UNIVERSIDAD DE CUENCA

FACULTAD DE JURISPRUDENCIA, CIENCIAS POLÍTICAS Y SOCIALES

CARRERA DE DERECHO

"LOS DOCUMENTOS ELECTRÓNICOS EN LA LEGISLACÍON ECUATORIANA"

Monografía previa a la obtención del Título de Abogada de los Tribunales de la República y Licenciada en Ciencias Políticas y Sociales

AUTORA:

Olga Priscila León Guevara

C.I. 0104508155

DIRECTOR:

Dr. Edy Daniel Calle Córdova

C.I. 0300776861

Cuenca – Ecuador

2017

RESUMEN

En la actualidad, las nuevas tecnologías de información y comunicación han ido evolucionando rápida y continuamente, de tal manera que han logrado que las personas puedan relacionarse entre sí de una manera más eficaz y eficiente, incidiendo progresivamente en la vida cotidiana de cada uno. A su vez, siendo el derecho una ciencia social dinámica, también se ha ido desarrollando en este ámbito de la tecnología, a tal punto que ha permitido que se puedan celebrar negocios jurídicos de formas diferentes a la convencional, como por ejemplo cuando las partes no se encuentran físicamente juntas, es posible utilizar medios como la videoconferencia o correos electrónicos, entre otros.

Por tal motivo, el presente estudio pretende ser un aporte importante para analizar la problemática de los documentos electrónicos, su equivalencia con el documento tradicional y la forma en la que puede constituirse como documento público. Por lo tanto, será necesario empezar este estudio desde la generalidad de los documentos tradicionales e irnos introduciendo específicamente hasta este tipo de documentos, estableciendo su valor jurídico, así como también sus consecuencias jurídicas.

Finalmente, la temática propuesta tendrá un gran aporte dentro del ámbito social, ya que permitirá que las personas tengan pleno conocimiento y seguridad jurídica al momento de realizar actos y contratos de esta naturaleza.

Palabras Clave: comercio electrónico, firma electrónica, mensajes de datos, documentos electrónicos, valor probatorio, instrumentos electrónicos públicos.

ABSTRACT

In present days, the new technologies of information and communication have evolved fast and continually, in such a way that is possible now that people can stay in touch among themselves in a better way and more efficient making a big impact in every day´s life of everyone. At the same time, with a social dynamic, also it has been developing in this field of technology, at such point that is possible now to take care of legal business in different ways compared to before, for example, when everybody involved in a legal matter, is not present in person, it is possible to use video conference or e-mails, among others.

For this reason, the recent study pretends to be an important contribution to analyze the problematic to the electronic documents, its equivalence with the traditional document and the way that it can become as a public document. Thus it is necessary to begin this study from the generality of the traditional documents and start introducing specifically this type of documents, setting its legal value, as legal consequence as well.

Finally, the theme proposal will have a big input within the social scope, since it would allow that people have full knowledge and legal security at the moment to do acts and contracts of this nature.

Key words: electronic commerce, electronica signature, texts of data, electronic documents, value probative, public instrument electronics

ÍNDICE

UNIVERSIDAD DE CUENCA
FACULTAD DE JURISPRUDENCIA, CIENCIAS
POLÍTICAS Y SOCIALES

CLÁUSULA DE DERECHOS DE AUTOR

Yo, Olga Priscila León Guevara, autora de la monografía "Los Documentos Electrónicos en la legislación Ecuatoriana", reconozco y acepto el derecho de la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Abogada de los Tribunales de Justicia de la República, y, Licenciada en Ciencias Políticas y Sociales. El uso que la Universidad de Cuenca hiciere de este trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor.

Cuenca, Enero de 2017

Olga Priscila León Guevara

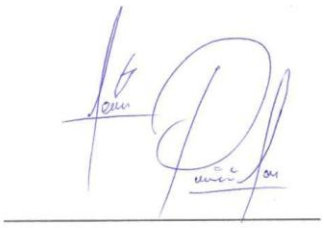
C. I.: 0104508155

UNIVERSIDAD DE CUENCA
FACULTAD DE JURISPRUDENCIA, CIENCIAS
POLÍTICAS Y SOCIALES

CLÁUSULA DE PROPIEDAD INTELECTUAL

Yo, Olga Priscila León Guevara, autora de la monografía "Los Documentos Electrónicos en la legislación Ecuatoriana", certifico que todas las ideas, opiniones y contenidos expuestos en la presente investigación son de exclusiva responsabilidad de su autor.

Cuenca, Enero de 2017



Olga Priscila León Guevara

C. I.: 0104508155

DEDICATORIA

A mis padres Carlos y Olga, quienes nunca me permitieron que me rinda a pesar de que muchas veces las circunstancias no fueron óptimas, siendo siempre mi mayor ejemplo de sacrificio y trabajo, gracias por el amor incondicional y por sus palabras de apoyo.

A mis hermanos, Juan Carlos, Miguel Angel y Bernarda, quienes con sus experiencias siempre me han impulsado a ser mejor cada día, dándome las pautas necesarias para poder siempre elegir el camino más conveniente .

A mis pequeños sobrinos, Mariangel y Mateo, que con sus locuras y juegos, han alegrado mi vida.

Simplemente, a ustedes les debo lo que soy, sin su apoyo, cariño y sobretodo su confianza, no hubiera sido posible terminar con esto que empezó como un sueño…

Mis esfuerzos y dedicación son para ustedes.

AGRADECIMIENTO

En primer lugar, gracias te doy amado Dios por permitirme terminar con éxito esta etapa de mi vida, para TÍ sea la honra y la gloria por siempre.

A la Universidad de Cuenca, en especial a la Facultad de Jurisprudencia y Ciencias Políticas y Sociales, que me ha formado académicamente permitiendo que pueda confrontarme a una sociedad de profesionales.

Expreso también mi agradecimiento a mi director Doctor Edy Calle Córdova, quien me ha brindado su conocimiento y amistad, gracias por su orientación y confianza que he recibido a lo largo del desarrollo de esta monografía.

A quién me enseñó que no existe edad ni tiempo para empezar a crecer y ser mejor que ayer, que con su tolerancia, paciencia y palabras de cariño me ha estado apoyando.

A mis amigos y compañeros, gracias por caminar conmigo...

A ustedes, mi infinita gratitud.

INTRODUCCIÓN

El estudio de la presente investigación implica la realidad jurídica y tecnológica actual, la cual radica en el desarrollo que ha tenido nuestra sociedad en los últimos años, pues por esta razón el legislador ha visto la necesidad de incluir a los documentos electrónicos dentro de nuestra legislación. A pesar de que el ordenamiento jurídico ecuatoriano no los ha definido como tal, el Artículo 202 del Código Orgánico General de Procesos al expresar que "Los documentos producidos electrónicamente con sus respectivos anexos, serán considerados originales para todos los efectos legales..." los ha reconocido, y no solo eso, sino son considerados como documentos originales, y legalmente válidos para cualquier situación e incluso pueden ser admitidos como medio probatorio, pues así nos manda el artículo mencionado en su inciso final "…podrá admitirse como medio de prueba todo contenido digital conforme con las normas de este Código." Al ser reconocidos de tal manera, es de gran trascendencia estudiarlos.

A su vez el Artículo 7de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en su tercer y cuarto inciso manifiesta lo siguiente: "…Por acuerdo de las partes y cumpliendo con todas las obligaciones previstas en esta Ley, se podrán desmaterializar los documentos que por ley deban ser

instrumentados físicamente…" y en el siguiente inciso "Los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la presente ley, y deberán ser conservados conforme a lo establecido en el artículo siguiente.". Como se puede observar, esta Ley especial hace referencia al término desmaterializar, pero ¿a qué se refiere la Ley cuando nos habla de ello?, ¿quién puede realizar la desmaterialización?

Por todo lo expuesto, es posible llegar a tener una idea de lo que se va a exponer en la presente investigación, teniendo en cuenta básicamente que un documento electrónico es aquella expresión, cualquiera que sea, la cual está contenida y almacenada en un soporte informático, mismo que nuestra legislación lo admite como medio de prueba e incluso por acuerdo de las partes y bajo el procedimiento de la Ley, pueden ser desmaterializados, entendiendo a éste como un proceso en el que un documento digital o electrónico es transformado en un documento físico y para ello las partes deben acudir ante Notario Público o autoridad competente para que certifique electrónicamente que el documento desmaterializado corresponde al documento original. Esta certificación electrónica se la realiza a través de la respectiva firma electrónica

del Notario Público o autoridad competente, siguiendo las disposiciones y reglamentos especiales pertinentes al tema.

Cabe entonces preguntarnos: ¿es en verdad una ventaja acudir a los medios electrónicos para el almacenamiento de documentos?, ¿Realmente son eficaces y admisibles como prueba en las obligaciones los documentos electrónicos?, ¿Pueden los documentos electrónicos constituir instrumento público?, ¿cuál es el procedimiento para desmaterializar un documento electrónico? estas y otras interrogantes tratarán de ser respondidas en el transcurso de esta investigación.

CAPITULO I

Herramientas jurídicas que permiten el uso de los servicios electrónicos.

1. Comercio Electrónico

1.1 Concepto

El comercio electrónico, también conocido como e-commerce (electronic commerce en inglés), ha sido definido por la Organización Mundial del Comercio (OMC) manifestando de una manera bastante simple que es la producción, publicidad, venta y distribución de productos y servicios a través de las redes de telecomunicaciones.

A su vez, de una manera más técnica, el Comercio Electrónico, consiste en todas las transacciones comerciales ejecutadas o basadas en sistemas electrónicos de procesamiento y transmisión de información a través de redes cerradas y abiertas como son la EDI (Electronic Data Interchange)[1] e Internet, respectivamente. Dichas transacciones comerciales electrónicas se refieren a la compraventa de bienes o prestación de servicios, las actividades previas de negociaciones como publicidad o búsqueda de información, atención al cliente,

[1] Es un formato estandarizado, utilizado para el intercambio electrónico de datos, facilitando el envío y la recepción de documentos comerciales como facturas y órdenes de compra. Este método ayuda a reducir errores y agilizar el proceso de comunicación, así también se puede intercambiar información comercial de manera electrónica con distribuidores, proveedores, operadores logísticos, aduanas, entre otros.

etc.; y otras relacionadas con las antes nombradas. También comprende los pagos electrónicos y aquellas actividades desarrolladas a través de los mecanismos suministrados por las nuevas tecnologías de comunicación (Martinez, 2001).

La Ley de Comercio electrónico, firmas electrónicas y mensajes de datos también la define como “toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información”.

De esta forma, podemos considerar que el comercio electrónico es una metodología moderna que consiste principalmente en intercambiar información comercial, que en primer lugar, radica en la generación de un servicio por parte de una organización, que se presta a un tercero a cambio de una contraprestación (Comercio) y que se distribuye mediante un soporte informático (Electrónico). Por lo tanto, lo que le va a diferenciar del comercio tradicional es la utilización del formato electrónico para la prestación del servicio.

Por lo manifestado, este método trata de dar respuestas a las necesidades tanto de empresas como de consumidores, mejorando la calidad de productos y servicios, acortando el tiempo de entrega y mejorando la comunicación con el

consumidor, en la que abarca transacciones comerciales transmitidas electrónicamente usando redes telemáticas.

A su vez, profesores de Sistemas de Información como el Doctor Enrique Dans, explican que la mensajería electrónica o e-mail, ha sido el primer incentivo para que Internet se convirtiese en una herramienta habitual en la vida de mucha gente, y que el comercio electrónico podría ser ese segundo gran empujón que la red necesita para que su uso se convierta de verdad en algo general y cotidiano. (Dans, 2013).

1.2 Modalidades del Comercio Electrónico

En virtud que el mercado tiene diversas necesidades, las técnicas empleadas en el ecommerce “se han adaptado para satisfacer a cada una de las partes involucradas, teniendo diferentes modalidades” (Garcia, 2001), siendo éstas las siguientes:

1) De acuerdo a los agentes intervinientes en el intercambio, en donde se distinguen las siguientes relaciones:

a) Entre empresas **Business to Business conocido como *E-a-E o B2B***: es la abreviación de business to business (negocio a negocio), en ésta no intervienen consumidores y se da cuando la transacción comercial se realiza

entre dos empresas que operan en Internet, una como vendedora y la otra compradora, misma que utilizará ese producto o servicio dentro de su actividad productiva, por lo tanto el objetivo de ambas empresas es vender tal producto o servicio final al consumidor. A su vez, dentro de esta modalidad existen tres submodalidades:

- El mercado controlado que únicamente acepta vendedores en busca de compradores.

- El mercado en el que el comprador busca proveedores.

- El mercado en el que los intermediarios buscan que se genere un acuerdo comercial entre los vendedores y compradores.

El comercio electrónico a este nivel reduce los errores que puedan aparecer, y aumenta la eficiencia en la venta y relación comercial.

b) Comercio entre empresas y consumidores **Business to Consumers conocido como *B2C***; este tipo de comercio electrónico es el más conocido y elemental, pues una empresa vende sus productos o servicios de forma directa a los consumidores finales, ya sea de forma personal o de forma virtual (tiendas o catálogos online). Siendo aquí donde participan los intermediarios

online, incluyendo a las plataformas de comercio electrónico como Shopify2, por lo tanto, esta modalidad facilita a los usuarios, pues puede acceder fácilmente a la tienda virtual y mirar las ofertas y precios actualizados para su comodidad.

c) Empresa y Administración **Business to Administration, conocido como *E-a-A o B2A***; es la modalidad en la que las empresas pueden pagar tasas e impuestos de forma electrónica.

d) Comercio entre consumidores y empresas, **Consumer to Business conocido como *C2B***, se da cuando un consumidor o un grupo de consumidores utilizan la Red para así obtener mejores condiciones que la oferta que presenta una empresa.

e) Comercio entre negocio a empleado. **Business to Employee, conocido como *B2E***; se centra principalmente entre una empresa y sus empleados, se refiere a las ofertas que la propia empresa hace a sus empleados directamente desde su tienda online o portal de Internet. Este tipo de comercio electrónico es un tema novedoso pues genera competencia entre los empleados.

