electrónico, por tanto, carece de la corporalidad física tradicional, y más bien, utiliza instrumentos informáticos en su proceso de formación; para ello, hace uso de técnicas de comunicación a distancia, lo cual lo ubica en la categoría de los contratos a distancia.*

1.2.1 Contrato a distancia y/o entre ausentes

BURGOS PUYO señala que los contratos a distancia nacen como una categoría especial que busca salvaguardar los intereses de consumidores y usuarios frente a posibles abusos que puedan producirse en su perfeccionamiento, siempre que éstos se celebren entre personas no presentes y utilizando como vehículo de expresión cualquiera de los innumerables procedimientos que la técnica actual en medios de comunicación de masas pone a disposición del comercio: escritos, auditivos, visuales, audiovisuales; a los cuales se agrega el Internet como herramienta de comunicación que permite la comunicación a distancia[10].

Las características que convierten al contrato electrónico en un *contrato a distancia* son:

a) La no presencia física simultánea de las partes en el mismo lugar de celebración del contrato; y,
b) El uso de una técnica o medio de comunicación a distancia.

La no presencia física simultánea de las partes contratantes significa que el soporte electrónico y la vía electrónica a través de la cual transcurren las diferentes etapas de la contratación, permite perfectamente que las partes contratantes se encuentren distantes físicamente e incluso en circunscripciones territoriales distintas.

En segundo lugar, el contrato a distancia requiere como elemento fundamental el uso de una "técnica de comunicación a distancia" – simultánea o no simultánea-. En el caso del

[10] Andrea Burgos Puyo, op. cit., p. 70.

comercio electrónico, las más difundidas en su utilización son: el correo electrónico, los sitios web, el chat o IRC[11], webchat, mensajería instantánea, videoconferencia.

La naturaleza de la técnica de comunicación a distancia utilizada determina la simultaneidad en la comunicación[12], y ello establecerá si estamos ante un contrato entre ausentes o entre presentes.

La diferencia viene dada por el "tiempo real" en la comunicación. La comunicación es sincrónica o en tiempo real cuando las partes que intervienen interactúan en ese mismo momento, sin tiempos de espera[13]. Es asincrónica, cuando si existen tiempos de espera.

Si analizamos las técnicas de comunicación a distancia más usuales del Internet, tenemos que únicamente en la mensajería instantánea la comunicación es en tiempo real, pues existe inmediatez en la comunicación entre oferente y aceptante. En otros casos, tales como correo electrónico, la comunicación no es en tiempo real (asincrónica), por tanto, se convierte en una contratación entre ausentes.

La *simultaneidad* en la técnica de comunicación utilizada es fundamental en los contratos electrónicos para ubicar el momento y el lugar en que se forma el consentimiento, y que determina en sí, el proceso formativo del contrato y el inicio de los efectos jurídicos que de él se deriven: si de la simultaneidad se infiere que la contratación es entre presentes o entre ausentes, variarán las reglas que la ley establece para la configuración del consentimiento (confluencia de oferta y aceptación).

[11] Internet Relay Chat o Canal de Charla de Internet: sistema a través del cual puede el usuario comunicarse por escrito u oralmente a tiempo real.
[12] La simultaneidad es definida por Guillermo Cabanellas como "la concurrencia en el tiempo y en la acción, con diversidad de planes u obras".
[13] La nueva comunicación virtual se concibe de dos maneras: a) Asincrónica: cuando no existe conexión directa con el interlocutor; b) Sincrónica: los intervinientes llegan un diálogo de manera conjunta, a una misma hora, con capacidad de reacción inmediata.

En conclusión, el contrato electrónico es un contrato a distancia al cual se aplican las reglas de los contratos entre ausentes o entre presentes, según sea el caso, esto, para efectos de determinar el inicio de los efectos jurídicos del mismo.

1.3 Seguridad de las redes: aspectos técnicos e informáticos

Los problemas de seguridad en las comunicaciones a través de redes abiertas son preocupación constante y recurrente de los usuarios del comercio electrónico.

Según GAETE GONZÁLEZ es sumamente importante dotar al documento electrónico de validez suficiente, es decir, éste debe contar

> *(…) con las medidas de seguridad técnicas necesarias para que se lo entienda premunido de la suficiente seguridad jurídica a objeto de impedir o al menos imposibilitar al máximo posible la concurrencia de riesgos originados en las etapas de elaboración y transmisión de datos, fueren éstos involuntarios o voluntarios. De esta manera, la creación de una infraestructura de seguridad favorece no sólo al documento, sino además al comercio electrónico que se ejerce a través de él*[14].

Siguiendo a ROSELLÓ MORENO[15], se considera que las comunicaciones electrónicas deben cumplir con ciertos fines para ser reconocidas como "comunicaciones seguras", tales fines son:

- ✓ la autenticación: se refiere a la certeza que quien envía un mensaje es quien dice ser.
- ✓ la integridad: certeza de que el mensaje no ha sido manipulado ilícitamente durante su transmisión o al menos, tener conocimiento de cualquier manipulación.
- ✓ el no repudio: se vincula a la seguridad en el sentido de que no se pueda negar la participación de los intervinientes en una comunicación electrónica. Existe el no

[14] Eugenio Alberto Gaete González, Instrumento público electrónico, Barcelona, Editorial Bosch, Tercera Edición, 2009, p. 229.
[15] Rocío de Roselló Moreno, El comercio electrónico y la protección a los consumidores, Barcelona, Editorial CEDECS, 2001, p. 24.

repudio de origen y de destino, es decir, que el emisor o el destinatario no nieguen más tarde haber enviado o recibido una comunicación.; y,

- ✓ la confidencialidad: se asocia a la seguridad de que la información que es enviada a través de la Red sólo puede ser conocida por su destinatario, de forma que resulte infructuoso para terceros el conocimiento de aquélla en caso de intercepción, sea accidental o voluntaria.

De esta manera, la tecnología ha creado mecanismos o funciones matemáticas que posibilitan el cumplimiento de dichos objetivos y brindan seguridad tecnológica a las transacciones realizadas a través de redes abiertas.

Estos mecanismos técnicos son:

a) Criptografía
b) Función Hash
c) Firma electrónica

a) Criptografía

La Enciclopedia Larousse define la criptografía como un "conjunto de técnicas que permiten cifrar y descifrar la información"[16].

Los mecanismos que se utilizan para cifrar o descifrar la información son las *claves*, las cuales constan de una gran longitud de números que siguen un algoritmo matemático.

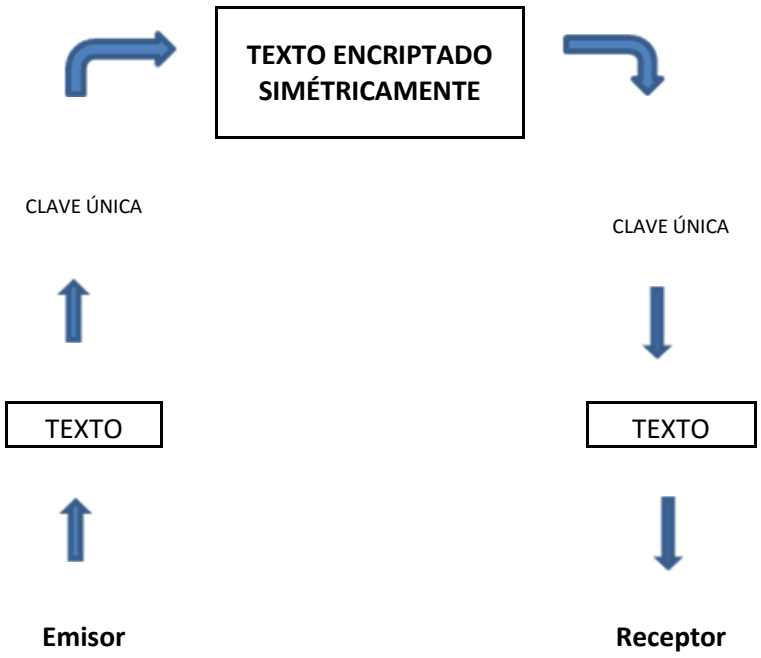
Se utilizan dos técnicas para encriptar o desencriptar, éstas son: *técnica de cifrado simétrico* y la *técnica de cifrado asimétrico*.

La primera es un mecanismo más sencillo donde tanto el emisor como el receptor del mensaje comparten una misma clave, que permitirá cifrar y descifrar la información. Presenta la

[16] Gran Enciclopedia Larousse, Tomo 6, Barcelona, Editorial Planeta, 1987.

ventaja de su sencillez; pero, el inconveniente es la dificultad de mantener en secreto una clave compartida por dos personas lo cual atentaría contra la seguridad que se pretende garantizar.

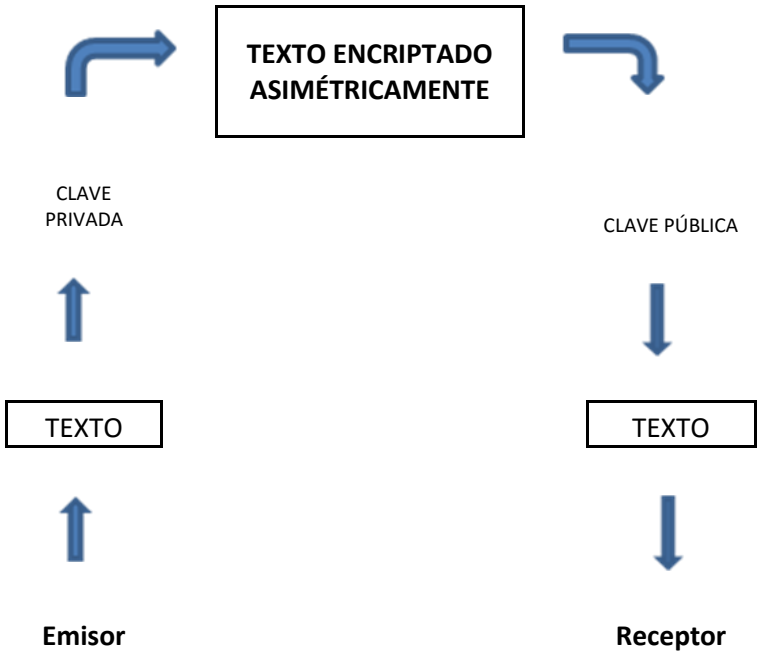
GRÁFICO 1: Técnica de cifrado simétrico



La segunda técnica de cifrado asimétrico utiliza dos claves, una pública y otra privada. La clave privada es entregada de manera confidencial a un usuario, y la pública es conocida por una generalidad. Ambas claves se encuentran asociadas matemáticamente[17] de modo que lo que cifra una clave sólo puede ser descifrado por su pareja y viceversa.

[17] Al principio se trataba de simples operaciones aritméticas, más tarde se recurrió a operaciones algebraicas más complicadas y en la actualidad se emplean técnicas de encriptación o cifrado que utilizan un sistema de curvas elípticas. (Fuente: www.derecho.org/redi).
El algoritmo de clave asimétrica más utilizado es R.S.A., equivalente al nombre de sus creadores: Rivest, Shamir y Adleman.

GRÁFICO 2: Técnica de cifrado asimétrico



b) Función Hash:

Consiste en una función matemática que tras su aplicación genera un resumen o compendio a través del cual se consigue verificar la integridad de las comunicaciones. ROSELLÓ MORENO señala que "la característica fundamental de la función *hash* estriba en su carácter único, dado que no pueden existir dos mensajes diferentes con el mismo resumen, siendo detectable por tanto cualquier alteración"[18].

c) Firma Electrónica:

A decir de Martínez Nadal, citado por ROSELLÓ MORENO, una **firma electrónica** es "*cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo con todas o algunas de las funciones características de una firma manuscrita"*[19].

[18] Rocío de Roselló Moreno, *op. cit.*, p. 46.
[19] Rocío de Roselló Moreno, *op. cit.*, p. 42.

La anterior es una definición que la doctrina cataloga como firma electrónica simple. Existe también la firma electrónica avanzada. La principal diferencia entre ambas radica en los mecanismos de seguridad que se utilizan, pues la primera no permite tener la certeza sobre la identidad del firmante ni sobre el buen uso que se haga de los datos del signatario. Por ello surge la firma electrónica avanzada, la cual permite

> *la identificación del signatario, que ha sido creada por medios que el signatario mantiene bajo su exclusivo control y además, está vinculada de manera única al signatario y a los datos a los que se refiere, permitiendo detectar cualquier modificación ulterior de éstos*[20].

En la actualidad, la firma electrónica más utilizada y que goza de mayor reconocimiento e incluso es considerada la única firma electrónica segura, es la llamada firma digital[21].

Cabe destacar aquí, que tal como señala ROCÍO DE ROSELLÓ, los ordenamientos jurídicos, entre ellos el ecuatoriano, se refieren genéricamente a la firma electrónica, sin hacer distinción entre simple, avanzada o incluso digital (que como mencionáramos anteriormente, es una variedad de la firma electrónica avanzada). No se hace distinción debido a que se acoge una postura abierta tecnológicamente, según la cual se espera el surgimiento de nuevas tecnologías que difieran de la tecnología utilizada actualmente por la firma digital.

El ordenamiento jurídico nacional y extranjero le da a la firma electrónica el mismo valor que si se tratara de una firma manuscrita[22], otorgándole todas las consecuencias jurídicas de ésta y dándole de valor de prueba dentro del proceso.

El funcionamiento de la firma electrónica parte de la existencia de una clave privada y otra pública, en cuyo proceso de creación se utiliza la *técnica de criptografía de clave asimétrica*.

---

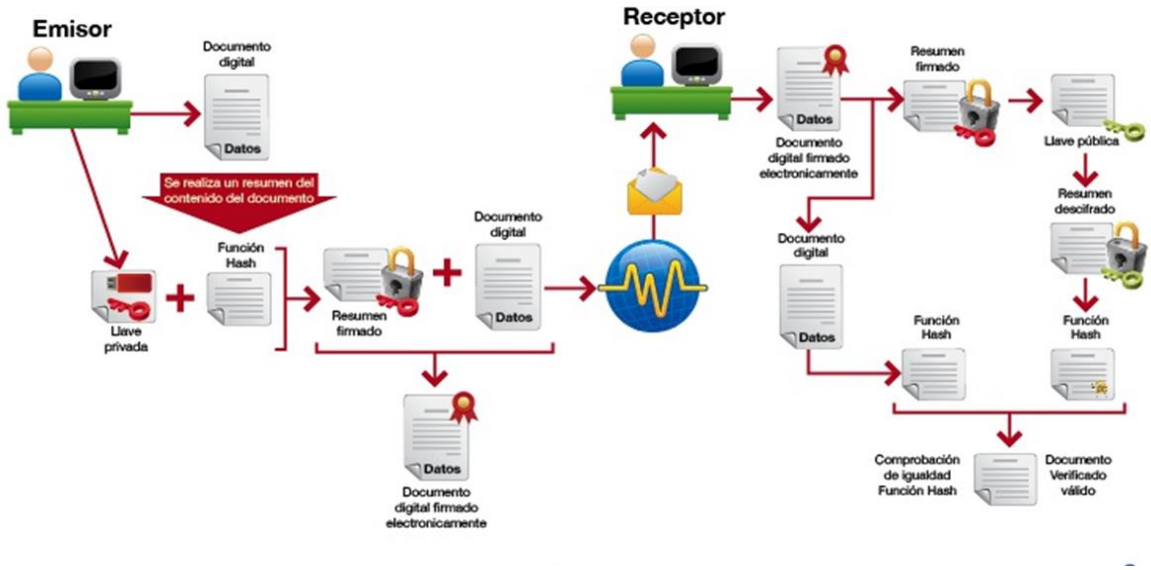
[20] Rocío de Roselló Moreno, op. cit., p. 45.
[21] Rocío de Roselló Moreno, op. cit., p. 46.
[22] La firma manuscrita ha sido, desde el aparecimiento del documento en soporte papel, el signo único que una persona realiza con el fin de identificarse y de asumir el acto que signa, cuya finalidad es doble: asumir la autoría y adquirir los derechos y obligaciones que del documento se desprende en Juan Francisco Ortega Díaz, ob. cit., p. 84.

La clave privada la mantiene en secreto el signatario o solicitante a una entidad de certificación de una firma electrónica.

El procedimiento es el siguiente: primero el Emisor crea su mensaje de datos. En segundo lugar, utiliza la función *hash* – explicada anteriormente – con la cual se obtiene un resumen de la información que se va a enviar. Por último, se hace uso de la clave privada que le permite acceder a su firma electrónica, la cual cifra dicho resumen y el mensaje de datos y, a su vez, autentica su identidad.

El Destinatario por su parte, utiliza la clave pública que el Emisor le ha proporcionado para descifrar el resumen. Al momento de descifrarse el Emisor será autenticado. Como segundo paso, el Destinatario debe aplicar también la función *hash* al mensaje original recibido para comprobar que el resumen resultante coincide con el resumen cifrado que ha recibido y que ha sido descifrado. Si los resúmenes resultan diferentes, significa que el mensaje ha sido alterado.

GRÁFICO 3: Proceso firma electrónica[23]



[23] Fuente: http://www.conatel.gob.ec/site_conatel/images/stories/firmaElectronica/Proceso_firma_electronica

d) Sellado de tiempo

El Timestamping o Sellado Digital de Tiempo es un mecanismo en línea que ofrece evidencias, técnicas y jurídicas, de que un objeto digital – documento, software, imagen, audio, video – existe y no ha sido modificado desde un instante determinado en el tiempo. Generalmente este servicio lo ofrece una tercera parte de confianza, reconocida oficialmente, que emite sellos de tiempo verificables y con valor probatorio. En el comercio on-line, garantiza que las transacciones se realizan en un momento particular, disminuyendo las posibilidades de fraude y repudio. Utilizado conjuntamente con una firma digital, ofrece una evidencia del instante en el que el documento se ha firmado, otorgándole medios adicionales para garantizar el no repudio[24].

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, en su Disposición General Novena que establece un Glosario de Términos, define el Sellado de Tiempo como una "anotación electrónica firmada electrónicamente y agregada a un mensaje de datos en la que conste como mínimo la fecha, la hora y la identidad de la persona que efectúa la anotación".

El artículo 34 del Reglamento para la Acreditación, Registro y Regulación de Entidades Habilitadas para prestar servicios de Certificación de Información y Servicios Relacionados, establece que el servicio de sellado de tiempo incluye:

1. Recepción del Mensaje de dato a sellar electrónicamente.
2. Anotación electrónica de la fecha, hora, lugar en que se produce el sellado de tiempo. Este proceso debe asegurar que sea imposible sellar un documento con un tiempo y fecha diferente de la actual. Tomando como tiempo de referencia UTC (Universal Time Coordinated).
3. Firmar electrónicamente el documento sellado para garantizar su integridad y autenticidad de acuerdo a la ley.

[24]Fuente: http://www.anf.es/es/productos/generales/timestamping.html

4. Servicios de encriptación o aseguramiento de confidencialidad cuando sea solicitado.
5. Opcionalmente y con la autorización expresa de los signatarios, la entidad de certificación de información podrá prestar un servicio de certificación u otorgar nuevas certificaciones mediante la reposición del original firmado. Para ello la entidad de certificación de información podrá realizar la generación de un respaldo del documento sellado para su consulta posterior y verificación de la información de sellado de tiempo.

Si recordamos los fines que persiguen los mecanismos técnicos para obtener comunicaciones seguras, obtendremos el siguiente cuadro resumen:

"COMUNICACIONES SEGURAS"	MECANISMOS TÉCNICOS DE SEGURIDAD
Autenticación	Firma electrónica
Integridad	Firma electrónica / Función hash
No Repudio	Firma electrónica
Confidencialidad	Criptografía
No repudio Momento de envío o recepción de mensajes de datos	Sellado de Tiempo

1.4 Entidades de certificación.- Mecanismos que protegen las fases de formación del contrato: oferta, aceptación y formación del consentimiento

El aparecimiento del comercio electrónico demanda del legislador la creación de medidas legislativas eficaces que resuelvan problemas concretos y al mismo tiempo atenúen los riesgos o inconvenientes que conlleva esta nueva forma de comercio, y en definitiva, creen las

condiciones necesarias para la existencia de un clima de seguridad jurídica. Como señala MIRANDA SERRANO:

> *(…) tales medidas deben estar encaminadas a generar confianza hacia el tráfico jurídico y económico celebrado a través de los modernos canales informáticos y electrónicos. Esto quiere decir, que los sujetos participantes confíen en el comercio electrónico al menos en los mismos términos en que vienen confiando en el comercio tradicional*[25].

El principal problema con el que se encuentran los sujetos intervinientes en una transacción electrónica se refiere a la falta de identificación de las partes. Este problema se resuelve acudiendo a "terceros de confianza" o entidades de certificación, definidos por nuestra legislación como Autoridades de Certificación.

La entidad de certificación, doctrinariamente hablando, podría ser persona natural o jurídica, pública o privada, siempre que cuente con la suficiencia técnica, financiera y legal que cada país exija para su funcionamiento. ROSELLÓ MORENO señala que se reconocen dos posibilidades para el establecimiento de las autoridades de certificación[26]: el libre establecimiento, el cual permitiría que cualquier persona natural o jurídica pueda instalarse libremente y ofrecer servicios de certificación basado únicamente en el acuerdo entre las partes; y, una segunda posibilidad que condiciona el inicio de operaciones de la certificadora a la obtención de una licencia pública. En Ecuador se aceptan ambas posibilidades, es decir, se habla de entidades acreditadas y no acreditadas, una de las diferencias entre ellas, por ejemplo, se refiere al valor probatorio de los certificados que emita: los certificados emitidos por entidades acreditadas gozan de una presunción de validez; mientras que en los emitidos por entidades no acreditadas, su validez debe ser probada[27].

