RESUMEN

En la actualidad nos encontramos frente a una revolución tecnológica que se despliega a pasos agigantados, y por ello debemos estar preparados para afrontar todos los retos que nos presenta este nuevo milenio.

La tecnología, en nuestra sociedad ha incidido de manera decisiva en nuestra forma de vivir y nos encontramos influenciados por ella mediante el uso de Internet, a través de ella se realiza actos como: contratos, compras, publicaciones, trasmisión de datos, comunicaciones y transacciones electrónicas, etc.

Existen diversas infracciones como: suplantación de identidad, sustracción de información confidencial, manipulación de información, etc.

Es importante que los Datos Personales o información que se trasmite en internet, deban ser salvaguardados, y precautelados por quienes al momento de realizar transacciones electrónicas en la red los exponemos.

Es por ello importante el uso de la Firma Digital constituyendo un método técnico esencial para proteger la información o datos que se transmiten mediante la red específicamente a la hora de realizar transacciones dentro del Comercio Electrónico.

Palabras Claves: Datos Personales, Firma electrónica, autenticidad de identidad, requisitos de seguridad.

ÍNDICE

REPÚBLICA DEL ECUADOR
UNIVERSIDAD DE CUENCA
FACULTAD DE JURISPRUDENCIA
ESCUELA DE DERECHO

TEMA: "UTILIZACIÓN DE LA FIRMA DIGITAL PARA LA PROTECCIÓN DE DATOS PERSONALES COMO MEDIO DE SEGURIDAD EN LAS TRANSACCIONES ELECTRÓNICAS"

TESIS PREVIA A LA OBTENCION DEL TÍTULO DE MAGÍSTER EN DERECHO INFORMÁTICO CON MENCIÓN EN COMERCIO ELECTRONICO

AUTORA:

ANA LUCIA ORDOÑEZ GUICHAY

DIRECTOR:

DOCTOR PABLO CADENA MERLO

Cuenca, Mayo de 2010

"UTILIZACIÓN DE LA FIRMA DIGITAL PARA LA PROTECCIÓN DE DATOS PERSONALES COMO MEDIO DE SEGURIDAD EN LAS TRANSACCIONES ELECTRÓNICAS"

Cuenca, Mayo de 2010

"La responsabilidad por los hechos, ideas y doctrinas expuestas en esta tesis, corresponde exclusivamente a la autora"

DEDICATORIA

La presente tesis la dedico a todas las personas que me ayudaron y motivaron a lo largo de este curso para terminarlo exitosamente

AGRADECIMIENTOS

Agradezco a mi Dios por su infinito Amor y por haberme permitido terminar este curso fruto de su promesa la cual ya es palabra cumplida.

Utilización de la Firma Digital para la protección de Datos Personales como medio de seguridad en las transacciones electrónicas.

Introducción

En la actualidad nos encontramos frente a una revolución tecnológica que se despliega a pasos agigantados, y por ello debemos estar preparados para afrontar todos los retos que nos presenta este nuevo milenio.

La globalización, es un fenómeno que ha trastocado fuertemente todos los estamentos de la sociedad mundial en diversos ámbitos, como en el político, económico, social, cultural, y por su puesto en el tecnológico.

Tal es el imperio de la tecnología, en la sociedad mundial del día de hoy, que ha incidido de manera decisiva en nuestra forma de vivir y comportamiento, a tal punto que nos encontramos influenciados por ella, principalmente mediante el uso de Internet, por medio del cual se puede realizar actos de diversa índole: contratos, compras, publicaciones, trasmisión de datos, comunicaciones y transacciones electrónicas, etc. Con respecto a estas últimas queda claro, que la antigua y tradicional manera de realizar negocios en forma física y personal, continúa siendo reemplazada por las negociaciones vía on-line, pudiendo efectuarse todo tipo de transacción desde cualquier parte del mundo y en todo momento con personas que no se encuentren físicamente presentes.

Múltiples son los beneficios que nos ofrece Internet, ya que con el avance de la tecnología, ésta ha implantando y consolidando nuevas costumbres comerciales, mediante el uso del Comercio Electrónico sin embargo no es menos cierto que existen diversas maneras a través de las cuales se puede cometer infracciones en la red, por ejemplo: suplantación de identidad, sustracción de información confidencial, manipulación de información, provocando verdaderos colapsos económicos en el caso de instituciones bancarias o afines, fraudes, estafas, robo de información secreta, etc. generando caos y devastadoras consecuencias derivadas del mal uso de la Tecnología, si no se cuenta con mecanismos

tecnológicos idóneos seguros, que protejan y garanticen la confianza para operar en las redes públicas de libre acceso.

Es importante que los Datos Personales o información que se trasmite en internet, deban ser salvaguardados, y precautelados por quienes al momento de realizar transacciones electrónicas en la red los exponemos, ya que alrededor del mundo se ha considerado a la red de redes como un canal inseguro de comunicación generando que los usuarios tomen prevenciones de seguridad y de protección para el aseguramiento de sus Datos Personales, e información trasmitida, con el fin de que dicha información no sea sustraída, o interceptada por terceros para ser usada en forma indebida.

Es por ello que en países de primer nivel se ha generalizado el uso de la Firma Digital constituyendo un método técnico esencial para proteger la información o datos que se transmiten mediante la red específicamente a la hora de realizar transacciones dentro del Comercio Electrónico, en virtud de que encuentra emblemada de confianza, y basada en fundamentos de criptografía de clave pública y funciones resúmenes, garantizando que quien firma un documento sea quien dice ser, contando para ello con respaldo de las Entidades Certificadoras o tercero de confianza, posibilitando de esta forma la consecución de actos y contratos a distancia, en vista que la tecnología por medio de la criptografía nos permite realizar contratos y transacciones, sin el futuro temor de enfrentar repudio, rechazo o suplantación de identidad en un mensaje de datos, reportando importantes efectos alrededor del mundo en cuanto al crecimiento del correo electrónico.

Por tanto podemos manifestar que técnicamente, la Protección de Datos Personales e información, que se trasmiten se precautela por la aplicación de mecanismos y técnicas, como protocolos de comunicación y seguridad, mecanismos de autentificación, aplicación de certificados digitales, firmas electrónicas, funciones resúmenes, etc. Cabe destacar que sin el empleo de estos importantes, elementos el Comercio Electrónico sería considerado inseguro y poco confiable por parte de los usuarios generando en estos pánico, temor y resistencia a realizar transacciones electrónicas, pues siempre estaría latente la incertidumbre respecto de la persona que se encuentra al otro lado, quien con certeza

asegurará ser la persona que dice serlo. Hoy observamos que esta situación solo se remedia con la aplicación de mecanismos de autentificación, en relaciones contractuales que supuestamente deberían basarse en la confianza entre las partes o para evitar posibles intercepciones del mensaje electrónico por terceras personas (hackers o crackers) quienes pudieran de mala fe sustraer el contenido de la información para utilizarla de manera negativa. De allí la importancia de que las personas que realicen transacciones electrónicas tomen las medidas de protección necesarias, para asegurarse que su información viajará segura y protegida por la red.

Lamentablemente en nuestro país el Comercio Electrónico no ha despertado en forma masiva, debido a la falta de información, o resistencia a la tecnología, pero sobre todo porque no existe protección legal efectiva. De acuerdo a las estadísticas, en Ecuador el comercio electrónico no alcanza un nivel importante justamente por la desconfianza que ha generado Internet, pues al no existir garantía de protección y respeto de los datos o información: privada, confidencial, sensible trasmitida como: nombres, apellidos, direcciones de domicilio, trabajo, teléfono, correo electrónico, país de ubicación, nacionalidad, números de: tarjetas, cuentas bancarias, entre otras y menos aun se proteja el Derecho a la intimidad informática, siempre imperará el miedo, recelo, y rechazo a realizar transacciones por la red. Es por ello que en Ecuador, es primordial que se adopten y utilicen las medidas de seguridad que la tecnología pone en nuestras manos, como la Firma Digital, la cual otorga resultados eficaces al momento de realizar transacciones convirtiéndose alrededor del mundo en el instrumento tecnológico más utilizado, en el Comercio Electrónico.

CAPITULO I

EL COMERCIO ELECTRONICO

1.1 Generalidades

El Comercio Electrónico o más conocido como E-commerce constituye una nueva modalidad de hacer comercio, el cual se ha desarrollado y tomado fuerza principalmente en Europa y Estados Unidos de Norte América generando entre otros múltiples temas, mucho capital.

El Comercio Electrónico es la realización de: negocios en línea o el vender y/o comprar productos y/o servicios a través de ofertas en la Web, tomando en cuenta que los productos que se comercializan en internet pueden ser físicos como carros, casas, etc. o servicios como: viajes, consultas médicas en línea, educación a distancia, etc. de igual modo se comercializan aquellos productos digitales como música, noticias, imágenes, bases de datos, software y todos los tipos de productos relativos a la información.

El Comercio Electrónico se realiza a través de medios informáticos, como el internet, y se encuentra promovido por una serie de factores como: globalización, economía, política, cultura, debiendo destacar principalmente el factor económico, debido a que reporta múltiples bondades como: reducción de costos administrativos, acortamiento del proceso, celeridad en las transacciones, ahorro de papel, opción de trabajar las 24 horas del día, demostrando así que el comercio por Internet en verdad reporta ahorro y utilidades.