[2] Shopify fue fundada en 2006 por Tobias Lütke (premio al CEO del año en Canadá), Scott Lake y Daniel Weinand. Desde su lanzamiento, la plataforma ha ido creciendo rápidamente hasta convertirse en uno de los líderes en soluciones de comercio electrónico. Actualmente, la compañía abastece a más de 150.000 tiendas online.

f) También el que se da entre consumidores **Consumers to Consumers conocido como *C-a-C o C2C*.** Esta modalidad es una evolución de las tradicionales y conocidas ventas de garaje, pues los consumidores actúan como vendedores y compradores, pero en este caso, a través de una plataforma en Internet, siguiendo el mismo proceso de compra tradicional, siendo "Ebay" el ejemplo más destacado.

g) **Administraciones Públicas:** pudiendo ellas actuar como agentes reguladores y promotores del comercio electrónico y a su vez como usuarios del mismo, como por ejemplo en los procesos de contratación pública.

2) Según el grado de complejidad de las actividades desarrolladas:

a) **Actividades Poco Complejas**: promoción de una empresa, el soporte pre/post venta y la presencia electrónica; y,

b) **Actividades Complejas:** las que radican en la cercanía de las relaciones entabladas entre agentes, por ejemplo la venta y distribución de productos y servicios en el perímetro nacional o internacional, pagos electrónicos entre otros.

3) De acuerdo a las características de los bienes y servicios:

a) **Comercio electrónico Indirecto:** se refiere a bienes tangibles cuyo pedido es por vía electrónica y su entrega por medio de servicios de correo comunes.

b) **Comercio electrónico Directo:** se refiere a bienes intangibles, por lo tanto el pedido y la entrega son en línea como por ejemplo servicios de consultoría, educación, entre otras.

4) Según la tecnología utilizada:

a) **Comercio Electrónico Cerrado:** trabaja sobre redes cerradas de propiedad de los participantes mismo que es utilizado por las organizaciones, oficinas particulares o empresas.

b) **Comercio Electrónico Abierto:** es el que se desarrolla en la red de Internet, sin necesidad de acuerdos previos negociables entre las partes facilitando las relaciones ocasionales o a corto plazo.

5) De acuerdo al ámbito geográfico de ejercicio: en esta modalidad tenemos al Comercio electrónico interno y al Comercio electrónico internacional.

1.3 Validez

La Ley de comercio electrónico, firmas electrónicas y mensajes de datos, manifiesta la validez de los contratos electrónicos diciendo: “Art. 45.- Validez de los contratos electrónicos.- Los contratos podrán ser instrumentados mediante mensajes de datos. 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”.

No cabe duda que nuestro ordenamiento jurídico determina la validez del contrato electrónico, en el cual se refiere en primer lugar a la integridad que debe existir en los mensajes de datos que se van a formar, y después, esa validez hace referencia al consentimiento como tal y no a que las partes contratantes se encuentren presentes físicamente.

Considerando ya la validez de dicho contrato, cabría la siguiente interrogante ¿qué debe contener un contrato electrónico para que sea válido? La respuesta es bastante simple, pues al no estar establecido en la ley especial, nos debemos remitir a la general, por lo tanto el Artículo 1461 de nuestro Código Civil nos dice que tales requisitos son:

a) Capacidad

b) Consentimiento libre de vicios (error, fuerza y dolo)

c) Causa Lícita

d) Objeto Lícito

La capacidad[3] y el consentimiento toman un papel bastante importante y necesario dentro del comercio electrónico ya que puede suscitarse problemas muy grandes justamente porque las partes no se encuentran presentes, y puede existir la suplantación de identidad, o que se contrate con personas absoluta o relativamente incapaces, siendo así que la parte con quién se contrató tendrá derecho a ser indemnizada por perjuicios ocasionados. Por esta razón, la contratación electrónica requiere establecer ciertos mecanismos técnicos que garanticen la celebración de dicho contrato:

a) La identidad del emisor de un mensaje, por ejemplo de la oferta o la aceptación contractual;

b) Que el mensaje no ha sido afectado o alterado;

c) Que no exista el repudio del mensaje, es decir, la negación por el emisor de que lo ha enviado o por el destinatario de que lo ha recibido.

[3] La capacidad jurídica puede definirse como "la aptitud legal para adquirir derechos y ejercitarlos". Las personas que no pueden gozar de un derecho, son las llamadas incapaces de goce; las que no pueden ejercerlo, incapaces de ejercicio. Arturo Alessandri R., Manuel Somarriva U., Antonio Vodanovich, "Curso de Derecho Civil", Tomo I, Santiago de Chile, Editorial Nascimento, 1971, p.351.

Dentro del segundo requisito de un contrato electrónico, tenemos al consentimiento, el cual debe ser entendido como la declaración de voluntad entre dos partes, mismo que debe coincidir en un determinado momento, cabe mencionar que tal consentimiento no puede estar afectado por ningún vicio (error, fuerza y dolo).

Sin embargo, puede llegar a ser común que este viciado, pues dentro de estas operaciones electrónicas pueden darse que al momento de elegir un producto que está descrito en la oferta de una manera, y al momento de recibirlo, sea diferente en su calidad, tamaño, color o textura, situación en la que el consumidor pudiera optar por la rescisión del contrato, acogiéndose a las reglas de la Ley Orgánica de Defensa del Consumidor.

Por su parte, como se mencionó anteriormente, el **dolo** también puede viciar el consentimiento de la declaración por vía electrónica, y esto se da cuando se utiliza cualquier tipo de engaño, afirmando lo que es falso o disimulando lo que es verdadero, o cuando, aparece claramente que sin él no hubieran contratado. Esta situación puede afirmarse cuando el proveedor de un producto, mediante publicidad engañosa en la página Web, induce a la elección de un bien o servicio afectando los intereses y derechos del consumidor.

Al hablar del tercero y cuarto requisito de los contratos, objeto y causa lícita, es importante manifestar que sin éstas no puede haber obligación. Por lo tanto, “el objeto materia del contrato debe ser: real, comerciable y determinada”. (Alessandri, 1970). El objeto es real cuando existe en la naturaleza o se espera que exista; es comerciable cuando es susceptible de dominio o posesión privada; y, es determinada, cuando se especifica su género y cantidad. En el caso que el objeto sea un hecho, se requiere que sea física y moralmente posible, siendo físicamente imposible el contrario a la naturaleza, y moralmente imposible el prohibido por las leyes, o contrario a las buenas costumbres y al orden público. Esto significa que, al tratarse de productos ofertados en la Web y en los que se concierte un contrato electrónico, la causa como motivo de la contratación y el objeto sobre el que recae el contrato, cuando verse sobre bienes, tendrá que encontrarse dentro del comercio y estar de acuerdo a la ley para que sea lícito. De similar forma cuando se relacione el acuerdo sobre algún servicio, no tendrá que contravenir a la naturaleza y estar permitido por las leyes sin transgredir lo establecido por el orden establecido por el Estado, las buenas costumbres y lo dispuesto en el artículo 1480 del Código Civil.

Dentro del contrato electrónica, con relación al objeto pueden existir inconvenientes, pues no se puede distinguir la verdadera apariencia ni características reales del producto o servicio que se exhibe en el espacio virtual, por ello la importancia que el objeto sea determinado y determinable en el convenio de manera que no afecte la eficacia del contrato y que la parte que adquiere no se sienta perjudicada. La ilicitud del objeto es otro problema que puede presentarse debido al carácter transnacional de la red de Internet, ya que consiente que personas ubicadas en distintos lugares del mundo puedan comprar y vender objetos prohibidos en unos países y permitidos en otros, ocasionando que el contrato no sea válido según el ordenamiento jurídico de unos países por el objeto sobre el que recae el acuerdo.

De todo lo manifestado, queda una interrogante, ¿en qué momento el contrato electrónico tiene vida jurídica? Para conocer en qué momento se perfecciona tal contrato, nos remitiremos al Artículo 46 de la ley de comercio electrónico, firma electrónica y mensajes de datos, la cual dispone:

> El perfeccionamiento de los contratos electrónicos se someterá a los requisitos y |solemnidades previstos en las leyes y se tendrá como lugar de perfeccionamiento el que acordaren las partes.

La recepción, confirmación de recepción, o apertura del mensaje de datos, no implica aceptación del contrato electrónico, salvo acuerdo de las partes.

Entendiendo que el contrato es perfecto cuando surte efectos jurídicos, es decir, el perfeccionamiento se produce con el consentimiento de las partes, al tratarse de contratos celebrados vía Internet, y no encontrarse presentes los contratantes de modo simultáneo, el artículo 46 señalado indica que "el perfeccionamiento de los contratos electrónicos se someterá a los requisitos y solemnidades previstos en las leyes…", nos damos cuenta que no habla del momento en que se efectúa, por lo tanto, la doctrina (Alessandri, 1970) ha planteado cuatro teorías clásicas del momento en que se forma el consentimiento:

1) Teoría de la declaración o de la aceptación,
2) Teoría de la información o del conocimiento,
3) Teoría de la expedición, y
4) Teoría de la recepción.

De las cuatro teorías anteriores, nuestra legislación acoge la teoría de la declaración o de la aceptación, que considera perfeccionado el contrato en el momento en que la aceptación es emitida aunque aquella sea ignorada por el

proponente. El consentimiento no se produce por el conocimiento recíproco de las voluntades de los declarantes, sino por el simple acuerdo de las voluntades exteriorizadas, y así lo ratifican el Código de Comercio Ecuatoriano.

1.4 Jurisdicción

El contrato electrónico, al efectuarse dentro de un espacio virtual, rompe con el principio de territorialidad en la celebración de los contratos civiles y comerciales, por lo que en caso de presentarse conflictos sobre el objeto, la causa, obligaciones de las partes o la interpretación del mismo, deberá existir una cláusula de sometimiento a una legislación establecida en la misma forma contractual. Pero el problema surge cuando las partes no han estipulado sobre una ley que rija el contrato, presentándose así dificultades al negociar, llevando consigo incluso la no aceptación y realización del acuerdo. Esta problemática debe ser resuelta por la determinación de la competencia de los jueces según sea el caso y por supuesto por el Derecho Internacional Privado.

La jurisdicción y la competencia de un contrato electrónico no deben ser exclusivas del Derecho interno de cada país, sino debe tomarse en consideración el Derecho internacional Privado por la concepción tan amplia del mundo de Internet. En el caso que el contrato ha sido celebrado en el mismo lugar donde residen ambas partes, y el cumplimiento también es en el

mismo lugar, se entiende que a pesar de haberse celebrado en Internet, es un contrato nacional o interno, regulado por las normas del país; pero si en la celebración del contrato existe una conexión de distintos ordenamientos jurídicos, es importante resolver la competencia de los tribunales que vayan a conocer del asunto y la ley aplicable y para ello, en primer lugar tenemos que sería aplicable lo que se ha resuelto por la vía contractual, siendo las partes quienes lo decidan según el principio de la autonomía de la voluntad. Sin embargo, en caso de que no esté acordado, se debe sujetar a normas procesales vigentes, tal como nos manifiesta la Ley de comercio electrónico en el primer inciso del artículo 47, expresando que:

> En caso de controversias se someterán a la jurisdicción estipulada en el contrato; a falta de ésta, se sujetarán a las normas previstas por el Código de Procedimiento Civil Ecuatoriano y esta Ley, siempre que no se trate de un contrato sometido a la Ley Orgánica de Defensa del Consumidor, en cuyo caso se determinará como domicilio del consumidor o usuario...",

Y a su vez lo que nos dice la quinta disposición general de la Ley ibídem:

> Se reconoce el derecho de las partes para optar libremente por el uso de tecnología y por el sometimiento a la jurisdicción que acuerden mediante

convenio, acuerdo o contrato privado, salvo que la prestación de los servicios electrónicos o uso de otros servicios se realice de forma directa al consumidor.

1.5 Tiempo y lugar de celebración.

El lugar de la celebración del contrato, tiene consecuencias importantes y más aún de un contrato electrónico, ya que con éste se fija la competencia de los tribunales, se establece la ley del país a aplicarse, el carácter nacional o internacional del contrato siendo común que se involucren diferentes legislaciones. El artículo 46 de la Ley de comercio electrónico, inciso primero, nos dice: "... se tendrá como lugar de perfeccionamiento el que acordaren las partes." Tal lugar de perfeccionamiento se refiere al sitio donde se celebra el contrato previamente acordado por las partes, ya que el consentimiento no se forma con la presencia física de los contratantes sino a través del medio electrónico empleado, por lo que no se presume un lugar determinado de celebración del contrato.

En primera instancia, el lugar de celebración del contrato es el que fijen las partes, tal como se mencionó en el punto anterior. En la mayoría de contratos electrónicos "se estipula una legislación y jurisdicción específica, que generalmente es la del vendedor" (Carrillo, 2011). Sin embargo, se puede

proponer que "se acepte el domicilio del consumidor como lugar de celebración, de manera que considere el domicilio de la parte vulnerable como forma de protección de la parte adherente". (Lorenzetti, 2002).

En el caso de que, "los contratantes se encuentran en lugares distintos, se presume que el contrato se celebró en el lugar donde se hizo la oferta" (Bescós, 2004). Al tratar de relacionar el domicilio virtual con un lugar fijo, algunas propuestas establecen la obligación de inscribirse en un registro, y fijan el domicilio del oferente en el lugar donde esté registrado, y el lugar de celebración del contrato lo relacionan con el del registro inscrito, regulando así los sistemas de intercambio electrónico para que sean seguros y, por tanto, controlables según parámetros del derecho común. Así, nos debemos remitir a lo que nos dice el Código de Comercio, mismo que señala en su artículo 147: "residiendo las partes contratantes en distintos lugares, se entenderá celebrado el contrato, para todos los efectos legales, el de la residencia del que hubiere aceptado la propuesta primitiva o la propuesta modificada"

2. Firma Electrónica

2.1 Concepto

Para hablar de firma electrónica, es necesario, en primer lugar referirnos al significado de una firma, por lo tanto, nos remitimos a lo que nos dice el

Diccionario de la Real Academia de la Lengua Española, el cual nos manifiesta que:

> Es el nombre y apellido, o título, de una persona, que ésta pone con rúbrica al pie de un documento escrito de mano propia o ajena, para darle autenticidad, para expresar que se aprueba su contenido para obligarse a lo que en él se dice.