---

[25] Luis Miranda Serrano, Comercio electrónico y protección a los Consumidores: *"Derecho de Desistimiento del Consumidor en la Contratación Electrónica"*, coordinado por Alejandra Botana García, Madrid, Editorial La Ley, 2001, p. 585.

[26] Rocío de Roselló Moreno, op. cit., p. 61. .

[27] Artículo 9 del Reglamento para la Acreditación, Registro y Regulación de Entidades Habilitadas para prestar servicios de Certificación de Información y Servicios Relacionados

Nuestro país ha considerado prioritario el promover políticas que fortalezcan el desarrollo y aplicación efectiva del comercio electrónico, en virtud de lo cual, en 2008 se realizaron reformas al Reglamento para la Ley de Comercio Electrónico y Mensajes de Datos[28]. En dichas reformas se amplió y consolidó el proceso de acreditación y registro de las Entidades de Certificación.

Es así como esta reforma, conjuntamente con el Reglamento para la Acreditación Registro y Regulación de Entidades Habilitadas para prestar Servicios de Certificación de Información y Servicios Relacionados[29], constituyen el marco legal existente que regula la autorización y funcionamiento de las entidades o autoridades de certificación en Ecuador, autorización que opera a través de acto administrativo del CONATEL.

El principio general que rige en el tema del establecimiento de entidades de certificación es el de libertad de constitución y establecimiento, el cual busca eliminar toda clase de discriminación en la obtención de la licencia y que a su vez fomenta la competitividad en el mercado.

La Autoridad de Certificación, una vez acreditada por las autoridades de telecomunicaciones de este país mediante el otorgamiento del respectivo título habilitante[30], estará facultada para emitir certificados de firma electrónica, principalmente, y cualquier otro tipo de certificado relacionado que proporcione seguridad. El listado de servicios relacionados que consta en las legislaciones europeas y americanas es siempre meramente enunciativo pues la innovación en la tecnología no permitiría hacer una limitación taxativa al respecto.

Tanto la legislación nacional como extranjera, han planteado también, la posibilidad de considerar al Notario, como un tercero relacionado, que podría prestar ciertos servicios de

[28] Reformas al Reglamento para la Ley de Comercio Electrónico y Mensajes de Datos, Registro Oficial n. 440, de 06 de octubre de 2008.
[29] Registro Oficial n. 196 de 23 de octubre de 2003.
[30] El título habilitante otorgado por el CONATEL contiene ciertos requisitos legales tales como la descripción de los servicios autorizados, obligaciones y responsabilidades, mecanismos para la protección de la información a la que tuvieren acceso, duración del título, la capacidad para prestar estos servicios a entidades públicas o privados, causales para la extinción del título.

certificación de documentos electrónicos o entrega de certificados a los solicitantes de firmas electrónicas.

En Ecuador la primera Autoridad de Certificación acreditada fue el Banco Central del Ecuador, autorizado y registrado por el CONATEL y SENATEL, respectivamente, en el año 2008.

En 2006 algunas compañías nacionales obtuvieron permisos por parte del CONATEL, institución que luego de dos años revocó las autorizaciones concedidas por cuanto se consideró que las resoluciones aprobatorias carecían de legitimidad, criterio al que se llegó luego de una consulta a la Procuraduría General del Estado[31].

A la presente fecha, existen tres personas jurídicas acreditadas por el CONATEL:

ENTIDADES DE CERTIFICACIÓN ACREDITADAS[32]

	Resolución de Acreditación	**Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados**
Banco Central del Ecuador	RES-481-20-CONATEL-2008 (08-10-2008)	SECCIÓN 1, TOMO 1 a FOJAS 1 OF-DGGST-2008-1006 (06-11-2008)
ANF Autoridad de Certificación	RES-639-21-CONATEL-2010 (22-10-2010)	SECCIÓN 1, TOMO 2 a FOJAS 1 OF-DGGST-2010-1794 (21-12-2010)

[31] SENATEL realizó una consulta a la Superintendencia de Bancos y Seguros con respecto a las garantías de responsabilidad con la que debían contar las entidades de certificación. Este organismo de control llevó dicha consulta a la Procuraduría General del Estado, quien consideró improcedentes las resoluciones aprobatorias emitidas por el CONATEL con las que se autorizaba el funcionamiento de las compañías mencionadas por cuanto estas contenían figuras (título habilitante y permisos) distintos a las que prevé la Ley de Comercio Electrónico y diferencias en cuanto a la rendición de garantías. Por el carácter vinculante de la consulta hecha a la Procuraduría, el CONATEL emite una nueva resolución mediante la cual deroga el anterior acto administrativo por considerarlo de imposible cumplimiento por cuanto está en contradicción con la Ley de Comercio Electrónico y con las últimas reformas al reglamento de dicha materia. **(Fuente: Resolución 478-20-CONATEL-2008, RO 455 de 28 de octubre de 2008)**.

[32] Fuente: www.conatel.gob.ec

Security Data	RES-640-21-CONATEL-2010 (22-10-2010)	SECCIÓN 1, TOMO 3 a FOJAS 1 OF-DGGST-2010-1802 (23-12-2010)

En cuanto a las obligaciones de las entidades de certificación, la principal radica en la comprobación de la identidad del solicitante del certificado. Adicionalmente, son también obligaciones del emisor de certificados el contar con sistemas y productos fiables protegidos ante cualquier alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación; tomar medidas contra la falsificación de certificados; disponer de recursos económicos suficientes para operar y hacer frente a su posible responsabilidad; confidencialidad en la información que manejan de los usuarios; éstas entre las principales.

1.5 Formación y terminación del contrato

1.5.1 Fase precontractual

1.5.1.1 Propuesta: oferta o policitación

La propuesta, a decir de PERALES VISCASILLAS, puede definirse como aquélla declaración de voluntad, que siendo suficientemente precisa, se encamina a la perfección del contrato mediante el concurso con la declaración del destinatario de la propuesta[33].

Dicha propuesta varia de nombre según esté dirigida a una persona determinada o al público en general; así surge el concepto de oferta y policitación[34], respectivamente. Ambas posibilidades son recogidas por el Código de Comercio ecuatoriano.

[33] María del Pilar Perales Viscasillas, Comercio electrónico y protección a los Consumidores, *"Formación del Contrato",* coordinado por Alejandra Botana García, Madrid, Editorial La Ley, 2001, p. 417.

[34]A criterio de OSPINA y OSPINA, la policitación, salvo el caso de que implique un claro compromiso del proponente, es una simple invitación general para que cualquier interesado formule una oferta

Habíamos mencionado anteriormente que cuando se trata de un contrato a distancia, es fundamental la intervención de una técnica de comunicación a distancia. La legislación comercial ecuatoriana se limita a reconocer las ofertas por escrito en aquellos casos en que las partes residen en diferentes plazas, sin determinar requisitos o cualidades que deba observarse en la transmisión de dicha oferta por escrito, más allá de entender que se refiere únicamente al correo tradicional. En la legislación colombiana, un poco más amplia en este tema, se establece que cuando se trata de contratos entre ausentes, las ofertas se entienden comunicadas cuando utilizan cualquier medio adecuado para hacerla conocer al destinatario.

Según BURGOS PUYO, esta situación queda resuelta en la legislación europea, cuya Directiva 97/7/CE en el artículo 2.1 establece como definición de *técnica de comunicación a distancia* "todo medio que permita la celebración del contrato sin presencia física simultánea de las partes"[35].

Las técnicas de comunicación a distancia más difundidas en el comercio electrónico son:

a) **Correo electrónico:** "constituye una variable electrónica, mediante la cual es posible intercambiar información de computador a computador, a través de un intermediario, generalmente Internet, a través de códigos alfanuméricos escritos mediante un texto legible que puede ser leído en el propio computador, o bien *per cartam* a través de una impresora, y que pueden ser almacenados"[36].

b) **Chat:** sistema de conversación en tiempo real en modo de texto que permite la interacción de dos o más personas simultáneamente, situadas en diferentes lugares[37].

---

concreta. Ver en Ospina Fernández Guillermo, Ospina Acosta Eduardo, Teoría General del Contrato y del Negocio Jurídico, Bogotá, Editorial Temis, 2005, Séptima edición, p. 156.

[35] Andrea Burgos Puyo, op. cit., p. 66.

[36] Eugenio Alberto Gaete González, op. cit., p. 144.

[37] Andrea Burgos Puyo, op. cit., p. 68.

c) **Sitio web:** Conjunto de páginas web que están relacionadas entre sí, por lo general, porque se ingresan desde un mismo dominio o porque mantienen constante la raíz de la dirección URL. Un sitio web puede estar constituido de una o más páginas web. La página web principal de un sitio web suele llamarse *index,* que puede tener la extensión .htm, .php, .asp, entre otras. Muchas veces "sitio web" y "página web" son tomados como sinónimos, pero no lo son[38].

d) **EDI:** significa Intercambio Electrónico de Datos. Es el uso de una serie de redes de computadores para transferirse información entre ellos[39].

En cuanto al soporte electrónico que contiene la propuesta, esto es, el documento electrónico o mensaje de datos, este goza de plena validez jurídica en virtud de los artículos 2 y 45 de la Ley de Comercio Electrónico y Mensaje de Datos, los cuales se refieren al reconocimiento jurídico de los mensajes de datos y a la validez de los contratos electrónicos, respectivamente.

En conclusión, la *propuesta electrónica* es aquella contenida en un mensaje de datos y que se transmite a través de una técnica de comunicación a distancia y que puede estar dirigida a determinada persona o al público en general.

1.5.1.1.1 Contenido de la propuesta

Para que la propuesta cause efectos jurídicos ésta debe ser completa, clara e íntegra, caso contrario, podría ser considerada como una mera exploración de ánimo.

Es necesario que "en la oferta conste la intención del oferente de quedar obligado, intención que ha de ser seria y manifestada de forma definitiva, completa, consciente y libre, esto es, que no esté aquejada de alguna irregularidad que pueda dar lugar a algún vicio del consentimiento"[40]

[38] Fuente: http://www.alegsa.com.ar/Dic/sitio%20web.php
[39] Eugenio Alberto Gaete González, op. cit., p. 143.
[40] María del Pilar Perales Viscasillas, op. cit., p. 418. .

En términos generales, la propuesta debe cumplir los siguientes requisitos:

- ✓ Indicación del destinatario determinado o si va dirigida al público en general.
- ✓ Indicación del tipo de contrato que se propone.
- ✓ Objeto: bien o servicio propuesto, así como sus especificaciones.
- ✓ Precio y forma de pago.
- ✓ Modalidades de entrega o de ejecución del contrato.
- ✓ Condiciones para modificaciones o retractación de la oferta.
- ✓ Plazo de validez de la oferta.

El plazo de validez de la oferta es requisito fundamental, pues de él se derivan algunos efectos jurídicos: a) Únicamente durante la vigencia de la oferta es posible su modificación o arrepentimiento de la misma; b) Durante vigencia de la oferta ésta es obligatoria y por tanto, genera responsabilidad por los daños y perjuicios causados; y, c) Sólo puede haber Aceptación mientras la propuesta está vigente.

En relación a la modificación o retractación en la oferta, nuestro Código de Comercio establece en el artículo 143 la oportunidad para la retractación de la propuesta, la cual procede siempre que se la realice "en el tiempo que medie entre el envío de la propuesta y la aceptación".

Respecto a la obligatoriedad de la Propuesta, OSPINA y OSPINA expresan:

> *"... si se quiere evitar todo reproche, antes de retirar la oferta, debe asegurarse de que ella aún no ha dado lugar a que el otro interesado haya comenzado a prepararse para la convención propuesta, haciendo gastos y tomando medidas que, a la postre, le resulte perjudiciales, caso de no celebrarse dicha convención. (...) retirar una oferta sin saber si este acto será indiferente o perjudicial para el otro interesado, equivale a incurrir en culpa manifiesta. (...) Además de la lógica, de la historia y de las exigencias de seriedad y seguridad en el comercio, la justicia que debe reinar en todas las relaciones entre los particulares también reclama el reconocimiento legal de la obligatoriedad de la oferta.*

> *Quien recibe la propuesta de un negocio, puede considerarla conveniente para sus intereses; puede desistir de otros proyectos que también le son ventajosos; puede tomar medidas y hacer gastos para ponerse en condiciones de cumplir el negocio propuesto; etc. O mejor dicho, queda expuesto a sufrir perjuicios más o menos graves, si el proponente no se allana a hacer honor a su palabra, so pretexto de que al formular la oferta no entendió obligarse"*[41].

Este es el criterio que acoge el legislador ecuatoriano en el artículo 144 del Código de Comercio cuando establece que la retractación tempestiva impone la obligación de indemnizar los gastos que la persona a quien fue dirigida la propuesta – persona determinada – hubiera incurrido y los daños y perjuicios que sufriera. En el caso de la policitación, el artículo 146 ídem, dispone que la oferta pública obliga a quien la hace, y determina dos excepciones: cuando se pretende aceptar la oferta fuera de su término de vigencia, o, cuando la oferta ha sido modificada por una oferta posterior.

Por aplicación del principio de autonomía de la voluntad y libertad contractual, el plazo de validez de la oferta está determinado por el Proponente. Sin embargo, el artículo 142 ídem señala que en los casos de Propuestas realizadas por escrito, la Aceptación se debe dar "a vuelta del primer correo que salga 24 horas después de recibida la oferta". Vencido ese plazo, la Aceptación se vuelve extemporánea. Esto nos permite entender que el legislador previó un tiempo de vigencia para la oferta realizada por escrito por medios tradicionales; pero, no olvidemos que estamos ante medios electrónicos, y su rapidez y dinamismo, evidentemente, no fueron considerados al momento de elaboración de esta norma. En consecuencia, esta norma es ineficaz en contratos formados por medios electrónicos y debería estarse a la autonomía de la voluntad contractual, atendiendo por supuesto a la naturaleza jurídica de cada contrato.

[41] Ospina Fernández Guillermo, Ospina Acosta Eduardo, op.cit., p. 151-153.

1.5.2 Aceptación

La aceptación es "el acto de adhesión a la propuesta por la persona o personas a quienes ésta se ha dirigido"[42].

El Diccionario Enciclopédico de Derecho Usual de Cabanellas define la aceptación contractual como:

> *acto por el cual se perfecciona un contrato, al formularse la manifestación de voluntad que presta el solicitado asentimiento o la proposición del oferente; o por admitir éste las modificaciones propuestas por el destinatario de la promesa u oferta. La aceptación contractual constituye a la vez la causa de existencia de las convenciones bilaterales, prueba de su perfección y origen de la obligación de cumplir lo expresamente pactado, y cuanto procede de su naturaleza, conforme a la buena fe, el uso o a la ley*[43].

La aceptación es una *"declaración de voluntad de carácter recepticio, al ir dirigida al oferente, y que, de coincidir con los mismos términos de la oferta, da nacimiento al contrato"*[44].

El efecto jurídico de la Aceptación pura y simple, al igual que en la contratación tradicional, es la configuración del consentimiento negocial, y con ello, la perfección del contrato que lo vuelve inmediatamente exigible a las partes.

En términos generales, las reglas que se aplican para la aceptación en la contratación tradicional son similares a las que rigen en el comercio electrónico. La forma de aceptación puede ser expresa o tácita; pero, sostiene Perales Viscasillas, que en materia de contratación electrónica, es imposible que el silencio del destinatario se pueda considerar como una

---

[42] Guillermo Ospina Fernández, Eduardo Ospina Acosta, op. cit., p. 161.
[43] Guillermo Cabanellas, Diccionario Enciclopédico de Derecho Usual, Buenos Aires, Editorial Heliasta, 1997, 25ª edición, Tomo I, p. 99.
[44] Lisette Hernández Fernández, La Oferta y la Aceptación: Especial referencia a los contratos celebrados por medios electrónicos, publicado en Alfa-Redi: Revista de Derecho Informático, n. 76, noviembre 2004.

aceptación tácita de la propuesta, excepción que cabe en aquellos casos en que las partes mantuvieran relaciones comerciales habituales en que se hubiera acordado darle este significado al silencio, o, cuando las partes lo han estipulado así[45].

La Aceptación debe exteriorizarse oportunamente, es decir, mientras esté vigente la Propuesta, considerando que de realizarse modificaciones o condicionamientos a la propuesta inicial, ésta se considerará como una nueva propuesta.

La innovación que incorpora el comercio electrónico es que la manifestación oportuna de la Aceptación, sea expresa o tácita, se hace conocer al Proponente a través de una técnica de comunicación a distancia, lo cual determina la inmediatez o unidad de acto que puede o no existir en la configuración del consentimiento realizada a través de medios electrónicos.

1.5.2 Formación del consentimiento

La confluencia entre propuesta y aceptación configura la formación del consentimiento de las partes intervinientes y el consecuente perfeccionamiento del contrato; dicho consentimiento –libre de vicios[46]- constituye requisito esencial de validez de todo contrato[47].

Al respecto, el artículo 45 de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos otorga protección al contrato electrónico formado a través de mensajes de datos, estableciendo

[45] Sobre este tema nos ha parecido adecuado seguir el criterio expuesto por Perales Viscasillas, quien se remite a lo contenido en la ley española 7/1996 que regula el comercio minorista.
[46] CARRASCOSA LÓPEZ, citado por Perales Viscasillas, sostiene que los vicios del consentimiento tradicionales también pueden afectar al "consentimiento electrónico". Ver: María del Pilar Perales Viscasillas, op.cit., p. 414.
[47] El contrato obliga cuando concurren las condiciones esenciales para su validez, que son el consentimiento de los contratantes, el objeto del contrato y la causa de la obligación. La perfección no es, pues, fundamento sino presupuesto de validez y eficacia del contrato, de forma que sólo a partir de un contrato perfeccionado podrá, de una parte, examinarse su validez, y de otra cuando puede decirse que el contrato obliga y es eficaz, comenzando a desplegar los efectos jurídicos que le son propios. Ver: María del Pilar Perales Viscasillas, op.cit., p. 415.

que “no se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos”.

La formación del consentimiento resulta vital para la determinación del momento y lugar en que se perfecciona el contrato, con los consecuentes efectos jurídicos que de ello se deriva: en cuanto al momento, para determinar desde cuando empiezan a surgir efectos jurídicos y los consecuentes derechos y obligaciones entre las partes; por otro lado, en cuanto al lugar, porque determinará la jurisdicción competente para conocer controversias.

En relación al lugar de formación del contrato, el artículo 46 ibídem, establece que “se tendrá como lugar de perfeccionamiento el que acordaren las partes”. Es decir, se acoge el principio de autonomía de la voluntad y libertad contractual. El artículo 47 ibídem, señala que en aquellos casos en que en el contrato no se estipule nada al respecto, se observarán las normas del Código de Procedimiento Civil o de la Ley Orgánica de Defensa del Consumidor, cuando se trate de consumidores.

Sobre el momento de formación del contrato, la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, nos remite a las reglas generales para los contratos: “*El perfeccionamiento de los contratos electrónicos se someterá a los requisitos y solemnidades previstos en las leyes (…)”*. Es decir, se estará a lo dispuesto por el Código de Comercio en artículo 145.

Para determinar con exactitud el momento de formación del consentimiento, es posible utilizar el servicio de Sellado de Tiempo, el cual es proporcionado por las Entidades de Certificación.

En contratación electrónica, la confluencia de oferta y aceptación puede darse en un solo acto o en varios actos, según la técnica de comunicación a distancia utilizada. Así tenemos que, en el caso del *chat*, la comunicación se da de manera simultánea, es decir, se podría asimilar a una negociación entre presentes, pues la oferta y la aceptación pueden manifestarse en un mismo acto. Por otro lado, al utilizar un correo electrónico, la comunicación es no simultánea, es decir, la negociación será entre ausentes, pues la oferta y la aceptación ocurren en distintos actos.

En conclusión, el *consentimiento electrónico* es aquél formado por la confluencia de la Propuesta electrónica y la Aceptación electrónica, manifestados a través de medios electrónicos, que determinarán el momento y lugar de perfeccionamiento del contrato electrónico, para lo cual es posible hacer uso de servicios de certificación como la firma digital y el sellado de tiempo.

1.6 Terminación del contrato electrónico

1.6.1 Desistimiento

Es fundamental, para volver confiable al derecho electrónico a la vista de usuarios y consumidores, el proporcionar mecanismos legales de protección que "adecuen el derecho tradicional a los nuevos hechos, representados hoy, en el campo comercial por este nuevo sistema de comercio cual es el comercio electrónico"[48].

Dentro de estos mecanismos, se ha contemplado la inclusión de la figura del desistimiento. El desistimiento es considerado para aquellos casos en que una de las partes intervinientes es un consumidor final

Se entiende el derecho de desistimiento como la extinción de una relación jurídica mediante una manifestación de voluntad que modifica una precedente, inducida por una nueva y diversa valoración de conveniencia del acto, sin necesidad de alegar justa causa y que pone fin al contrato antes del tiempo previsto, por razones de oportunidad o por constatación de nuevos hechos[49].