No obstante, el Comercio Electrónico en la actualidad ha logrado un gran desarrollo, especialmente en países de Europa donde se cuenta con mayor normativa, que asegura y garantiza la efectividad del comercio realizado a través de medios tecnológicos, razón por la cual las estadísticas demuestran el crecimiento acelerado y sostenido que han alcanzado en los últimos tiempos las grandes potencias. Cabe recalcar que esto, se debe a que países industrializados, cuentan con una cultura tecnológica, así como educación e información oportuna

respecto del E-commerce, y sobre todo porque se brinda tutela y seguridad a Datos Personales los mismos que se encuentran precautelados por normativas que aportan confiabilidad en el sistema, como en el caso de la Unión Europea.
Al contar Europa con una Ley de Protección de Datos Personales, cuya aplicación incide de forma directa en el Comercio Electrónico ha permitido a los usuarios gozar de confianza y seguridad, al momento de realizar sus transacciones en línea, convirtiéndose este escenario en un motor importante, para el desarrollo del E-commerce.

En la realidad ecuatoriana pese a que, desde 1970 se ha reportado una importante actividad de transacionalidad, mediante cajeros automáticos considerados como medios electrónicos y transferencias por teléfono, los mismos que constituyen componentes de una transacción comercial, observamos que el uso de los medios tecnológicos siempre han estado presentes, dentro de nuestra sociedad alcanzado una relevancia significativa, debido a la masificación en el uso que han tenido estos medios, sin embargo en cuanto al comercio electrónico en el país se puede indicar que el mismo no ha despegado completamente, pese a contar con una Ley de Comercio Electrónico, debido principalmente a factores como: falta de difusión e información, desconfianza en la red al tener que proporcionar los usuarios sus datos personales y confidenciales, tales como número de tarjeta de: crédito, debito, o de cuenta bancaria, en una página web, generando en ellos temor de ser estafados en internet, pero también la falta de educación y cultura en el uso de los medios electrónicos, siendo importante manifestar la ausencia de protección técnica y jurídica a través de la norma, (Ley Protección de Datos) a los usuarios provocado barreras relacionadas de alguna manera con la brecha digital.

Pero existen otras barreras que impiden y constituye un freno para el despegue del Comercio Electrónico en nuestro país, como lo son:
1. Funcionamiento tardío de "Entidades Certificadoras de Firmas Digitales".
2. Habilitación tardía de "Facturas Electrónicas"

3. Desarrollo de mecanismos adicionales de pago electrónico, particularmente micro pagos.

4. Integración de las empresas de correo y Courier.

5. Aspectos legales e impositivos del comercio electrónico (fiscalidad-bussines).

6. Difusión y Capacitación del uso y aplicaciones del "Comercio Electrónico" en el Ecuador. 1

Pero sobre todo, requeriremos la implementación nacional de una Ley de Protección de Datos Personales en cuyos capítulos se haga referencia a la tutela de la información brindada en las comunicaciones o transacciones electrónicas, ya que para los usuarios en el Comercio Electrónico ecuatoriano será muy importante la: privacidad, seguridad, confidencialidad, así como la protección de datos personales, la cual aportará en gran medida a esta nueva modalidad de hacer comercio.

La protección que debe brindarse dentro del campo de las nuevas tecnologías de la información, que según los doctrinarios constituiría un derecho clásico, preexistente, es decir que no es nuevo, es la protección al derecho a la intimidad o el respeto a la vida privada, que se consagra en nuestra Constitución Política, la cual se requiere que sea extendida a la información suministrada, contenida o almacenada por cualquier medio electrónico o tecnológico.

Al Comercio Electrónico le han atribuido en múltiples foros alrededor del mundo, varias definiciones mas ahora nos remitiremos a un concepto emitido por Secretaria General de comunicaciones Española "***comercio electrónico es cualquier forma de transacción o intercambio de información comercial basada en la transmisión de datos sobre redes de comunicación como Internet"***. Según este organismo español el Comercio Electrónico **no solo incluye la compra venta** electrónica de bienes, información o servicios, **sino también el uso de la red** para actividades anteriores y posteriores a la venta como son: la publicidad; la búsqueda de información sobre producción proveedores, la negociación entre comprador y vendedor, sobre precio

1- Compilación documentos otorgados por la Dra. Sofía Espinoza Coloma en la cátedra Sociedad de la Información Proyecto de equipo Comercio Electrónico

condiciones de entrega, etc. la atención al cliente antes y después de la venta; la consecución de trámites administrativos relacionados con la actividad comercial; y la colaboración entre empresas con negocios comunes" 2

1.2 Principales consideraciones legales para el desarrollo del Comercio Electrónico.

Existen diversos conflictos y situaciones que entorpecen la utilización masiva del Comercio Electrónico, siendo principalmente la falta de garantías y seguridad que este canal de comunicación presenta el mismo que genera desconfianza a los usuarios del sistema.

Pero también el Comercio Electrónico plantea problemas o agudiza algunos otros ya existentes en el comercio tradicional tales como:

1.- La validez legal de las transacciones y contratos "sin papel"

2.- La necesidad de acuerdos internacionales que ajusten, y armonicen las legislaciones sobre comercio.

3.- El control de las transacciones internacionales

4.- **La protección de los derechos de propiedad intelectual.**

5.- La protección de los consumidores en cuanto a la publicidad engañosa o no deseada**, fraude,** contenidos ilegales y **uso abusivo de los datos personales.**

6.- La dificultad de encontrar y evaluar la fiabilidad del vendedor.

7.- **Las seguridad de las transacciones y medios de pago Electrónico.**

8.- La falta de estándares y la proliferación en la aplicación de protocolos de comercio electrónico incompatibles. 3

Para todos estos problemas que frenan la evolución del Comercio Electrónico existen soluciones, más se deberá enfatizar en ciertas situaciones como:

- **Asegurar el acceso a la infraestructura de la información, resolver los problemas logísticos de pago y de entrega, pero sobre todo minimizar la**

2- Régimen Jurídico de Internet Edit. La Ley. Madrid año 2002 por J.M. DE LA CUETARA Y J. MA.ECHEVARRIA pág. 1086 Cita pie de página (Secretaria General de Comunicaciones "Estudio de situación del comercio electrónico en España" mayo 1999 Disponible en el sitio web de la Asociación de Usuarios de Internet española AUI-www.aui.es")

3- Régimen Jurídico de Internet Edit. La Ley. Madrid año 2002 por J.M. DE LA CUETARA Y J. MA.ECHEVARRIA pág. 1090.

incertidumbre regulatoria, así como generar confianza en los usuarios de los sistemas de información y transacciones electrónicas.

Por lo tanto desde mi personal punto de vista, lo que realmente importará en el Comercio Electrónico para su desarrollo eficaz es el generar seguridad y confianza en los usuarios, la cual efectivamente se consigue, mediante la armonización de las diversas legislaciones, tratados internacionales, que permitan al Comercio Electrónico ser confiable para los usuarios debiendo dar **validez a las formas electrónicas** de contratación, a través de la Firma electrónica, **estableciendo y determinando una jurisdicción efectiva aplicable en caso de controversias en el ciberespacio** o se creen las reglas para determinar un lugar convencional en el que se entienda: realizados los contratos o trasgredidos los derechos. 4

1.3 El Comercio Electrónico en el Ecuador.

Existen leyes alrededor del mundo que específicamente velan por la protección y seguridad de Datos Personales de los usuarios en internet, quienes los ingresan para realizar un sin número de transacciones ya sea para comprar en una tienda virtual, efectuar intercambio y transferencia de información o realizar una transacción Bancaria, cuya aplicación de la normativa a convergido para generar confianza en los usuarios internautas, tanto en el tratamiento, como en el procesamiento de su información.

La aplicación de protocolos de comunicación, seguridad, mecanismos criptográficos, funciones hash, certificados digitales, y la utilización de la Firma Electrónica han permitido realizar transacciones, o conversaciones seguras, por el canal de Internet, siendo lo que realmente preocupa a los usuarios de la red al momento de realizar negocios, es la falta de: seguridad y confidencialidad, en el comercio electrónico pues se han producido suplantaciones de identidad, compras fraudulentas, o escuchas en las comunicaciones por parte de terceros con fines maliciosos.

4- Régimen Jurídico de Internet Edit. LA Ley. Madrid año 2002 por J.M. DE LA CUETARA Y J. MA.ECHEVARRIA pág. 1090.

En la realidad, se han generado fraudes por medio de la red, ya sea a través de las transacciones o compras efectuadas, siendo vital destacar que la tecnología se ha desarrollado a pasos agigantados ofreciéndonos nuevos métodos de autentificación infalibles como los biométricos o la aplicación de programas informáticos como el fire wall a los servidores, con el fin de asegurar que las transacciones electrónicas se realicen de manera confiable.

En el Ecuador, no se cuenta actualmente con una Ley específica de Protección de Datos Personales, no obstante dicha situación no debería ser considerada como una piedra de tropiezo para el arranque definitivo del comercio electrónico, ya que deberíamos analizar otros factores, que constituyen verdaderos obstáculos, y que inciden en el desarrollo del comercio electrónico como: falta de infraestructura tecnológica, falta de acceso a las Tics, falta de: información, cultura digital, así como intereses políticos, económicos, el funcionamiento parcial de entidades certificadoras, y la falta de estándares para el intercambio electrónico de documentos de negocio, así como la parcial habilitación de facturas electrónicas, la falta de regulación concerniente a los aspectos legales e impositivos atinentes al comercio electrónico, pero sobre todo la falta de " **difusión y capacitación del uso y aplicaciones del Comercio Electrónico**" lo que produce que en el Ecuador esta nueva modalidad de comercio, no pueda arrancar definitivamente y así acortar la brecha digital, pues nos retrasa del avance respecto de otros países en el mundo en cuanto al tema tecnológico, en virtud que la población con: acceso, educación e información respecto de las TICs constituye un factor valioso para el desarrollo del E-commerce en nuestro país.