Así también, la doctrina nos explica que:

> La firma es la manera habitual con que una persona escribe su nombre y apellido, con el objeto de asumir responsabilidades inherentes al documento que suscribe, en donde el carácter de habitualidad es decisivo para que un rasgo sea considerado firma de una persona. (Borda, 1985)

A su vez, se debe tener en cuenta que existen varias técnicas usadas para la firma, como la firma manual transformada en un sello, la firma digitalizada, la clave criptográfica, etc., la diferencia entre ellas es que cada una ofrece diferentes seguridades.

Técnicamente, la firma electrónica es considerada como un método criptográfico[4] que asegura la identidad del remitente, siendo también una herramienta tecnológica que permite la posibilidad que éstos gocen de una característica que antes era propia de los documentos en soporte de papel o tradicionales, requiriendo para ello de procedimientos técnicos que permitan su creación y verificación así como de una legislación que respalde su validez jurídica, como es el caso de nuestra legislación, pues la ley de comercio electrónico, firmas electrónicas y mensajes de datos nos dice en su artículo 13:

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

2.2 Requisitos

El Artículo 15 de la Ley de Comercio Electrónico, Firmas electrónicas y mensajes de datos, nos manifiesta cuales son los requisitos de la firma electrónica:

[4] La criptología es la ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicaciones. Sus objetivos son la privacidad o confidencialidad de los datos, garantizando la autenticación de los mismos, su integridad y su no repudio.

> "Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:
>
> a) Ser individual y estar vinculada exclusivamente a su titular,…"

Este requisito se refiere a relacionar el documento electrónico con su autor, imputándole a su esfera intereses a los efectos jurídicos de la declaración que obra en un soporte determinado. Esto debido a que en el mundo virtual, la firma electrónica busca dar seguridad en todas las actividades en el Internet y al existir firmas conjuntas o al haber una firma electrónica vinculada a varias personas, nos preguntamos quien es el responsable. Por lo que es válido individualizar y vincular a una persona.

> *"…*b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta Ley y sus reglamentos;"

Con este requisito, lo que se busca es garantizar la autoría del signatario, y asociar al proceso de llaves privada y pública para poder firmar digitalmente, así lo que se ha codificado o encriptado mediante una de las llaves, solo podrá ser desencriptado por otra. Así, cuando se quiera establecer una comunicación segura con otra parte, basta encriptar el mensaje con la clave pública del sujeto para que a su recepción solo el sujeto que posee la clave privada pueda leerlo.

"…c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado."

Indica que la firma electrónica no ha sido modificada, sin que falte ninguno de los elementos que la componen por lo que la información no ha sido adulterada al momento de almacenarla.

"…d) Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario; y…"

La firma electrónica asegura la autenticidad de la información, es decir, que nos permite en forma efectiva y eficiente determinar si quien envía el mensaje es verdaderamente quien dice ser. Quien emite una firma electrónica no puede negar haberla emitido ya que dicha firma es aceptada como medio de prueba.

"…e) Que la firma sea controlada por la persona a quien pertenece."

En este caso, el titular de la firma electrónica debe notificar a la otra parte del inconveniente, y actuar de conformidad al Art. 17 ibidem (obligaciones del titular de la firma electrónica).

2.3 Efectos de la Firma Electrónica

Para hablar de los efectos de la firma electrónica, es necesario analizar lo que nos dice el Artículo 14 de la ley ibídem, "La firma electrónica tendrá igual

validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio."

Por lo tanto, la firma electrónica constituye un modo idóneo para suscribir un documento electrónico, dando paso a que se cumpla con la exigencia de vincular el acuerdo de voluntades entre los suscriptores, o al autor del documento con su contenido, permitiendo así que el documento electrónico sea apto como prueba dentro de un proceso judicial.

La Firma electrónica "es pieza clave para la seguridad del Comercio Electrónico, por lo que no es fácil que éste crezca jurídicamente en paralelo a su crecimiento empresarial si no existe regla cierta de derecho y ejecutable sobre la firma electrónica" (Illescas, 2001).

Se debe tener en cuenta que la firma electrónica se encuentra en la misma posición que la manuscrita, considerando una diferencia, y es que, en el caso de la firma manuscrita, la estampación de ella por parte del signatario se crea y existe físicamente en el documento al momento de firmar, quedando impresa en él mediante el uso de la tinta; en cambio en el caso de la firma electrónica, no existe físicamente al momento de su aplicación para suscribir el documento, sino que se produce un reemplazo del trazo autográfico por un cifrado electrónico que se agrega al documento, el cual se realiza mediante un

criptosistema, por lo que la creación de la misma, requiere de la utilización de procedimientos matemáticos complejos que relacionan al documento firmado, con la voluntad del suscriptor, y así, dando la posibilidad a terceros para que reconozcan su identidad y tengan la certeza que el documento electrónico no se haya alterado, ya que se basa en la generación de una serie matemática de número que se cifra con una clave privada usada por el suscriptor del documento digital, el cual va a acompañar al mensaje original, adjuntando una marca única y que solo la persona que lo firma es capaz de producirlo. Al analizar dicho documento, el receptor genera una serie numérica del emisor en base al mensaje recibido, luego se descifrará la firma digital del documento, utilizando la clave del firmante, por lo que se obtiene la serie numérica del mensaje original, si ambas series numéricas son concordantes, no ha habido alteración.

2.4 Certificación de Firma Electrónica

El capítulo II de la Ley a la que nos hemos estado haciendo referencia, nos habla sobre la certificación de la firma electrónica, el Artículo 20 dice *"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."*

De lo expresado, podemos deducir que el certificado de una firma electrónica es un registro electrónico que atestigua que una clave pública pertenece a determinada persona, sea ésta natural o jurídica. De esta forma, se puede verificar que una clave pública pertenece a determinada persona, y así se evita que una persona utilice una clave falsa intentando hacerse pasar por otra persona.

2.5 Duración de Firma Electrónica

Al hablar de la duración de la firma electrónica, es necesario referirnos a lo que nos manifiesta la ley especial mencionada:

> *"***Art. 23.- Duración del certificado de firma electrónica.-** Salvo acuerdo contractual, el plazo de validez de los certificados de firma electrónica será el establecido en el reglamento a esta Ley."

El artículo 11 del Reglamento a la Ley de Comercio Electrónico a su vez nos dice;

> **"Duración del certificado de firma electrónica.-** La duración del certificado de firma electrónica se establecerá contractualmente entre el titular de la firma electrónica y la entidad certificadora de información o quien haga sus veces. En caso de que las partes no acuerden nada al

respecto, el certificado de firma electrónica se emitirá con una validez de dos años a partir de su expedición. Al tratarse de certificados de firma electrónica emitidos con relación al ejercicio de cargos públicos o privados, la duración del certificado de firma electrónica podrá ser superior a los dos años pero no podrá exceder el tiempo de duración de dicho cargo público o privado a menos que exista una de las prórrogas de funciones establecidas en las leyes."

Por lo tanto, en primera instancia va a depender lo que se haya acordado contractualmente entre el titular de la firma electrónica y la entidad de certificación. Pero en el caso de no existir ningún acuerdo, este reglamento absorbe este vacío diciendo que tendrá una duración de dos años, teniendo en cuenta que puede extenderse más de este tiempo, como por ejemplo cuando el titular desempeña una función pública o privada que dure más de este tiempo.

2.6 Extinción de firma Electrónica.

"Art. 24.- Extinción del certificado de firma electrónica.- Los certificados de firma electrónica, se extinguen, por las siguientes causas:

a) Solicitud de su titular;

b) Extinción de la firma electrónica, de conformidad con lo establecido en el Art. 19 de esta Ley; y,

c) Expiración del plazo de validez del certificado de firma electrónica.

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

2.7 Entidades que Certifican una firma electrónica

"Art. 29.- Entidades de certificación de información.- Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República."

Para que la firma electrónica tenga validez, debe estar aprobada y registrada por una entidad de certificación de información la cual emite el respectivo

certificado avalando la veracidad de la información que sirvió como base para la firma y certificando que efectivamente corresponde a su titular. Sin embargo, existen muchas controversia respecto de la eficacia de las entidades certificadoras nacionales e internacionales, pues hay quienes opinan que tales agencias si son nacionales serán más confiables pues tienen su asentamiento dentro del territorio nacional, por otro lado, hay quienes sostienen que las certificadoras internacionales al tener mayor tiempo de funcionamiento tienen mayor conocimiento sobre el tema.

A su vez, claramente nuestra ley nos manifiesta que tales entidades deben estar legalmente constituidas y registradas en el Consejo Nacional de Telecomunicaciones, por lo tanto, estas instituciones deben contar con una garantía de responsabilidad suficiente para responder por posibles daños y perjuicios que se pudieran ocasionar por incumplimiento de sus obligaciones, respondiendo hasta por culpa leve, así también, deben demostrar solvencia técnica, logística y financiera. De esta forma, estas entidades, al manejar infinidad de datos e información personal de usuarios, deben ser extremadamente confidenciales, por lo que la prestación de sus servicios debe ser permanente, oportuna e inmediata.

Las entidades de certificación deben mantener una publicación del estado de los certificados otorgados por ella, a pesar de que en este sentido la ley no ha

sido clara al establecer el lugar de publicación, sin embargo, en artículos siguientes, nos habla de un organismo encargado de la promoción y difusión de los servicios electrónicos, el COMEXI.

3. Mensajes de Datos

3.1 Concepto

El glosario de términos de la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos, define a los mensajes de datos como

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

Otra definición nos dice que los mensajes de datos "son el punto central de toda la tecnología de la información dedicada a soportar las operaciones comerciales electrónicas" (Gutierrez, 2010).

De esta forma, se debe entender que los mensajes de datos son un concepto propio de las firmas digitales, entendiéndolas como cualquier tipo de mensaje enviado o recibido por un medio electrónico u óptico. Por regla general, se considera mensajes de datos a las comunicaciones efectuadas mediante correo electrónico; extendiéndose también a otras comunicaciones como el telegrama, el télex o el telefax.

3.2 Protección de Datos

Según el Artículo 9 del cuerpo legal al que nos hemos hecho referencia, en su primer inciso nos dice siguiente:

> Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros…

Muchas empresas observan a la información como riqueza intangible y se evidencia que en el Internet el titular de datos tiene poco control legal sobre quien posee y almacena la misma. En el internet la información es proporcionada por los usuarios por diferentes motivos personales y quienes administran las bases de datos pueden sin autorización nuestra hace uso de la información con fines ilícitos como el llamado marketing directo. Las empresas

que adquieren la base de datos saben nuestras referencias personales, usos comerciales y realizan campañas publicitarias diseñadas para adquirir determinados bienes, de esta manera se viola nuestro derecho a la intimidad y privacidad del titulad de la información.

Cabe mencionar que el consentimiento podrá ser revocado a criterio del titular de los datos y la revocatoria no tendrá en ningún caso efecto retroactivo.

En el segundo inciso de la misma ley nos manifiesta:

> …La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente…

Frente a la recopilación de datos con nuevas tecnologías nos preguntamos ¿cómo controlar la difusión de nuestra información y cuáles son las herramientas jurídicas que tenemos para oponernos a la divulgación de la misma sin nuestro consentimiento? En nuestro país tenemos la garantía constitucional del Habeas Data, por la cual tenemos derecho al acceso a las bases de datos que sobre nosotros o nuestros bienes consten en entidades

públicas o privadas, así saber el uso que se haga de nuestra información y su finalidad.

Con la incorporación de la protección de datos en la Ley de comercio electrónico del Ecuador, se responde la pregunta planteada en el párrafo anterior. Además se avanzó en la materia acorde a países industrializados que poseen un cuerpo legal para normar la protección de datos.

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

Cabe indicar que la Ley de Control Constitucional en su Artículo 36 inciso primero, nos expresa cuando no se puede plantear una acción de Habeas Data:

> **Improcedencia.** No es aplicable el hábeas data cuando afecte al sigilo profesional; o cuando pueda obstruir la acción de la justicia; o cuando los

documentos que se soliciten tengan el carácter de reservados por razones de Seguridad Nacional..."

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.

3.3 Duplicación del Mensaje de Datos

En este sentido, la Ley de Comercio Electrónico, firma electrónica y mensajes de datos nos manifiesta lo siguiente en su Artículo 12:

Duplicación del mensaje de datos.- Cada mensaje de datos será considerado diferente. En caso de duda, las partes pedirán la confirmación del nuevo mensaje y tendrán la obligación de verificar técnicamente la autenticidad del mismo.

Dentro de la doctrina se ha expresado la intención de establecer una analogía directa con lo que conocemos, es decir, conceptos, técnicas y reglas de la cultura escrita a la electrónica. El inconveniente de la mencionada analogía es que en el mundo físico es posible realizar una comparación entre el documento original y uno duplicado para deducir la autenticidad por lo que es factible la prueba empírica. En el mundo digital, no cabe la comparación empírica ya que

el documento original puede ser igual al duplicado porque los dos se componen de bits[5] y no existen los bits falsos.

El documento electrónico puede o no ser firmado electrónicamente y en ambos casos puede haber un documento electrónico original y un documento electrónico duplicado. Este último puede ser legítimamente emitido por el autor o por un tercero o puede ser una falsificación ilegítima como se mencionó anteriormente no existen bits falsos. La problemática del concepto de documento original puede ser definido por las partes n un contrato o por el legislador pero la tendencia es tomar en cuenta la primera generación.

Debe señalarse que en sí mismo el documento electrónico no representa riego, en cuanto se faculta la utilización de la tecnología, el problema surge cuando en el mismo se plasman voluntades que generan efectos jurídicos. En los actuales momentos, el comercio electrónico ha permitido a las empresas el uso de nuevas técnicas de venta, muchos de ellos agresivos, por cuanto limitan la libertad de elección y de consentimiento.

[5] Bit es un dígito del sistema de numeración binario, es la unidad mínima de información empleada en informática, en cualquier dispositivo digital o en la teoría de la información. Se puede representar dos valores por ejemplo uno verdadero o falso; abierto o cerrado, blanco o negro, etc. Basta con asignar uno de esos valores al estado de "apagado" (0), y el otro al estado de "encendido"

3.4 Conservación del Mensaje de Datos

Existe la impresión generalizada de que el documento electrónico puede desaparecer en un instante y ofrece menos seguridades que el escrito. Pero paradójicamente es la principal fuente de archivo de la cultura escrita. El tema está en establecer obligaciones de conservación que las partes deben asumir y que esta guarda tenga las siguientes características:

- Que sea accesible para una posterior consulta.
- Que sean conservados en su formato original de generación, envío o recepción u otro formato que reproduzca en forma demostrable la exactitud del contenido del documento digital.