La *ratio* de este derecho es neutralizar la ventaja que pueda tener la parte proponente por el factor distancia, "reduciendo esta modalidad de contratos a la situación típica de un contrato

[48] Luis Miranda Serrano, op.cit., p. 583.
[49] Luis Miranda Serrano, op.cit., p. 603.

entre presentes"[50] y, con ello, atenuar los riesgos inherentes a este tipo de contratación cuando el consumidor recibe un bien o servicio defectuoso o que no coincide con lo solicitado.

En cuanto al ejercicio de este derecho, el artículo 45 de la Ley Orgánica de Defensa del Consumidor establece el Derecho de Devolución para aquellos "consumidores que adquieran bienes o servicios por teléfono, catálogo, televisión, internet"; quienes podrán ejercer este derecho dentro de los tres días posteriores a la recepción del bien o servicio, siempre que su naturaleza lo permita y que el estado del bien sea el mismo en el que se lo recibió. Cuando se trata de servicios, el derecho de devolución se ejercerá mediante la cesación inmediata del contrato de provisión de servicios.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, en el Capítulo III relativo a los Derechos de Usuarios y Consumidores, se limita a establecer el consentimiento que deben expresar los consumidores para aceptar registros electrónicos o mensajes de datos, y, para desistir sobre la aceptación de tales registros ante cambios para mantener o acceder a registros o mensajes electrónicos sobre los que hubiera otorgado su consentimiento.

La consecuencia principal del ejercicio del derecho de desistimiento, en general, consiste en desligar al contratante del contrato celebrado.

En conclusión, el *desistimiento en contratación electrónica*, es el derecho de una de las partes – consumidores – para terminar unilateralmente un contrato electrónico en razón de su inconformidad con el bien o servicio contratado, siempre que lo ejerza dentro del plazo que la ley otorga.

1.6.2 Resolución del contrato

La resolución del contrato es definida por Cabanellas como el "acto jurídico que deja sin efecto un contrato válidamente concertado"[51] que encuentra su causa en el desequilibrio

[50] Luis Miranda Serrano, op.cit., p. 598.

(económico) causado a una de las partes por el incumplimiento de la otra parte. Opera únicamente en contratos sinalagmáticos. Su principal supuesto es la mora culpable o dolosa por parte del contratista incumplido. Una vez el contratista incumplido es declarado en mora y posteriormente, declarado el incumplimiento, el efecto principal e inmediato es el derecho a indemnización por los daños y perjuicios ocasionados al contratista cumplido.

Aparecen así dos momentos: la declaratoria en mora de las obligaciones contraídas y la declaratoria del incumplimiento del contrato.

Para ambas declaraciones, y aunque se trata de contrataciones privadas en donde prima el principio de autonomía de la voluntad, es necesario que sea el juez quien las haga a petición de parte interesada, convirtiéndose esto en una dificultad para el comercio electrónico, pues toda la celeridad pretendida se ve entorpecida por trámites judiciales tradicionales y lentos.

Este es uno de los asuntos problemáticos en la aplicación del contrato electrónico. Una vez más sería necesario aplicar las reglas generales de contratación, sin embargo, la falta de normativa especial lo debilita sobremanera, principalmente cuando una de las partes intervinientes es un consumidor.

Una solución viable sería implementar trámites sumarísimos en judicaturas especializadas, pues al tener que seguir el procedimiento ordinario, se restaría la efectividad práctica del contrato electrónico; sin embargo, ello implicaría reformas legales, es decir, el trabajo activo del legislador y la voluntad política para sacar adelante este tipo de normas legales.

Si volvemos a ser reiterativos sobre la necesidad de la actualización y desarrollo normativo especializado es justamente, porque a lo largo de esta investigación, la principal constatación ha sido la escasa normatividad en el ámbito de la contratación electrónica que existe y con ello, la falta de seguridad jurídica. Es cierto que la Ley de Comercio Electrónico autoriza el uso de mensajes de datos y los reviste de seguridad jurídica en lo referente a la formación de

[51] Guillermo Cabanellas, op.cit., Tomo VII, p. 188.

los contratos. Pero hasta allí solamente, pues en temas como la judicialización ante inconvenientes para el cumplimiento del contrato, sean de buena o mala fe, el legislador ecuatoriano ha omitido desarrollar esta ley o reformar leyes conexas, como el Código de Procedimiento Civil y el Código de Comercio.

No olvidemos que en la parte considerativa de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, el legislador ecuatoriano ha reconocido la importancia del uso de medios electrónicos, y establece como uno de sus objetivos el **impulsar** y **fomentar** estos medios electrónicos, para con ello, desarrollar el comercio y la producción, tanto en el sector público como privado, de modo que los servicios de redes de información e Internet se conviertan en un medio para el desarrollo del comercio, la educación y la cultura.

CAPÍTULO II

2. Responsabilidad en la contratación electrónica

En términos generales, la responsabilidad surge ante la conducta de una persona que se materializa en un daño, patrimonial o extrapatrimonial, el cual debe ser reparado y, que en muchas ocasiones, lesiona también un bien jurídico protegido por la ley penal lo que conlleva a una sanción de la misma naturaleza. Tal es el contenido principal de la responsabilidad civil y penal.

Para entrar en análisis de la responsabilidad en materia de contratación electrónica es necesario no perder de vista los elementos caracterizadores de este tipo de contrato, a los cuales ya nos hemos referido anteriormente: la técnica de comunicación a distancia empleada durante la negociación y proceso de formación como tal, así como, el soporte electrónico en el cual reposa el contrato. Ahora, añadiremos un tercer elemento caracterizador de la contratación electrónica, fundamental a la hora de estudiar la responsabilidad por las conductas que se realizan a través de medios electrónicos: la constante circulación de información.

En cuanto a la intervención de una *técnica de comunicación a distancia* significa, siguiendo a HOCSMAN, referimos que se podrían ocasionar los mismos daños que a través de cualquier otro medio de comunicación[52]. El típico ejemplo de una conducta dañina realizada por medios de comunicación es la que afecta al derecho a la intimidad.

Por otro lado está el soporte electrónico que contiene al contrato y que circula a través de *sistemas informáticos*, sistemas que podrían sufrir daños, principalmente económicos, merecedores de reparación civil y que, de estar tipificada dicha conducta, constituirían también ilícitos penales.

[52] Heriberto Simón Hocsman, Negocios en Internet, Buenos Aires, Editorial Astrea, 2005, p. 295.

Finalmente, tenemos la circulación permanente de información que, imprescindiblemente, se realiza en la etapa de formación del contrato y en la elaboración del documento – contrato en sí mismo.

Debemos tener presente que Internet es un medio interactivo de comunicación que funciona como medio de comunicación y de publicación al mismo tiempo, en donde cualquier usuario es generador de contenidos.

De allí que las posibilidades de *daños informáticos* derivados de un contrato electrónico, que puedan ser causantes de responsabilidades civiles o penales, superan ampliamente a los daños contra intereses particulares o públicos que tradicionalmente pueden ocasionarse. Si damos una mirada general a las variables incorporadas a la contratación por medios electrónicos tenemos que: se utiliza una técnica/medio de comunicación, en donde se da un flujo permanente de información de todo tipo – económica y personal –, cuyos titulares pueden ser personas naturales o jurídicas, y, en donde el contrato electrónico reposa en sistemas informáticos vulnerables desde el punto de vista técnico, tanto a daños físicos como al acceso no autorizado al contenido del documento, sea con fines de destrucción, modificación o simplemente para conocer aquello que no debe ser divulgado.

Una vez planteados estos aspectos, analizaremos la responsabilidad civil y penal en relación al contrato electrónico como contrato a distancia.

2.1 Responsabilidad civil

Para VALENCIA y ORTIZ, una persona es responsable civilmente cuando en razón de haber sido la causa del daño que otro sufre, sea patrimonial o extrapatrimonial, está obligada a repararlo. La responsabilidad civil es la consecuencia jurídica de una relación entre dos sujetos – uno que causa el daño y el otro que lo ha sufrido-, es decir, la obligación del autor del daño

de reparar el perjuicio ocasionado. La responsabilidad civil se resuelve en todos los casos en una obligación de reparación[53].

A partir de esta definición, tenemos varios elementos de la Responsabilidad Civil que serán analizados desde las características que definen al contrato electrónico.

1. En primer lugar, citamos a las **personas intervinientes** en la relación contractual electrónica. Como participantes directos, tenemos al sujeto Iniciador o Emisor, y al sujeto Destinatario. Pero existe también un Intermediario involucrado indirectamente en la relación contractual.

   a) Iniciador o Emisor: el sujeto iniciador será el proponente, es decir, quien emite la oferta para celebrar un contrato electrónico.

   b) Destinatario: es aquél que recibe el contenido de la Propuesta, es decir, el Aceptante.

   c) Intermediario: es el colaborador técnico que facilita el uso de las redes por parte de los usuarios. LÓPEZ ORTEGA clasifica a los intermediarios en tres categorías[54]:

   - ✓ Operadores de telecomunicaciones: quien coloca a disposición de los usuarios del Internet la interconexión de las redes, la infraestructura que permite la trasmisión de la información;
   - ✓ Proveedores de acceso a la red: quienes colocan su servidor a disposición de los usuarios para permitirles el acceso a la red; y,
   - ✓ Proveedores de servicios: quienes facilitan la trasmisión de la información a través de redes electrónicas. Entre los servicios que se pueden brindar tenemos: 1) Proveedores de alojamiento, que alquilan un espacio del disco duro de su sistema para que sus clientes puedan albergar en él una página web; 2) Operadores de líneas de distribución o foros de discusión, que alquilan o ceden espacio en el

[53] Arturo Valencia Zea, Álvaro Ortiz Monsalve, op.cit., p. 169.
[54] Juan José López Ortega, Internet y Derecho Penal: "*Libertad de expresión y responsabilidad por los contenidos de Internet*", dirigido por Juan José López Ortega, Madrid, editado por Consejo General del Poder Judicial, 2001, p. 107.

disco de sus sistemas informáticos para que sus abonados envíen y reciban mensajes en su buzón de correo; 3) Operadores de grupos de noticias, que alquilan o ceden espacio en sus sistemas informáticos para que los usuarios puedan consultar la gran variedad de grupos de noticias existentes en la red; y; 4) Operadores de conversaciones en tiempo real, que permiten a los usuarios comunicarse al momento con otros usuarios.

En los contratos electrónicos no siempre existe la certeza sobre la identidad de las partes intervinientes, principalmente en el caso de la policitación o propuesta cuyo contenido usualmente es puesto en conocimiento del público a través de sitios webs o de correos electrónicos masivos.

La falta de certeza en este aspecto, dificulta la situación de la víctima del daño al momento de querer identificar al sujeto pasivo de una obligación reparatoria.

En el caso de contratos en los que interviene la firma electrónica avalada por una autoridad de certificación la situación se simplifica, pues, justamente una de las ventajas de la firma electrónica es la certificación de *autenticación.*

2. En segundo lugar, debe existir la **conducta** que genera un daño, conducta propia o ajena que puede obedecer al dolo o culpa del sujeto o, incluso, a una mera causalidad material[55].

   La conducta que nos interesa, para efectos de esta investigación, es aquella que se realiza a través de medios electrónicos, ya sea vulnerando sistemas informáticos, por ejemplo con la difusión de un virus informático, o vulnerando la información circulante por las redes abiertas, como en el caso del acceso no autorizado a información personal.

3. Finalmente está el **daño**, autores como Rafael Calderón y Pilar Hiruela, citados por Claudio Leiva hablan del *daño informático* considerando que *"... es toda lesión causada*

[55] Arturo Valencia Zea, Álvaro Ortiz Monsalve, op.cit.

a un derecho subjetivo mediante la utilización de medios electrónicos destinados al tratamiento de la información, y que concurriendo determinados presupuestos, genera responsabilidad"[56].

Con este antecedente, continuaremos con el estudio de la responsabilidad civil contractual y extracontractual en la contratación electrónica.

2.1.1 Responsabilidad extracontractual por daño informático

La responsabilidad extracontractual se genera cuando una persona, por sus propios hechos o por hechos ajenos, causa o incurre en una conducta que provoca un daño a otra persona, al margen de un contrato. Es decir, sin existir una relación contractual, una persona causa un daño a otra, ocasionando con ello una obligación de reparación.

Hemos mencionado en reiteradas oportunidades que el contrato electrónico introduce variables que lo diferencian de otros contratos: la técnica de comunicación a distancia empleada y el soporte electrónico que contiene al contrato electrónico. Y, añadimos una tercera característica, la circulación constante de información.

Es posible incurrir en responsabilidad extracontractual en contra de terceros cuando en los sitios webs o correos electrónicos a través de los cuales se difunden policitaciones, se han incorporado contenidos ilícitos o nocivos.

También ocurre que en la interacción de mensajes de datos entre las partes intervinientes, que se realiza en todo el proceso de formación y elaboración de un contrato electrónico, se pone en riesgo tanto la información – patrimonial y extrapatrimonial - de los usuarios, como la seguridad de los sistemas informáticos a través de los cuales circula tal información, y que tienen también un valor patrimonial.

[56] Ponencia de Claudio Fabricio Leiva en el VIII Congreso Internacional de Derecho de Daños, Buenos Aires, 2005: Responsabilidad por daños derivados de Internet. Ver: http://www.aaba.org.ar/bi22n004.htm

En ambos casos, la conducta dañina hacia la información o hacia los sistemas informáticos, podría generar responsabilidad civil extracontractual cuando la protección de ambos bienes no esté recogida en las cláusulas contractuales, indiferentemente de cuál sea el objeto del contrato.

A continuación, revisaremos cada uno de estos supuestos, que constituyen conductas generadoras de responsabilidad civil extracontractual en las contrataciones electrónicas.

2.1.1.1 Contenidos ilícitos y nocivos

Los contenidos ilícitos son aquellos que infringen alguna norma jurídica.

Los contenidos nocivos son aquellos que expresan opiniones o creencias políticas, religiosas, culturales, que pueden ser consideradas ofensivas respecto de terceros[57].

El ejemplo más palpable en contratación electrónica, en que pudiera haber una exposición a un contenido ilícito o nocivo, se produce en la policitación, cuando las propuestas son puestas en conocimiento de los usuarios de redes abiertas a través de medios como páginas webs o correos electrónicos. Recordemos que al ser la policitación una propuesta dirigida al público en general, nos encontraremos en la mayoría de los casos ante propuestas de consumo, que se concretarán a través de contratos de adhesión, contratos en los cuales, la parte débil o consumidor goza de protección especial consagrada en la Constitución de la República y desarrollada en la Ley Orgánica de Defensa del Consumidor y su reglamento.

En esta situación, cobra importancia la figura de uno de los intervinientes del contrato electrónico: el Intermediario, es decir, el proveedor de servicios de Internet y el proveedor de accesos.

[57] Heriberto Simón Hocsman, op.cit., p. 299.

El Intermediario puede incurrir en responsabilidad extracontractual cuando el proponente de un negocio jurídico electrónico hace conocer su propuesta, por ejemplo, a través de un sitio web y, el contenido de tal sitio, contiene además de la policitación, publicidad abusiva[58] – en los términos de la Ley Orgánica de Defensa del Consumidor - o mensajes ilícitos o nocivos.

En estos casos, el Intermediario sobre el que pudiera recaer mayor responsabilidad es aquél que brinda el servicio de alojamiento o *hosting.*

Ante esta situación, tenemos varios supuestos:

- ✓ Si los contenidos ilícitos o nocivos son cargados por los clientes del Intermediario, con o sin conocimiento de este último.
- ✓ Si al enterarse el Intermediario sobre el contenido ilícito o nocivo, actúa con prontitud para retirar o bloquear dicho contenido, siempre que tecnológicamente esté en posibilidad de hacerlo.
- ✓ Si existe o no vinculación entre las actividades ilícitas de los usuarios y el servicio prestado por el Intermediario.
- ✓ Si el proveedor obtiene o no beneficio económico directamente relacionado con la actividad ilícita.

Sobre este tema, la legislación ecuatoriana protege a los consumidores electrónicos de los posibles abusos cometidos en las contrataciones por medios electrónicos.

El artículo 8 del Reglamento a la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, esclarece la situación de los proveedores de servicios electrónicos relacionados con:

1. Envío o recepción de comunicaciones electrónicas.
2. Alojamiento de bases de datos,

[58] La Ley Orgánica de Defensa del Consumidor define a la *publicidad abusiva* como toda información o comunicación comercial, capaz de incitar al a violencia, explotar el miedo, aprovechar la falta de madurez de los niños y adolescentes, alterar la paz y el orden público o inducir al consumidor a comportarse en forma perjudicial o peligrosa para la salud y seguridad personal y colectiva.

3. Registro Electrónico de datos
4. Alojamiento de sitios en medios electrónicos o servicios
5. O servicios similares o relacionados.

Para todos los proveedores mencionados, se establece que no "implica responsabilidad sobre el contenido de los mensajes de datos por parte de quien presta estos servicios, siendo la responsabilidad exclusivamente del propietario de la información". El siguiente inciso de este artículo dispone que en casos en que la autoridad competente declare que una información que consta en redes electrónicas es ilegal o atenta contra las leyes o la seguridad nacional, ordenará la suspensión del acceso a dicha información, para lo cual el proveedor de servicios deberá hacerlo de inmediato bajo prevenciones de ley.

En el caso de contratos que no sean de consumo, no existe regulación en la legislación especial existente, es decir, se aplicarían las reglas generales que rigen la materia civil y comercial.

2.1.1.2 Daños a los sistemas informáticos: programas dañinos

En primer lugar, es importante definir qué son los sistemas informáticos. En términos generales, un sistema informático es un conjunto de partes que funcionan relacionándose entre sí con un objetivo preciso. Sus partes son: hardware y software[59].

Hemos mencionado en numerosas oportunidades, los beneficios de la utilización de redes abiertas a través de sistemas informáticos. Sin embargo, en Internet los sistemas informáticos se ejecutan e interactúan a través de redes abiertas o redes electrónicas las cuales están expuestas a una serie de vulnerabilidades técnicas. HOCSMAN menciona algunas de las principales vulnerabilidades de los sistemas en redes abiertas[60]:

[59] Fuente: www.alegsa.com.ar/Dic/sistema%informatico.php
[60] Heriberto Simón Hocsman, op.cit., p. 220.

1. La instalación deficiente de sistemas operativos que causan la apertura innecesaria de puertos que se convierten en posibilidad para los hackers para vulnerar los sistemas;
2. Manejar información en cuentas carentes de claves o claves fáciles de descifrar;
3. No contar con *back ups* o respaldos completos o ser estos insuficientes;
4. Mantener una gran cantidad de puertos abiertos;
5. Falta de filtros para detectar direcciones falsas IP;
6. Deficiente uso de *logging*, que es la acción que permite detallar lo ocurrido en un sistema y determinar qué partes de él han sido vulnerados.

La falta de control en las redes puede acarrear que tanto *hackers* y *crackers*[61] accedan a los sistemas informáticos sin contar con autorización, con la finalidad de destruir o modificar información, divulgar información, causar interrupciones o mal funcionamiento de la red a través de amenazas – virus-, robos de información.

Los peligros técnicos que puedan generarse en las redes abiertas, repercuten en el ámbito jurídico, pues pueden causar inconvenientes a la hora de comerciar electrónicamente por la pérdida de seguridad que proyectan en los negocios: falta de identificación y autenticación del emisor de un mensaje de datos; falta de control de accesos a la información; peligro en la integridad de los datos; pérdida de la confidencialidad de los datos; imposibilidad de disponer de los datos; desprotección ante el repudio de los mensajes de datos.

Si analizamos las actividades de *hackers* y *crackers* observaremos que la finalidad de cada una de estas conductas dañinas puede diferir. Así tenemos que las vulneraciones pueden estar orientadas únicamente a burlar las seguridades de los sistemas informáticos o interferir en su funcionamiento sin el ánimo de destruirlos; pero, también puede ser su objetivo la destrucción de los sistemas informáticos.

[61] HACKER es una persona interesada en conseguir el conocimiento por cualquier medio, sea este legal o ilegal. Buscan información, robar software; sus trabajos siempre son inspirados por una ideología determinada, ya sea de contenido social, político, laboral, etcétera. CRACKER es el verdadero "pirata informático". Realiza sus trabajos con ánimo de lucro; no poseen ideología; piratean software protegido, destruyen sistemas complejos mediante trasmisión de virus. Ver: Juan José Páez Rivadeneira y Santiago Acurio, Derecho y nuevas tecnologías, Ecuador, Corporación de Estudios y Publicaciones, 2010, p. 191 ss.

Haremos una especial mención al virus informático, como principal programa dañino causante de problemas que afectan a los sistemas informáticos por la pérdida de información que causan y por la alteración de la estructura interna del sistema operativo. Cabe aclarar que los programas dañinos pueden llegar al sistema informático por medio de dispositivos externos o a través de Internet, por ejemplo en un correo electrónico, o al hacer clic en algún link de origen desconocido. Un virus es un programa que posee la capacidad de auto reproducirse sobre cualquier soporte apropiado que tenga acceso al computador afectado, multiplicándose en forma descontrolada hasta el momento en que tengan programado actuar. El virus, para ser tal, debe contener las características de ser: subrepticio, dañoso y con capacidad de auto duplicarse[62].