Por otro lado en el caso del gobierno electrónico podemos evidenciar que en el Ecuador se va afirmando las sendas para el desarrollo del mismo tal es el caso de algunas instituciones públicas como: el Servicio de Rentas Internas, el Instituto de Seguridad Social, Instituto Nacional de Estadística y Censos y el Instituto Nacional de Compras Públicas a través de su página web "compras públicas.gov.ec".

1.4 Datos Personales y Comercio Electrónico.

En el Comercio Electrónico la protección de datos personales es fundamental, ya que los sujetos intervinientes en las diversas fases del negocio jurídico, requieren de confianza y seguridad, siendo importante contar para ello con normativa específica de protección de datos personales en virtud de que en el campo de las nuevas tecnologías dicha protección constituiría la aplicación de un derecho clásico es decir: el derecho a la intimidad o el respeto a la vida privada.

Lo más importante para los sujetos que intervienen en las negociaciones a través de Internet, constituye la protección y resguardo de: sus datos personales o información trasmitida en forma segura y confiable, a fin de evitar que dichos datos sean utilizados en forma: ilícita, o fraudulenta ya sea en suplantación de identidad, o en la realización de estafas por tanto se debe aplicar las garantías técnicas y legales que sean necesarias, pues para el desarrollo del comercio electrónico es importante, la certidumbre y confianza entre consumidores y empresarios, siendo necesario considerar situaciones como: ubicación física real del proveedor, solvencia del mismo, integridad de la información, protección de datos e intimidad personal, ejecución de contratos a distancia, fiabilidad de pagos, remedio en caso de error o fraude, así como mecanismos electrónicos de pago.

El Derecho anglosajón consagra: **Right to be a lone:** que significa **"**Derecho a estar solo" por lo tanto podemos manifestar que es el Derecho que tenemos todas las personas a que se respete nuestra privacidad, e intimidad, así como la confidencialidad, en cuanto a los datos personales o a la información que suministramos a instituciones, organismos, además del derecho a la privacidad en las comunicaciones, que se generen, trasmitan o intercambien, considerando necesario el uso de sistemas informáticos en el tratamiento y transmisión de la información.

Algunos países de la Comunidad Europea han implantado leyes rigurosas que establecen controles sobre el procesamiento y transmisión de datos personales, estableciendo responsabilidades a aquellas personas que recopilan, procesan y

divulgan información personal, limitando aún la capacidad de transferir dichos datos a otros países.

Es por ello que las organizaciones e instituciones de servicios electrónicos deben tener la obligación y responsabilidad de precautelar los datos personales consignados por los usuarios en la red, como el acatamiento a ese derecho clásico fundamental.

Constituyendo importante el rol de los estados, en el gran concierto internacional de naciones al celebrar, convenios y acuerdos multilaterales a fin de proteger a los usuarios y consumidores dentro del mercado electrónico mundial.

1.5 Los sujetos del derecho a la protección de datos Personales en el Comercio electrónico.

Dentro del Comercio Electrónico intervienen varios sujetos que son: **Sujeto activo**: comprador y **sujetos pasivos**: servidor en la red, vendedor y certificador

1.5.1. Sujeto activo:

El comprador es el titular o sujeto activo **del derecho a la intimidad informática** por lo que tiene derecho a determinar, qué información sobre él (y, por tanto, no pública) puede ser comunicada a terceros.

Considerando, que este derecho pudiera ser limitado, cuando hay consentimiento del titular ejemplo cuando el usuario de la red es un menor y se requiere de la autorización de los padres.

Dicho derecho también pudiera ser limitado cuando existen requerimientos fundamentales importantes como la "necesidad" y la "proporcionalidad". Estas reglas suponen que es lícita la obtención de ciertos datos personales del individuo en la escala en que los mismos sean "adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido"

Para obtener datos del sujeto activo este debe ser informado de modo "expreso, preciso e inequívoco" la finalidad y los destinatarios de dicha información, los

datos obtenidos "no podrán usarse para finalidades distintas para las que hubieran sido recogidos" de acuerdo a la legislación española.

Los datos recolectados deberán ser almacenados de tal modo que se garantice el "derecho de acceso" y serán "exactos", debiéndose rectificar en caso de ser necesario.

La Ley Orgánica de Garantías Constitucionales en concordancia con la Constitución Ecuatoriana en el Art. 94.- Acción de hábeas data manifiesta que "Toda persona por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico."

"Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley."

"La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de los datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, esta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados."

Los datos se cancelarán una vez que hayan dejado de ser necesarios para lo que hubieren sido obtenidos. La LOPD de España- 5 establece que está prohibida la recogida de datos por medios fraudulentos, desleales o ilícitos (arts. 4 y 5 LOPD; art- 6 DPDP 6

5- LOPD: Ley Orgánica Española 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

6- DPDP Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Sin embargo la utilización de la red en los Estados Unidos, para realizar una operación o transacción de comercio electrónico pudiera permitir obtener ciertas informaciones del sujeto sin su consentimiento y sin que esté acredite su necesidad y proporcionalidad como, lo constituye el uso y la aplicación de las "cookies" o galletas informativas al visitar diversas páginas webs, software informático que puede recolectar información acerca de qué páginas son las más visitadas por el usuario creando perfiles de consumo.

En los Estados Unidos donde no se reconoce el derecho a la intimidad informática, y que luego de lo sucedido el 11 de septiembre esto pudiera tener cabida legal, sin embargo nada justifica que la intimidad y privacidad de las personas pueda ser violada bajo la excusa de que "obstaculiza" las transacciones electrónicas, no así en países de Europa donde la utilización de esta práctica, no tiene asidero legal en virtud de vulnerar el derecho a la protección de datos.

1.5.2. Sujetos pasivos: el servidor en la red, el vendedor y el certificador.

El reconocimiento del derecho a la intimidad informática en las relaciones entre particulares obliga a respetar tanto a los poderes públicos, como a los agentes privados.

En el comercio electrónico intervienen agentes, que pueden ser considerados sujetos pasivos del derecho: **el servidor** a través del cual, se accede a la red, el particular **vendedor** y eventualmente, **el certificador** de la identidad del comprador o del vendedor los cuales tienen deberes para con el sujeto activo del derecho a la intimidad informática.

De conformidad con la Ley Orgánica de Protección de Datos española, se establece que el particular en este caso, el vendedor podrá "crear un fichero de datos personales cuando sea necesario para el logro de su actividad y se respeten las garantías establecidas por el ordenamiento" (art. 25 LOPD Española) 7

7- LOPD: Ley Orgánica Española 15/1999, de 13 de diciembre, de protección de datos de carácter personal

Entendiéndose como Fichero, al conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso, siendo importante tener en cuenta que los datos de carácter personal son cualquier información concerniente a personas físicas identificadas o identificables.

En España "toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal debe notificarlo previamente a la Agencia de Protección de Datos."

La Agencia de Protección de Datos es un ente de derecho público español, con personalidad jurídica, capacidad pública y privada, además tiene las siguientes funciones: velar por el cumplimiento de la legislación sobre protección de datos, controlar su aplicación en cuanto a los derechos de información, acceso, rectificación, oposición y cancelación de datos, así como atender las solicitudes y reclamaciones de las personas afectadas, asesorar a las personas sobre sus derechos en cuanto al tratamiento de datos de carácter personal, solicitar a los responsables y custodios de los datos la adopción de medidas para el adecuado tratamiento de los mismos de acuerdo a las disposiciones de la Ley, a fin de evitar su alteración, pérdida, tratamiento o acceso no autorizado (art. 9 LOPD; art. 17 DPDP; art. 4 DPDIT) así como la cancelación de ficheros, cuando no se ajuste a las disposiciones.

Responsable del fichero o tratamiento es aquella persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento de la información.

Tratamiento de datos son las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Es muy importante el deber del secreto y es por esto que el responsable del fichero como

todos los que intervengan en el tratamiento de los datos personales están obligados al secreto profesional respecto de la información recogida, o suministrada. De acuerdo a la ley Española dicha obligación subsiste aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo (art. 10 LOPD).

La vulneración del secreto profesional acarrea una responsabilidad civil (art. 7.4 LODHI) y penal (art. 197.4 del Código Penal).
Pero que debe realizar el responsable del fichero, en el caso de la primera cesión de los datos personales? deberá comunicar al titular de los mismos, la naturaleza de los datos cedidos y el nombre y dirección del cesionario, así como la finalidad del fichero.

Existen deberes generales impuestos a todos los sujetos pasivos del derecho a la intimidad informática:

1.- En cuanto al vendedor, para que sus operaciones sean más seguras deberá utilizar claves criptográficas, para de esta manera proteger la confidencialidad de la información en virtud de que, lo más importante para el usuario será que los datos sean protegidos, lo que constituye la clave para fomentar el desarrollo del Comercio Electrónico.
En España en cuanto al uso de técnicas criptográficas, para salvaguardar de mejor manera los datos, por parte de los sujetos pasivos estos deben notificar a un órgano de la Administración General del Estado o a un organismo público, **los algoritmos o cualquier procedimiento de cifrado** utilizado, a efectos de control de acuerdo con la normativa vigente.