Que sea conservado de tal manera que sea posible determinar el origen, destino, fecha y hora de envío y recepción.

CAPITULO II.

Documentos electrónicos

1. Concepto de Documento

El vocablo Documento, proviene del latín documentum que significa, lo que se señala. En un sentido más amplio, se puede manifestar que consiste en todo lo que consta por escrito o gráficamente en cualquier elemento o cuerpo físico. Para Cabanellas, documento "es el escrito, escritura, instrumento con que se prueba, confirma, demuestra o justifica una cosa, o al menos que se aduce con tal propósito, asimilando". (Cabanellas, 2014)

Desde el punto de vista jurídico - probatorio, el documento es todo medio escriturado o no, admitido por la ley, para justificar o confirmar algo, una cosa, una cantidad, un hecho, etc., como un recibo, una letra de cambio, un contrato, una acta de nacimiento, etc, que pueden nacer de la declaración unilateral de una persona o del convenio entre dos o más partes, de un acto ya público o privado, judicial o extrajudicial. Así también, es necesario manifestar que no todo documento, puede tener la misma eficacia probatoria.

2. Diferencia entre Documento e Instrumento

Es necesario considerar que la palabra documento, es un término genérico, el cual no es igual que el vocablo instrumento, pues impropiamente se los ha relacionado a ambos términos como si fueran sinónimos.

Por lo manifestado, es necesario hacer tal distinción, entendiendo que como se dijo anteriormente, el término documento es el género, mientras que el término instrumento es la especie, es decir, documento es todo objeto que contiene una determinada manifestación del pensamiento, todo cuanto consta ya por escrito o gráficamente en cualquier materia, toda cosa resultado de una actividad humana perceptible por los sentidos especialmente de la vista; por otro lado, el instrumento, es un documento público o privado de índole escrita o escriturada en el que consta un hecho o acto encaminado a surtir efectos jurídicos. Por lo tanto, se puede decir que todo instrumento es un documento, pero no todo documento puede ser considerado un instrumento.

De esta forma, nuestro ordenamiento jurídico hace referencia al término Documentos, y esto es porque al momento de probar un hecho, suceso o cosa, no solamente tienen validez los instrumentos, sino de forma general los documentos, dedicando a ellos la Sección I del Capítulo III del Código Orgánico General de Procesos, en donde prevé reglas generales de los documentos.

Si analizamos la sección de la prueba documental, nos daremos cuenta que los documentos han sido clasificados en públicos y privados, por lo que haremos una breve referencia a cada uno de ellos.

El cuerpo legal anteriormente mencionado, en sus artículos 205 y 216, nos da la definición legal de cada uno de estos tipos de documento, diciéndonos:

> **Art. 205.- Documento público.** Es el autorizado con las solemnidades legales. Si es otorgado ante notario e incorporado en un protocolo o registro público, se llamará escritura pública. Se considerarán también instrumentos públicos los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmada electrónicamente.
>
> **Art. 216.- Documento privado.** Es el que ha sido realizado por personas particulares, sin la intervención de funcionario público alguno, o con éstos, en asuntos que no son de su empleo.

Por lo manifestado, se debe entender entonces, que su diferencia radica en que el documento público está sometido a solemnidades y el privado no; así también, son distintos con respecto al valor probatorio de cada uno, y por ende, a su impugnación.

A sí también, por regla general, todo documento público puede ser consultado por cualquier persona, a excepción de aquellos documentos que por expresa disposición legal son reservados. En cambio, el documento privado, por su propia naturaleza no puede estar disponible al público, sino en los casos en que una autoridad así lo decida.

3. Diferencias y Similitudes entre Documento y Documento Electrónico

Después de tener claro el concepto de los documentos, y su clasificación, es necesario profundizar el tema motivo de la presente investigación, por lo que empezaremos analizando al documento electrónico. Sin embargo, como breve introducción, se debe tener en cuenta que no es igual hablar de documento electrónico y uno digital.

El documento electrónico, debe ser considerado como todo mensaje que contiene información escrita en datos, generada, transmitida, presentada, recibida o archivada por medios electrónicos, por otro lado, el documento digital, es todo mensaje que contiene información por reproducción electrónica de documentos escritos o impresos, transmitida, presentada, recibida o archivada por medios electrónicos. Mientras el documento electrónico se genera y archiva en un medio electrónico; los documentos digitales se reproducen y se archivan en medios electrónicos.

Por lo expuesto, dentro de la presente investigación, a lo que nos haremos referencia siempre, serán a los documentos electrónicos, por lo tanto, es posible hacer una comparación con el documento convencional.

SIMILITUDES

- Mediante la creación de documentos públicos o privados ya sea en soporte tradicional o digital, permiten la expresión del acuerdo de voluntades de las partes, posibilitando establecer cualquier tipo de negocios jurídicos, necesitando en ambos casos tanto la suscripción y reconocimiento de la misma, entendiendo que se lo puede realizar de modo tradicional, es decir, con el reconocimiento de firmas ante un Notario Público, o en el caso de ser documentos electrónicos, mediante métodos digitales en base a los entes de certificación. Es necesario recalcar que cualquiera de las dos formas, lo que se busca de la suscripción respecto de su autor es el mismo y responde a la misma necesidad de seguridad, verificación y autenticidad, por ello tanto el titular de una firma manuscrita como el de una firma electrónica está obligado a actuar diligentemente y tomar todas las medidas en pos de mantener la exclusiva utilización de la misma.
- Tanto los documentos tradicionales como electrónicos, requieren de algún soporte para su representación, pues constituye la forma de almacenar la

información, otorgándole constancia dentro de un proceso judicial; lo que varía será que en el un caso tal soporte será el papel físico, y en el otro caso un dispositivo de carácter electrónico.

- Finalmente, tenemos que en ambos casos, documentos públicos, privados y electrónicos, han sido reconocidos jurídicamente dentro de nuestro país, pues pueden ser invocados en cualquier proceso judicial.

DIFERENCIAS

- Como primera diferencia entre los documentos tradicionales y electrónicos tenemos el soporte de cada uno de ellos, que a su vez, viene a ser la naturaleza de los mismos, mientras en el documento tradicional su soporte es el papel, en los documentos electrónicos su soporte es informático; de esta manera, se puede considerar que el documento tradicional tiene varias ventajas con respecto a los electrónicos, como por ejemplo, el poder ser distinguido entre un documento original y una copia, o la posibilidad de reconocer ciertas alteraciones o enmendaduras.
- En el documento convencional, el registro esta acogido en un medio, en la que su información se hace accesible a través de símbolos implícitos en él, mientras que en los documentos electrónicos, se recoge esa información en un medio en los que los símbolos solo pueden ser leídos por un ordenador.

- En cuanto a su valor probatorio, si bien es cierto ambos tipos de documentos tienen una eficiente valoración probatoria, sin embargo al ser diferentes tipos de documentos, también será diferente la forma de validación, pues en el caso de los documentos tradicionales, su valor probatorio va a ser medido por las características de autenticidad, como por ejemplo cuando se reconoce una firma; en el caso de los documentos electrónicos, su autenticidad depende del hardware y del software en el que fue creado, el cual solo se va a poder mantener si se conserva en su estructura original.

4. Instrumentos Electrónicos Públicos

Los instrumentos públicos electrónicos, son mensajes de datos en soporte electrónico, en el cual se registra la voluntad de las partes que intervienen en un acto o negocio jurídico. “Son otorgados por la autoridad competente, así puede ser el notario virtual o a quien la Ley de las facultades para hacerlo”. (García, 2010)

Al tratarse de instrumentos públicos, la autoridad competente deberá dejar constancia del medio empleado y conservar una versión íntegra para una posterior consulta, siguiendo las condiciones expresadas en el artículo 8 de la Ley de Comercio Electrónico, Firmas electrónicas y mensajes de datos.

A su vez, el Artículo 51 ibidem, reconoce la validez jurídica de los instrumentos públicos electrónicos diciéndonos que:

> Se reconoce la validez jurídica de los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmadas electrónicamente.
>
> Dichos instrumentos públicos electrónicos deberán observar los requisitos, formalidades y solemnidades exigidos por la ley y demás normas aplicables.

De esta forma, la noma mencionada, hace viable el uso del instrumento firma electrónica de carácter público, existiendo en ella la presunción de que al ser presentada como medio de prueba, se entiende que cumple con todos los requisitos legales, tal como nos menciona el artículo 53 de la ley mencionada anteriormente.

4.1 El Notario Público ante los instrumentos electrónicos.

El Doctor Luis Vargas Hinostroza, considera que al notario se lo debe considerar como "el funcionario que recibe del Estado la potestad legal de otorgar fe pública para autorizar actos, contratos, trámites y diligencias, establecidos en la ley en los que interviene en razón de su cargo…" (Hinostroza, 2006), por lo tanto, cumple con un papel estratégico dentro de

nuestra sociedad, pues es quien brinda certeza en las relaciones entre los particulares, ajustando su voluntad a lo que se encuentra establecido en la ley.

Con respecto a esta nueva forma de documentos, así mismo, la función del notario se vuelve aún más indispensable debido a que, como se estudió en el capítulo anterior, los documentos electrónicos y específicamente la firma electrónica atiende a un sistema de cifrado, mismo que se convierte en una variable primaria, por lo que debe contener un valor intrínseco que se le dará por la eficacia que le otorga en derecho en cuanto a seguridad y garantía, de la misma forma que ocurre con el documento público tradicional por la intervención del Notario quien será el encargado de dotar fe pública y autenticidad, para así tener valor jurídico.

Ante este auge del comercio electrónico, se debe replantear muchos de los principios e instituciones que le rigen al sistema notarial que tenemos actualmente en nuestro medio que impliquen la contratación electrónica y la utilización de documentos electrónicos en aras de garantizar la confidencialidad de las comunicaciones, la identidad y capacidad de las partes intervinientes, así como también la integridad y autenticidad de los mensajes en todo el proceso de intercambio electrónico de información en actos y negocios jurídicos de naturaleza civil o mercantil.

Desde el punto de vista internacional, han existido ya reformas en materia de comercio electrónico y notarial, como por ejemplo en México, en donde a partir del Decreto del 29 de mayo del 2000 existen reformas en materia de comercio electrónico al código civil federal, al código federal de procedimientos civiles y a la Ley Federal de Protección al Consumidor, en las que no solamente se discute el papel del notario como fedatario público en actos y negocios jurídicos por medios electrónicos, sino que se está instrumentando jurídicamente a normas que atañen a instituciones como es el Protocolo Notarial.

4.2 El futuro cibernotario.

En el año de 1993, siete años después de la elaboración de la ley Modelo sobre Comercio electrónico, de las Naciones unidas, la Unión Internacional del Notariado Latino (UINL) conjuntamente con la American Bar Association (Colegio de Abogados de los Estados Unidos), iniciaron varios estudios en los que concluyeron con la creación de una figura denominada "Cibernotario" mismo que ha sido objeto de disputas por el protagonismo en la Certificación Digital.

El cibernotario, como solución dentro del mundo del comercio electrónico va a tener una doble función:

- **La función de tipo jurídico.** Es función propia del notario latino, en la que asegura a los documentos y actos en los que interviene dando fe pública, cumpliendo con los requisitos legales necesarios para ser plenamente reconocidos por los países basados en el derecho civil y común.
- **La función de tipo electrónica:** es la más importante ya que por ésta el Cibernotario debe tener un nivel de especialización alto en cuanto a conocimientos informáticos, debiendo actuar como autoridad de registro. Esta función va a comprender no sólo el verificar la legalidad y capacidad del solicitante, sino que puede ser requerido para investigar sus datos económicos o penales.

Por lo antes dicho, los cibernotarios deben ser profesionales con preparación de abogados, siendo necesario que se formen en el área de las nuevas tecnologías y transacciones electrónicas, en virtud de que darán fe pública a documentos electrónicos que se presenten en el mundo del comercio electrónico, para así adquirir el carácter de documentos electrónicos públicos.

En países desarrollados tecnológicamente como Estados Unidos, el proyecto cibernotario, propone crear una oficina “cuasi pública” conocida justamente como CyberNotario, el cual combinara la experiencia legal y técnica en una

sola especialización, asegurando que las transacciones en las que intervenga, vaya a reunir requisitos de procedimiento y formalidades requeridas.

Entonces, por medio de la utilización de la firma electrónica, el cibernotario va a poder certificar la identidad del emisor de un mensaje, dar un nivel alto de seguridad con respecto a su contenido, fechar la notarización (fecha y hora de su intervención), y su protocolización con fines de archivar los mismos, siendo así como se desenvolvería normalmente.

4.3 La desmaterialización de documentos electrónicos.

El glosario de la Ley de Comercio electrónico, firmas electrónicas y mensajes de datos, define a la desmaterialización manifestando que es la transformación de la información contenida en documentos físicos a mensajes de datos.

A su vez el artículo 5 del Reglamento a la Ley de Comerico electrónico nos dice lo siguiente:

> **Desmaterialización.-** El acuerdo expreso para desmaterializar documentos deberá constar en un documento físico o electrónico con las firmas de las partes aceptando tal desmaterialización y confirmando que el documento original y el documento desmaterializado son idénticos. En caso que las partes lo acuerden o la ley lo exija, las partes acudirán ante Notario o autoridad competente para que certifique electrónicamente que

el documento desmaterializado corresponde al documento original que se acuerda desmaterializar. Esta certificación electrónica se la realiza a través de la respectiva firma electrónica del Notario o autoridad competente.

Los documentos desmaterializados deberán señalar que se trata de la desmaterialización del documento original. Este señalamiento se constituye en la única diferencia que el documento desmaterializado tendrá con el documento original.

En el caso de documentos que contengan obligaciones, se entiende que tanto el documento original como el desmaterializado son la expresión de un mismo acuerdo de las partes intervinientes y por tanto, no existe duplicación de obligaciones. De existir multiplicidad de documentos desmaterializados y originales, con la misma información u obligación, se entenderá que se trata del mismo, salvo prueba en contrario.