El carácter subrepticio del virus significa que éste se introduce de manera oculta en el sistema y cuando eclosiona se pone en evidencia el daño causado. Una vez ingresado, el virus va a buscar un lugar donde alojarse de manera estable, por ello busca establecerse en áreas reservadas del disco duro, en programas de arranque y administración, en el sistema operativo o dentro de algún archivo ejecutable. Una vez alojado, empieza su reproducción y trasmisión a otras computadoras. El daño causado por un virus es evidente, dado que destruye la información que contiene el ordenador y puede llegar a borrar todo un sistema operativo o incluso el disco duro de la computadora.

Ribas citada por HOCSMAN señala que: "la responsabilidad de la persona que inicia la cadena de efectos nocivos de un virus, planificando la difusión intencionada del mismo a través de medios de trasmisión está clara, pues el daño es perfectamente previsible y seguro"[63].

La difusión de programas dañinos se debe principalmente a la falta de seguridades técnicas con la que cuentan los sistemas informáticos. Por ejemplo, en la contratación electrónica que utiliza como técnica o medio de comunicación un correo electrónico gratuito. Este tipo de técnica de comunicación no cuenta con las seguridades suficientes y ello permite que los virus

[62] Heriberto Simón Hocsman, op.cit., p. 300.
[63] Heriberto Simón Hocsman, op.cit., p. 301.

sean difundidos fácilmente a través de ellos. Similar situación ocurre en las negociaciones realizadas a través de mensajería instantánea.

Si la técnica de comunicación a distancia utilizada es insegura, facilita la difusión de programas dañinos.

Hocsman señala que existen diferentes tipos de programas dañinos: los virus propiamente dichos, a los cuales nos referimos anteriormente; los programas "bomba" o "trampa"[64], los programas "gusanos"[65] y los virus "troyanos"[66].

Ante daños de esta naturaleza, el soporte electrónico que contiene al contrato electrónico será víctima fácil de destrucción o modificación.

En cuanto a la información que circula a través de sistemas informáticos, ésta queda expuesta al ataque de programas dañinos que pueden ocasionar la pérdida temporal o definitiva de información.

Para concluir, la conducta que vulnera sistemas informáticos, sea o no con el ánimo de destruirlos, configura o da lugar a responsabilidad civil y la consecuente obligación de reparación. La situación ideal sería que los contratos electrónicos contengan cláusulas que obliguen a contar con programas de antivirus eficaces. Pero la ley no obliga a ello así que debería ser la práctica comercial la que adopte tal comportamiento para asegurar el éxito del comercio electrónico. La dificultad, sin duda, sería el costo económico que representaría y que en ocasiones los usuarios no están dispuestos a asumir. En definitiva, para que las vulnerabilidades técnicas de las redes abiertas no perjudiquen al comercio electrónico, se

[64] Los programas bomba o trampa son programas autónomos que se ocultan con una fachada de utilidad pero que puestos en ejecución alteran, borran o formatean el disco.
[65] Los programas gusanos son aquellos que se reproducen a partir de un inútil consumo de los recursos pero que pueden detectarse fácilmente, pues se advierte un notable crecimiento de los *bytes* ocupados por programas.
[66] Los virus troyanos hacen referencia a cualquier virus que puede entrar en ejecución sorpresivamente. Son virus que sobre escriben el archivo en el que residen, destruyéndolo.

deben tomar medidas de carácter técnico así como jurídico. Sólo así se fomentaría la participación y concreción de negocios por estos medios[67].

2.1.1.3 Daños a los sistemas de información: derecho a la intimidad

Empezaremos el análisis de la responsabilidad generada por el *daño informático* en los sistemas de información, definiendo qué es un sistema de información.

El sitio web *Wikipedia* define el sistema de información como un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo. El sistema de información, en la mayoría de los casos, utiliza como recurso material a los sistemas informáticos.

Andrea Sarra nos ofrece una diferenciación semántica entre los términos *dato* e *información*, señalando que:

> "*dato* viene del latín "*datum*" que significa "lo que se da", se aplica a los hechos sin forma y sin orden. Por su parte, *información* viene del latín *"informatio"*, lo que equivale a "lo que tiene forma" y se refiere a los datos que poseen forma, estructura, orden y organización. En consecuencia, puede decirse que un dato es una representación de entidades o hechos y que carece de valor propio. Hasta aquí, el dato *per se* no constituye información, puesto que sólo adquiere valor cuando un procesador, en un momento determinado y por medio de alguna forma de procesamiento, se lo asigna. Es decir, un dato adquiere el carácter de información porque tiene significado para un procesador, puesto que reducen su ignorancia o incertidumbre de una determinada situación. En suma, puede afirmarse que información es el significado que un procesador le asigna a un dato. Así, vemos que, por ejemplo, cuando hablamos de datos personales deberíamos hablar, en realidad, de

[67] Heriberto Simón Hocsman, op.cit., p. 221.

información relativa a las personas, puesto que lo que requiere protección es la información"[68].

Es decir, la información es un concepto más amplio que implica un complejo proceso de tratamiento de los datos que la integran.

Al respecto, la Disposición General Novena de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos ofrece las siguientes definiciones:

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

- ✓ *Sistema de información:* Es todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar, de cualquier forma mensaje de datos.

En conclusión, nuestra legislación recoge ambos conceptos: [mensajes de] datos y [sistemas de] información, otorgándoles validez y protección jurídica de acuerdo a los principios desarrollados en el Capítulo I de la ley, que se refieren al sometimiento al régimen de propiedad intelectual, confidencialidad y reserva, conservación y disponibilidad para posterior consulta, integridad y unicidad.

Continuando con el análisis de los riesgos para la información que circula a través de redes abiertas, la información puede ser de varios tipos. Para efectos de esta investigación la dividiremos en: patrimonial y extrapatrimonial. Al primer grupo pertenece la información

[68] Andrea Viviana Sarra, Comercio electrónico y derecho, Buenos Aires, Editorial Astrea, 2001, p. 223.

económica de personas naturales y jurídicas, por ejemplo, dentro de la contratación electrónica sería normal que circulara información bancaria o crediticia, secretos comerciales o información calificada como no divulgada por la Ley de Propiedad Intelectual. En el segundo grupo tenemos la información de carácter personal o sensible, por ejemplo, aquella referente a las creencias religiosas, filiación o pensamiento político, salud y vida sexual, y otras similares.

Nos referiremos en especial a la información de carácter personal, pues aquella goza de protección constitucional. Así tenemos que el artículo 66 de la Constitución de la República, que se refiere a los derechos de libertad, reconoce de manera expresa los siguientes derechos:

> "Artículo 66.- Se reconoce y garantiza a las personas:
> 11. El derecho a guardar reserva sobre sus convicciones. Nadie podrá ser obligado a declarar sobre las mismas. En ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros o sobre sus creencias religiosas, filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica.
>
> 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley".

Desde siempre, la información ha sido merecedora de protección por todos los ordenamientos jurídicos, tanto en la afectación que los particulares pudieran sufrir por su vulneración, como por la irrupción al orden público que implica.

Los problemas clásicos de este derecho, a decir de ANDREA SARRA, han sido: la forma como los datos son recolectados, tratados y utilizados, la finalidad de los datos recabados; el tiempo que los datos deben ser conservados; la exactitud de los contenidos; el derecho de las

personas de acceder a los datos que de ella se disponen, el derecho para ordenar la supresión o rectificación de contenidos erróneos o falsos[69].

Sin embargo, este derecho debe ser ahora examinado a la luz de la influencia de las tecnologías de la información, siendo necesario hacer hincapié en la relación que existe entre la protección de la información y el tema de seguridades en las redes.

Si bien los daños pueden afectar a la información de carácter patrimonial, los daños materiales sufridos por las víctimas son insignificantes en relación con la agresión a sus sentimientos cuando el daño se da en la información personal. Sarra considerada que en la mayoría de los casos, la violación de la información personal en las redes, causa un daño moral profundo[70].

En el caso del comercio electrónico, la información va a estar expuesta en medios electrónicos y transmitidos a través de técnicas de comunicación a distancia. Es por ello, que la protección a la información debe operar a otro nivel.

De ahí la conexión entre el derecho a la protección de la información y el derecho a la intimidad o privacidad.

Tomás Vidal Marín señala que el derecho a la intimidad "surge hace más de un siglo en Estados Unidos, a través de la obra de Warren y Brandeis que bajo el título *The right to privacy* se publicó en 1890 (…). En él van a retomar la definición que sobre el precitado derecho había formulado pocos años antes el Juez Cooley: *the right to be let alone*. Así, afirmarán que la protección otorgada a los pensamientos, sentimientos y emociones, manifestados por escrito o en forma artística, en tanto en cuanto consista en impedir la publicación, no es más que un ejemplo de la aplicación del derecho más general del individuo a no ser molestado"[71].

[69] Andrea Viviana Sarra, op.cit., p. 188.
[70] Andrea Viviana Sarra, op.cit., p. 193.
[71] Tomás Vidal Marín, El derecho al honor y su protección desde la Constitución Española, Madrid, Editado por Imprenta Nacional del Boletín Oficial del Estado, 2000, p. 68.

Se trata también de uno de los derechos de libertad reconocido y garantizado por nuestra Constitución en el artículo 66 numeral 20.

Siguiendo al autor antes citado, él considera que en la actualidad, dado el enorme desarrollo de los medios tecnológicos que se está produciendo en la sociedad, el derecho a la intimidad está integrado por un doble aspecto: un aspecto negativo y otro positivo. El primero se refiere al derecho a excluir del conocimiento de terceros, aquellos actos, hechos sentimientos, actitudes, etc., que forman parte de la esfera íntima del individuo. El segundo, consiste en la facultad del individuo de controlar aquellos datos referentes al mismo, así como la divulgación o no de los mismos[72].

Es por ello que, considera el profesor Fermín Morales Prats, que con la influencia de las tecnologías de la información, este derecho está expuesto a nuevos riesgos por cuanto posibilita formas de control certero, penetrante y continuado, que son inadvertidas por los usuarios de las redes[73].

Entre estos nuevos riesgos para el derecho a la intimidad tenemos:

1. Problema de *archivos logs*: estos son registros de conexiones de usuarios. Todos los datos son almacenados por un proveedor de acceso, lo que permite configurar un perfil digital del usuario.
2. Problema de *cookies*: son archivos emitidos por sitios webs visitados que se graban en disco duro. El envío sucesivo de cookies permite obtener una fotografía digital del usuario.
3. Correos electrónicos: este instrumento de comunicación es altamente vulnerable desde el punto de vista técnico. Es la técnica de comunicación más utilizada en la formación de los contratos electrónicos.
4. *Sniffers*: son programas rastreadores de mensajes en el ciberespacio, utilizados a partir del empleo de palabras o códigos clave. Su objetivo es la captación de mensajes.

[72] Tomás Vidal Marín, op.cit., p. 75.
[73] Fermín Morales Prats, Internet y Derecho Penal: "*Internet: riesgos para la intimidad*", dirigido por Juan José López Ortega, Madrid, editado por Consejo General del Poder Judicial, 2001, p. 72 y ss.

Como podemos apreciar, las conductas dañosas detectadas, obedecen a los nuevos riesgos que se derivan eminentemente de la circulación de la información a través de redes abiertas.

Recapitulando, los sistemas de información contenidos en sistemas informáticos se encuentran en continua interacción en las redes abiertas, motivo por el cual están expuestos a los riesgos que hemos explicado que lesionarían directamente a las personas titulares de tal información, tanto en sus derechos patrimoniales como en los fundamentales.

Es importante destacar que al participar en una contratación electrónica, la información entre las partes contratantes estará fluyendo permanentemente, lo que los vuelve responsables – al margen de sus obligaciones relativas al cumplimiento del objeto del contrato – por la custodia de la información y por la falta de protección técnica que se aplique en el manejo de sus sistemas informáticos.

En relación al origen de los *daños informáticos* a los sistemas de información, encontraremos dos posibilidades:

- Ataques internos: son aquellos ocasionados por las mismas personas en las que recae la custodia de los sistemas de información. En estos casos la responsabilidad será mayor.
- Ataques externos: los causados por *hackers* o *crackers,* quienes actúan en las formas antes explicadas, vulnerando de manera externa los mecanismos de seguridad de los sistemas informáticos y de sistemas de información.

Es fundamental que las técnicas de comunicación utilizadas por las partes, estén provistas de suficientes seguridades técnicas a fin de evitar las repercusiones jurídicas que sus posibles deficiencias puedan acarrear a las partes, y una negociación electrónica termine causando más daño que los beneficios esperados del contrato electrónico en sí.

2.1.2 Responsabilidad contractual

La Responsabilidad Contractual se produce al momento de verificarse el incumplimiento total, tardío o defectuoso de las obligaciones contraídas por las partes en el contrato, salvo los casos de excepción previstos en la ley.

Ante cualquiera de estos supuestos, el Código Civil en su artículo 1505 prevé dos opciones: exigir el cumplimiento o la resolución del contrato. Para ambas posibilidades, existe el derecho de reclamar indemnizaciones por los daños y perjuicios causados, en los términos del artículo 1572 ídem.

Sea que se decida por la opción de exigir el cumplimiento o sea pedir la resolución, es necesario requerir en mora al contratista incumplido. En la práctica, significa presentar un escrito que debe cumplir los requisitos de la demanda establecidos en el artículo 67 del Código de Procedimiento Civil. Con la citación, el contratista incumplido estaría requerido en mora tal como lo señala artículo 97.5 ídem. El procedimiento descrito es el tradicionalmente utilizado en materia civil y comercial.

Recordemos que estamos analizando la responsabilidad civil en relación a las características del contrato electrónico como contrato a distancia. Siendo así, es importante referirnos a las cláusulas contractuales que puedan afectar la naturaleza del contrato electrónico.

2.1.2.1 Cláusulas abusivas: cláusulas exonerativas o limitativas de responsabilidad

La legislación comunitaria europea ha definido a las cláusulas abusivas como aquellas cláusulas contractuales que no se han negociado individualmente por las partes y que por ello se oponen al principio de buena fe contractual[74] y que a su vez causan, en perjuicio de la parte

[74] El principio de buena fe se refiere a observar las reglas objetivas de la honradez enel comercio o en el tráfico jurídico, no se refiere honradez subjetiva de la persona. Ver más: Lourdes Blanco Pérez-Rubio, Comercio

débil de la negociación, un desequilibrio importante entre los derechos y obligaciones de las partes. Se considera que una cláusula no ha sido negociada individualmente, cuando esta ha sido redactada anteriormente por una de las partes sin que la parte débil haya podido influir sobre su contenido[75].

Es común encontrar este tipo de cláusulas en la mayoría de contratos de adhesión. Sin embargo, las cláusulas abusivas también pueden aparecer en aquellos contratos en donde las cláusulas son impuestas por la parte fuerte de la negociación, aun cuando el contrato no sea de adhesión. A decir de Lourdes Blanco este tipo de cláusulas son incluidas en general, en cualquier tipo de negociación en la que el empresario o usuario proponente es la parte fuerte, económicamente hablando, lo que lo coloca en una posición privilegiada en la contratación y *"obliga a la utilización de medios electrónicos para sus futuros negocios, sin ofrecer medidas de garantía suficientes y forzando de tal forma al a otra parte, que incluso podría llegar a viciar no sólo el contrato de que se trate, sino también los futuros contratos que con base a éste se celebren"*[76].

La Ley Orgánica de Defensa del Consumidor ecuatoriana, en su Capítulo VII establece una serie de cláusulas prohibidas para los contratos de adhesión, entre ellas, el numeral 1 prohíbe aquellas estipulaciones que *"eximan, atenúen o limiten la responsabilidad de los proveedores por vicios de cualquier naturaleza de los bienes o servicios prestados"*.
La consecuencia jurídica prevista para este tipo de cláusulas es la nulidad de pleno derecho.

El típico ejemplo de cláusula abusiva, y que es el caso que nos interesa para efectos de esta investigación, es el de las *cláusulas de limitación o exoneración de responsabilidad* las cuales consisten, como su nombre lo indica, en limitar el alcance de la responsabilidad de la parte fuerte de la negociación, a fin de beneficiarse económicamente de ello en detrimento de la parte débil. Este tipo de cláusulas se encuentran dentro de la categoría de cláusulas abusivas que suponen privación de derechos básicos.

---

electrónico y protección a los Consumidores: *"Cláusulas abusivas en la Contratación Electrónica"*, coordinado por Alejandra Botana García, Madrid, Editorial La Ley, 2001, p. 528.
[75] Artículo 3 de la Directiva 93/13 de la Comunidad Europea. Fuente: http://eur-lex.europa.eu
[76] Lourdes Blanco Pérez-Rubio, op.cit., p. 507.

Es fundamental que los contratos electrónicos contemplen cláusulas de responsabilidad en relación a la confidencialidad con la que debe manejarse la información, sea personal o económica, y que circula en las redes al momento de negociar o de simplemente enviar información que debe incluirse en el documento electrónico que contendrá el contrato; así como, contar con sistemas informáticos seguros y confiables, considerando que el documento electrónico que contiene el contrato reposará en dichos sistemas.

2.2 Responsabilidad penal

Las tecnologías de la información han transformado radicalmente nuestra sociedad ocupando a gran velocidad casi todas las facetas de la actividad humana.

El tratadista español Manuel Lezertua afirma que gracias a las tecnologías de la información se puede tener acceso a gran cantidad de información almacenada en sistemas informáticos lo cual posibilita opciones ilimitadas de intercambio y distribución de datos. La consecuencia de ello es la explosión de la cantidad de información y de conocimiento disponible en soporte electrónico, y a su vez, una profunda transformación económica y social. Sin embargo *"también tiene su lado oscuro: la aparición de nuevas formas de criminalidad, la utilización de las redes informáticas para la comisión de delitos nuevos y antiguos, la macro-victimización que genera la delincuencia informática"*[77].

A medida que se incrementa la dependencia a las redes abiertas, se hace más evidente la vulnerabilidad de los usuarios frente al abuso de los sistemas informáticos y a la agresión criminal contra los sistemas informáticos y la información en sí misma.

Son muchas las razones que vuelven prioritario la protección de las redes. LEZERTUA considera que estas razones son:

[77] Manuel Lezertua, Internet y Derecho Penal: "*El Proyecto de Convenosobre el cybercrimen del Consejo de Europa*", dirigido por Juan José López Ortega, Madrid, editado por Consejo General del Poder Judicial, 2001, p. 18.

1. La emergencia de una sociedad global de información prácticamente sin fronteras, que ofrece inmensas posibilidades de actuación tanto legítima como criminal;
2. La desaparición de obstáculos que permite que en cualquier momento y en cualquier parte del mundo, se pueda acceder a enormes cantidades de datos, públicos y privados, almacenados en sistemas informáticos y de información.
3. La existencia de una nueva era del comercio electrónico, cuyas transacciones representan grandes cantidades de dinero.

Por supuesto nos interesa sobremanera la última razón citada, pues, la amenaza de la criminalidad sobre ella influye sobre la integridad y el desarrollo futuro del comercio electrónico.

Sabemos que el Derecho Penal tipifica aquellas conductas que considera lesivas para bienes jurídicos protegidos y que caotizan la sociedad con el consecuente perjuicio para el orden público. Dichas conductas pueden ser de la más variada índole; me referiré únicamente a aquellas conductas que lesionan bienes jurídicos expuestos en contratación electrónica.

Considero que el principal bien jurídico lesionado a través de conductas tipificadas por la ley penal, que se encuentra expuesto en contratación electrónica, es la información, con su conexión evidente con el derecho a la intimidad y a la propiedad.

2.2.1 La información como bien jurídico: carácter económico y privacidad de la información

El objeto material, sobre el que recaen los ilícitos de esta naturaleza, es la información, como bien intangible y sobre el que se puede ejercer un derecho de propiedad[78].

[78] Juan Vizueta Ronquillo, Delitos informáticos en el Ecuador, Guayaquil, Editorial Edino, 2011, p.35.

Como habíamos mencionado anteriormente, la información posee un valor adicional dada por el complejo proceso de tratamiento que han recibido los datos que la integran.

Como señalamos en la parte relativa a los sistemas informáticos, la información puede ser de varios tipos: patrimonial o extrapatrimonial. En el caso de la información patrimonial, se trata de información susceptible de apreciación económica. En el caso de la contratación electrónica, la información patrimonial circulante se refiere a secretos comerciales o industriales, que gozan del carácter de información protegida, en los términos establecidos en la Ley de Propiedad Intelectual y en la Decisión 486 de la Comunidad Andina.