Los servidores son quienes prestan servicios de telecomunicaciones al público o explotan redes de telecomunicaciones accesibles al público, y están obligados a respetar el derecho fundamental a la intimidad.

Los servidores deben garantizar: el secreto de las comunicaciones (arts. 18.3 y 55.2 CE8 art. 579 de la Ley de Enjuiciamiento Criminal; art. 49 LGTel 9 ; art. 5 DPDPIT10 el ejercicio de su actividad, la protección de datos de carácter personal, conforme a lo dispuesto en la normativa vigentes (art. 50 LGTel; art. 4 DPDPIT).

Nuestra ley especial de telecomunicaciones manifiesta en el Art. 14 que: El Estado garantiza el derecho al secreto y a la privacidad de las telecomunicaciones. Es prohibido a terceras personas interceptar, interferir, publicar o divulgar sin consentimiento de las partes la información cursada mediante los servicios de telecomunicaciones.

De acuerdo al proyecto de directiva de la Unión Europea el servidor puede almacenar en forma automática, provisional y transitoria los datos transmitidos siempre que dicho almacenamiento sirva exclusivamente para ejecutar la transmisión en la red de comunicaciones y que su duración no supere el tiempo razonablemente necesario para dicha transmisión. Como excepción se establece para el servidor el deber de posibilitar el acceso a tales datos cuando tenga conocimiento de que algún tribunal o autoridad administrativa ha ordenado la retirada o el acceso a esos datos (art. 12.2 y 13.1.e PCDCE 11

La regla general siempre será que "el prestador del servicio no pueda **ser considerado responsable** del almacenamiento automático, provisional y temporal de esta información, realizada con la única finalidad de hacer más eficaz la transmisión ulterior de la información a otros destinatarios del servicio (art. 13.1 PCDCE).

"Los Estados miembros no impondrán a los prestadores de servicios una obligación general de supervisar los datos que transmitan o almacenen, ni una

8-. Constitución Española

9-. - LGTel Ley 11/1998, de 24 de abril, General de Telecomunicaciones

10-. Directiva 97/66/CE, del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones)

11-. PCDCE Posición común nº 22/2000, aprobada por el Consejo el 28 de febrero de 2.000, con vistas a la adopción de la Directiva sobre el comercio),

obligación general de realizar búsquedas activas de hechos o circunstancias que indiquen actividades ilícitas" (art. 13.1 PCDCE).

La Directiva europea establece que los Estados miembros velarán, para que los proveedores de servicios de certificación cumplan las exigencias que en materia de protección de datos establece la DPDP, y sólo puedan recabar datos personales si concurren las notas de necesidad y consentimiento del titular (art. 8 y Anexos II y III DFE).

La normativa española, por su parte, establece que todo prestador de servicios de certificación tiene **obligación de no almacenar ni copiar los datos de creación de firma** electrónica de la persona a la que haya prestado sus servicios, salvo que ésta lo solicite (art. 11.c RDLFE). El incumplimiento de esta obligación puede ser objeto de sanción por la Agencia de Protección de Datos (art. 16.3 RDLFE). 12

Teniendo en cuenta que la protección de Datos Personales nunca pudiera ser considerada como una excusa, que obstaculiza las transacciones electrónicas, en nuestro país El Consejo Nacional de Telecomunicaciones CONATEL se ha impuesto el objetivo de impulsar la regulación acerca de la seguridad de la información y la privacidad de los datos a fin de evitar el uso indebido de la información.

Destacando la iniciativa de establecer: normas técnicas y jurídicas que eviten acciones fraudulentas que pudieran ocasionarse con el uso y explotación de los servicios de las telecomunicaciones y de las TIC's, deben crearse reglamentos para el tratamiento de documentos digitales a través de los sistemas informáticos de trasmisión de la información a fin de lograr la confidencialidad, seguridad, e integridad de las transacciones electrónicas mediante sistemas de trasmisión de voz y datos, estableciendo sanciones para las acciones fraudulentas.

Desde mi punto de vista personal la legislación española incide positivamente en lo que concierne a datos personales y debería ser adoptada en nuestro país,

12-.- RDLFE Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica

adaptándola a nuestra realidad, en virtud que tiene por objeto, limitar el uso de la informática y medios de tratamiento automatizado de los datos de carácter personal a fin de garantizar principalmente el honor, y la intimidad de las personas físicas así como el pleno ejercicio de sus derechos.

Cabe recalcar que en nuestro país solamente existen algunas disposiciones que se encuentran aisladas en diferentes cuerpos normativos respecto al tema y no se cuenta con una ley especifica encargada de velar por datos personales cuya necesidad es de interés común dentro de la sociedad, la misma que pasa por desapercibida siendo producto de ello el atropellamiento del derecho al honor, privacidad e intimidad de las personas, necesidad que el legislador al momento de ejercitar su facultad de instaurar y aprobar la norma omite por desconocimiento de la evolución tecnológica, sin preveer problemáticas futuras.

Es importante destacar que en nuestra sociedad, no existe suficiente conocimiento en cuanto a la salvaguarda de los derechos esenciales como privacidad y honra de las personas en lo atinente al uso de las nuevas tecnologías de la información y conocimiento, (comercio electrónico) siendo notorio que el derecho no evoluciona de manera dinámica frente a la contemporaneidad informática.

El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos han expuesto a la privacidad e intimidad, debiendo considerar que la intimidad protege la esfera, en que se desarrollan las facetas reservadas de la vida: el domicilio donde el individuo realiza su vida cotidiana, las comunicaciones, etc. La privacidad constituye en cambio el conjunto, de facetas de la personalidad de un individuo privacidad, que puede resultar menoscabada por la utilización de las tecnologías informáticas

La ley española prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos y precautela la calidad de los datos de carácter personal, estableciendo que los mismos solo podrán ser recogidos previo el consentimiento de una persona cuando sean adecuados, pertinentes y no excesivos en relación con las

finalidades, para los que se hayan obtenido, siendo cancelados, destruidos o devueltos una vez que hayan dejado de ser necesarios para el propósito por el cual fueron recogidos, estableciendo las sanciones pertinentes en el caso de las actuaciones contrarias a la ley, en la que resultare perjudicado el titular de los mismos con el derecho de ser indemnizado, mientras que en la realidad de nuestro país no se efectúa ninguna gestión para proteger los datos de índole personal, que muchas de las veces son obtenidos sin el consentimiento del titular, mucho menos se notifica cuando estos han sido cedidos a terceros.

1.6 La protección de datos y obligaciones del negocio Jurídico.

Se considera como negocio jurídico, aquel acto voluntario lícito de las personas, que tiene por finalidad inmediata la producción de un efecto jurídico.

En el negocio jurídico existen etapas que se cumplen por lo general:

1.6.1 Fase precontractual: oferta y demanda

Empieza con la oferta por parte del comerciante al comprador, la misma que se precisará en una publicidad que deberá ser clara y concisa, respecto de los bienes y/o servicios que este ofrece, utilizando medios como: páginas web, blogs o correos electrónicos, para poder llegar a los potenciales clientes13.

Al no contar en el Ecuador con un antecedente de normativa relacionada con la Protección de Datos Personales nos remitiremos a las ventajas que ofrece la normativa comunitaria de la unión europea, la cual ha sido adoptada como ley modelo por algunos países y que a excepción de EEUU y Canadá, otorga protección a la información, contenida, y almacenada, en el correo electrónico.

De acuerdo a la Ley de la Comunidad Europea, el correo electrónico se beneficia de la protección constitucional del derecho al secreto de las comunicaciones (art. 18.3 CE), por lo que su contenido sólo puede ser develado con el consentimiento del titular o con autorización judicial.

13- Fuente http://web.usc.es/~ruizmi/pdf/e~com.pdf consultado el 24 de Julio del 2008 hora: 11.00am.

Los Estados miembros de la Comunidad Europea en concordancia con su normativa de Protección de Datos vigilarán que, las técnicas de comunicación a distancia a través del correo electrónico sólo puedan utilizarse a falta de oposición manifiesta del consumidor (art. 10.2 DPCCD; 14 art. 7.2 PCDCE). 15

Otro medio utilizado para realizar la oferta es mediante la publicación en la red de "páginas" o "sitios" que son visitados por los usuarios. La dificultad se plantea cuando los responsables de dichos sitios se benefician de la visita para insertar en el ordenador del visitante "cookies" o galletas informáticas.

Nuestra Constitución Política en cuanto a los derechos civiles manifiesta que sin perjuicio de los derechos establecidos en esta Constitución y en los instrumentos internacionales vigentes, el Estado reconocerá y garantizará a las personas los siguientes:
8. "El derecho a la honra, a la buena reputación y a **la intimidad personal y familiar**. La ley protegerá el nombre, la imagen y la voz de la persona."