La desmaterialización de los documentos de identificación personal estará sujeta a las disposiciones especiales y procedimiento que las entidades competentes determinen.

De lo señalado por el reglamento, debemos entender que al momento en que la información contenida en papel o es convertida a mensajes de datos o

documento electrónico estamos frente a la desmaterialización de un documento. Así también, señala que necesariamente debe existir un acuerdo expreso físico o electrónico con las firmas de las partes para desmaterializar documentos, confirmando que el documento original y el documento desmaterializado son idénticos, observándose que se cumpla con las obligaciones previstas en el artículo 7 de la Ley de comercio electrónico, específicamente en su inciso final:

> …Los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la presente ley, y deberán ser conservados conforme a lo establecido en el artículo siguiente.

De la misma forma, las partes que solicitan tal desmaterialización deben firmar su confirmación, de esta forma aceptan que el documento original será igual al documento desmaterializado, y en caso de acuerdo de las partes o si la Ley lo pide, podrán acudir ante un Notario Público o autoridad competente para que certifique por medio de su firma electrónica esta operación.

Cuando se trate de instrumentos públicos, intervendrá el Notario, siendo así que no se negará valor y efectos jurídicos a los documentos desmaterializados.

El reglamento también nos manifiesta que cuando el documento a desmaterializar contiene obligaciones, se entenderá que tanto el documento original como el desmaterializado, es la expresión de un mismo acuerdo de voluntades, ya que el efecto de la desmaterialización no produce cambios en el contenido de lo que se ha convenido por los contratantes sin cambiar la esencia del documento.

Finalmente, en lo concerniente a la desmaterialización de documentos de identificación personal, se debe sujetar a lo que disponen las leyes especiales y de procedimiento.

5. Certificación de la desmaterialización del documento electrónico.

El artículo 4 del reglamento nos manifiesta:

> **Información original y copias certificadas.-** Los mensajes de datos y los documentos desmaterializados, cuando las leyes así lo determinen y de acuerdo al caso, deberán ser certificadas ante un Notario, autoridad competente o persona autorizada a través de la respectiva firma electrónica, mecanismo o procedimiento autorizado.
>
> Los documentos desmaterializados se considerarán, para todos los efectos, copia idéntica del documento físico a partir del cual se generaron y deberán contener adicionalmente la indicación de que son

desmaterializados o copia electrónica de un documento físico. Se emplearán y tendrán los mismos efectos que las copias impresas certificadas por autoridad competente.

De ello, debemos entender claramente que el Notario Público de forma general, y la autoridad competente en casos que especifique la ley, van a ser los encargados de certificar los documentos desmaterializados a través de la firma electrónica respectiva con un mecanismo autorizado, teniendo en cuenta que estos documentos serán considerados como una copia del documento físico.

CAPITULO III

Alcance jurídico del documento electrónico

1. Documento electrónico como medio probatorio en la Legislación Ecuatoriana.

Al hablar sobre el tema del valor probatorio de un documento electrónico, es necesario resaltar que en nuestro ordenamiento existe este reconocimiento jurídico, el cual está establecido en la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos en su artículo 2, el cual expresa lo siguiente: "Reconocimiento jurídico de los mensajes de datos.- Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento." Y no solo de los mensajes de datos, sino también la firma electrónica, esto nos manifiesta el artículo 14 ibidem "La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio." De esta manera, se puede observar que nuestro ordenamiento jurídico brinda valor jurídico tanto a mensajes de datos como a la firma electrónica, de la misma forma que a los documentos en soporte de papel, considerando que deben tener ciertos

requisitos específicos para ser tomados como tales, los mismos que serán estudiados a lo largo del presente capítulo.

Al tener un documento con firma electrónica certificada, se lo puede incorporar como prueba, contando ya con una presunción legal a su favor y trasladando la carga de la prueba a quien pretenda negar la validez de dicho documento, esto lo establece el artículo 53 de la ley en mención:

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

Puede darse el caso que no sea posible contar con un documento con una certificación autorizada, sino estemos frente únicamente a un correo electrónico o e-mail, el mismo que contenga algún tipo de información que necesite ser probada, en este caso, la jurisprudencia chilena, francesa, entre otras, nos indican que al no tener ningún tipo de suscripción no tiene valor jurídico relevante, criterio también que ha sido discutido. Sin embargo, ¿qué pudiera impedir que este documento sea considerado como un principio de prueba por escrito?

En todo caso, será el juzgador quien le dé la valoración conveniente haciendo uso de la sana crítica, siendo el sistema de valoración aceptado por nuestro ordenamiento, por lo que será quien considere la seguridad de los medios utilizados para lo cual, va a tener que designar un perito para que realice un estudio técnico y tecnológico de las pruebas presentadas. De esta forma, el juez tendrá que expresar en su resolución la valoración de todas las pruebas producidas.

2. Requisitos de Validez de un Documento Electrónico

Para que el documento electrónico pueda alcanzar la calidad de documento probatorio, es necesario que al menos cumpla con cuatro requisitos básicos, mismos que son considerados por Julio Téllez Valdés, en su obra denominada "Derecho Informático", los cuales son los siguientes:

a) Inalterabilidad.

Para que los documentos electrónicos puedan ser admisibles como un medio probatorio, deben tener carácter de permanencia. "El temor sobre la posibilidad de reinscripción o reutilización de los soportes informáticos, se dice, disminuye su seguridad y confiabilidad." (Téllez Valdés, 2004)

b) Autenticidad.

Los documentos son auténticos cuando los mismos no han sufrido ningún tipo de alteración que varíe su contenido, mientras más seguridad tiene el documento, menor es la posibilidad de que pueda ser alterado, y a su vez, se vuelve más fácil verificar algún tipo de alteración. Por lo tanto, este requisito, está completamente vinculado a la inalterabilidad.

c) Durabilidad.

Se refiere a que el documento debe ser definitivo, y, que "importe una modificación irreversible del soporte"[6] (Téllez Valdés, 2004). De esta forma, es muy complicada su alteración al momento de su conservación, situación que sucede con los documentos en soporte de papel, pues al momento de almacenarlos, con el paso del tiempo absorbe cierto tipo de partículas que pueden distorsionar su contenido.

d) Seguridad.

Para que tenga validez un documento electrónico, también es necesario que existan firmas de responsabilidad según las condiciones ya analizadas en los capítulos anteriores, teniendo en cuenta las obligaciones y responsabilidades que debe tener el peticionario del documento o emisor de la firma electrónica,

[6] Modificación irreversible del soporte, se refiere a la imposibilidad de poder reinscribir el texto del soporte. (Téllez Valdés, 2004)

siendo ésta una condición esencial, ya que de esta forma puede alcanzar el mismo valor que los documentos en soporte de papel.

A parte de los requisitos anteriormente mencionados, en caso de que sean instrumentos solemnes, tendrán que reunir los requisitos específicos para ser tales.

3. Problemas en la valoración de un Documento Electrónico.

En el medio que actualmente vivimos, considerado como una etapa de cambios en lo que concierne la tecnología, mismo que ha dado pasos agigantados en las últimas décadas, se ha vuelto bastante común que la sociedad tenga dudas con respecto a la validez de los documentos electrónicos al momento de incorporarlos como un medio de prueba, recalcando que no solo los particulares, sino son los mismos jueces quienes llegan a cuestionar tal validez probatoria, y esto se da por el simple hecho de que no ha existido la capacitación técnica para operar computadores y consiguientemente, trabajar con documentos electrónicos, ni con todo lo concerniente al Comercio Electrónico, a pesar de que nuestro ordenamiento ya lo ha reconocido desde hace unos años atrás.

Se debe considerar también, que no solamente la falta de capacitación de los funcionarios públicos es un problema, sino también el hecho de que no se ha

podido contar con la infraestructura técnica necesaria que pueda permitir y desarrollar su práctica dentro de los juzgados y tribunales.

Esta situación no solo afecta nuestro país, por citar un ejemplo, la legislación chilena también reconoce a los documentos electrónicos como medios de prueba dentro de un juicio, sin embargo, el problema viene cuando el administrador de justicia va a valorar dicha prueba, es decir, no encuentra un mecanismo para poder reproducirla y por ende ya no se vuelve eficaz, recalcando que no es por falta de reconocimiento jurídico.

Por lo tanto, al momento en que se vaya a reproducir las pruebas dentro de un proceso en el que haya también un documento electrónico, es necesario contar con algún tipo de dispositivo que pueda reproducir dicha prueba y pueda llegar a los sentidos de los destinatarios, como por ejemplo el caso de un correo electrónico contenido en un CD, y de esa forma el juez, a través de sus sentidos, va a poder valorarla de mejor manera.

Así también, nos encontramos frente a otro problema que está estrechamente relacionado con lo expuesto anteriormente, y es con respecto de quién va a proveer los recursos necesarios para reproducir la prueba. El criterio lógico nos llevaría a pensar que debería ser responsabilidad de la parte quien presenta esa prueba, poniendo a disposición del juzgador los elementos necesarios para

que la prueba pueda ser eficazmente reproducida, en caso de que no lo hagan los propios tribunales y juzgados.

4. Análisis de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y su Reglamento

Con el desarrollo de la tecnología y el avance del comercio electrónico el Estado Ecuatoriano se ha preocupado de expedir una ley que regule esta nueva forma de Comercio, por lo cual publica en el Registro oficial No. 557 el 17 de abril de 2002 una nueva ley, la de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, siendo ésta un avance muy significativo encuadrándose en las nuevas exigencias que están presentes en la actualidad.

La Ley de Comercio Electrónico además de explicar lo que debemos entender por esta nueva forma de comercio, se encarga también de salvaguardar los intereses de la colectividad, trayendo modificaciones en el ámbito penal, al referirse a Delitos contra la información protegida, Destrucción maliciosa de documentos, Falsificación Electrónica, Daños informáticos, etc., los mismos que serán estudiados posteriormente.

Ésta es una ley que ha tratado de cubrir con la mayoría de aspectos que se derivan del comercio electrónico. El comercio electrónico, al ser un concepto nuevo, es probable que su aceptación empiece a causar resistencia, de esta

forma esta ley trata a la confidencialidad, reserva, conservación, protección y autenticidad de los datos, descritos en los artículos 4, 5, 8 y 9, hablando de su importancia; la procedencia e identidad de un mensaje de datos, su envío y recepción de datos se tratan en los artículos 10 y 11 y en cuanto a la duplicación de mensajes de datos en el artículo 12.

La firma electrónica se conceptualiza y reconoce su validez jurídica en los artículos 13, 14 y del 52 al 56, sus características de autenticidad, integridad y confidencialidad descritas en el artículo 15; en el 16 se especifica el envío de la firma electrónica en unión lógica con el mensaje de datos. El artículo 17 habla de las obligaciones del uso de la misma ante la ley y la entidad de certificación; el 18 establece su tiempo de duración y en el 19 los motivos para que se extinga. Los artículos 20, 21 y 22 tratan los certificados de firma electrónica, siendo indispensables para establecer la identidad de quien envía el mensaje de datos, desde el 23 al 27 explica la duración del certificado de la firma electrónica, su extinción, suspensión y revocatoria; su reconocimiento internacional se explica en el artículo 28.

Desde el articulo 29 al 35, expresa la existencia de entidades de certificación de información como empresas autorizadas por el CONATEL, que presten el servicio de certificación de información y sometidas al mandato de la SUPTEL para la suspensión o revocatoria de los certificados; en el artículo 36 nos

explica que para efectos de esta ley, se ha asignado al Consejo de Comercio exterior e inversiones COMEXI como el organismo de promoción y difusión del comercio electrónico y firma electrónica; en los artículos 37, 38 y 39 se nombra al CONATEL como organismo regulador que autoriza y registra las entidades de certificación, actuando bajo dirección de la SUPTEL que es el organismo de control de las entidades de certificación de información.

Desde el artículo 44 al 47 se expresa la validez jurídica a transacciones mercantiles, financieras o de servicios y a los contratos electrónicos, y en caso de conflictos se someterán a las reglas establecidas en el COGEP. Los artículos 48 al 50 hacen referencia al derecho de los consumidores de servicios electrónicos. Así también, se reconoce a los mensajes de datos conferidos por entidades de certificación de información como instrumentos públicos electrónicos con validez jurídica en el artículo 51. Y finalmente, desde el artículo 57 al 64 encontramos las infracciones informáticas

5. Análisis de la Legislación Ecuatoriana y Legislación Comparada

Colombia

En primer lugar, se empezará este análisis con Colombia, en virtud de que es un país relativamente parecido al Ecuador, tanto en su realidad económica como en la jurídica. De esta forma, ellos han tenido un desarrollo tecnológico

en el aspecto jurídico bastante avanzado y notorio, y por ende satisfactorio. En su legislación, toda la instauración de la digitalización y sistematización del área judicial se realiza por medio del Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la ley número 527 de 1999, en la que se instaura dentro de su legislación el reconocimiento legal del mensaje de datos, la firma digital, el comercio electrónico y la certificación electrónica, tal como manifiesta el Artículo 5 de la mencionada ley, *"RECONOCIMIENTO JURÍDICO DE LOS MENSAJES DE DATOS. No se negarán efectos jurídicos, validez o fuerza obligatoria a todo tipo de información por la sola razón de que esté en forma de mensaje de datos."* Así también, existe la ley número 962 de 2005 denominada como la ley anti trámite, la cual contiene todos los elementos legales necesarios para facilitar las gestiones con la administración pública por medio del uso de las tecnologías de la información y comunicación, reconociendo el uso de documentos electrónicos por medios tecnológicos, tal como nos expresa el parágrafo segundo, numeral cuarto del artículo 1 de la mencionada ley:

> **4. Fortalecimiento tecnológico**. Con el fin de articular la actuación de la Administración Pública y de disminuir los tiempos y costos de realización de los trámites por parte de los administrados, se incentivará el uso de medios tecnológicos integrados, para lo cual el Departamento

> Administrativo de la Función Pública, en coordinación con el Ministerio de Comunicaciones, orientará el apoyo técnico requerido por las entidades y organismos de la Administración Pública.