El artículo 183 de la Ley de Propiedad Intelectual establece:

> *"Art. 183.- Se protege la información no divulgada relacionada con los secretos comerciales, industriales o de cualquier otro tipo de información confidencial contra su adquisición, utilización o divulgación no autorizada del titular, en la medida que:*
>
> *a) La información sea secreta en el entendido de que como conjunto o en la configuración o composición precisas de sus elementos no sea conocida en general ni fácilmente accesible a las personas integrantes de los círculos que normalmente manejan el tipo de información de que se trate;*
>
> *b) La información tenga un valor comercial, efectivo o potencia, por ser secreta; y,*
>
> c) *En las circunstancias dadas, la persona que legalmente la tenga bajo control haya adoptado medidas razonables para mantenerla secreta."*

Por su parte, el artículo 260 de la Decisión 486 de la Comunidad Andina señala:

> *"Art. 260.- Se considerará como secreto empresarial cualquier información no divulgada que una persona natural o jurídica legítimamente posea, que pueda usarse en alguna actividad productiva, industrial o comercial, y que sea susceptible de trasmitirse a un tercero, en la medida que dicha información sea:*
>
> *a) Secreta en el sentido que como conjunto o en la configuración y reunión precisa de sus componentes, no sea generalmente conocida ni fácilmente accesible por*

quienes se encuentran en los círculos que normalmente manejan la información respectiva;

b) *Tenga un valor comercial por ser secreta; y,*

c) *Haya sido objeto de medidas razonables tomadas por su legítimo poseedor para mantenerla secreta.*

La información de un secreto empresarial podrá estar referida a la naturaleza, características o finalidades de los productos; a los métodos o procesos de producción; o, a los medios o formas de distribución o comercialización de productos o prestación de servicios".

Javier Fernández Teruelo, citado por Vizueta, menciona que también "son susceptibles de protección como información no divulgada el conocimiento tecnológico, integrado por procedimientos de fabricación y producción en general; y, el conocimiento relativo al empleo y aplicación de técnicas industriales resultantes del conocimiento, experiencia o habilidad intelectual, que guarde una persona con carácter confidencial, y que le permita mantener u obtener una ventaja competitiva o económica frente a terceros". Se considera titular de estos derechos, a la persona natural o jurídica que tenga el control legítimo de la información no divulgada.

Así mismo, debe considerarse como merecedora de protección a la información bancaria y crediticia, tanto de personas naturales como jurídicas. Si bien esta información tiene un contenido económico a su vez constituye información de carácter personal.

En cuanto a la información extrapatrimonial, nos referimos a aquella información de carácter personal, que sin tener la característica de ser "secreta", pertenece a la persona y su reserva y secreto respecto de terceros recibe protección constitucional y legal. Dentro de esta categoría se encuentra la información relacionada a la ideología, religión, creencias, afiliación sindical, origen racial, vida sexual, orientación sexual, salud, infracciones penales o administrativas, entre otras.

Cuando la información es extrapatromonial, es decir, información personal o sensible, aparece una estrecha relación con el derecho a la intimidad, que como se analizó anteriormente, posee un doble ámbito de protección: por un lado, el derecho para evitar injerencias por parte de terceros así como el derecho para revelar sólo aquello que se desee de sí mismo[79].

Recordemos también que uno de los principios rectores recogidos por la Ley de Comercio Electrónico, Firmas y mensajes de datos, es el de Confidencialidad y Reserva:

> *Art. 5- Se establecen los principios de confidencialidad y reserva para los mensajes de datos cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación de secreto profesional será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.*

Por todo lo expuesto, considero que el bien jurídico directamente afectado por los delitos informáticos, que pueden producirse en contratación electrónica, es la información y, es de la vulneración a la información, que se desprenden las vulneraciones al derecho a la intimidad – derecho al control sobre los datos personales - y al derecho de propiedad.

El planteamiento que propongo es que en todas las conductas criminales relacionadas con lo contratos electrónicos, y actualmente tipificadas por nuestro Código Penal, mantienen una relación directa con la información como bien jurídico protegido, e indirecta con otros bienes jurídicos como la intimidad y la propiedad. Es decir, podría existir una vulneración a la intimidad, por la intromisión en los sistemas informáticos que tiene por finalidad acceder a la información. De la misma manera, existirá un delito contra la propiedad por el daño en sistemas informáticos, y la magnitud de este daño viene dada por el valor de la información que se pueda perder producto de tal daño.

[79] Juan Vizueta Ronquillo, op.cit., p.43

A continuación, me limitaré a explicar con más detalle los tipos penales en sentido amplio, siempre en relación al contrato electrónico como contrato a distancia.

3.2.2 Delitos informáticos

A decir de Juan Vizueta, en relación al *delito informático* la doctrina mantiene dos posturas[80]. Por un lado están quienes se alinean en un sector que considera "el uso de la informática como medio novedoso para afectar bienes jurídicos ya resguardados en el Derecho Penal". Por otro lado, están aquellos que consideran que estamos ante conductas que afectan a un nuevo interés social, "íntimamente ligado al tratamiento de la información".

Siguiendo la línea planteada a lo largo de esta investigación, considero que *delito informático* es aquella conducta típica, antijurídica y culpable que lesiona bienes jurídicos ya existentes, valiéndose para ello de medios informáticos. Tales bienes jurídicos, como mencionamos y desarrollamos anteriormente, son la información, la propiedad y la intimidad.

De manera general, la ejecución de un delito supone la existencia de: un *sujeto activo* que ejecuta la acción tipificada por la norma; el *sujeto pasivo*, es decir, el titular del bien jurídico lesionado; este último, constituye el *objeto* del delito. Y por último, el *fin* de cualquier delito que es la alteración del orden público y jurídico.

El sujeto activo, es decir, quien comete un delito informático es una persona que posee cierta característica especial: posee habilidad en el manejo de sistemas informáticos[81]. Estas personas reciben denominaciones especiales y que es importante diferenciar, pues ofrecen sutiles diferencias; estos son: *hackers, crackers y phreakers.*

Sobre estas definiciones seguiremos lo desarrollado por Serra[82]. El *hacker* es toda persona que, valiéndose de medios informáticos y de telecomunicaciones, accede remotamente y en

[80] Juan Vizueta Ronquillo, op.cit., p.32.
[81] Juan José Páez Rivadeneira y Santiago Acurio, op.cit., p. 185.
[82] Andrea Viviana Sarra, op.cit., p. 167.

forma no autorizada a sistemas de información cuyo acceso le está vedado. Su motivación es el simple deseo de quebrantar el sistema y ve en ello un desafío a su intelecto. Realiza esta actividad sin intención de provocar daño en las cosas, aunque ocasionalmente y de manera accidental puede destruir información o dañar los sistemas.

El *cracker* es toda persona que, por idénticos medios – informáticos y de telecomunicaciones- accede a sistemas de información que le son vedados, pero con la intención de provocar daño o apoderarse indebidamente de información.

El *phreaker* es la persona que, para llevar a cabo la actividad de *hacker* o de *cracker*, utiliza indebidamente líneas telefónicas puesto que, más allá del valor de los pulsos telefónicos utilizados, su motivación es evitar ser rastreado.

En el análisis de la responsabilidad penal generada por el cometimiento de un delito penal, nos referiremos únicamente a aquellos tipos penales posibles al momento de contratar electrónicamente, que afectan al bien jurídico información, relacionando por supuesto con la técnica de comunicación a distancia y con la lesión al soporte electrónico que contiene al contrato electrónico.

a) Acceso ilegítimo a sistemas de información

El acceso no autorizado a información de carácter personal es un delito informático cuyo objeto material es la obtención de información. Puede presentar múltiples variantes, y su objetivo es infringir un sistema de seguridad informático sin autorización.

Pueden cometer este tipo de delitos los *hackers*. En este caso estaremos ante un caso de ataque externo. Pero, también es posible que el acceso ilegítimo lo ejecute la persona encargada de la custodia de tales sistemas de información, en cuyo caso, el acceso se realizará sin necesidad de vulnerar los sistemas, pues esta persona posee las claves de acceso y conoce perfectamente

cómo acceder a los sistemas de información. En el primer caso, podríamos decir que el acceso ilegítimo se da con fuerza en las cosas; mientras que en el segundo caso no.

Considera Hocsman que, para que se configure el acceso ilegítimo a sistemas de información "debe darse una serie de presupuestos, como la intención de quebrantar barreras de seguridad por parte del delincuente y que el titular del sistema -informático o de información- no preste su consentimiento o voluntad para ingresar en él"[83].

Este es un caso de *intrusismo informático*, es decir, de penetración por la fuerza en un sistema de información. Basta tan solo el ingreso subrepticio a la información para la concreción de este comportamiento[84].

Cuando el acceso no autorizado se refiere a información protegida, como secretos comerciales o industriales, se convierte en una variedad de espionaje industrial informático. En estos casos, el acceso ilegítimo a sistemas de información tiene el propósito de obtener para sí o para terceros, un provecho indebido.

Luis Miguel Reyna, citado por Vizueta[85], expone algunas de las modalidades más conocidas de espionaje informático:

1. La fuga de datos o *Data Leakage*: modalidad informática de las prácticas de espionaje industrial. Aparece en tanto todas las empresas y entidades custodian sus informaciones más valiosas en los archivos informáticos posibilitándose su sustracción.
2. Las puertas falsas o *Trap Doors*: conducta consistente en la introducción a los sistemas informáticos a través de accesos o puertas de entrada o previstas en las instrucciones de aplicación de los programas, aunque estas conductas puedan ser verificados sólo por quienes tengan un conocimiento cualificado de los sistemas informáticos propensos a estos ataques.

[83] Heriberto Simón Hocsman, op.cit., p. 252.
[84] Juan Vizueta Ronquillo, op.cit., p.34.
[85] Juan Vizueta Ronquillo, op.cit., p.38.

3. Las Llaves maestras o *Superzapping*: es el uso no autorizado de programas con la finalidad de modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivaos en los sistemas de información, su denominación se debe a un programa llamado *superzap*, que permite ingresar a cualquier archivo a modo de llave maestra, así se encuentre reservado.
4. El pinchado de líneas o *Wiretapping*: modalidad que consiste en la interferencia en líneas telefónicas o telemáticas, mediante las cuales se transmiten las informaciones procesadas.
5. La apropiación de informaciones residuales o *scavenging*: consiste en la obtención de información abandonada por los usuarios legítimos de los sistemas informáticos.

Otra variante de esta misma conducta, acceso no autorizado a sistemas de información, ocurre cuando el acceso a información protegida, secretos comerciales o industriales, tiene por finalidad la divulgación de la misma.

b) Daño o sabotaje informático

En este caso el bien jurídico protegido es la integridad de los sistemas, informáticos y de información. Se precautelan los sistemas de los daños informáticos por la información valiosa que ellos guardan. Es decir, aunque el bien jurídico protegido por este tipo penal es la propiedad, la protección de estos bienes encuentra su motivación en el valor de la información que contienen y que circula a través suyo.

Este tipo delictivo se forma con dos elementos. Un elemento objetivo que es el borrado, destrucción o alteración de un sistema informático o de información. Y un elemento subjetivo compuesto por la intención de dañar, es decir, el dolo.

Páez y Acurio nos ofrecen una serie de técnicas que permiten cometer sabotajes informáticos[86]:

[86] Juan José Páez Rivadeneira y Santiago Acurio, op.cit., p. 218.

1. Bombas lógicas: son especie de bombas de tiempo que deben producir daños posteriormente. Requiere la programación de la destrucción o modificación de datos en un momento dado. Al contrario de los programas dañinos o virus, las bombas lógicas son difíciles de detectar antes de su explosión, por ello, son los dispositivos informáticos criminales con mayor potencial de daño.

   La bomba lógica también puede ser utilizada como instrumento de extorsión.
2. Gusanos: son parecidos a los virus en cuanto a tienen como objetivo infiltrarse en programas legítimos para modificar o destruir información, per se diferencian en que no tienen capacidad de regenerarse. La consecuencia de un programa gusano, es que puede dar instrucciones a un sistema informático para mantener una acción de manera continua a fin de perpetrar un ilícito.
3. Virus informáticos o *malware* son elementos informáticos que tienden a reproducirse y a extenderse dentro del sistema informático al que acceden, se propagan de un sistema a otro y pueden desarrollar resistencia a los programas de antivirus
4. Ataques de denegación de servicios: son ataques que se basan en utilizar la mayor cantidad posible de recursos del sistema informático de manera que nadie más pueda usarlos, por ejemplo, el consumo de memoria de la computadora de la víctima, hasta que se produce un error general del sistema informático por falta de memoria que lo deja fuera de servicio.

La legislación penal ecuatoriana, se refiere al daño informático pero únicamente al que es cometido por servidores públicos. Es decir, si la conducta es cometida por una persona que no ostente tal calidad, la conducta no podría ser juzgada por no estar contemplada por la ley, en atención al principio de legalidad que rige la materia.

CAPÍTULO III

3. Seguridad jurídica en el comercio electrónico

Cuando hablamos de seguridad jurídica nos referimos al marco jurídico que los países han desarrollado a fin de proteger a los ciudadanos en la esfera de sus actividades y en su relaciones en sociedad. Se refiere a la existencia de normas claras, previas y públicas.

El tema de la seguridad jurídica en el comercio electrónico es el aspecto que más ha preocupado desde sus inicios, pues, la existencia de una normativa clara favorece el clima de tranquilidad que debe primar en las negociaciones contractuales electrónicas. En consecuencia, se ha tratado de establecer marcos jurídicos de carácter general para ciertos aspectos de las transacciones electrónicas, con el objetivo de garantizar la seguridad de los destinatarios o usuarios

Es así como la Asamblea General de las Naciones Unidas, a través de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, aprobó la Resolución 51/162, la cual contenía una Ley Modelo, elaborada por la referida comisión, destinada a orientar a los países de la región en la elaboración y promulgación de una ley que regule el comercio electrónico.

En su parte considerativa, dicha Resolución recuerda que es un mandato para la Comisión el fomentar la armonización y unificación progresiva del derecho mercantil internacional, lo cual beneficiará a todos los países, en especial a los países en desarrollo. De igual forma, considera que es creciente el número de transacciones comerciales internacionales que se realizan por medio del intercambio electrónico de datos y por otros medios de comunicación. Así mismo, toma en consideración la Resolución 40/75, aprobada por la Asamblea General el 11 de diciembre de 1985, en la cual se pide a los gobiernos y a las organizaciones internacionales que, cuando así convenga, adopten medidas acordes con las recomendaciones de la Comisión a fin de garantizar la seguridad jurídica en el contexto de la utilización más amplia posible del procesamiento automático de datos en el comercio internacional. Finalmente, la Asamblea General recomienda que todos los Estados consideren de manera favorable la Ley Modelo

cuando promulguen o revisen sus leyes, tomando en cuenta la necesidad de que el derecho aplicable a los métodos de comunicación y almacenamiento de información sustitutivos de los que utilizan papel, sea uniforme.

La Constitución de Montecristi en el Título II, Sección tercera, artículo 16.2, establece el derecho constitucional de todos los ecuatorianos a la Comunicación e Información[87]:

> Artículo 16.- Todas las personas, en forma individual o colectiva, tienen derecho a:
> 2. El acceso universal a las tecnologías de información y comunicación

Las normas infra constitucionales que de manera especializada rigen la materia son:

- ✓ Ley de Comercio Electrónico, Firma Electrónica y Mensajes de Datos, fue aprobada en el año 2002 y publicada en el Suplemento del Registro Oficial n. 557 de 17 de abril de 2001;
- ✓ Reglamento General a la Ley de Comercio Electrónico, Firma Electrónica y Mensajes de Datos expedido mediante Decreto Ejecutivo n. 3496 y publicado en el Registro Oficial n. 735 de 31 de diciembre de 2001:
- ✓ Reglamento para la Acreditación, Registro y Regulación de Entidades Habilitadas para prestar Servicios de Certificación de Información y Servicios Relacionados, aprobado mediante Resolución 548-23-CONATEL-2003 del Consejo Nacional de Telecomunicaciones y publicado en el Registro Oficial n. 196 de 23 de octubre de 2003;
- ✓ Reglamento para la organización y Funcionamiento del Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditados y Terceros Vinculados, aprobado mediante Resolución 479-20-CONATEL-2008 del Consejo Nacional de Telecomunicaciones y publicado en el Registro Oficial n. 455 de 28 de octubre de 2008.

A continuación realizaremos un estudio sobre esta Ley, remarcando sus aciertos y falencias.

[87] Constitución de la República del Ecuador 2008

3.1 Análisis de la Ley de Comercio Electrónico, Firma Electrónica y Mensajes de Datos ecuatoriana, en el ámbito de la contratación

La Ley de Comercio Electrónico, Firma Electrónica y Mensajes de Datos fue publicada en el Suplemento del RO 557 de 17 de abril de 2002; su última modificación fue en octubre de 2011.

Para la elaboración y aprobación de esta ley se siguieron las recomendaciones internacionales, principalmente las dictadas por las Naciones Unidas y la Comisión de Derecho Mercantil Internacional. En el debate, revisión y formulación de la Ley de Comercio Electrónico participaron: Corporación Ecuatoriana de Comercio Electrónico, CORPECE; Consejo Nacional de Telecomunicaciones, CONATEL; Federación de la Cámaras de la Producción; Cámara de Comercio de Quito; Cámara de Comercio de Guayaquil; Superintendencia de Telecomunicaciones; Asociación de Bancos Privados del Ecuador; Microsoft del Ecuador; Asociación Ecuatoriana de Tarjetas de crédito; Tribuna del Consumidor; Superintendencia de Bancos; Asociación de Financieras del Ecuador; Banco Central del Ecuador; Superintendencia de Compañías; Bolsa de Valores de Quito; Corporación de Promoción de exportaciones e inversiones, CORPEI; Andinatel; Pacifictel; Bellsouth; Porta Celular; Asociación Ecuatoriana de Proveedores de Servicios de Internet, AEPROVI; Asociación Ecuatoriana de Empresas de Telecomunicaciones; Ministerio de Relaciones Exteriores; Servicio de Rentas Internas; Corporación Aduanera Ecuatoriana; Ministerio de Turismo; Escuela Politécnica del Litoral; Organización Mundial de la Propiedad Intelectual, OMPI; Organización Mundial de Derecho Informático, OMDI; Comunidad virtual de Derecho informático Alfa- Redi; Asociación Chilena de Derecho Informático; Asociación Argentina de Derecho y Alta tecnología; Asociación Venezolana de Derecho Informático; Asociación Peruana de Derecho Informático; Centro Internacional de Derecho Informático (España); Asociación Ecuatoriana de Derecho Informático[88].

[88] Fuente: http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/2005/11/24/se-aprobo-la-ley-de-comercio-electronico

La Ley consta de un Título Preliminar y cinco Títulos adicionales, con sus respectivos Capítulos y Artículos, en total 64. No menos importante es su parte Considerativa, es decir, en donde se encuentran los fundamentos legales y su necesidad de emisión. Más allá de normar, regular y controlar las actuaciones dentro del comercio electrónico, es fundamental analizar los tres primeros considerandos de la Ley:

1. Que el uso de sistemas de información y redes electrónicas, incluida la Internet, ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado.
2. Que es necesario impulsar el acceso de la población a los servicios electrónicos que se generan por y a través de diferentes medios electrónicos.
3. Que se debe generalizar la utilización 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.

De la lectura de estos considerandos podemos evidenciar que esta ley no se limita a normar y regular, sino que busca incentivar y fomentar el comercio electrónico, *impulsarlo* y *generalizarlo* debido a la importancia para el *desarrollo del comercio y la producción.*

El Diccionario de la Real Academia Española define el término *Impulsar* como "Dar empuje para producir movimiento"; y *Generalizar:* "Hacer algo público o común". Es decir, esta ley no debe servir únicamente para normar actividades, regularlas, controlarlas o establecer sanciones. Debe ir más allá, porque su fundamento es dar empuje al comercio electrónico y convertirlo en algo común, con la finalidad de volverlo un "*medio para el desarrollo del comercio y la producción"*.

Una vez realizado este planteamiento, continuaré con la exposición de la estructura y contenido de la Ley para al final poder determinar cuáles son las falencias que presenta y que no le permiten cumplir con la motivación de su creación.

La Ley está estructurada de la siguiente manera:

- **Título Preliminar**: *Objeto de la Ley*. Capítulo I

- **Título II**: *De las Firmas Electrónicas, Certificados de Firma Electrónica, Entidades de Certificación de Información, Organismos de Promoción de los Servicios Electrónicos, y de Regulación y Control de las Entidades de Certificación Acreditadas*. Capítulo I, Artículos 13-19; Capítulo II, Artículos 20-28; Capítulo III, Artículos del 29-35; Capítulo IV, Artículos 36-43.
- **Título III**: *De los Servicios Electrónicos, la Contratación Electrónica y Telemática, los Derechos de los Usuarios, e Instrumentos Públicos.* Capítulo I, Artículo 44; Capítulo II, Artículos del 45-47; Capítulo II, Artículos del 48-50; Capítulo IV, Artículo 51.
- **Título IV:** *De la Prueba y Notificaciones Electrónicas.* Capítulo I, Artículos 52-56
- **Título V:** *De las Infracciones Informáticas.* Capítulo I, Artículos 57-64
- **Disposiciones Generales, Disposiciones Transitorias y Disposición Final.**

El mensaje de datos consta como la base conceptual de la Ley. Se otorga reconocimiento jurídico a los mensajes de datos, a sus anexos y a la firma electrónica.

Analizaremos los Títulos y Capítulos que tienen trascendencia para el comercio electrónico.

En el Capítulo I del Título Preliminar aparecen los Principios Generales en los que se basa esta Ley:

1. Valor jurídico de los mensajes de datos y sus anexos
2. Sometimiento a la ley de propiedad intelectual
3. Confidencialidad y Reserva
4. Disponibilidad de la información
5. Integridad de los mensajes de datos
6. Conservación de los mensajes de datos
7. Protección de datos
8. Duplicación del mensaje de datos, cada mensaje es considerado diferente.