Las Cookies

La enciclopedia virtual wikipedía manifiesta que el gran problema de ofertar productos
y/o servicios mediante la red se presenta cuando el comerciante, luego de que los usuarios han ingresado en su página, instala en el ordenador de los mismos un programa

informático, llamado cookies, el cuál se forma por medio de instrucciones que los servidores web envían a los programas navegadores del usuario, almacenándose en un directorio especifico, el cual tiene por finalidad recolectar información o hábitos de compra, respecto del usuario creando un perfil del mismo, archivo informativo que servirá en lo posterior al comerciante para enviarle al cliente información acerca de productos o servicios mediante spam,(correo basura o no

14- DPCCD Directiva 97/7/CE, del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia

15- PCDCE Posición común nº 22/2000, aprobada por el Consejo el 28 de febrero de 2.000, con vistas a la adopción de la Directiva sobre el comercio electrónico

deseado) siendo considerado en algunos países como en Estados Unidos de Norte América delito.16

Cuando el usuario configura o personaliza su navegador pudiera conseguir que la información recogida, por la cookie, siempre sea considerada como personal, pues se encontrará asociada con una persona identificada, por tanto el programa del navegador establecerá automáticamente el nombre del usuario al directorio que se genere como cookie pero además la galleta informativa puede recoger información como la dirección IP (o protocolo de internet que es la dirección numérica con la que el ordenador se encuentra conectada a la red) fija del usuario.
En el caso de las IP's dinámicas (IP que tiene una duración determinada, pues cambia cada vez que el usuario se reconecta por cualquier causa, la misma que es asignada al usuario mediante un servidor de protocolo de configuración dinámica)**, será necesario un requerimiento al proveedor del servicio que le permita el acceso a la red, antes de que los datos de la sesión desaparezcan del Log del sistema.17**

Hoy en día existen programas navegadores tipo "anti-cookies" que permiten rechazarlas, en muchas de las páginas web como tiendas virtuales, o periódicos, venden la emisión de estas cookies desde sus servidores.

De acuerdo a la Directiva 95/46 de Protección de Datos Personales de España la emisión de cookies constituye una grave infracción por lo que está sujeta a multas o sanciones que pudieran ir desde los 10 hasta 100 millones de euros.

Pero son los servidores los que deberán siempre estar protegidos, ya que de lo contrario, admitirán que la trasmisión de información pueda ser interceptada, o atraída por un tercero no identificado.

El usuario una vez que conoce la oferta si le conviene realizará una solicitud, tomando en cuenta que los datos que transmita deberán ser resguardados de

16- Viktor Mayer-Schönberger, "The Internet and Privacy Legislation: Cookies for a Treat?" The West Virginia Law Journal of Law and Technology, vol. 1, nº 1 (1997).
17- - Xavier Ribas Alejandro, Aspectos jurídicos del uso de cookies, 1997, http://www.onnet.es/03008001.htm

manera optima garantizándose la seguridad y privacidad, de tal forma que siempre prime el respeto al derecho de su intimidad informática por quienes tengan acceso a los datos.

El factor principal para que el cliente se atreva a comprar en Internet será la confianza, que sin lugar a dudas se puede alcanzar con la aplicación de métodos y técnicas de encriptación, funciones hash, así como firmas electrónicas en cuyo caso los datos personales del usuario serán cifrados por el cliente y solo podrán ser descifrados por quien tenga o conozca la clave.

1.6.2. Fase de perfeccionamiento: aceptación.

Se da luego de que el comerciante, previo haber hecho la oferta al cliente y este a su vez haber formulado una solicitud respecto de un bien y/o servicio que desea, el comerciante obtendrá toda una serie de datos personales del cliente como: nombres y apellidos, dirección IP del ordenador, dirección de cuenta de correo electrónico, número de tarjeta de crédito o número de cuenta bancaria, dirección física (si se trata de entregar un bien físico).
Existen razones por las cuales los oferentes, pueden archivar los datos personales de los clientes, como en el caso de los servicios post venta para ello dichos servidores deberán estar bien protegidos para evitar eventuales ataques en el futuro.

1.6.3. Fase de ejecución: pago o prestación y responsabilidad.

De acuerdo a lo que manifiesta el Dr. Carlos Ruiz Miguel, Profesor de Derecho Constitucional en la Universidad de Santiago de Compostela España, luego de que el contrato en línea es perfeccionado con el consentimiento de las partes, se pasa a la siguiente fase de ejecución, aquí la intimidad informática debe cumplir con sus garantías y en el caso de incumplimiento o cumplimiento defectuoso del contrato cualquiera de las partes podría hacer efectivas las exigencias de responsabilidad, como: pago de indemnizaciones.

El comprador deberá cumplir con su obligación de realizar el pago ya sea por el bien y/o servicio que adquirió tomando en cuenta que el pago podrá realizarse de dos maneras:

a) Pago contra rembolso
b) Pago a través de medios electrónicos

En el caso del pago contra rembolso (aquel que se abona en el momento de realizarse la entrega con dinero en efectivo) no existe ningún riesgo para los datos personales o confidenciales del usuario como: numero da tarjeta de crédito, número de cuenta bancaria entre otros, más bien el riesgo radicará en el pago realizado por el cliente a través de medios electrónicos.

Existen modos inseguros de pago, mediante los cuales el comprador comunica al vendedor los datos de su tarjeta o de su cuenta, para que el comerciante cobre el dinero de la empresa emisora de la tarjeta o de la entidad en la que se halla la cuenta, tomando en consideración que en esta modalidad no consta la firma del titular de la tarjeta, por lo que en un futuro podría alegar repudio por parte del cliente al no existir documentación de tal consentimiento para dicho pago. 18

Hoy en día a nivel internacional se cuenta con excelentes mecanismos como la firma digital o electrónica y avanzada, certificados digitales y técnicas criptográficas de alto cifrado muy utilizados en la Banca en línea y que junto con el uso de protocolos seguros para comunicación, la información como datos confidenciales no solamente viajan de manera confiable, sino garantizan seguridad y privacidad pues al estar combinado con métodos de autentificación, permite reducir altamente los riesgos de suplantación de identidad en el caso de compras fraudulentas, o repudio por parte del cliente.

18- Los Medios de Electrónicos de Pago, Los Mecanismos de Seguridad en el Pago Electrónico por Mercedes Martínez González Capitulo I.

Pero además la firma digital brinda otros beneficios como: la integridad y confidencialidad de la información. Lamentablemente en el Ecuador no se ha difundido suficiente información acerca de la firma electrónica, Entidades Certificadoras, y al no existir legislación sobre Protección de Datos Personales dicha información trasmitida en forma insegura a través de Internet, viaja sin tutela jurídica ni técnica por lo que no se garantiza el derecho a la protección informática.

El vendedor, por su lado también deberá cumplir con parte de su obligación, como es la entrega o prestación del bien y/o servicio por el cual se comprometió, entrega que puede ser física o electrónica y que puede realizarse por medios seguros o inseguros.

En el caso de que la entrega del bien y/o la prestación de servicios se realice en forma física, siempre se requiere de ciertos datos personales esenciales del cliente destinatario como: dirección del domicilio, etc. y en el caso de la entrega de un bien electrónico o prestación de servicio vía electrónica como un archivo musical, obra literaria, video, software, siempre se requerirá por lo menos de la información básica del destinatario como dirección de correo electrónico.

El vendedor podrá crear un archivo de datos personales, también le será factible establecer un sistema de asistencia post-venta para el cliente, a cuyo efecto creará el correspondiente archivo de clientes, y dichos datos archivados tendrá como finalidad primordial, exigir las eventuales responsabilidades o garantizar un mejor servicio post-venta. 19

1.7 La protección de datos personales y lugares del negocio Jurídico.

La principal característica del comercio electrónico, dentro de negociaciones que se realizan a distancia es aquella en que las partes intervinientes, al no encontrarse físicamente presentes en el mismo lugar, presentan problemas sustantivos y procesales de Derecho Internacional en cuanto a la aplicabilidad de diversas reglas, normativas, y tratados de Derecho Internacional a los que estén

19- Fuente http://web.usc.es/~ruizmi/pdf/e~com.pdf consultado el 24 de Julio del 2008 hora: 11:30am

sujetas las partes involucradas, con el fin de poder determinar cuál es la jurisdicción o competencia aplicable en caso de un conflicto en el futuro, afectando al régimen jurídico de datos personales de los involucrados.

Un problema que pudiera generarse en cuanto a la aplicabilidad de la normativa de Protección de Datos Personales, es en el caso en que uno de los contratantes no cuente con legislación de Protección de Datos o su ley sea diferente a la del otro contratante, caso contrario si ambos estados involucrados en el contrato brindan las suficientes garantías y protección en cuanto al derecho de la intimidad informática, como ocurre en el caso de los Estados de la Unión Europea, quienes tienen el mismo Derecho Comunitario de Protección Datos Personales, la probabilidad de que exista conflicto en el comercio electrónico disminuye en gran medida.

Dentro del Comercio Electrónico es normal que los intervinientes se encuentren en diferentes partes del mundo, o en una localidad como en el caso de la Comunidad Europea, la misma que tiene normativa propia que rige en todos sus estados miembros.

Por ende el problema se presenta, cuando uno de los contratantes esta fuera de esta comunidad que se encuentra debidamente regulada en cuanto al tema de Protección de Datos, dando lugar a dificultades respecto de la normativa aplicable.

En virtud de contar con normativa sobre Protección de Datos dicha Comunidad sostiene como regla general que: sólo puede hacerse transferencias de datos con consentimiento de su titular (art. 34.e LOPD) y con destino a Estados miembros de la Unión Europea (art. 34.k LOPD). 20

Con carácter general, se dispone que **podrán llevarse a cabo transferencias de datos** que **tengan como destino Estados extra-comunitarios cuando los órganos** competentes **de la Unión Europea,** en el ejercicio de sus competencias, hayan **declarado que garantizan un nivel de protección adecuado**" (art. 34.k LOPD; arts. 25.6 y 31 DPDP).

20- LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

No obstante puede presentarse el caso en que los datos sean tratados fuera de la Unión Europea y sea transferido a un estado de esa Comunidad, por tanto si esos datos correspondieran a ciudadanos extracomunitarios es factible que estos no formulen reclamaciones en defensa de su intimidad informática, sin embargo este derecho corresponde a todas las personas sin distinción de nacionalidad (art. 1 LOPD; considerando 2º DPDP), por tanto que una eventual reclamación produciría plenos efectos. 21

Por el contrario si los datos correspondieran a un español, es posible que él pudiera reaccionar contra una eventual transferencia de sus datos, en virtud que su ley le faculta, el derecho para poder hacerlo, en vista que desde el momento en que la información o datos lleguen a un sujeto radicado en España se hace factible su "autodeterminación informativa" y la posibilidad de controlarlos, así como exigir las garantías orgánico-procedimentales de tal derecho, estableciendo sanciones.

Según la Ley española posibilita a la Agencia de Protección de Datos la realización de inspecciones y el establecimiento de sanciones, cuando los datos fueran obtenidos sin el consentimiento de los afectados.

Al interior de la Comunidad Andina el tema del comercio electrónico ha sido debatido intensamente, a fin de promover el desarrollo armónico y equilibrado de sus Países Miembros, a través del uso de las nuevas tecnologías por medio del comercio virtual, generándose observaciones, recomendaciones y resultados muy importantes adoptando los siguientes principales:

- Exhortar a los países de la Comunidad Andina a que aproximen su legislación sobre la materia, para su posterior armonización.
- Evaluar todos y cada uno de los cuerpos jurídicos de cada país para evitar contradicciones o posteriores acciones en contra de las Leyes Marco que se implementen.

21- DPDP Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- Establecer los mecanismos e instrumentos jurídicos que brinden seguridad a las transacciones comerciales que se realizan por el medio digital. 22

Siendo lo óptimo que la CAN adopte una decisión comunitaria, que se aproxime a la construcción de una legislación supranacional, en el tema de seguridad y protección de Datos Personales para las transacciones realizadas por medio digital, a fin de alcanzar el desarrollo sostenible del comercio regional. Si bien el Comercio Electrónico es una modalidad de comercio que traspasa toda frontera, debe tomarse en consideración para su regulación, algunos aspectos como:

En el caso del **Consumidor**, quien debería ampararse en un acuerdo internacional sobre la "declaración de derechos del consumidor respecto de las garantías y las prácticas aplicadas en el comercio" así como a su derecho a la protección de la intimidad, teniendo en cuenta que existen leyes como la UNCITRAL, que establece, regula y determina los aspectos concernientes al comercio electrónico como: aplicación, definición, interpretación, modificación mediante acuerdo, requisitos y reconocimiento jurídico de los mensajes de datos, fuerza probatoria de los mismos, y validez de los contratos, entre otros.

Tributación: la fiscalidad o impuestos respecto de E-Bussines (o negocio electrónico), sobre las ventas electrónicas deberían ser objeto de una armonización internacional.

Derechos de Propiedad Intelectual: deberían basarse en los tratados multilaterales así como en los convenios pertinentes. La asignación de los nombres de dominios son establecidos por la ICANN (corporación que asigna las direcciones IP, asignación y registro de los nombres de dominio de primer nivel y gestión del sistema nombres de dominio en internet) la cual es una entidad de coordinación técnica de internet, organización mundial y no gubernamental, sin fin de lucro dedicada a: procurar y preservar la correcta y permanente operatividad de internet, impulsando la competencia en la red, promocionado su uso, y

22- Legislación sobre Comercio Electrónico en los Países Miembros de la Comunidad Andina. Análisis comparativo Recomendaciones para su armonización Junio de 2002.

promoviendo políticas consensuadas con todos los sectores para el desarrollo de la red de redes, con el fin de reducir los casos de infracción y litigios.

Flujo libre de información: Protegiendo por sobre todo los Datos Personales, no debe restringirse el flujo libre de información entre países garantizando de esta forma el derecho a la comunicación e información.

1.8 Incidencia de la protección de datos personales en el Comercio electrónico.

El Ecuador no cuenta lamentablemente, con una Ley de Protección de Datos Personales razón por la cual cuestiones de seguridad y privacidad respecto de los datos de carácter personal y/o confidencial no son tutelados en forma responsable y objetiva por parte de empresas, instituciones, comerciantes, o establecimientos de compras y/o servicios, etc. quienes cuentan con amplia información, que los usuarios les proporcionan mediante la red, quedando al arbitrio del comerciante: la utilización, manipulación, y disposición sobre dicha información, en vista de haberla obtenido con el consentimiento del cliente, lamentable realidad generada por la ausencia y desconocimiento de dicha Ley que en otros países como en Argentina, o en los Estados de la Unión Europea pueden tener.

La legislación de protección de datos en otros países del mundo tiene un papel importante a través del cual se atribuye a las empresas en la red algunos compromisos:

- La primera está relacionada con los compradores de manera directa en cuanto a: condiciones de uso, políticas de seguridad, ejercicio de derechos, transparencia de la información, etc.

- El segundo aspecto se encuentra relacionado con la estructura interna de la empresa y las relaciones con las autoridades de Protección de datos personales.

En el ámbito legislativo de la Comunidad Europea por ejemplo, en cuanto a la Protección de Datos en su Directiva 95/46/CE establece que se debe informar y obtener el consentimiento del ciudadano o del cliente, lo cual se encuentra

instituido en la mayoría de páginas electrónicas como Hotmail, Yahoo, HI5, entre otras que determinan las políticas y términos de uso, para que luego de aceptadas por el usuario, el comerciante o dueño de la pagina web pueda realizar con los datos recolectados lo que pretendiera, ya que los obtuvo en forma legal y los procesará con el consentimiento informado del cliente, de acuerdo a la Ley.

El cumplir con la Ley permite la consolidación del comercio electrónico, pues los consumidores al sentir confianza en internet, permiten que la brecha de especulación e incertidumbre y desconfianza sobre este canal de comunicación sea reducida. En otros países como en Argentina las empresas cumplen con la Ley de Protección de Datos al implantar sellos que indican el acatamiento con dicha Ley, pero es importante destacar que no solo con el efectivo cumplimiento de la Ley para la eficaz tutela de los Datos Personales se determina el factor preponderante para obtener confianza y grandes volúmenes en ventas a través de la red, ya que en la realidad en países como en los Estados Unidos donde no se reconoce el derecho a la intimidad informática, y luego del ataque terrorista del 11 de septiembre es él país que mayor reportes de crecimiento en ventas tiene a través del uso del comercio electrónico pese a tener una legislación vaga.

Existen estadísticas que demuestran, la preocupación por parte de los usuarios respecto de la seguridad y confiabilidad en Internet23:

El 87% de los usuarios de la red declaran estar preocupados, y un 56% pertenece a la categoría de los "muy preocupados"

El 86% de los usuarios que compran productos y servicios se muestran preocupados, y un 55%, "muy preocupados".

Un 85% de los cibernautas califican la recopilación de información personal de niños, sin el permiso paterno, como una práctica "muy grave" y el 48% de ellos otorgaron la misma calificación a la recepción de mensajes de correo electrónico no solicitado ("spam").

23- Fuente http://derin.uninet.edu/cgi-bin/derin/vertrabajo?id=16 consultado el 25 de julio del 2008 hora 8:30 am.

En torno al 70% de los usuarios de la red catalogaron las cuatro acciones siguientes como "muy graves":

- Seguimiento de qué sitios en la red visita cada persona y utilización indebida de esa información: 72%
- Introducción en Internet de información sobre personas presentes en registros públicos que permite la identificación de las mismas: 72%
- Lectura de mensajes de correo electrónico por personas a las que no van dirigidos: 71%
- Sitios de la red que recopilan las direcciones de correo electrónico de sus visitantes para recopilar listas de comercialización sin su conocimiento ni autorización: 70%

Es por esto que las organizaciones y empresas involucradas en el campo del comercio electrónico, deben invertir para: proteger los datos de sus clientes guardados en sus servidores en los que se almacena información importante, así como también en la utilización de protocolos de seguridad, firewall, etc. ofreciendo en sus páginas web a los clientes la opción del anonimato; estableciendo políticas de protección de datos personales y publicándolas en el sitio web, especificando la finalidad de la recopilación de la información, las futuras utilizaciones así como divulgación de éstos, la disponibilidad de la exclusión voluntaria, los procedimientos de acceso y corrección de los datos, los mecanismos de reclamación y enmienda, condiciones que constan, en la normativa de Protección de Datos Personales de la Comunidad Europea, la misma que debería ser adoptada como una Ley modelo para nuestros países de Sudamérica, adaptándola a nuestras realidades.

1.9 La protección de datos personales en el Ecuador.

En el Ecuador al pesar de no contar con ley especifica, sobre Protección de Datos podemos encontrar ciertas normas que destacan, la importancia de los mismos como son: La **Constitución**, **Ley Orgánica de Defensa al Consumidor**, **Ley de Propiedad Intelectual**, **Ley de Telecomunicaciones,** la **Ley de Comercio**

Electrónico, Firmas y Mensaje de Datos del 2002, y la **Ley Orgánica de Garantías Constitucionales.**

- **La Constitución Ecuatoriana** en el Art. 66.- establece que "Se reconoce y garantiza a las personas":

18. "El derecho al honor, y al buen nombre. La **ley protegerá, la imagen y la voz de la persona**."

19. "El derecho de la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución, o difusión de estos datos o información requerirán la autorización del titular o el mandato de la Ley."