Como se puede observar, dentro de esta ley, existe algo muy interesante, pues brinda la facultad de que cada institución podrá imponer sus propias condiciones para el uso de medios tecnológico, siendo esto bastante permisivo en el área legal, pero de importante uso funcional debido a que cada institución particularmente debe implementar y reglamentar el uso de TICS.

España

Es importante el análisis de la legislación española, pues es un país en el que se instauró el uso de las tecnologías de la información y la comunicación dentro de sus instituciones notariales, sin embargo se debe recalcar que su realidad económica y legal es muy diferente a la ecuatoriana, pero la propuesta se manifiesta como un proceso de desarrollo el cual proporciona ventajas, entendiéndolo como un ejemplo para nuestra legislación.

En un período desde el año 1997 hasta el 2007, se ha ido cimentando la administración electrónica, pues este país no solo trabaja en la desmaterialización de documentos, sino también, para que gradualmente todos los actos judiciales, sean estos procesos o resoluciones, puedan manejarse de

forma electrónica, de tal forma que se transforma la organización administrativa estatal y como consecuencia de esto, el funcionamiento en la rama judicial.

La Carta Magna Española, ha dictado normas que limitan el uso de la Informática, para así poder garantizar el respeto al honor y a la intimidad personal, como nos manifiesta el Artículo 18.4 de la mencionada ley "…4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

Esta ley ha ido desarrollando a otras de gran trascendencia como por ejemplo la Ley 30/1992, que trata sobre el Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo. El Artículo 38 numeral 4 nos manifiesta:

> Las solicitudes, escritos y comunicaciones que los ciudadanos dirijan a los órganos de las Administraciones Públicas podrán presentarse:
>
> a) En los registros de los órganos administrativos a que se dirijan.
> b) En los registros de cualquier órgano administrativo, que pertenezca a la Administración General del Estado, a la de cualquier Administración de las Comunidades Autónomas, o a la de alguna de

las Entidades que integran la Administración Local si, en este último caso, se hubiese suscrito el oportuno Convenio.

c) En las oficinas de Correos, en la forma que reglamentariamente se establezca

d) En las representaciones diplomáticas u oficinas consulares de España en el extranjero.

e) En cualquier otro que establezcan las disposiciones vigentes.

Mediante convenios de colaboración suscritos entre las Administraciones Públicas, se establecerán sistemas de intercomunicación y coordinación de registros que garanticen su compatibilidad informática y la transmisión telemática de los asientos.

A su vez, el Artículo 45 de la misma ley expresa:

Incorporación de medios técnicos.

1. Las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que a la utilización de estos medios establecen la Constitución y las Leyes.

2. Cuando sea compatible con los medios técnicos de que dispongan las Administraciones Públicas, los ciudadanos podrán relacionarse con ellas para ejercer sus derechos a través de técnicas y medios electrónicos, informáticos o telemáticos con respecto de las garantías y requisitos previstos en cada procedimiento.

3. Los procedimientos que se tramiten y terminen en soporte informático garantizarán la identificación y el ejercicio de la competencia por el órgano que la ejerce.

4. Los programas y aplicaciones electrónicas, informáticos y telemáticos que vayan a ser utilizados por las Administraciones Públicas para el ejercicio de sus potestades, habrán de ser previamente aprobados por el órgano competente, quien deberá difundir públicamente sus características.

5. Los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y

conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por ésta u otras Leyes.

En estas normas se observan que se han previsto sistemas de comunicación y coordinación de registros que garanticen la compatibilidad informática y la transmisión telemática de los asientos así como el mandato explícito para lograr la impulsión del empleo y aplicación de las técnicas y medios electrónicos y telemáticos para el desarrollo de la actividad administrativa, en el ejercicio de sus respectivas competencias.

Esta Ley, a su vez es complementada con el Real Decreto (RD) 263/1996, de 21 de febrero, la misma que en su Artículo 1 nos dice que " El presente Real Decreto tiene por objeto regular la utilización de las técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado y, cuando ejerzan potestades administrativas, por las entidades de derecho público vinculadas o dependientes de aquélla, en el ejercicio de sus competencias y en el desarrollo de sus actividades, así como en sus relaciones internas o externas."

Así también, han existido modificaciones adoptadas en materia hipotecaria, notarial y de Registro Mercantil, las cuales están contenidas en el RD

1867/1998, de 4 de septiembre, pues se regula la utilización de medios informáticos proponiendo la existencia de una red de intercomunicación entre Registros, así como también, la posibilidad de recibir solicitudes de notas simples presentadas en otros Registros; la comunicación obligatoria de los Registradores por fax, correo electrónico o cualquier otro medio técnico, y, directamente, con el Índice General Informatizado de Fincas y Derechos, a que se refiere el Artículo 388.c del Reglamento Hipotecario (Artículo 332.7, 8 y 9).

Por lo expuesto, la legislación española no solo reconoce y promueve el uso de los medios electrónicos en casi todas sus materias, sino además, considera al soporte magnético que contiene información como equivalente al documento tradicional, dándole el adjetivo de electrónico, pues asi lo podemos observar en el Artículo 45 de la Ley 30/1992 sobre el Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común:

> Los documentos emitidos cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copia de los originales almacenados por estos mismos medios, gozarán de la validez y eficacia del documento original, siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado,

así como el cumplimiento de las garantías y requisitos exigidos por ésta u otras leyes.

Además el Artículo 230 de la Ley Orgánica del Poder Judicial, en sus numerales 1 y 2 manifiestan que:

1. Los Juzgados y Tribunales y las Fiscalías están obligados a utilizar cualesquiera medios técnicos, electrónicos, informáticos y telemáticos, puestos a su disposición para el desarrollo de su actividad y ejercicio de sus funciones, con las limitaciones que a la utilización de tales medios establecen el Capítulo I bis de este Título, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y las demás leyes que resulten de aplicación. Las instrucciones generales o singulares de uso de las nuevas tecnologías que el Consejo General del Poder Judicial o la Fiscalía General del Estado dirijan a los Jueces y Magistrados o a los Fiscales, respectivamente, determinando su utilización, serán de obligado cumplimiento.

2. Los documentos emitidos por los medios anteriores, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el

cumplimiento de los requisitos exigidos por las leyes procesales." Por lo tanto, el documento electrónico, ha sido admitido por esta legislación, dándole validez y eficacia.

Chile

En el año 2002 fue aprobada en Chile la Ley 19799 que regula el uso de la firma electrónica, en la cual se indica el procedimiento de acreditación al que se debe sujetar los prestadores de servicio de certificación de firma electrónica, contando también con principios reguladores, tales como la libre competencia, la neutralidad tecnológica y la equivalencia del soporte técnico al papel. Dentro de esta ley, se señala que los documentos electrónicos con calidad de instrumento público, deberán suscribirse mediante firma electrónica avanzada, pero, ¿a qué se refiere con firma electrónica avanzada? La misma ley la define en su artículo 2 literal g) *"Firma electrónica avanzada: aquella certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría…"*

De esta forma, se puede observar que la legislación chilena reconoce los documentos electrónicos, y no solo eso, sino los eleva a categoría de instrumento público, por lo tanto, son medios probatorios eficaces siguiendo las reglas del artículo 5 de la ley ibídem

> Los documentos electrónicos podrán presentarse en juicio y, en el evento de que se hagan valer como medio de prueba, habrán de seguirse las reglas siguientes:
>
> 1.- Los señalados en el artículo anterior, harán plena prueba de acuerdo con las reglas generales, y
>
> 2. Los que posean la calidad de instrumento privado, en cuanto hayan sido suscritos con firma electrónica avanzada, tendrán el mismo valor probatorio señalado en el número anterior. Sin embargo, no harán fe respecto de su fecha, a menos que ésta conste a través de un fechado electrónico otorgado por un prestador acreditado.
>
> *En el caso de documentos electrónicos que posean la calidad de instrumento privado y estén suscritos mediante firma electrónica, tendrán el valor probatorio que corresponda, de acuerdo a las reglas generales.*

Venezuela.

Venezuela es el país en donde más tarde incorpora en sus normas el uso de los medios electrónicos, ya que recién en el año 1999, con la Constitución de la República Bolivariana de Venezuela se expresa la regulación del uso de la Informática, tal como menciona el Artículo 60 de la norma en mención *"Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos."*

Además de la Norma Constitucional, se regula el uso de los medios electrónicos en el Artículo 162, ordinal 3º del Código Orgánico Tributario, refiriéndose a la forma de practicar las notificaciones, así, señala que estas pueden realizarse "…mediante correo público o privado, por sistemas de comunicación telegráficos, facsimilares, electrónicos y similares siempre que se deje constancia en el expediente de su recepción*".*

En el 2001, con la puesta en vigencia del Decreto con Fuerza de Ley de Mensajes de Datos y Firmas Electrónicas, que se reconoce el valor probatorio de los medios electrónicos, de esta forma, el Artículo 4º del mencionado

Decreto, señala que los Mensajes de Datos gozarán de la misma eficacia probatoria que la ley le otorga a los documentos que constan en formato papel.

También es importante señalar que en aquellos casos en que la ley exija de la firma autógrafa para que un negocio jurídico surta efectos, quedará satisfecho al tener incorporada una firma electrónica. Por último, otro aspecto relevante que incorpora este Decreto es el principio de Neutralidad Tecnológica, mediante el cual no existe inclinación hacia una tecnología en particular, y que ha sido explicado previamente.

CAPITULO IV

Las infracciones informáticas

1. Marco Conceptual

De todo lo expuesto en capítulos anteriores, se considera que el Internet es una herramienta muy trascendente dentro de nuestra vida cotidiana, pues es ofrece a todo el mundo, de manera ilimitada, la facilidad de expresarse con gran libertad, de manera eficaz y eficiente ya sea mediante la publicación de contenidos en páginas personales, fotografías o aportaciones en foros y correo electrónicos.

Sin embargo, se debe recalcar que esa libertad ilimitada de expresión y el anonimato con que se aporta a la red, también se han llevado a cabo conductas poco lícitas y molestas contra personas, llegando así a calumnias e injurias, distorsionando esta herramienta dándole un mal uso.

Desde el año de 1995 se han producido varios debates con respecto a la necesidad de prevenir y sancionar estos malos usos en la red Internet, lo cual obliga a localizar las distorsiones más habituales que se producen y analizar los argumentos que se han dado a favor de una legislación que regule el uso de la red y los criterios contrarios a esa regulación.

Hay quienes se apoyan en la tesis de que las redes de telecomunicaciones, tales como el Internet, han generado un submundo en el que los delitos son difíciles de perseguir por su propia naturaleza y la falta de tipificación de las modalidades de comisión y medios empleados. Frente a ello, se ha considerado la necesidad de proteger el derecho a la intimidad pero también a la libertad de expresión, teniendo equilibrio entre ambos derechos.

En la actualidad, el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto.

Por la trascendencia del tema, se ha visto la necesidad de definir a este tipo de conductas ilícitas, en primer lugar, tenemos a la Organización de Cooperación y Desarrollo Económico (OCDE), misma que ha definido el término “delitos relacionados con las computadoras” como “cualquier comportamiento antijurídico, no ético o no autorizado, relacionadoo con el procesado automático de datos y / o transmisiones de datos”

A su vez, Jijena Leiva habla de “toda acción típica antijurídica y culpable para cuya consumación se usa la tecnología de las computadoras, o se afecta la

información contenida en un sistema de tratamiento automatizado de datos y la transmisión de datos." (Leiva, 2009)

Asimismo Klaus Tiedmann afirma que "con la expresión criminalidad mediante computadoras se alude a los actos antijurídicos según la ley penal vigente realizados con el empleo de un equipo automático de procesamiento de datos"

El autor Julio Téllez Valdez, en su obra Derecho Informático, señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)."

De esta forma, se puede apreciar que a medida de que ha ido creciendo la tecnología, de la misma forma han llegado a desarrollarse los delitos informáticos, por lo que empiezan a tener un alto grado de trascendencia dentro de la sociedad, llegando al punto de ser una amenaza para la economía de un país y por su puesto para la sociedad

2. Bien jurídico protegido

Al hablar del bien jurídico protegido se debe tener como idea principal que nos estamos refiriendo al objeto de protección; es decir, es necesario que exista un

bien jurídico que se esté vulnerando o se encuentre en riesgo, para que exista un motivo jurídico para tipificar la conducta que atenta contra este como un delito penal. En el caso de los delitos informáticos, tal objeto se vuelve un tanto impreciso delimitar los derechos que han sido vulnerados, pues aparentemente dependería de la acción u omisión específica que se haya transgredido para así poder determinarlo.

Una de las mayores dificultades que se presentan al momento de legislar sobre los delitos informáticos es la falta de precisión y vaguedad que existe en la doctrina para determinar los intereses jurídicos que el legislador debe amparar. Al tipificar las conductas que puedan vulnerarlos.

Se puede decir que la tendencia es que la protección a los bienes jurídicos, se la realiza desde la perspectiva de los delitos tradicionales, con una re-interpretación teleológica de los tipos penales ya existentes, para subsanar las lagunas originadas por estos nuevos comportamientos delictivos. Como regla general, los bienes jurídicos protegidos, serán los mismos que los delitos re-interpretados teleológicamente o que se les ha agregado algún elemento nuevo para facilitar su persecución y sanción por parte del órgano jurisdiccional competente.

Por otro lado, hay quienes sostienen que se debe incorporar a la información como un bien jurídico sujeto de protección, tomando en cuenta las diferencias existentes entre la propiedad tangible y la intangible, sin embargo, a criterio de Pablo Palazzi, al ser un bien incorporal, debe ser tratada de la misma forma en que se aplica la legislación actual a los bienes corporales, pues éstos tienen un valor intrínseco compartido, siendo una valoración económica, por lo que la información y otros intangibles, son objetos de propiedad, misma que esta constitucionalmente protegida.

De esta forma, la protección de la información como bien jurídico protegido debe tener siempre en cuenta el principio de la necesaria protección de los bienes jurídicos que señala que la penalización de conductas se desenvuelva en el marco del principio de “dañosidad” o “lesividad”. Así, una conducta sólo puede conminarse con una pena cuando resulta incompatible con los presupuestos de una vida pacífica, libre y materialmente asegurada.