Otros principios aplicables a la firma electrónica son incorporados a través del Reglamento a la Ley de Comercio Electrónico, así tenemos:

1. Principio de Neutralidad Tecnológica
2. Principio de No discriminación de cualquier tipo de firma electrónica
3. Principio de compatibilidad internacional

Dentro del capítulo de la Ley que nos encontramos analizando, aparecen otros criterios, que sin ser principios, pretenden conferir de cierta seguridad jurídica a las actividades dentro de la contratación electrónica; tales criterios son: la forma como debe operar la desmaterialización de los documentos, sobre la identidad de originador y receptor de mensaje de datos, presunciones sobre el momento y lugar de envío y recepción de mensajes.

Título II: *De las Firmas Electrónicas, Certificados de Firma Electrónica, Entidades de Certificación de Información, Organismos de Promoción de los Servicios Electrónicos, y de Regulación y Control de las Entidades de Certificación Acreditadas*

Empieza el Capítulo I refiriéndose a la Firma Electrónica a la cual define como los "datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que pueden ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos".

La ley atribuye a la firma electrónica el mismo valor y efectos jurídicos que tiene la firma manuscrita, tanto que puede ser admitida como prueba en juicio, siempre que cumpla con los requisitos del artículo 15.

Uno de los principios que rige a la firma electrónica es el de Unidad de Acto, es decir, la firma se fijará en un mensaje de datos y deberá enviarse en un mismo acto, como parte integrante o lógicamente asociada al mensaje. Se establece también una presunción en cuanto a la voluntad del emisor de emitir tal mensaje y de obligarse en los términos de aquél.

Al final del capítulo, se establecen las obligaciones del titular de la firma electrónica, el tiempo de duración, el cual pude perfectamente ser indefinido, y sobre las formas de extinción de la firma electrónica.

El Capítulo II de este mismo Título se refiere al Certificado de Firma Electrónica, el cual, a decir del artículo 20, “es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad”.

Estos Certificados deben cumplir con una serie de requisitos para ser considerados válidos, requisitos que tienen que ver con la identificación clara del titular de la firma, identificación y firma electrónica de la autoridad de certificación que certifica, de las fechas de vigencia del certificado, las limitaciones para su uso, la constancia del método de verificación de la firma.

De igual forma, se fijan las causales para la extinción, suspensión y revocatoria del certificado de firma electrónica, y, se otorga reconocimiento a los certificados de firma electrónica emitidos por entidades de certificación extranjeras, siempre que cumplan con los requisitos señalados por la ley.

El inciso final del artículo 28 señala que los Estados deben buscar armonizar sus normas sobre esta materia, a través de la suscripción de convenios o tratados internacionales.

El Capítulo III se refiere a las Entidades de Certificación e Información y las define como aquellas “empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones…”.

Las Entidades de Certificación deben cumplir con una serie de obligaciones que las mencionaremos por su importancia, por cuanto del estricto cumplimiento de este requisito depende en mucho la seguridad jurídica de las negociaciones realizadas a través del comercio electrónico.

En primer lugar, encontrarse legalmente constituidas y registradas en el CONATEL; demostrar solvencia técnica, logística y financiera; garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de información; mantener sistemas de respaldo de la información relativa a los certificados; proceder de forma inmediata a la suspensión o revocatoria de los certificados electrónicos ordenados por

Superintendencia de Telecomunicaciones; mantener una publicación del estado de los certificados emitidos; proporcionar a los titulares de certificados de firma electrónicas un medio efectivo y rápido para dar aviso que una firma electrónica tiene riesgo de uso indebido. Y, por último, una de las más importantes, "contar con una garantía de responsabilidad para cubrir daños y perjuicios que ocasionaren por el incumplimiento de las obligaciones previstas en la presente Ley, y hasta por culpa leve en el desempeño de sus obligaciones". Esta garantía será de al menos el 5% del monto total de las operaciones.

A continuación, el artículo 31 establece las responsabilidades de las Entidades de Certificación:

> Art. 31.- Las Entidades de certificación de información serán responsables hasta de culpa leve y responderán por los daños y perjuicios que causen a cualquier persona natural o jurídica, en el ejercicio de s actividad, cuando incumplan las obligaciones que les impone esta Ley o actúen con negligencia.
>
> Los contratos con los usuarios deberán incluir una cláusula de responsabilidad que reproduzca lo que señala el primer inciso.
>
> Cuando la garantía constituida por las autoridades de certificación acreditadas no cubra las indemnizaciones por daños y perjuicios, aquellas responderán con su patrimonio.

Esto quiere decir, que el Intermediario llamado Entidad de Certificación está obligado por ley a cumplir con los daños y perjuicios que ocasionaren a los usuarios y para ello, cuentan con una garantía de responsabilidad por valor suficiente que deben presentar al momento de acreditarse ante el CONATEL. Con ello los contratos electrónicos, al ser firmados electrónicamente, están protegidos ante los daños de los que sean responsables este Intermediario.

Este tema, se desarrolla a profundidad en las reformas al Reglamento a la Ley, que fueron incorporadas en 2008, en las cuales se establecen los parámetros de la Garantía de Responsabilidad. Así tenemos que el doceavo artículo innumerado agregado a continuación del artículo 17 de la ley, establece:

1. Para el primer año de operaciones, la Entidad de Certificación deberá contratar y mantener a favor de la SENATEL una garantía para responder por los daños y perjuicios ocasionados por el posible incumplimiento de sus obligaciones de un monto de USD 400.000,00.
2. Para el segundo año de operaciones, hasta el final del plazo de acreditación, la Entidad de Certificación deberá contratar la garantía por un monto que estará en función de un valor de base de garantía por certificado y que será determinado por el CONATEL, en función de la evolución del mercado y la protección de los derechos de los usuarios.

Este mismo artículo exonera de responsabilidad por los daños y perjuicios cuando el usuario exceda los límites de uso indicados en el certificado: "*la Entidad de Certificación de Información y Servicios Relacionados Acreditada quedará exenta de responsabilidad por daños y perjuicios cuando el usuario exceda los límites de uso indicados en el certificado".*

En cuanto a las responsabilidades de las entidades de certificación, las reformas incluyeron un artículo innumerado que señala que es de su responsabilidad verificar la autenticidad y exactitud de todos los datos que consten en el certificado de firma electrónica, siendo también de su responsabilidad el emitir Certificados Únicos.

En cuanto al tema de protección de datos, el artículo 32 de la Ley establece un criterio fundamental para la seguridad del comercio electrónico y se refiere a la obligación de protección de datos por parte de las entidades de certificación. Sobre este mismo punto, el artículo 21 del Reglamento contiene la obligación para quienes prestan servicios electrónicos, de contar con sistemas seguros en todas las etapas del proceso de prestación de dichos servicios, sobre todo cuando la prestación del servicio implique el envío por parte del usuario de información personal, confidencial o privada. Para ello, es obligación del prestador de servicios,

> "informar en detalle a los usuarios sobre el tipo de seguridad que utiliza, sus alcances y limitaciones, así como sobre los requisitos de seguridad exigidos legalmente y si el

sistema puesto a disposición del usuario cumple con los mismos. En caso de no contar con seguridades se deberá informar a los usuarios de este hecho en forma clara y anticipada previo el acceso a los sistemas o a la información e instruir claramente sobre los posibles riesgos en que puede incurrir por la falta de dichas seguridades".

El artículo del reglamento que nos encontramos analizando, establece también en su segundo inciso un criterio sobre lo que se considera "datos sensibles" indicando que se trata de información personal como información financiera de cualquier tipo, como números de tarjetas de crédito o similares, que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten.

En el Capítulo IV se establece que el Organismo de Regulación será el CONATEL, el Organismo de Control, la Superintendencia de Telecomunicaciones y el Organismo de Promoción el COMEXI. Sobre esta disposición cabe anotar que actualmente el Consejo de Comercio Exterior e Inversiones COMEXI fue reemplazado por el Comité de Comercio Exterior COMEX, creado por el artículo 71 del Código Orgánico de la Producción, Comercio e Inversiones.

Título III: *De los Servicios Electrónicos, la Contratación Electrónica y Telemática, los Derechos de los Usuarios, e Instrumentos Públicos*

El Capítulo I se refiere a los servicios electrónicos, los cuales, sean transacciones mercantiles, financieras o de servicios que se realicen con mensajes de datos, se encuentran dotados del mismo valor y efectos jurídicos que cualquier transacción tradicional, siempre que se sometan a los requisitos y solemnidades de la ley que los rija.

El Capítulo II trata de la Contratación Electrónica. Los artículos 45 y 46 son los que otorgan validez y obligatoriedad a los contratos que se forman y perfeccionan a través de mensajes de datos.

En este capítulo se fijan reglas sobre el lugar de perfeccionamiento del contrato electrónico y sobre la jurisdicción aplicable, que estarán sujetas al principio de libertad contractual. Si no se

hubiera pactado nada al respecto, se sujetarán a las reglas generales señaladas en el Código de Procedimiento Civil siempre que no se trate de consumidores, en donde se observará lo estipulado en la Ley Orgánica de Defensa del Consumidor.

El Capítulo III se refiere a los derechos de los usuarios o consumidores de servicios electrónicos, derechos que se basan en el principio de disponibilidad de la información y consentimiento de las partes para aceptar registros electrónicos o mensajes de datos.

3.1.1 Sanciones penales y administrativas

La Ley de Comercio Electrónico, Firma Electrónica y Mensajes de Datos, en los artículos del 40 al 43 hace referencia a las infracciones administrativas, sanciones, medidas cautelares y sus procedimientos.

Las Infracciones Administrativas son clasificadas en dos grupos: leves y graves.

Son infracciones administrativas leves:

1. La demora en el cumplimiento de una instrucción o en la entrega de información requerida por los organismos de control; y,
2. Cualquier otro incumplimiento de las obligaciones impuestas por esta ley y sus reglamentos a las entidades de certificación acreditadas.

Son infracciones graves:

1. El uso indebido del certificado de firma electrónica por omisiones imputables a la entidad de certificación de información acreditada;
2. Omitir comunicar al organismo de control, de la existencia de actividades presuntamente ilícitas realizadas por el destinatario del servicio:
3. Descartar la petición del organismo de control de suspender la prestación de servicios de certificación para impedir el cometimiento de una infracción;
4. El incumplimiento de las resoluciones dictadas por los organismos de Autorización, Registro y Regulación, y de Control; y,

5. No permitir u obstruir la realización de auditorías técnicas por parte del organismo de control.

En cuanto a las sanciones, la ley establece los siguientes criterios:

- ✓ Las sanciones impuestas no eximen del cumplimiento de las obligaciones
- ✓ Las sanciones podrán agravarse si los infractores son empleados de instituciones del sector público.
- ✓ Para establecer la gradación de las sanciones se tomará en cuenta:
  a) La gravedad de la infracción cometida y su reincidencia;
  b) El daño causado o el beneficio reportado al infractor; y,
  c) La repercusión social de las infracciones.

Las sanciones que la Ley prevé se impondrán de oficio o a petición de parte, según la naturaleza y gravedad de la infracción y pueden estar dirigidas a las entidades de certificación, a sus administradores y representantes legales, o a terceros que presten sus servicios.

Las sanciones previstas en el artículo 41 son:

1. Amonestación escrita;
2. Multa de quinientos a tres mil dólares de los Estados Unidos de Norteamérica;
3. Suspensión temporal de hasta dos años de la autorización de funcionamiento de la entidad infractora, y multa de mil a tres mil dólares de los Estados Unidos de Norteamérica;
4. Revocatoria definitiva de la autorización para operar como entidad de certificación acreditada y multa de dos mil a seis mil dólares de los Estados Unidos de Norteamérica

En cuanto a las infracciones penales y sus sanciones, el Título V de la Ley realiza una serie de reformas al Código Penal como aparece a continuación:

TÍTULO II
De los delitos contra las garantías constitucionales y la igualdad racial

A continuación del artículo 202, se incluyen los siguientes artículos:

	MEDIO	ACCIÓN	FIN	SANCIÓN
1	El que por cualquier medio electrónico, informático o afín	violentare claves o sistemas de seguridad	1.- Para acceder u obtener información protegida, contenida en sistemas de información	Prisión: 6 meses - 1 año Multa: 500 a 1000 dólares
			2.- Para vulnerar el secreto, confidencialidad y reserva	
			3.- O simplemente para vulnerar la seguridad	
			4.- Si la información obtenida se refiere a seguridad nacional, a secretos comerciales o industriales	Prisión: 1 a 3 años Multa: 1000 a 1500 dólares
			5.- Para divulgar o utilizar fraudulentamente la información protegida, así como lo secretos comerciales o industriales	Reclusión: 3 a 6 años Multa: 2000 a 10000 dólares
			6.- Si la divulgación o utilización fraudulenta se realiza por parte de la persona encargada de la custodia o utilización legítima de la información	Reclusión: 6 a 9 años Multa: 2000 a 10000 dólares
2	El que por cualquier medio electrónico, informático o afín	obtuviere información sobre datos personales	1.- Para cederla, publicarla, utilizarla o transferirla a cualquier título, sin autorización del titular	Prisión: 2 meses a 2 años Multa: 1000 a 2000 dólares

CAPÍTULO V

TÍTULO III
De los delitos contra la Administración Pública

Capítulo V De la Violación de los deberes de Funcionarios Públicos, de la Usurpación de atribuciones y de los abusos de autoridad

Sustítuyase el artículo 262 por el siguiente

	SUJETO ACTIVO	ELEMENTO SUBJETIVO	ACCIÓN	SANCIÓN
1	Todo empleado público y toda persona encargada de un servicio público	que hubiere maliciosa y fraudulentamente	Destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica	Reclusión: 3 a 6 años

TÍTULO IV
De los delitos contra la fe pública

Capítulo III De las falsificaciones de documentos en general

A continuación del artículo 353, agréguese el siguiente artículo innumerado

	SUJETO ACTIVO	ELEMENTO SUBJETIVO	ACCIÓN	SANCIÓN
1	La persona o personas que	con ánimo de lucro o para causar un perjuicio a un tercero	por cualquier medio alteren o modifiquen mensajes de datos o la información incluida en estos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea	No especifica sanción para este caso. Se remite a las sanciones que el Código Penal prevé para la falsificación de documentos. Pena puede variar de 9 a 12 años de reclusión extraordinaria.

TÍTULO V
De los delitos contra la seguridad pública

Capítulo VII Del incendio y otras destrucciones, de los deterioros y daños

A continuación del artículo 415, agréguese los siguientes artículos innumerados:

	ELEMENTO SUBJETIVO	MEDIO	ACCIÓN	SANCIÓN
1	El que dolosamente,	de cualquier modo o utilizando cualquier medio	destruya, altere, inutilice, suprima o daño, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica.	Prisión: 6 meses a 3 años Multa: 60 a 150 dólares
			1.- Si se trata de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada a la defensa nacional	Prisión: 3 a 5 años Multa: 200 a 600 dólares
2			2.- Destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la trasmisión, recepción o procesamiento de mensajes de datos.	Prisión: 8 meses a 4 años Multa: 200 a 600 dólares

TÍTULO X
De los delitos contra la propiedad

Capítulo II Del robo

A continuación del artículo 553, agréguese los siguientes artículos innumerados:

	ACCIÓN	FIN	ACCIÓN	SANCIÓN
1	Los que utilizaren fraudulentamente sistemas de información o redes electrónicas	para facilitar la apropiación de un bien ajeno	alterando, manipulando o modificando el funcionamiento en redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos	Prisión: 6 meses a 5 años Multa: 500 a 1000 dólares
2	Los que procuren la transferencia no consentida de bienes, valores o derechos de una persona	en beneficio suyo o de otra persona		
		Si el mismo delito se realiza por los siguientes medios:	1. Inutilización de sistemas de alarma o guarda.	Prisión: 1 a 6 años Multa: 1000 a 2000 dólares
			2. Descubriendo o descifrando claves secretas o encriptadas	
			3. Utilizando tarjetas magnéticas o perforadas	
			4. Utilizando controles o instrumentos de apertura a distancia	
			5. Violando seguridades electrónicos, informáticas u otras semejantes	

Capítulo V De las estafas y otras defraudaciones

A continuación del artículo 563, agréguese los siguientes artículos innumerados:

	SUJETO ACTIVO	MEDIO	SANCIÓN	
1	Quien estafe	utilizando medios electrónicos	Prisión: 5 años Multa: 500 a 1000 dólares	

TÍTULO I
Capítulo III De las contravenciones de tercera clase

A continuación del numeral 19 del artículo 605, agréguese los siguientes artículos innumerados

"Los que violaren el derecho a la intimidad en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas o Mensajes de Datos"

SANCIÓN: Prisión: 2 a 4 días; Multa: 7 a 14 dólares

3.2 El comercio electrónico en la Comunidad Andina

Los países de la región están tomado conciencia sobre la exigencia que se requiere, por parte del legislador, para afrontar con éxito las demandas de un mundo revolucionado por un nuevo orden económico internacional.

La región tiene que ajustarse a las tendencias mundiales para hacerse más atractiva y atraer nuevas inversiones, crear mayores oportunidades de negocios, fomentar la apertura de nuevos mercados y garantizar un crecimiento económico sostenido[89].

Sin embargo de ello, la inseguridad jurídica del contrato electrónico existe en muchos temas, por ejemplo respecto a la exigibilidad de responsabilidades civiles y penales y a la protección eficiente de los datos económicos y personales que circulan en las redes abiertas.

Por lo tanto, es vital trabajar en conjunto para el fortalecimiento del comercio electrónico, a fin de eliminar la incertidumbre que rodea al documento electrónico firmado electrónicamente, y éste logre el mismo valor que el documento tradicional con firma manuscrita. Ese es el camino a seguir y uno de los objetivos de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional.

Como mencionaba anteriormente, la Ley Modelo recomendada por las Naciones Unidas ha sido observada por la mayoría de legislaciones de América Latina, pues se trata de un documento que busca orientar a las legislaciones sobre las reglas aceptadas en el ámbito internacional y que permitirán crear un marco jurídico que favorezca el desarrollo seguro de las vías electrónicas de negociación[90].

Analizaremos ahora el tratamiento que ha recibido el comercio electrónico por parte de la Comunidad Andina de Naciones, organismo supranacional cuyo objetivo es alcanzar el

[89] Ver mas: www.parlatino.org/es/comisiones-permanentes/servicios-públicos
[90] Ver más: Guía para la incorporación al derecho interno de la Ley Modelo de la CNUDMI sobre comercio electrónico.

desarrollo integral, equilibrado y autónomo, mediante la integración y cooperación económica y social[91].

Algunas de las recomendaciones adoptadas en la CAN, organismo regional andino, sobre este tema, han sido las siguientes[92]:

- ✓ Ejecutar un plan integral para superar las dificultades y obstáculos que impiden el desarrollo del comercio electrónico.
- ✓ Exhortar a los países de la Comunidad Andina a que aproximen su legislación sobre la materia, para su posterior armonización, contribuyendo así al establecimiento del Mercado Común.
- ✓ Evaluar todos y cada uno de los cuerpos jurídicos de cada país para evitar contradicciones o posteriores acciones en contra de las Leyes Marco que se implementen.
- ✓ Establecer los mecanismos e instrumentos jurídicos que brinden seguridad a las transacciones comerciales que se realizan por el medio digital.
- ✓ Lograr la consolidación del principio de equivalencia funcional del documento electrónico y firma electrónica en las leyes, para que puedan competir en igualdad de condiciones con los documentos tradicionalmente aceptados.

Actualmente, la CAN está llevando a cabo un estudio de las legislaciones vigentes sobre comercio electrónico de sus Países Miembros a fin de armonizar su contenido y proponer el texto de una Decisión comunitaria.

Hasta la fecha no se ha concertado un régimen común sobre comercio electrónico, pero cada uno de los Estados lo han abordado en sus legislaciones de una manera diferente:

[91] Fuente: www.comunidadandina.org
[92] Fuente: http://www.itu.int/ITU-D/cyb/publications/archive/Legislacion%20Comercio%20Electronico%20CAN1.pdf

COLOMBIA

La normativa vigente en la República de Colombia, relacionada con el comercio electrónico, es la siguiente[93]:

- ✓ Ley No. 527, vigente desde 1999 que reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación, basada en la Ley Modelo sobre Comercio Electrónico dado por Naciones Unidas.
- ✓ Decreto 1747 de 2002 que reglamenta parcialmente a la Ley 527 en lo relacionado a las entidades de certificación.
- ✓ Ley 1450 de 2011 que expide el Plan Nacional de Desarrollo 2010-2014, el cual incorpora dentro de sus ejes transversales la innovación en las actividades productivas nuevas y en las ya existentes.