20. "El derecho a la intimidad personal y familiar."

21. "El derecho a la inviolabilidad y al secreto de la correspondencia física y **virtual;** ésta no podrá ser retenida abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación."

La Ley Orgánica de Garantías Constitucionales en concordancia con la Constitución en el Art. 94. manifiesta : Acción de hábeas data.- "Toda persona por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico."

"Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos."

"Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley."

"La persona titular de los datos podrá, solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de los **datos sensibles**, cuyo archivo deberá estar

autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, esta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados."

Ley Orgánica de Garantías Constitucionales en el Art. 49 inciso 1estable "No podrá solicitarse la eliminación de datos personales que por disposición de la ley deban mantenerse en archivos públicos."
"Las presentes disposiciones son aplicables a los casos de rectificación a que están obligados los medios de comunicación, de conformidad con la Constitución."
"El concepto de reparación integral incluirá todas las obligaciones materiales e inmateriales que el juez determine para hacer efectiva dicha reparación."

Art. 50.- Ámbito de protección.-"Se podrá interponer la acción de hábeas data en los siguientes casos:

1. Cuando se niega el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que consten en entidades públicas o estén en poder de personas naturales o jurídicas privadas.
2. Cuando se niega la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten sus derechos.
3. Cuando se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa....."

Art. 51.- Legitimación activa.- "Toda persona, natural o jurídica, por sus propios derechos o como representante legitimado para el efecto, podrá interponer una acción de hábeas data."

En el reglamento de la **Ley Orgánica de Defensa del Consumidor**, en el Capítulo VII encontramos la importancia de la Protección Contractual Art. 38.- Para los efectos previstos en el Art. 41 de la ley, tanto los contratos de adhesión como los textos a los que éstos se remitan, o formen parte del mismo, deberán tener un tamaño de fuente no menor de diez puntos, salvo lo previsto en regulaciones internacionales.

Art. 39.- "Se entenderán incorporadas al léxico aquellas palabras que den a entender su significado como vocablos de uso frecuente y de general aceptación por parte de toda la comunidad, y no sólo por los entendidos en la materia de que se trate."

Art. 40.- "El consentimiento expreso del consumidor de someterse a los procedimientos de arbitraje y mediación en los contratos de adhesión, se podrá manifestar mediante una ratificación impresa debajo de la cual suscriba el consumidor, o con una señalización en un casillero, de la que se desprenda la aceptación para someterse a arbitraje, o cualquier fórmula que permita entender inequívocamente la aceptación expresa de cualquiera de estos procedimientos por parte del consumidor."

Art. 43.- Para el cumplimiento del inciso segundo del Art. 44, el abonado o usuario podrá exigir el cese inmediato de la provisión del servicio contratado, debiendo cumplir con las obligaciones indicadas en el citado artículo.

- **La Constitución en el Titulo III Sección novena de las Personas usuarias y consumidoras Art. 52 manifiesta** **"**las personas tienen derecho a disponer de bienes y servicios de optima calidad y a elegirlos con libertad, así como a una información precisa no engañosa sobre su contenido y características**"**

No obstante es importante, que el usuario (comprador) cuente con toda la información veraz y precisa sobre las características del producto que va adquirir a través de Internet en virtud, que previa a la adquisición del bien o servicio el comprador debe conferir al vendedor los datos personales pertinentes a fin de formalizar el contrato.

- **La Ley de Propiedad Intelectual también** establece algunas regulaciones al respecto:

Art. 26.- "También Constituyen violación de los derechos establecidos en este Libro cualquiera de los siguientes actos:

a) Remover o alterar, sin la autorización correspondiente, **información electrónica** sobre el régimen de derechos; y,

b) Distribuir, importar o comunicar al público el original o copias de la obra sabiendo que la información electrónica sobre el régimen de derechos ha sido removida o alterada sin autorización."

Se entenderá por información electrónica aquella incluida en las copias de obras, o que aparece en relación con una comunicación al público de una obra, que identifica la obra, el autor, los titulares de cualquier derecho de autor o conexo, o la información acerca de los términos y condiciones de utilización de la obra, así como número y códigos que representan dicha información.

Por tanto podemos manifestar que el Comercio Electrónico y los derechos de los usuarios en nuestro país se encuentran comprometidos y tutelados principalmente por la Ley Orgánica del Consumidor, La Ley de Comercio Electrónico, y la Constitución de la República.

- **La Ley especial de Telecomunicaciones numero 84.** manifiesta en el Art. 14.- Derecho **al secreto de las Telecomunicaciones**.- El Estado garantiza el derecho al secreto y a la privacidad de las telecomunicaciones. Es prohibido a terceras personas interceptar, interferir, publicar o divulgar sin consentimiento de las partes la información cursada mediante los servicios de telecomunicaciones.

Esta disposición demuestra claramente que en el Ecuador, se garantizará que el servicio de Internet o telefonía móvil prestado tanto por las operadoras estatales como privadas deben cumplir con las disposiciones de la Ley Especial de Telecomunicaciones.

- **La Ley de comercio electrónico, firmas y mansajes de Datos del Ecuador** manifiesta en el Art. 1.- Objeto de la Ley.- Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

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

Art. 9.- Protección de datos.- 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.
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.

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.
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.

La ley ecuatoriana de comercio electrónico, firmas y mensajes de datos es clara en demostrar que precautela la seguridad de datos, al **legislar respecto del** uso de la firma electrónica como medio técnico de seguridad dentro de las comunicaciones que se realizan por medio de Internet, mecanismo que en la actualidad es utilizado alrededor del mundo con muy buenos resultados, como por ejemplo en el caso de las transacciones que se realizan a través del comercio electrónico, otorgando protección a las partes intervinientes. En nuestra ley se

consideran dos principios fundamentales con los que estoy de acuerdo como: la confidencialidad y reserva de los mensajes de datos, pues se debe precautelar el derecho a la privacidad e intimidad personal, siendo importante resaltar la prohibición que dicha normativa determina en cuanto a la intrusión por parte de terceros así como a la transferencia ilegal de datos trasmitidos, pues será necesario para ello el consentimiento expreso del titular de los mismos en virtud de precautelar los derechos a la intimidad, privacidad, y confidencialidad de la persona los cuales se encuentran amparados y garantizados por la Constitución. Sin embargo desde mi punto de vista personal, esta ley debería ser mayormente difundida, a la sociedad en razón que en la actualidad a diario se producen muchas infracciones informáticas a través de la red, y los usuarios no tenemos el conocimiento oportuno sobre los mecanismos de seguridad que podemos utilizar dentro de las comunicaciones así como los derechos que la ley nos otorga, pues la tecnología ha puesto en nuestras manos las herramientas necesarias para hacer efectivo el goce de nuestros derechos.

10 Técnicas de protección de datos: CRIPTOGRAFIA

El ser humano siempre ha estado en la constante búsqueda, de métodos a través de los cuales pudiera sobre guardar sus secretos y así evitar ponerlos al alcance de terceros. Ejemplo es el caso del emperador romano Julio Cesar quien empleaba en aquel tiempo un sencillo algoritmo para evitar que sus comunicaciones militares fueran interceptadas o en el caso de Leonardo Da Vinci quien tenía un interesantísimo mecanismo de escribir las anotaciones sobre sus trabajos de derecha a izquierda y con la mano zurda entre otros.

Un claro ejemplo de Criptografía clásica a través de la historia la encontramos en la "escítala lacedemonia" que data del siglo V a. C. y consistía en utilizar dos bastones idénticos, empleados uno en emisión y otro en recepción, alrededor de ellos se envolvía una tira de pergamino y se escribía el mensaje en vertical, y se extraía la cinta.

Etimológicamente la criptografía viene**:** "(del griego *kryptos*, «ocultar», y *grafos*, «escribir», literalmente significa «escritura oculta») es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos." 24

El diccionario de la Real Academia define a la criptografía como " el arte de escribir con clave secreta o de un modo enigmático".
Autores definen a la criptografía como: "aquella ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones". Mientras que otros la definen como la ciencia de la comunicación segura y que su objetivo consiste en que dos partes puedan intercambiar información sin que una tercera no autorizada, sea capaz de descifrar la información a pesar de que capte los datos."

El ámbito de aplicación de la Criptografía abarca a: datos, textos, e imágenes, voz por medio de la Criptofonía (voz) y Criptoanálisis (ciencia que estudia los pasos y operaciones orientados a transformar un criptograma en el texto claro original, sin conocer inicialmente el sistema de cifrado utilizado y/o la clave). 25
La criptografía es la disciplina o ciencia que estudia el modo de transformar un mensaje (texto original) en un texto en cifra (criptograma) mediante una operación de cifrado que hace imposible a un tercero tener acceso y tomar conocimiento del contenido de un mensaje, que circule por Internet, entre otras vías.

El uso de la criptografía es tan antiguo como la escritura, de manera que podemos observar que la misma ha renacido con fuerza, debido a la multitudinaria aplicación que tiene a través de los sofisticados sistemas informáticos y el desarrollo de métodos y algoritmos de cifrado.