En conclusión, podemos decir que el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico, o por los sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como:

- **El patrimonio**, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar.
- **La reserva, la intimidad y confidencialidad de los datos**, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de bancos de datos.
- **La seguridad o fiabilidad del tráfico jurídico y probatorio**, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.
- **El derecho de propiedad**, en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los de daños y el llamado terrorismo informático.

De esta misma forma, Jijena Leiva ha encontrado tres bienes jurídicos que pueden ser afectados mediante el mal uso de la información, así:

- Si la información es nominativa o relacionada con las personas se atenta contra la intimidad;
- De ser económica o representar valores, se atenta contra el patrimonio y la propiedad, y
- Si es estratégica o relacionada con la seguridad o la soberanía de un Estado (siempre y cuando esté inserto en la comunidad internacional), estamos frente a la intimidad nacional. (Leiva, 2009)

Por lo tanto el bien jurídico protegido, a su vez, resguarda a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere.

Para los autores chilenos Claudio Magliona y Macarena López, los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir "que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo" (Echandía, 1991).

Por lo tanto, se puede manifestar que esta clase de delincuencia no solo afecta a un bien jurídico determinado, sino a la multiplicidad de conductas que la componen, es decir, afectan a una diversidad de ellos que ponen en relieve intereses colectivos, en tal la autora María Luz Gutiérrez Francés, manifiesta respecto de la figura del fraude informático que: "

> …las conductas de fraude informático presentan indudablemente un carácter pluriofensivo. En cada una de sus modalidades se produce una doble afección: la de un interés económico (ya sea micro o macrosocial), como la hacienda pública, el sistema crediticio, el patrimonio, etc., y la de un interés macrosocial vinculado al funcionamiento de los sistemas informáticos. (Francés, 2006)

De esta forma, con el nacimiento de esta nueva tecnología se está facilitando nuevos elementos para atentar contra bienes ya existentes tales como la intimidad, la seguridad nacional, el patrimonio, entre otros más; sin embargo, se ha ido obteniendo importancia nuevos bienes, como la calidad, pureza e idoneidad de la información y de productos de que ella se obtengan; la confianza en los sistemas informáticos; nuevos aspectos de la propiedad en cuanto recaiga sobre la información personal registrada o sobre la información nominativa, haciendo hincapié que este tipo de conductas criminales son de carácter pluriofensivo.

Para tener una mejor visión acerca del tema, se puede poner como ejemplo a un hacker, quien ingresa a un sistema informático con el fin de vulnerar su seguridad y averiguar la mayor cantidad de información sobre una persona determinada, en este caso se estaría lesionando el derecho a la intimidad que posee tal información ya que es vista por un extraño sin su autorización. Sin embargo, detrás de este bien jurídico, encontramos también un bien colectivo que conlleva al ataque a la confianza en el funcionamiento de los sistemas informáticos; es decir, no solo importa a la afección de bienes jurídicos clásicos, sino intereses socialmente valiosos afectados por estas nuevas figuras.

3. Sujetos de los Delitos informáticos

La ejecución de una conducta punible supone la existencia de dos sujetos, uno activo y el otro pasivo, las mismas que pueden ser una o varias personas, naturales o jurídicas, considerando también el bien jurídico protegido, el elemento localizador de los sujetos y de su posición frente al delito. Así entonces, analizaremos estos dos tipos de sujetos dentro de los delitos informáticos:

– **Sujeto Activo:** es cualquier persona que realiza toda o parte de una acción descrita por el tipo penal. Es muy acertado considerar que los sujetos que cometen este tipo de delitos poseen características que no presentan el denominador común de delincuentes, ya que estos sujetos tienen habilidades para el manejo de sistemas informáticos, como en el caso de los hackers quienes son expertos en romper sistemas de seguridad informática, quienes generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o en su defecto, son simplemente hábiles en el uso de estos sistemas informáticos sin desarrollar actividades laborales que faciliten la comisión de este tipo de delitos.

Según un estudio publicado en el Manual de Naciones Unidas en la prevención y control de delitos informáticos, el 90% de los delitos realizados mediante la

computadora fueron ejecutados por empleados de la propia empresa afectada. Así mismo, otro estudio realizado en América del Norte y Europa indicó que el 73% de las instrusiones informáticas cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los "**delitos informáticos**", estudiosos en la materia los han catalogado como "**delitos de cuello blanco**" término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943.

– **Sujeto Pasivo:** es la persona titular del bien jurídico que legislativamente ha sido protegido y sobre el que recae la acción u omisión típica, antijurídica del sujeto activo. Es necesario distinguir que en este tipo de delitos, las víctimas o sujetos pasivos pueden ser una o varias personas, naturales o jurídicas, y en algunos casos podría sufrir la sociedad misma, el gobierno, etc. Sus posibilidades de defensa respecto de los ataques de los sujetos activos son mínimas, por lo que se encuentra obligado a extremar sus medidas de seguridad que tiendan a evitar los delitos. Muchas veces se niegan a denunciar por razones de imagen y otras por desconocimiento o desconfianza en el éxito de encontrar responsables.

De lo expuesto, se puede colegir que ha sido imposible conocer la verdadera magnitud de los llamados delitos informáticos, pues la mayor parte de estos delitos no son descubiertos o no son denunciados a las autoridades responsables, sumándole a ello la falta de leyes que protejan a las víctimas de estos delitos, la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática, entre otros más, trayendo como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada "cifra oculta" o "cifra negra".

4. Delitos Informáticos.

La administración de justicia dentro de nuestra sociedad ha atravesado por una profunda transformación gracias a la aparición de las nuevas tecnologías de la información y las comunicaciones (TICs), las computadoras interconectadas en la red mundial denominada Internet son la muestra más clara del impacto que tienen en la actualidad, de tal forma que, también para las telecomunicaciones, el tráfico comercial y el entretenimiento, estas tecnologías son caracterizadas como indispensables. Por esta misma razón, el medio electrónico se ha convertido en un blanco perfecto para cometer un

sinnúmero de actos ilegales tales como el robo, el fraude, la suplantación de identidad, entre otros.

De todo lo analizado en capítulos anteriores, se puede deducir que la delincuencia informática es complicada de comprender o conceptualizar de forma plena, ya que la mayoría de los datos probatorios son intangibles y transitorios, considerándola también como una conducta aislada por la legislación, que implica la utilización de tecnologías para la comisión del delito.

Para analizar estas nuevas conductas delictivas, es necesario remitirnos a lo que nos dice el Código Orgánico Integral Penal, pues según su Disposición Derogatoria Novena, el título V, desde el artículo 57 al artículo 64 de la Ley de Comercio Electrónico, Firmas y Mensaje de Datos publicada en el suplemento del Registro Oficial No. 557 de 17 de abril de 2002 se encuentra derogada.

La mencionada Ley contiene una gran variedad de delitos relacionados con los medios electrónicos, por lo tanto, en la presente investigación serán analizados únicamente aquellos que van en contra del derecho a la propiedad y aquellos que van contra la seguridad de los activos de los sistemas de información y comunicación.

4.1 Delitos que van contra el derecho a la propiedad.

Artículo 186 del COIP.- ESTAFA: La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años.

La pena máxima se aplicará a la persona que:

1.- Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.

2.- Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copiar o reproducir información de tarjetas de crédito, débito, pago o similares…

La estafa informática está considerada como un delito que contiene los mismos elementos que la estafa ordinaria, el cual tiene como elemento central la conducta relativa al engaño, a la acción fraudulenta, por lo que la estafa

informática viene a ser una modalidad pero siempre dentro de la dogmática y criterios interpretativos propios de la estafa. Algunos doctrinarios sostienen en cambio que el elemento de engaño o error difiere de la estafa tradicional y que por lo tanto, la estafa informática conlleva una nueva figura penal. Sin embargo, lo relevante es que esta modalidad se caracteriza por la manipulación informática que debe conducir como objetivo al engaño de la víctima, ya que esta manipulación informática va a provocar el perjuicio patrimonial para un tercero, como el elemento requerido en todos los supuestos de estafa. El autor de la estafa siempre está guiado por el ánimo de lucro que es el elemento subjetivo que completa los elementos objetivos del hecho punible.

> **Artículo 190.- Apropiación fraudulenta por medios electrónicos.-** La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

> La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes."

Dentro del ámbito bancario, las víctimas de este delito son las personas naturales y jurídicas que realizan transacciones vía Internet o mediante sistemas informáticos que utilizan redes de tráfico de datos proporcionados por la institución financiera. La forma común en que se desenvuelve este delito es cuando el ciberdelincuente genera el ataque informático desde una terminal o servidor ubicado generalmente en otro país distinto a aquel en que se produce el resultado del delito. Con anterioridad, el atacante informático ha obtenido fraudulentamente el modo de vulnerar las claves y el acceso a la cuenta de la víctima (en muchos casos a través del pishing[7] o pharming[8]) y logra de esta

[7] Término utilizado para referirse a un método utilizado por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

[8] Es una modalidad de fraude cibernético que consiste en el re direccionamiento malintencionado de un sitio web de confianza a un sitio web malicioso. Este tipo de fraudes afecta principalmente a instituciones bancarias, debido a que este tipo de fraudes está diseñado para robo de datos

manera transferir los fondos que existen en dicha cuenta bancaria, a la cuenta de otra persona que también consta como cliente de dicho banco, o bien a las cuentas de usuarios de otras instituciones financieras. En algunos casos, el beneficiario de la transferencia no autorizada, desconoce que su cuenta bancaria fue utilizada, este es el caso denominado “uso de cuentas puente”, en las cuales el dinero transferido permanece por unas horas, mientras el ciberdelincuente elige el destino final de los fondos obtenidos; este tipo de triangulación en el desarrollo del delito, dificulta su persecución.

4.2 Delitos que van en contra a la seguridad de los activos de los sistemas de información y comunicación.

> **Artículo 229.- Revelación ilegal de base de datos.-** La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.
>
> Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular

y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

Antes de que entre en vigencia el COIP, la Ley Orgánica de Instituciones del Sistema Financiero establecía como delito la *violación al sigilo bancario*, con pena de prisión de uno a cinco años, siendo ésta, una figura que sancionaba toda conducta de los servidores bancarios cuando divulgan la información sujeta al sigilo y reserva bancaria, es decir, la información de operaciones activas y pasivas de los clientes de las instituciones financieras. Frente a ello, la actual ley penal, mantiene la protección de datos personales constantes ya sea en forma física o digital, bases de datos, sancionando a quien revele tal información, en el caso que fuere una persona con calidad de empleado bancario, se constituye un agravante, sancionándolo con pena privativa de libertad de tres a cinco años, entendiendo que no solo trae consecuencias penales, sino civiles también. El Artículo 155 del Código Orgánico Monetario y Financiero, establece que: *"*En los términos dispuestos por la Constitución de la República, este Código y la ley, los usuarios financieros tienen derecho a que su información personal sea protegida y se guarde confidencialidad*",* así mismo en los artículos 352 y 353 ibídem, se consagra la protección a los datos de carácter personal de los usuarios del sistema financiero nacional, pudiendo

entregar esta información únicamente al titular o a quien lo autorice. A su vez, se establecen varias sanciones administrativas sin perjuicio de la responsabilidad penal que conlleva la divulgación de esta información

Es necesaria la formación ética de los empleados bancarios, siendo ésta una de las medidas de seguridad que se deberían establecer en las instituciones del sistema financiero para el combate del cibercrimen, al igual que la desconcentración de funciones en varios empleados, de manera que no se permita que un determinado funcionario maneje muchos aspectos operacionales relacionados con el servicio al cliente a través de medios informáticos. Se debe recalcar que la mayor vulnerabilidad que puede tener una institución del sistema financiero del sector privado, no son sus sistemas o redes informáticas, sino más bien, la posibilidad de que sus empleados sean corrompidos y se vuelvan parte del ciberdelito a cambio de una recompensa económica.

Artículo 230.- Interceptación ilegal de datos.- "Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema

> informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible…

Este primer numeral del artículo mencionado, se refiere cuando por ejemplo el personal de una sala de escuchas trata de interceptar llamadas sin la respectiva orden judicial.

> 2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

Ejemplo: Las personas que diseñan programas para jaquear información de empresas o de personas importante en el mundo y cometer estafas perjudicando a la ciudadanía.

> *3.* La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u

otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Artículo 231.- Transferencia electrónica de activo patrimonial.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

La transferencia electrónica de activo patrimonial significa apropiarse de un activo patrimonial de otra persona sin el consentimiento de ella, perjudicándola

a la misma o a terceros, por medio de modificación, manipulación de un programa informático, o mensaje de datos, para apropiarse. Este delito será penado y si la persona diere su consentimiento para enriquecer su activo patrimonial por medio de una transferencia electrónica, será igualmente sancionado. Por ejemplo cuando un empleado de una institución financiera realiza transferencias electrónicas de dinero a su cuenta personal de la misma institución o de una tercera persona.

Artículo 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años. Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Al hablar de acceso ilegítimo a sistemas de información, se debe considerar que estamos frente al denominado *hacking,* que no es más que un conjunto de técnicas utilizadas para acceder a un sistema informático. De lo dicho, se debe entender que puede ser utilizado de una forma lícita y con el debido permiso, o se lo puede utilizar como un medio ilícito, vulnerando medidas de seguridad con las cuales se pueda ver afectado el titular de la cuenta.

Así mismo, la misma cultura hacker generó el término “crackers” para aludir a sujetos, diferenciándose por tener fines supuestamente más altruistas. Posteriormente, la doctrina receptó esta diferenciación manifestando que el intrusismo informático ilegítimo se refiere al hacking y el sabotaje informático al cracking, basándose en que el elemento subjetivo de éste último es la intencionalidad del agente de obstaculizar, dejar inoperante o dañar el funcionamiento de un sistema informático, mientras que en el primer caso, la

acción realizada busca únicamente el ingreso a tales sistemas sin dirigir sus actos a la afectación de la integridad o disponibilidad de la información, pero sí, a la confidencialidad y exclusividad de ella y en algunos casos, a vulnerar la intimidad del titular de aquélla.

> **Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.-** La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

En este artículo, el legislador se hace referencia a cuando una persona ingresa a un sistema informático o algún servidor de internet, y sin autorización del proveedor de éste, se mantenga dentro para proceder a modificar o re direccionar datos u ofrecer servicios a terceros sin el debido pago al dueño de

este programa; como por ejemplo las personas que se dedican a realizar los softwares piratas.