La Ley 527 también ha sido inspirada en la Ley Modelo de la Comisión de Derecho Mercantil Internacional de Naciones Unidas. Contiene Cuatro Partes divididas en Capítulos, en total 47 artículos. Se encuentra estructurada de la siguiente manera:

- **Parte I**: *Parte General*. Capítulo I: Disposiciones Generales, glosario de términos; Capítulo II: Aplicación de los requisitos jurídicos de los mensajes de datos; Capítulo III: Comunicación de los mensajes de datos.
- **Parte II**: *Del Comercio Electrónico en Materia de Transporte de Mercancías*. Artículos 26 y 27 que se refieren a los actos relacionados con los contratos de transporte de mercancías y a los documentos de transporte, respectivamente.
- **Parte III**: *De las firmas digitales, certificados y Entidades de Certificación*. Capítulo I: de las firmas digitales; Capítulo II: Entidades de Certificación; Capítulo III: De los certificados; Capítulo IV: de los suscriptores de firmas digitales; Capítulo V: de la Superintendencia de Industria y Comercio; Capítulo VI: Disposiciones varias, relativas a certificaciones recíprocas e incorporación por remisión.
- **Parte IV:** *De la Reglamentación y vigencia*

[93] Fuente: http://programa.gobiernoenlinea.gov.co

La primera diferencia que salta a la vista, en relación con la legislación ecuatoriana, es en cuanto al ámbito de aplicación de la ley, la cual excluye de manera expresa a las obligaciones contraídas por el estado colombiano en virtud de tratados o convenios internacionales y para el caso de aquellos documentos que por disposición legal deban ir necesariamente impresos en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo.

Establece como principios de interpretación el carácter internacional de la Ley, por ello, la necesidad de promover la uniformidad en su aplicación, y el principio de buena fe.

En cuanto al reconocimiento jurídico de los mensajes de datos la norma es similar a la ecuatoriana, así como los principios que rigen su utilización.

El articulado que desarrolla las normas que rigen para la contratación electrónica, se en encuentra mucho más desarrollado en la legislación colombiana. Destaca el artículo 14 de la Ley que se refiere a la formación y validez de los contratos, y establece que *"en la formación del contrato, salvo acuerdo expreso entre las partes, la oferta y su aceptación podrán ser expresadas por medio de un mensaje de datos"*. La norma ecuatoriana en ese sentido, dice textualmente: *"los contratos podrán ser instrumentados mediante mensajes de datos"*. Es decir, la norma colombiana es mucho más específica al respecto.

En los artículos 15 y siguientes, se establecen una serie de parámetros que rigen la atribución y presunción de origen de los mensajes de datos; acuse de recibo y la presunción de recepción; la concordancia entre el mensaje de datos enviado con el mensaje de datos recibido; la presunción de que cada mensaje de datos recibido es una mensaje de datos único y diferente de cualquier otro, salvo prueba en contrario; y, normas relativas al momento y lugar de envío y de recepción de un mensaje de datos, en las que regirán el principio de libertad contractual. Es así que podemos concluir que la etapa de formación y el perfeccionamiento del contrato electrónico se encuentran mucho más regulados.

La Parte II de la Ley referente al comercio electrónico en materia de transporte de mercancías, representa una novedad respecto de la legislación ecuatoriana; esta sección está tomada de la Ley Modelo que contempla el Comercio Electrónico en materias específicas.

En cuanto a las Entidades de Certificación, la legislación colombiana permite que estas actividades puedan también ser desarrolladas por las cámaras de comercio. Contiene un artículo adicional en este tema relacionado con la remuneración por los servicios de las entidades de certificación, la cual podrá ser establecida libremente por ella.

La autoridad competente para la autorización y control de las entidades de certificación es la Superintendencia de Industria y Comercio. Las sanciones que se pueden aplicar ante infracciones administrativas, son similares a las establecidas en ley ecuatoriana, sin embargo, no existe desarrollo sobre cuáles serían tales infracciones.

PERÚ

La normativa vigente en la República de Perú, relacionada con el comercio electrónico, es la siguiente:

- ✓ Ley n. 27269 de Firmas y Certificados Digitales
- ✓ Ley n. 27309 que incorpora los Delitos Informáticos al Código Penal
- ✓ Ley n. 27291 que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica.

La Ley de Firmas y Certificados Digitales está compuesta por 15 artículos que giran alrededor de la validez y eficacia jurídica de la firma electrónica utilizada en mensajes de datos que vinculan al firmante con dicho mensaje.

En general, se refiere a la definición de firma digital, su titularidad y obligaciones del titular.

En cuanto a los certificados digitales, establece su definición, contenido, principio de confidencialidad, normas para la cancelación y revocación de los certificados.

Finalmente, regula escuetamente a las entidades de certificaciones definiendo su significado, sus funciones, la obligación de llevar un registro de los certificados que emita y sobre su inscripción en el Registro de Entidades de Certificación.

La Ley 27309 que incorpora los delitos informáticos se refiere únicamente a:

- ✓ Ingreso o utilización indebida de bases de datos añadiendo dos variante: si tal conducta tuvo por finalidad un beneficio económico; y, si tal conducta fue realizada haciendo uso de información privilegiada obtenida en función de su cargo o si con ello pone en peligro la seguridad nacional.
- ✓ Utilización, ingreso o interferencia en bases de datos con el fin de alterarlos, dañarlos o destruirlos, agravándose la sanción si la conducta fue cometida haciendo uso de información privilegiada obtenida en función de su cargo o si con ello se pone en peligro la seguridad nacional.

Lo más novedoso y destacable en la legislación peruana es la reforma al Código Civil que realizan mediante la Ley 27291. El artículo 1 de la citada ley modifica los artículos del Código Civil que se refieren a la Manifestación de Voluntad, Conocimiento y contratación entre ausentes y Formalidad para la manifestación de voluntad, incorporando los "medios electrónicos" como forma de expresión de voluntad y de contratación en sí mismo.

BOLIVIA

Actualmente Bolivia aprobó en 2011 la Ley n. 164 denominada Ley General de Telecomunicaciones, Tecnologías de información y Comunicaciones.

Este cuerpo normativo está formado por ocho Títulos, con un total de 113 artículos. La estructura de esta ley es la siguiente:

- Título I: Disposiciones generales.
- Título II: Competencias y atribuciones del nivel central del Estado y las entidades territoriales autónomas.
- Título III: Telecomunicaciones.

- Título IV: Desarrollo de contenidos y aplicaciones de tecnologías de información y comunicación**.**
- Título V: Infracciones y sanciones.
- Título VI: Servicio Postal.
- Título VII: Participación y control social en telecomunicaciones, tecnologías de información y comunicación y servicio postal.
- Título VIII: Otras disposiciones.

Podemos apreciar que esta ley regula diversos aspectos de las telecomunicaciones, siendo los Capítulos III y IV del Título IV, aquellos que se refieren a los mensajes de datos, firmas electrónicas y al comercio electrónico. Por ello podemos también concluir que no se tomó como base la Ley Modelo de Naciones Unidas.

El capítulo III De los documentos y firmas digitales, comienza otorgando validez jurídica a: 1. Los actos o negocios jurídicos realizados por personas naturales o jurídicas en documentos digitales aprobados a través de firma digital y celebrados por medios electrónicos u otros de mayor avance tecnológico; 2. Los mensajes electrónicos de datos; y, 3. La firma digital.

En esta norma podemos observar principalmente dos cosas: la validez jurídica del mensaje de datos, base de toda la legislación sobre comercio electrónico, y un reconocimiento indirecto al principio de neutralidad tecnológica.

Se exceptúan de manera expresa, tres actos que no podrán ser realizados por medios electrónicos:

1. Los actos propios del derecho de familia;
2. Los actos en que la Ley requiera la presencia física de las partes; y,
3. Los actos en que la Ley o el acuerdo de las partes requieran de documentos físicos para su validez.

Se establece a la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes como la autoridad encargada de autorizar, regular y supervisar a las entidades certificadoras.

El artículo 80 de la Ley otorga validez y eficacia jurídica a los certificados emitidos por autoridades de certificación extranjeras, siempre que tales certificados sean avalados por autoridades certificadores nacionales.

Por su parte, el artículo 82 establece quiénes pueden ser acreditados como entidades de certificadores, reconociendo para ello a cualquier persona natural o jurídica siempre que cumpla con los requisitos establecidos en la Ley.

El capítulo IV del Comercio Electrónico establece que la oferta de bienes y servicios por medios digitales, que cumplan con las condiciones generales y específicas que la Ley impone, debe ser realizada en un ambiente técnicamente confiable y en las condiciones señaladas en el Código de Comercio.

El artículo 86 otorga validez a los contratos electrónicos y plantea algunos criterios para la valoración de los documentos digitales, estos son:

1. Los documentos digitales carentes de firma digital, serán admisibles como principio de prueba o indicios; y,
2. Se tomará en cuanta la confiabilidad de la forma en que se haya generado, archivado y comunicado el documento digital, la forma en que se haya conservado la integridad de la información y la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

El artículo 91 establece que existirán condiciones especiales para las comunicaciones publicitarias realizadas por cualquier medio electrónico, que serán reguladas mediante el Reglamento a esta Ley.

Aspectos comunes de la legislación sobre comercio electrónico en los países andinos

1. Reconocimiento Jurídico. Validez de mensajes de datos y Firmas electrónicas.

Ecuador: Arts. 2 y 14 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Colombia: Arts. 5 y 28 de la Ley 527

Perú: Art 1 de la Ley 27269 de Firmas y certificados digitales

Bolivia: Art. 78 de la Ley General de Telecomunicaciones, Tecnologías de información y Comunicaciones.

3. Equivalente funcional:

Ecuador: Arts. 6 y 7 de la Ley la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos; y, artículos 3 y 4 del reglamento.

Colombia: Artículos 6, 7 y 8 de la Ley 527.

Perú: Art. 1 de la Ley 27269 de Firmas y certificados digitales

Bolivia: No consta

4. Neutralidad Tecnológica

Ecuador: Art. 10 del reglamento

Colombia: No es expreso

Perú: Artículo 4 del Reglamento de la Ley 27269

Bolivia: Artículo 78.1 de la Ley General de Telecomunicaciones, Tecnologías de información y Comunicaciones

5. Autonomía de la voluntad

Ecuador: Disposición General Quinta de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Colombia: Art 4 de la Ley 527.

Perú: Artículo 2 del reglamento de la Ley 27269.

Bolivia: Artículo 88 de la Ley General de Telecomunicaciones, Tecnologías de información y Comunicaciones.

3.3 Normativa expedida por la Comunidad Europea sobre comercio electrónico

La Comunidad Europea es una comunidad política de Derecho constituida en régimen de organización internacional *sui generis*, nacida para propiciar y acoger la integración de los estados de Europa. Su objetivos son[94]:

- Constituir un espacio de libertad, seguridad y justicia sin fronteras interiores.
- Desarrollar un mercado interior en el que la competencia sea libre, en el marco de una economía social de mercado tendente al pleno empleo.
- El desarrollo sostenible, es decir, un crecimiento económico capaz de cubrir las necesidades de bienestar de nuestras sociedades a corto, medio y, sobre todo, largo plazo.
- La promoción del progreso científico y técnico.
- La lucha contra la exclusión social y la discriminación, a favor del fomento de la justicia y la protección social, la igualdad entre mujeres y hombres, la solidaridad entre las generaciones, y la protección de los derechos del niño.

[94] Fuente: http://www.deperu.com/organismos/internacional/organismo.php?org=1787

- El fomento de la cohesión económica, social y territorial y la solidaridad entre los Estados miembros.

La Comunidad Europea considera al desarrollo de la sociedad de la información como el espacio sin fronteras interiores esencial para eliminar las barrearas que dividen a los países europeos convirtiéndose en fuente de oportunidades para las pequeñas y medianas empresas, incrementando la competitividad de la industria europea.

Es por ello, que este organismo se ha preocupado de emitir una serie de Directivas aplicables a los Estados Miembros a fin de que se logren superar los obstáculos jurídicos que se oponen al buen funcionamiento del mercado interior y que hacen menos atractivo el ejercicio del comercio electrónico. Dichos obstáculos han sido identificados y son: la disparidad de legislaciones y la inseguridad jurídica de los regímenes naciones aplicables a los servicios de la sociedad de la información.
La normativa Comunitaria europea sobre comercio electrónico se sintetiza en las siguientes directivas, comunicaciones y recomendaciones:

1. Directiva 97/7/CE relativa a la protección de los consumidores en materia de contratos a distancia

Fue dictada el 20 de Mayo de 1997[95]. El objetivo de esta directiva es salvaguardar a los consumidores en materia de contratos a distancia.

El artículo 2 de la Directiva ofrece una serie de definiciones, entre las que destacan las siguientes:

- ✓ Contrato a distancia: todo contrato entre un proveedor y un consumidor sobre bienes o servicios celebrado en el marco de un sistema de ventas o de prestación de servicios a

[95]Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo de1997, *relativa a la protección de los consumidores en materia de contratos a distancia*. Fuente: http://europa.eu/legislation_summaries/consumers/protection_of_consumers/l32014_es.htm. Acceso: 15-05-2012

distancia organizado por el proveedor que, para dicho contrato, utiliza exclusivamente una o más técnicas de comunicación a distancia hasta la celebración del contrato, incluida la celebración del propio contrato

- ✓ Técnica de comunicación a distancia a "todo medio que permita la celebración del contrato entre un consumidor y un proveedor sin presencia física simultánea del proveedor y del consumidor" y, remite al Anexo I en el cual figura una lista indicativa de las técnicas contempladas en la presente Directiva. En el mencionado anexo, se incluye a los correos electrónicos como técnica de comunicación a distancia válida.

La Directiva procura armonizar las legislaciones nacionales instituyendo un conjunto de normas mínimas que deben ser observadas cuando se celebran contratos de consumo; además, brinda a los consumidores europeos derechos legales que aseguren sus transacciones comerciales dentro de la Unión Europea e incluye los siguientes derechos:

- El consumidor debe recibir información clara y comprensible antes de la conclusión de cualquier contrato a distancia (Art 4).
- La información proporcionada debe confirmarse por escrito o en soporte duradero (correo electrónico) en el momento de la ejecución del contrato (Art. 5)
- El consumidor puede ejercer el derecho de retractación. (Art 6)
- El proveedor dispone de un plazo de treinta días para ejecutar el pedido. En caso de defecto, el consumidor debe ser informado y reembolsado.
- Protección frente a los pagos fraudulentos mediante tarjetas de crédito.
- Protección frente a ventas no solicitadas[96]

Vale destacar la inclusión del derecho de resolución a favor del consumidor, el cual establece el derecho de los consumidores para rescindir el contrato después de siete días laborables, sin necesidad de justificar un motivo.

2. Directiva 1999/93/CE por la que se establece un marco comunitario para la firma electrónica

[96]Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo de1997, *relativa a la protección de los consumidores en materia de contratos a distancia*. Internet: http://europa.eu/legislation_summaries/consumers/protection_of_consumers/l32014_es.htm. Acceso: 15-05-2012

Fue dictada el 13 diciembre de 1999. Su objetivo principal es fomentar la heterogeneidad normativa en materia de reconocimiento legal de la firma electrónica y acreditación de los proveedores de servicios de certificación pues considera que un marco claro sobre las condiciones aplicables aumentará la confianza en las nuevas tecnologías y la aceptación general de las mismas.

Esta Directiva señala que la firma electrónica se utilizará en muy diversas circunstancias y aplicaciones, dando lugar a una gran variedad de nuevos servicios y productos relacionados con ella y que por ello es necesario incrementar la confianza de los usuarios, a quienes se deberá asegurar la debida protección de sus datos y el respeto a su intimidad.

En cuanto al contenido de la Directiva, destacan las normas relativas a los efectos jurídicos que se le atribuyen a la firma electrónica, en cuanto al valor similar al de la firma manuscrita y el ser admisible como prueba en un proceso judicial.

La Directiva también se preocupa en asegurar que los certificados emitidos por terceros países, gocen de reconocimiento jurídico equivalente al que tienen los certificados expedidos por un proveedor de servicios de certificación establecido en la Comunidad.

Finalmente, señala el respeto que debe observarse en relación a la protección de los datos de las personas físicas respetándose siempre las directivas que rigen en tal material.

3. Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior

Esta directiva fue adoptada el 8 de junio de 2000. Tiene como objetivo el desarrollo de los servicios de la sociedad de la información a partir de la unificación de legislaciones, propiciando la creación de un marco jurídico que garantice la libre circulación de los servicios de la sociedad de la información entre Estados miembros.

La Sección tercera de la Directiva se refiere a los contratos por vía electrónica, en donde el artículo 9 establece que los Estados miembros velarán para que sus legislaciones permitan la

celebración de contratos por vía electrónico, para ello garantizarán que el régimen jurídico aplicable al proceso contractual no entorpezca la utilización real de los contratos electrónicos.

Los artículos 16, 17 y 18 de la Directiva incorporan novedades importantes para el comercio electrónico.

En primer lugar, el artículo 16 se refiere a los Códigos de Conducta que la Comunidad Europea considera deben ser fomentados con el fin de contribuir a que se aplique la supervisión necesaria a los prestadores de servicios y que deberían ser elaborados por asociaciones u organizaciones comerciales de profesionales o consumidores.

Por su parte, el artículo 17 plantea la posibilidad de establecer soluciones extrajudiciales a los conflictos que se puedan presentar, y que incluso, podría utilizarse también para ello medios electrónicos.

Finalmente, el artículo 18 propone que "los Estados miembros deben velar por que los recursos judiciales existentes en virtud de la legislación nacional en relación con las actividades de servicios de la sociedad de la información permitan adoptar rápidamente medidas, incluso medidas provisionales destinadas a poner término a cualquier presunta infracción y a evitar que se produzcan nuevos perjuicios contra los intereses afectados".

4. Directiva 2002/58/CE relativa al tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)

Esta Directiva fue aprobada el 12 de julio de 2001 y reemplaza a la Directiva 95/46/CE.

Su objetivo es garantizar el respeto de los derechos fundamentales y observar los principios consagrados en la Carta de los Derechos Fundamentales de la Unión Europea.

A través de esta Directiva, se pretende garantizar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de los datos personales y en especial, su derecho a la intimidad, de forma que los datos personales puedan circular libremente en la Comunidad.

Se considera que debido a las nuevas tecnologías digitales se crean nuevas necesidades en materia de protección de datos personales y de la intimidad de los usuarios. El desarrollo de la sociedad de la información se caracteriza por la introducción de nuevos servicios de comunicaciones electrónicos, por ello es importante brindar confianza a los usuarios, quienes podrán tener la seguridad de que su intimidad no estará en peligro.

Según la Directiva, los proveedores de servicios deben tomar las medidas adecuadas para salvaguardar la seguridad de sus servicios, de ser necesario en conjunción con el suministrador de la red, e informar a los abonados de todo riesgo especial relativo a la seguridad de la red.

Informe 2006/2048 sobre la confianza de los consumidores en el entorno digital[97]

Este es un informe elaborado por el Parlamento Europeo el 21 de julio de 2007, el cual, considerando que es necesario incrementar la confianza de las empresas y los consumidores en el entorno digital, solicita a la Comisión que se proponga una estrategia para mejorar el comercio electrónico que cree un entorno empresarial más atractivo.

Es así como surge el la iniciativa *e-Confidence*, como estrategia que contribuiría a fortalecer la confianza de los consumidores, y que generará avances en los siguientes ámbitos:

- ✓ Creación de un programa de subvenciones para proyectos dirigidos a incrementar la confianza de los consumidores en el entorno digital, incluidas las campas de formación e información.
- ✓ Reforzar los centros de consumidores, así como de otros instrumentos para la protección de los consumidores, para garantizar que se puedan utilizar en el entorno digital.

[97] Fuente: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/pr/657/657543/657543es.pdf

- ✓ Creación de un foro de expertos a escala europea para el intercambio de las mejores prácticas nacionales que presenten estrategias legislativas y no legislativas a largo plazo, para aumentar la confianza de los consumidores en el entorno digital.
- ✓ La coordinación y el apoyo de los códigos auto reguladores europeos.
- ✓ La creación de un sistema europeo de alerta rápida, incluida una base de datos para la lucha contra las actividades fraudulentas en el entorno digital.

CONCLUSIONES

Nos habíamos propuesto al inicio de este trabajo investigativo lograr establecer si en nuestro país, el ordenamiento jurídico en materia comercial electrónica es suficiente para proteger e incentivar a los usuarios de Internet para intervenir en contrataciones electrónicas.

Para satisfacer tal objetivo, empezaré recapitulando los problemas detectados a lo largo de esta investigación, que dificultan la utilización del contrato electrónico, en relación a su característica de ser *a distancia*, organizándolos conforme fueron detectados en los respectivos capítulos.

Abordaremos las conclusiones desde dos situaciones diferentes para el contrato electrónico y que obedecen a la razón de ser de la estructura de esta disertación.

El primer capítulo nos lleva a concluir que las técnicas o medios de comunicación utilizados en contratación electrónica, tanto en su formación como en su perfeccionamiento, conllevan una serie de riesgos que no se presentaban con el uso del teléfono o correo tradicional. Los nuevos medios de comunicación son mucho más vulnerables que los tradicionales, pues ellos se trasmiten por redes abiertas que pueden ser fácilmente interceptados.

De allí que, lo que vuelve riesgoso al contrato electrónico, es su característica de contrato a distancia, en donde no existe la presencia física simultánea de las partes.

Tal circunstancia favorece el clima de incertidumbre en torno a él, por las siguientes razones:

- ✓ Falta de certeza sobre la identidad de los intervinientes.
- ✓ Falta de certeza sobre el lugar en que dicen encontrarse las partes.
- ✓ Falta de seguridad sobre la seriedad de la Propuesta y de las contraofertas o nuevas propuestas recibidas.

- ✓ Falta de seguridad respecto a la confidencialidad y reserva con que será tratada la información obtenida y la consecuente vulneración a la intimidad.

El listado es solo referencial, pero evidencia con claridad las dudas frecuentes de los posibles usuarios del comercio electrónico.

Un tema que también llama la atención, es el desconocimiento que existe respecto de las seguridades o inseguridades técnicas de los medios de comunicación escogidos por los usuarios para sus negociaciones electrónicas, principalmente sobre los correos electrónicos gratuitos, medio de comunicación preferido por los usuarios de Internet.

La respuesta que el ordenamiento jurídico otorga para brindar protección a las comunicaciones electrónicas son los servicios de certificación a cargo de las entidades de certificación en donde los servicios de certificación tienen importancia fundamental, específicamente la firma electrónica y el sellado de tiempo.

Producto de esta investigación, podemos afirmar que el ordenamiento jurídico ecuatoriano está ampliamente desarrollado y acogen los estándares tecnológicos internacionales que se aplican en materia de servicios de certificación. Ejemplo de ellos son los artículos 34 y 37 del Reglamento Para la acreditación, Registro y Regulación de Entidades Habilitadas para prestar Servicios de Certificación de Información y Servicios Relacionados. El artículo 34 establece que el servicio de sellado de tiempo debe asegurar que sea imposible sellar un documento con un tiempo y fecha diferente de la actual y que para ello deberá tomar como tiempo de referencia el UTC que significa Universal Time Coordinated. Por su parte, el artículo 37 señala que los organismos de regulación y control realizarán sus controles tomando como referencia la recomendación X.509 de la UIT-T, las recomendaciones del Instituto Europeo de Estándares de Telecomunicaciones ETSI y del Comité Europeo de Normalización CEN.

Es decir que, la firma electrónica avanzada no solo es el mecanismo tecnológico suficiente para conferir seguridad a las contrataciones electrónicas, sino que también está reconocida y protegida por la normativa nacional. Con ello la incertidumbre respecto a la identidad de las

partes, el lugar y momento de celebración del contrato, la confidencialidad sobre su contenido, entre otras, estarían garantizado desde el aspecto tecnológico y jurídico.

Un tema importante de mencionar es la crítica que algunos sectores hacen a la firma electrónica, cuya materialización se realiza a través de un *token* o dispositivo electrónico. Estos grupos señalan que nada asegura que la firma electrónica sea utilizada exclusivamente por quien aparezca como su titular, lo que dejaría a la firma electrónica rodeada de incertidumbre. Para aclarar esta crítica, creemos necesario plasmar un ejemplo práctico y asimilar la firma electrónica con la tarjeta de crédito. Hoy por hoy, después de décadas de usar habitualmente la tarjeta de crédito, ningún tarjetahabiente tiene dudas sobre los beneficios de su uso, sobre sus riesgos y principalmente sobre la responsabilidad que tiene, como titular, de dar un uso responsable al crédito que a través de ella obtiene, así como su responsabilidad de custodia, conservación y privacidad de las claves vinculadas a ella. Y, salvo excepciones particulares, nadie pone en duda que quien usa una tarjeta de crédito es su titular.

Sin embargo de todo lo anteriormente expuesto, no podemos dejar de mencionar que existe desconocimiento en el mercado sobre las bondades de los servicios de certificación, que los siguen considerando como medios inseguros o como un costo innecesario que cargar a sus negocios; actitud que, repetimos, se debe al desconocimiento, más no a una insuficiencia normativa o tecnológica.

En segundo lugar, en relación a la resolución de los contratos electrónicos, señalamos en la parte pertinente que la declaración en mora y del incumplimiento del contrato, debe ser realizada por el juez, aplicando las reglas generales de la contratación, ante la falta de normativa especial.

Similar situación se presenta en cuanto a los procedimientos para hacer exigible la responsabilidad civil, contractual o extracontractual.

En términos generales, los mecanismos existen, la legislación civil y comercial nos provee de ellos. Pero el comercio electrónico exige mecanismos novedosos que estén a la par de los

beneficios que incorpora la sociedad de la información y que contemplen los nuevos riesgos ante las conductas dañinas que se pueden realizar por medios electrónicos. Al no existir legislación especial, los afectados deberán recurrir a la justicia ordinaria comercial, la cual contempla procedimientos lentos y poco efectivos, que restan sobremanera la efectividad que supone el comercio electrónico.

La insuficiente legislación al momento de exigir responsabilidades en materia comercial electrónica puede ser una de las razones por las cuales el crecimiento del comercio electrónico en nuestro país es lento, pero aún con todas estas dificultades. existe. En el e-Commerce Day celebrado en Guayaquil el último 04 de julio, el presidente del Instituto Latinoamericano de Comercio Electrónico así como el presidente de la Cámara de Comercio de Guayaquil hablaron de un crecimiento sostenido de las transacciones que se realizan con tarjeta de crédito a través de Internet, según cifras dadas por ellos, alrededor de 600 millones de dólares. Según datos del INEC, el 88% de estas transacciones son para adquirir bienes de consumo[98].

Hasta aquí, hemos planteado algunos de los problemas que significarían en la práctica, en relación a los beneficios del comercio electrónico, realizar el requerimiento de declaratoria de mora, demandar el incumplimiento o la resolución, reclamar indemnizaciones por daños y perjuicios, por los métodos tradicionales. En materia civil, podría sugerirse que los métodos alternativos de solución de conflictos aparecen como una opción siempre que la Ley de Mediación y Arbitraje reconozca medios electrónicos a ser aplicados, específicamente, ante el caso de conflictos derivados de contratos electrónicos.

Recordemos que la razón de ser del comercio electrónico, y con ello de la existencia del contrato electrónico, es la participación en una nueva era global y tecnológica, en donde lo intangible se convierte en el nuevo motor de la economía y de la sociedad. Por tanto, los mecanismos que se consideren para solucionar este tipo de situaciones deben ser pensados inseparablemente de la finalidad del contrato electrónico, de manera que, al momento de

[98] Fuente: www.eluniverso.com/noticias y www.elcomercio.com/negocios/Comercio-electronico, ediciones digitales del 05 de julio de 2013.

presentarse la situación no ideal del incumplimiento del contrato o de un daño informático de naturaleza extracontractual, existan mecanismos idóneos que puedan brindar tutela y con ello seguridad jurídica a las partes.

En lo que respecta a los delitos informáticos, pudimos verificar la existencia de una serie de tipos penales agregados al Código Penal por la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. A pesar de que estas incorporaciones, todavía es posible mejorar y normas como la que sanciona la violación al derecho a la intimidad por medios electrónicos, como una contravención de tercera clase, cuya sanción es de USD 7.00 a USD 14.00 y prisión de dos a cuatro días, resultan totalmente fuera de contexto al lado de la gravedad de la conducta.

En este sentido, hubiera sido importante la aprobación de la Ley de Protección a la Intimidad y a los Datos Personales. Sin embargo, dicho proyecto de ley fue archivado por resolución de la Comisión de Justicia y Estructura del Estado el 07 de mayo de 2012[99].

Volviendo al análisis de la responsabilidad penal en materia de contratación electrónica, la dificultad, en este caso, aparece al momento de intentar demostrar la existencia del delito, y luego, poder establecer la autoría.

[99] En el informe para segundo debate la comisión señala que: 1) El proyecto no tiene condición ni el alcance jerárquico de Ley Orgánica, y que tal inexactitud cualitativa evidencia su deficiencia; 2) Presentaba errores en la determinación de los medios legales potenciales en el proyecto de ley; 3) Creaba innecesariamente un organismo administrativo-burocrático; 4) Presentaba error en la determinación de la norma legal como instrumento para alcanzar un objetivo, siendo repetitivo en la acción de habeas data; 5) Finalmente, que el proyecto expandía y repetía acciones judiciales constitucionales y ordinarias que ya existen y que por lo demás son suficientes para regular y proteger el derecho a la intimidad y a los datos personales. Fuente. www.asambleanacional.gob.ec

La razón de esta dificultad se desprende de la naturaleza del contrato electrónico. Dada su falta de corporalidad física y la intervención de medios de comunicación electrónicos, el cometimiento de conductas delictivas alcanza altos índices de impunidad pues la prueba de la existencia del delito puede resultar imposible, por ejemplo, ante el acceso no autorizado a sistemas de información, cuya finalidad haya sido únicamente el vulnerar los accesos o cuando los sistemas sean copiados pero no destruidos. El titular de los sistemas de información podría jamás enterarse de que fue víctima de un delito. Peor todavía podría resultar perseguir la conducta ilícita.

En cuanto al establecimiento de responsables, surge el problema de cómo lograr identificar al sujeto activo de un delito informático, si muchos de ellos, al ser profesionales en redes, no dejan rastro.

Sobre este tema, existen muchos ejemplos en la justicia penal ecuatoriana y me referiré brevemente a un caso concreto, con la finalidad de evidenciar lo que ocurre con el juzgamiento de los delitos informáticos.

La compañía A, tiene por objeto social la elaboración de bases de datos de personas a quienes enviarles, vía correo electrónico, información de servicios de sus clientes. Esta compañía contaba entre su personal con el empleado X y Y. Ambos renunciaron a la compañía en el año 2010. X formó otra compañía con similar objeto social y con el tiempo Y entró a trabajar en dicha compañía. Durante estos años, Y mantuvo el acceso a una cuenta de correo electrónico, que para fines laborales, le fue asignada mientras prestaba sus servicios a la compañía A. Esta situación era ignorada por los propietarios y representantes legales de la compañía, quienes se enteran de manera casual que la cuenta de correo electrónico mencionada continuaba siendo utilizada y no solo eso, sino que también a través de dicha cuenta, se enviaba información confidencial que había sido recabada por la compañía A en el ejercicio de su objeto social. Al enterarse de ello presentan denuncia ante la Fiscalía, institución que concluyó que existían indicios de la comisión del delito. El juez de garantías penales inicia juicio penal por delito contra la información protegida, tipificado en el artículo 202.1 del Código Penal y dicta auto de llamamiento a juicio. El Tribunal Penal resuelve en sentencia que “no se ha logrado probar

la existencia jurídica del delito tipificado en el artículo 202.1 del Código Penal, por lo que resulta inoficioso entrar a considerar el grado de responsabilidad de los acusados". En apelación se confirmó la decisión de primera instancia. La compañía presentó recurso de casación que actualmente está en trámite.

En este ejemplo, podemos apreciar que establecer responsabilidades penales por delitos informáticos puede resultar muy difícil.

Por último, al analizar la ley ecuatoriana y la de países de la región andina, dictada en la materia, pudimos evidenciar las similitudes existentes, pues es notorio el acatamiento a la Ley Modelo expedida por la Comisión de las Naciones Unidas, siendo la excepción Bolivia, cuya ley es la más reciente, y aparentemente se aleja de las demás, probablemente obedeciendo a la política hostil que mantiene ese país respecto de los organismos internacionales con sede en Estados Unidos.

Es positiva esta armonización de normas, sin embargo, falta continuar trabajando en ella. Las mismas deficiencias de la ley ecuatoriana, referidas a la exigibilidad judicial se observaron en las legislaciones de los otros países de la región andina.

Al estudiar la legislación comunitaria europea, lo que más ha llamado nuestra atención es el Informe sobre Confianza de los Consumidores en el Entorno Digital. En este documento se realiza un auto examen sobre las razones por las cuales Europa permanece por detrás de Estados Unidos y Asia en cuanto a la utilización del comercio electrónico. Esto nos ha llevado a la deducción, que incentivar la confianza de los usuarios en el comercio electrónico es una actividad permanente por parte de los sectores interesados que requiere un compromiso y trabajo activo continúo. En Europa, que nos lleva 20 años de ventaja en esta materia, se organizan sesiones de trabajo a nivel de Parlamento Europeo para revisar sus debilidades. Tal vez la diferencia entre ellos y nosotros, es que la Comunidad Europea se ha percatado de la importancia fundamental para su economía de fortalecer los mecanismos que aceleren el comercio a todo nivel y hagan crecer su producción.

Para concluir, en respuesta al objetivo propuesto inicialmente, podemos decir con seguridad que la legislación ecuatoriana vigente en materia de comercio electrónico, protege parcialmente a los usuarios de Internet que quisieran intervenir en contratación electrónica. Pero, es importante asumir que las soluciones no van únicamente por el camino de más reformas o mayor desarrollo normativo. Se requiere también de políticas públicas que impulsen y fomenten el uso de medios electrónicos, así como una mayor participación de la sociedad civil, por ejemplo a través de las asociaciones de comerciantes o cámaras de comercio.

RECOMENDACIONES

Parte de los objetivos propuestos en esta investigación, fueron sugerir posibles soluciones, jurídicas y fácticas, a los problemas identificados, que sean aplicables a la realidad de nuestro país.

Es así que me permito realizar las siguientes recomendaciones, que pudieran ser aplicadas a fin de disminuir la desconfianza e incentivar y fomentar la participación en contrataciones electrónicas:

En el Capítulo I, se planteó la opción de implementar trámites sumarísimos en judicaturas especializadas, que permitan resolver situaciones derivadas de contratos electrónicos por medios diferentes a los establecidos por el procedimiento ordinario, para así devolver efectividad práctica al contrato electrónico, y temas como la resolución del contrato electrónico o la reparación a través de la acción de daños y perjuicios sea resuelta de manera inmediata.

Sin embargo, cualquier tipo de reforma legal, necesitaría de la voluntad política y de mayorías coyunturales en el seno de la Asamblea Nacional.

Es por ello que considero más adecuado plantear una alternativa que pueda nacer de los mismos intervinientes de la contratación electrónica, amparándose en los principios de Libertad Contractual y de Equidad. Me refiero a mecanismos de auto regulación, que podrían ser coordinados por las cámaras de comercio, por ejemplo.

La auto regulación, plasmada en códigos de conducta de adhesión voluntaria, tiene como finalidad mitigar la desconfianza de los potenciales participantes en contrataciones electrónicas. DAVID LÓPEZ JIMÉNEZ señala que “las ventajas del sistema de autorregulación en materia de comercio electrónico, entre otras, son: voluntariedad, lo que facilita considerablemente su aplicación práctica y su cumplimiento sin necesidad de

intervención e imposición de los poderes públicos; especialización; flexibilidad; favorecer el desarrollo de estándares que garantizan elevados niveles de corrección; prevención de infracciones en el ámbito reglamentado; bajo coste en diferentes ámbitos, a título de ejemplo, es en los procedimientos por infracciones; el hecho de cubrir eventuales lagunas de carácter general; y fácil acceso"[100].

Al momento de elaborar este tipo de códigos deontológicos, debe considerarse como referencia fundamental, la legislación vigente.

Sobre el contenido de un código de conducta, este tendría que ser muy amplio: podría referirse a las entidades de certificación y sus responsabilidades; normar las políticas sobre reserva y confidencialidad de la información, principalmente la protección de datos personales; instituir como obligación el que se incluya la mayor cantidad de información tendiente a la identificación y ubicación de los participantes; sobre la creación de normas que disminuyan la desigualdad que suele aparecer en los contratos de adhesión; la regulación de la responsabilidad precontractual; pero sobretodo, es importante abordar aspectos sobre resolución de conflictos, de modo que temas como los antes mencionados, relacionados con la resolución del contrato o el establecimiento de responsabilidades, alcancen soluciones de manera ágil.

Adicionalmente, existen otras medidas que también impactarían en la comunidad, y, que serían acogidas favorablemente, como por ejemplo, los sellos de confianza.

Los sellos de confianza pueden ser concedidos por las mismas entidades de certificación o creados a través de un código de conducta. Para poseerlos, los usuarios que pretenden comerciar electrónicamente deben demostrar el cumplimiento de parámetros de seguridad y someterse a la vigilancia de quien otorgó el sello, respecto al cumplimiento de dichos lineamientos. Este sistema brinda confiabilidad a los usuarios, quienes incluso podrían dirigirse directamente a quien otorgó el sello de confianza para solicitar referencias.

[100] David López Jiménez, El sistema de autodisciplina europea en materia de comercio electrónico: el código de conducta Euro-Label. Internet: http://revistas.upcomillas.es/index.php/revistaicade/article/view/260

La auto regulación, en materia de comercio electrónico, es una práctica puesta en ejecución en otros países, en forma significativa, sin embargo, como habíamos mencionado en las conclusiones de este trabajo, el aumento de la confianza en el contrato electrónico no obedecerá a una solución. Es un trabajo conjunto que exige coordinación del poder ejecutivo, legislativo y de la sociedad civil en general.

BIBLIOGRAFÍA

Libros:

Botana García, Alejandra, coordinadora, Comercio electrónico y protección a los Consumidores, Madrid, Editorial La Ley, 2001.

Burgos Puyo, Andrea, El Consumidor y los Contratos en Internet, Bogotá, Universidad Externado de Colombia, 2000, p. 61.

Cabanellas, Guillermo, Diccionario Enciclopédico de Derecho Usual, Buenos Aires, Editorial Heliasta, 1997, 25ª edición.

De Roselló Moreno, Rocío, El comercio electrónico y la protección a los consumidores, Barcelona, Editorial CEDECS, 2001.

Gaete González, Eugenio Alberto, Instrumento público electrónico, Barcelona, Editorial Bosch, Tercera Edición, 2009.

Gran Enciclopedia Larousse, Tomo 6, Barcelona, Editorial Planeta, 1987.

Hocsman, Simón Heriberto, Negocios en Internet, Buenos Aires, Editorial Astrea, 2005.

López Ortega, Juan José, director, Internet y Derecho Penal, Madrid, editado por Consejo General del Poder Judicial, 2001.

Ortega Díaz, Juan Francisco, Contratación, Notarios y Firma Electrónica, Bogotá, Editorial Temis, 2010.

Ospina Fernández, Guillermo, Ospina Acosta, Eduardo, Teoría General del Contrato y del Negocio Jurídico, Bogotá, Editorial Temis, 2005, Séptima edición.

Páez Rivadeneira, Juan José, Acurio, Santiago, Derecho y nuevas tecnologías, Ecuador, Corporación de Estudios y Publicaciones, 2010.

Riquert, Marcelo Alfredo, Protección Penal de la Intimidad en el espacio virtual, Buenos Aires, Editorial Ediar, 2003.

Sarra, Andrea Viviana, Comercio electrónico y derecho, Buenos Aires, Editorial Astrea, 2001.

Valencia Zea, Arturo, Ortiz Monsalve, Álvaro, Derecho Civil: de las Obligaciones, Bogotá, Editorial Temis, Décima Edición, 2010.

Vidal Marín, Tomás, El derecho al honor y su protección desde la Constitución Española, Madrid, Editado por Imprenta Nacional del Boletín Oficial del Estado, 2000.

Vizueta Ronquillo, Juan, Delitos informáticos en el Ecuador, Guayaquil, Editorial Edino, 2011.

Revistas:

Hernández Fernández, Lisette, "La Oferta y la Aceptación: Especial referencia a los contratos celebrados por medios electrónicos", Alfa-Redi: Revista de Derecho Informático, n. 76, noviembre 2004.

Internet:

Leiva, Claudio Fabricio, Responsabilidad por daños derivados de Internet, VIII Congreso Internacional de Derecho de Daños, Buenos Aires, 2005:. Internet: http://www.aaba.org.ar/bi22n004.htm

www.conatel.gob.ec

http://www.derechoecuador.com/articulos/detalle/archive/doctrinas/derechoinformatico/2005/11/24/se-aprobo-la-ley-de-comercio-electronico

www.parlatino.org/es/comisiones-permanentes/servicios-públicos

www.comunidadandina.org

http://www.itu.int/ITU-D/cyb/publications/archive/Legislacion%20Comercio%20Electronico%20CAN1.pdf

http://programa.gobiernoenlinea.gov.co

http://www.deperu.com/organismos/internacional/organismo.php?org=1787

http://www.europarl.europa.eu/meetdocs/2004_2009/documents/pr/657/657543/657543es.pdf

http://www.anf.es/es/productos/generales/timestamping.html

http://www.alegsa.com.ar/Dic/sitio%20web.php

http://eur-lex.europa.eu

www.eluniverso.com/noticias. Edición digital del 05 de julio de 2013.

www.elcomercio.com/negocios/Comercio-electronico. Edición digital del 05 de julio de 2013.

www.asambleanacional.gob.ec

Normativa:

Código Civil

Código de Comercio

Constitución de la República

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

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

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

Ley No. 527 que reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales en Colombia.

Ley n. 27269 de Firmas y Certificados Digitales de Perú.

Ley n. 27309 que incorpora los Delitos Informáticos al Código Penal de Perú.

Ley n. 27291 que modifica el Código Civil permitiendo la utilización de los medios electrónicos para la comunicación de la manifestación de voluntad y la utilización de la firma electrónica de Perú.

Ley General de Telecomunicaciones, Tecnologías de información y Comunicaciones de Bolivia.

Directiva 97/7/CE del Parlamento Europeo y del Consejo, de 20 de mayo de1997, *relativa a la protección de los consumidores en materia de contratos a distancia*.

Directiva 1999/93/CE por la que se establece un marco comunitario para la firma electrónica.

Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

Directiva 2002/58/CE relativa al tratamiento de los datos personales y la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

Informe 2006/2048 sobre la confianza de los consumidores en el entorno digital.