CONCLUSIONES

En el momento que se redactaron las disposiciones contenidas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, nuestros legisladores se basaron en el criterio del “equivalente funcional”, tomado de la Ley modelo de la Comisión de las Naciones Unidas para el derecho mercantil internacional (CNUDMI), criterio que procura buscar que la información constante en un soporte electrónico cumpla las mismas funciones que cumple la información cuanto está plasmada de una forma tradicional, es decir en papel.

De esta forma, al culminar el presente estudio, se puede llegar a las siguientes conclusiones:

1. En primer lugar, nuestro ordenamiento jurídico reconoce y da valor jurídico tanto a mensajes de datos como a la firma electrónica, de la misma forma que a los documentos en soporte de papel, sin embargo es necesario que los mismos cumplan requisitos específicos como lo que ya se han analizado a lo largo de la presente investigación, así como también, deben existir firmas de responsabilidad según las condiciones ya analizadas, teniendo en cuenta las obligaciones y responsabilidades

que debe tener el peticionario del documento o emisor de la firma electrónica siendo ésta una condición esencial.

2. Otro punto interesante es que existen también instrumentos públicos electrónicos, siendo éstos mensajes de datos en soporte electrónico, en el cual se registra la voluntad de las partes que intervienen en un acto o negocio jurídico otorgados por la autoridad competente, quien deberá dejar constancia del medio empleado y conservar una versión íntegra para una posterior consulta dentro de su archivo, la ley menciona como ejemplo de autoridad competente los Notarios Públicos.
3. El Notario Público cumple con un papel estratégico e importante dentro de nuestra sociedad, pues es quien brinda certeza en las relaciones entre los particulares, ajustando su voluntad a lo que se encuentra establecido en la ley. Así también, es el encargado de dotar esa fe pública y certificar la desmaterialización del documento electrónico.
4. Finalmente, pueden así mismo, existir fraudes en la utilización de este tipo de documentos e instrumentos, llamados delitos informáticos, y éstos no solo afecta a un bien jurídico determinado, sino que tienen carácter de ser pluriofensivos o complejos, es decir, atacan simultáneamente a varios bienes jurídicos protegidos.

RECOMENDACIONES

Al finalizar la realización del presente proyecto y luego de haber analizado a profundidad los documentos electrónicos dentro de nuestra legislación ecuatoriana, me permito recomendar que debe existir una correcta y permanente capacitación informática por parte de los Notarios Públicos como de las entidades de certificación que trata la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, pues no ha existido una unanimidad de criterios en la práctica, siendo casi imposible que se pueda tener una correcta certificación de documentos de esta clase, siendo ésta una razón por la cual los legisladores no la pueden admitir a para probar hechos que se configuran dentro de la vida cotidiana.

De la misma forma, el sistema jurídico en el que vivimos debe ser riguroso en este aspecto, para que de esta forma, nos obligue a tener en cuenta las regulaciones de la ley y el verdadero procedimiento de los mismos.

CASO PRÁCTICO

INJURIAS. Expediente 553, Registro Oficial Suplemento 358, 12 de Junio del 2008.

No. 553-2006.

El Sr. Guido José Páez Puga, interpone una querella por el delito de injurias calumniosas en contra de la señora MARÍA AUGUSTA GALARZA DÁVILA DE ESPINOSA, quien es Asistente de Presidencia de la compañía AUTEC S.A., misma empresa donde labora el denunciante.

El señor Páez manifiesta que la denunciante profirió una serie de injurias calumniosas en su contra, mediante correo electrónico enviado desde la dirección electrónica: augusta.espinosa@autec-mb.com, con copia a tres personas más, en el cual se expresaba de la siguiente forma: "El Sr. Páez ha sido separado de Autec y los abogados han entablado una acción judicial en su contra con los cargos de abuso de confianza, disponibilidad indebida de fondos y boicot".

Sin embargo, tanto en el Juzgado Décimo Tercero de lo Penal de Pichincha, como en la Primera Sala Penal de la Corte Superior de Justicia de Quito desecha la querella por improcedente y dicta sentencia absolutoria a favor de

María Augusta Galarza Dávila, declarando a la vez que la acusación particular no es maliciosa ni temeraria.

El recurrente, presenta recurso de casación en el año 2006, en la que manifiesta que se ha violado el Art. 491 del Código Penal Ecuatoriano, en cuanto el delito de injuria calumniosa puede cometerse no solamente por las imputaciones que se hace en reuniones y lugares públicos, en presencia de diez o más individuos, sino también los que se hacen "…por medio de escritos, impresos o no…", pues los que establece el artículo mencionado, corresponden a ejemplos pudiéndose utilizar, como en este caso, otros tales como el correo electrónico, siendo así que defiende su teoría citando al Art. 2 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos, la que dice: "Los mensajes de datos tendrán igual valor jurídico que los documentos escritos". Se fundamenta también en el inciso segundo del Art. 121 del Código de Procedimiento Civil, el cual expresa que como medios de prueba se admitirán *"las grabaciones magnetofónicas, las radiografías, las fotografías, las cintas cinematográficas, los documentos obtenidos por medios técnicos, electrónicos, informáticos, telemáticos o de nueva tecnología. La parte que los presente deberá suministrar al juzgado en el día y hora señalados por el juez los aparatos o elementos necesarios para que pueda apreciarse el valor de los*

registros y reproducirse los sonidos o figuras. Estos medios de prueba serán apreciados con libre criterio judicial según las circunstancias en que hayan sido producidos"

Consideraciones de la Sala:

La Sala considera el reconocimiento jurídico del correo electrónico mediante diligencia pericial practicada en el centro de cómputo de la Función Judicial de Pichincha y cuyo informe pericial técnico informático concluye diciendo: "Que el mensaje electrónico remitido el 12 de agosto del 2005, desde la dirección GinoSaer@Freightliner.com y almacenado en el buzón de mensajes de la dirección electrónica Guido.paez@hotmail.com es auténtico y no se encuentra modificado en su contenido de este buzón".

Por lo tanto, una vez que se ha establecido que realmente el correo electrónico ha sido el medio por el cual se difundieron las injurias, la Sala hace un análisis para determinar que tal medio probatorio es expresamente reconocido por nuestra legislación, por lo que se expresa en la sentencia que: "No se ha incorporado aún como elemento del tipo, el correo electrónico como medio o instrumento del que pueda servirse el ofensor para cometer un delito de injuria calumniosa". Al respecto, el Artículo 149 inciso primero del Código de Procedimiento Penal, en el que se refiere a la Prueba Documental, manifiesta

que *"Los fiscales, jueces y tribunales pueden requerir informes sobre datos que consten en registros, archivos, incluyendo los informáticos"*; por otro lado, en el Art. 156 del mismo cuerpo legal, se expresa que *"El Juez autorizará al fiscal para el reconocimiento de las grabaciones mencionadas en el artículo, así como de películas, registros informáticos, fotografías, discos u otros documentos semejantes…"*, disposición legal que tiene como medios supletorios de prueba, los que constan en el Art. 121 del Código de Procedimiento Civil. La Tribunal ad quem asevera que para la comisión de delitos de injurias, no existe ninguna exclusión que impida producirlo a través de un correo electrónico como medio de prueba, teniendo en cuenta que en la actualidad, la comunicación comercial, noticiera, personal, privada, reservada y otras, se hace casi exclusivamente por medios electrónicos, por eso es que, el legislador, de manera sabia y a fin de impedir la impunidad de los delitos cometidos por medios electrónicos, ha hecho una realidad la aplicación del avance tecnológico como medios probatorios de la conducta delictiva y no solamente que las ha insertado en nuestra legislación, sino que además, ha dictado la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Así también, se analiza que la experticia pericial constante dentro del proceso tiene plena validez, ya que ha sido ordenada por el Juez de la causa y practicada por peritos legalmente designados para este efecto, supliendo así la necesidad de ser certificada por un notario público o autoridad competente, conforme lo que manda el Art. 4 del Reglamento a la Ley de Comercio Electrónico. Por lo tanto, la falsa imputación de varios delitos supuestamente cometidos por el ciudadano Guido José Páez Puga tales como el abuso de confianza, disponibilidad indebida de fondos y boicot, que fueron difundidos con la deliberada intención de causar daño a la honra, reputación y dignidad del acusador, constituyen la comisión del delito de injurias, pues existe el "animus injuriandi", elemento fundamental de la injuria calumniosa, de parte de la señora María Augusta Galarza Dávila de Espinosa.

Resolución:

De conformidad con lo que establece el Art. 358 del Código de Procedimiento Penal, el Tribunal acepta el recurso interpuesto, casa la sentencia y condena a la señora María Augusta Galarza Dávila de Espinosa.

GLOSARIO

B

Bits: es un dígito del sistema de numeración binario, es la unidad mínima de información empleada en informática, en cualquier dispositivo digital, o en la teoría de la información. Con él, podemos representar dos valores cualesquiera, como verdadero o falso, abierto o cerrado, blanco o negro, norte o sur, masculino o femenino, rojo o azul, etc. Basta con asignar uno de esos valores al estado de "apagado" (0), y el otro al estado de "encendido"

C

Certificado electrónico de información: Es el mensaje de datos que contiene información de cualquier tipo.

Criptología es la ciencia que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicaciones. Sus objetivos son la privacidad o confidencialidad de los datos, garantizando la autenticación de los mismos, su integridad y su no repudio.

Comercio Electrónico: Es toda transacción comercial realizada en parte o en su totalidad, a través de redes electrónicas de información.

D

Datos de creación: Son los elementos confidenciales básicos y necesarios para la creación de una firma electrónica.

Datos personales: Son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta Ley.

Datos Personales Autorizados: Son aquellos datos personales que el titular ha accedido a entregar o proporcionar de forma voluntaria, para ser usados por la persona, organismo o entidad de registro que los solicita, solamente para el fin para el cual fueron recolectados, el mismo que debe constar expresamente señalado y ser aceptado por dicho titular.

Desmaterialización electrónica de documentos: Es la transformación de la información contenida en documentos físicos a mensajes de datos.

Destinatario: Persona a quien va dirigido el mensaje de datos. Signatario: Es la persona que posee los datos de creación de la firma electrónica, quién, o en cuyo nombre, y con la debida autorización se consigna una firma electrónica.

Dispositivo de comprobación: Instrumento físico o lógico utilizado para la validación y autenticación de mensajes de datos o firma electrónica.

Dispositivo de emisión: Instrumento físico o lógico utilizado por el emisor de un documento para crear mensajes de datos o una firma electrónica.

Dispositivo electrónico: Instrumento físico o lógico utilizado independientemente para iniciar o responder mensajes de datos, sin intervención de una persona al momento de dicho inicio o respuesta.

E

Emisor: Persona que origina un mensaje de datos.

I

Intimidad: El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta Ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros, a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.

M

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

P

Phishing: Término utilizado para referirse a un método utilizado por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

Pharming: Es una modalidad de fraude cibernético que consiste en el re direccionamiento malintencionado de un sitio web de confianza a un sitio web malicioso. Este tipo de fraudes afecta principalmente a instituciones bancarias, debido a que este tipo de fraudes está diseñado para robo de datos**.**

R

Red Electrónica de Información: Es un conjunto de equipos y sistemas de información interconectados electrónicamente.

S

Servicio Electrónico: Es toda actividad realizada a través de redes electrónicas de información

Shopify: fue fundada en 2006 por Tobias Lütke (premio al CEO del año en Canadá), Scott Lake y Daniel Weinand. Desde su lanzamiento, la plataforma ha ido creciendo rápidamente hasta convertirse en uno de los líderes en soluciones de comercio electrónico. Actualmente, la compañía abastece a más de 150.000 tiendas online.

BIBLIOGRAFÍA

- Corporación de Estudios y Publicaciones. CÓDIGO ORGÁNICO GENERAL DE PROCESOS. Quito, 2015.
- Corporación de Estudios y Publicaciones. CÓDIGO ORGÁNICO INTEGRAL PENAL. Quito, 2014.
- Corporación de Estudios y Publicaciones. LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS. Quito, 2010.
- Alessandri, Arturo. CURSO DE DERECHO CIVIL, Editorial Nascimiento, Santiago de Chile, 1970.
- Aranzandi, Thomson. ASPECTOS JURÍDICOS DEL COMERCIO ELECTRÓNICO EN INTERNET, Editorial Aranzadi S.A., 2003.
- Bescós, Modesto. FORMAS CONTRACTUALES EN EL COMERCIO ELECTRÓNICO, Editorial El Comercio en la Sí, 2004.
- Borda, Guillermo. TRATADO DE DERECHO CIVIL ARGENTINO, Editorial Abeledo – Perrot, 1999.
- Carillo, Mariana. EL CONTRATO ELECTRÓNICO COMO FUENTE DE LAS OBLIGACIONES, Colección Libros Homenaje, 2011.

- Dans, Enrique. COMERCIO ELECTRÓNICO. http://profesores.ie.edu/enrique_dans/download/ecommerce.pdf. Web 18 de Noviembre 2016.
- García, Gemma. NOCIÓN DEL COMERCIO ELECTRÓNICO Y PROTECCIÓN DE LOS CONSUMIDORES, Editorial La Ley, Madrid, 2001.
- Gutierrez, Álvaro. EL COMERCIO ELECTRÓNICO, Editorial Abeledo – Perrot, Buenos Aires, 2010.
- Herrmann, Patricia. COMERCIO ELECTRÓNICO, Loja, 2005.
- Illescas, Rafael. DERECHO DE LA CONTRATACIÓN ELECTRÓNICA, Civita Ediciones, Madrid, 2001.
- Lorenzetti, Ricardo. LOS CONTRATOS ELECTRÓNICOS, Ediciones Abeledo – Perrot, Buenos Aires, 2002.
- Martínez, Apolonia. COMERCIO ELECTRÓNICO, FIRMA DIGITAL Y AUTORIDADES DE CERTIFICACIÓN, Civita Ediciones, Madrid, 2001.
- Téllez, Julio. DERECHO INFORMÁTICO, McGraw-Hill Interamericana Editores S.A., Ciudad de México, 2004.
- Vargas Hinostrosa, Luis. PRACTICA FORENSE CIVIL, Pudeleco Editores S.A., Quito, 2006.