24 http://es.wikipedia.org/wiki/Criptograf%C3%ADa consultado el 24 de julio del 2008 a las 12:00am
25*http://www.delitosinformaticos.com/firmaelectronica/analisis.shtml por Hugo Daniel Carrión consultado el 20 de julio del 2008 a las 10:00 am*

En la Actualidad la criptografía ofrece las siguientes ventajas; Seguridad: certeza de que el texto del mensaje solo puede ser leído por el destinatario Integridad: convicción de que el mensaje, asegura que no ha existido manipulación posterior de datos Autenticidad: certeza del remitente, pues acredita quien es su autor No rechazo: no se puede negar la autoría de un mensaje enviado26

HISTORIA DE LA CRIPTOGRAFIA

En la antigüedad los espartanos habían ideado un inteligente instrumento de criptografía, el biógrafo y ensayista griego Plutarco en su obra "Vidas Paralelas" narra cómo los magistrados en aquella época cuando enviaban a un jefe militar al exterior de su territorio, le entregaban un bastón de madera, llamado escítala, y otro exactamente igual lo conservaban ellos, cuando existía la necesidad de comunicar algo de gran valor e importancia que ningún otro debía saber. Entonces cortaban un rollo de papiro y lo envolvían alrededor de la escítala que tenía en posesión, cubriendo toda la superficie del bastón sin dejar ningún espacio, una vez cumplida esta operación, escribían sobre el mismo el mensaje, luego enviaban el papiro sin el bastón, el general cuando lo recibía, no podía leer el mensaje hasta tanto no envolvía el papiro en su bastón. 27

En este ejemplo ya podemos reconocer claramente los elementos constitutivos de cualquier sistema criptográfico como son: el algoritmo que es el conjunto de operaciones que permite hacer incomprensible el mensaje descomponiéndolo en una secuencia de caracteres no inteligibles inmediatamente, en el ejemplo que acabamos de ver sería el papiro y la clave (llave) es el elemento que, asociado a un algoritmo criptográfico, permite la encriptación y la descencriptación del texto cifrado, en el ejemplo sería el bastón.
Cuatro siglos después surge un innovador método de criptografía y es así como en la obra "Vita Del Divo Giulio", se describe el método empleado por Julio Cesar cuando quería intercambiar mensajes con los comandantes de su legión.

26 Apuntes de clases del módulo la Firma Digital del Dr. José Luis Barzallo en la Maestría Derecho Informático de la Universidad Estatal de Cuenca.

27Enciclopedia virtual Microsoft Student con Encarta Premium 2009.

Para lo cual usa escribir en cifra, y esta consistía en una aparentemente disposición desorganizada de las letras, lo cual no permitía reconstruir la palabra original, puesto que la persona que aspiraba descubrir el mensaje y descifrarlo tenía que saber que debía sustituir cada letra por la tercera siguiente en el alfabeto y así sucesivamente.

Por lo tanto encriptar un texto será, aplicarle un algoritmo que en relación a una cierta variable (clave de encriptación), lo transformará en otro texto incomprensible e indescifrable para quien no posee la clave por lo cual la aplicación del mismo algoritmo y de la misma clave al texto cifrado devolverá el texto original. 28

A lo largo de los tiempos existieron grandes inventores como: León Battista Albertini quien en 1465 invento un método de sustitución polialfabética el cual constituyó un gran avance para la época. En el siglo XVI el criptólogo francés Blaise escribió un tratado sobre "la escritura secreta". Durante los siglos XVII, XVIII y XIX, los monarcas se interesaron por la criptografía, y las huestes de Felipe II utilizaron durante mucho tiempo una cifra con un alfabeto de más de 500 símbolos y el matemático francés François Viète consiguió criptoanalizar aquel sistema para el rey de Francia, el conocimiento de este impulsó una queja de la corte española ante el papa Pío V acusando a Enrique IV de utilizar magia negra para vencer a los ejércitos. Por otro lado María Estuardo, reina de los escoceses, fue ejecutada por su prima Isabel I de Inglaterra al descubrirse un complot de aquella tras un Criptoanálisis exitoso.

En el siglo XX durante la Gran Guerra y la Segunda Guerra Mundial, la criptografía empezó a mostrar avances significativos, utilizando nuevas herramientas que permitirían conseguir cifras seguras como las máquinas de cálculo, no obstante la máquina de cifrado, más trascendente fue la máquina alemana Enigma que era de rotores y automatizaba los cálculos significativamente para las operaciones de cifrado y descifrado de mensajes.

---

28 -LA FIRMA DIGITAL COMO MEDIO DE SEGURIDAD EN TRANSACCIONES ELECTRÓNICAS Y SU IMPLICANCIA JURÍDICA Autor Ing. Roberto Nina Ale Ingeniero en Informática y Sistemas, Corte Superior de Justicia de Tacna y Moquegua, Poder Judicial del Perú

Gracias a Claude Shannon y sus investigaciones sobre teoría de la información cuando termino la Segunda Guerra Mundial, la criptografía alcanzó un desarrollo teórico importante. A mediados de los años 70 el Departamento de Normas y Estándares norteamericano publicó el primer cifrador que sería el principal sistema criptográfico de finales de siglo, el Estándar de Cifrado de Datos o DES, gestando así el desarrollo de la criptografía teórica y práctica para aplicarla en la actualidad a la firma digital. 29

11.- Clases de Criptografía

Existen actualmente dos tipos principales de criptografía:

1.- Criptografía simétrica o de clave privada: consiste en el conjunto de métodos que permiten tener comunicación segura entre las partes siempre y cuando en forma previa se hayan intercambiado la clave correspondiente, o clave privada o simétrica. Es decir que de acuerdo a la simetría las partes deben tener la misma clave tanto para encriptar como desencriptar el mensaje con el riesgo de que un tercero pueda acceder a dicha clave creándose para superar este inconveniente en el año 1976 el sistema de criptografía asimétrica o de clave pública. 30

2.- Criptografía asimétrica o de clave pública*:* es el sistema basado en propiedades matemáticas de los números primos y que funciona con dos claves distintas estas dos claves se asignan a una persona siendo una pública y otra privada.

La criptografía de clave pública funciona de tal manera que lo que se encripta con la clave privada se desencripta con la pública y viceversa ejemplo: si un usuario desea recibir mensajes encriptados a través de este sistema, debe dar a conocer su clave pública de manera que cualquiera puede luego utilizarla para encriptar mensajes y enviárselos, estos sólo podrán ser desencriptados con la clave privada del usuario, a su vez el titular de la clave privada puede enviar

29 http://es.wikipedia.org/wiki/Criptograf%C3%ADa consultado el 24 de julio del 2008 a las 12:00am

30 http://www.delitosinformaticos.com/firmaelectronica/analisis.shtml consultado el 19 de julio del 2008 a las 10:00am por Hugo Daniel Carrión..

mensajes encriptados con su clave privada, y estos serán desencriptados con su clave pública.31

12 DE LA CRIPTOGRAFÍA A LA FIRMA DIGITAL.

De la criptografía antigua, se ha llegado a la firma digital gracias al desarrollo de la
tecnología y métodos informáticos, constituyendo una réplica moderna y segura de dicho sistema. Hoy la firma digital es un mecanismos capaz de garantizar que el mensaje enviado (previo haber sido firmado) no sea alterado, modificado, ni mutilado en su transmisión, llegando integro hacia el destinatario, certificando al receptor que el emisor es realmente quien dice ser (autenticación), y que el mensaje ha sido enviado por él y no por otro (no repudio), permitiendo comprobar la relación entre un mensaje y la clave utilizada.

Desde mi personal punto de vista la criptografía es una ciencia que ha evolucionado y se ha perfeccionado a través del tiempo, la misma que en la actualidad se encuentra íntimamente relacionada con la firma electrónica, constituyendo su base fundamental la cual deberíamos adoptarla todas las personas en el país a la hora de realizar transacciones por medio de la red, pues constituye un medio tecnológico de seguridad dentro de las comunicaciones, pues al estar basada en la criptografía a través de la aplicación de operaciones matemáticas transforma un texto original en un criptograma (texto indescifrable) imposibilitando a terceras personas tener acceso y conocimiento del contenido del mensaje que se comunica, precautelando principalmente datos personales que se trasmiten por medio de las transacciones que se realizan en el comercio electrónico, pues de lo contrario todo tipo de datos (personales, comerciales, etc.) que se comunican quedarían expuestos en forma vulnerable, ante la intercepción de terceras personas quienes de mala fe, pudieran utilizar dicha información maliciosamente (suplantaciones de identidad, estafas, etc.) convirtiéndose en total caos las comunicaciones que se desarrollan a través de Internet.

31http://www.foroabogadossanjuan.org.ar/Doctrina_Provincial/articulo_doctrina_olivares280501.htm consultado el http://www.entornoempresarial.com/?ed=18&pag=articulos&id=1211 por Dr. Leoncio Landáez Otazo consultado el

CAPÍTULO II

LA INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI), AUTORIDADES DE CERTIFICACION Y FIRMA DIGITAL

2.1 Generalidades y Antecedentes PKI

El PKI se fundamenta en la criptografía de Clave Pública, creada por Whitfield Diffie y Martín Hellman en 1976 la cuál ha sido utilizada en comunicaciones de carácter privada empleando claves públicas, de tal modo que la clave privada es importante para: "descifrar criptogramas y para firmar digitalmente, mientras que la clave pública debe ser utilizada para encriptar mensajes dirigidos al propietario de la clave privada y para verificar su firma, mientras el guarda en secreto su propio procedimiento de descifrado (clave privada)" 32

Técnicamente en la criptografía, una infraestructura de clave pública (PKI, Públic Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución de operaciones criptográficas, a fin de asegurar la identidad de los participantes en un intercambio de datos.

La infraestructura de clave pública se basa en identificaciones digitales, conocidas como "certificados digitales", que permite a los usuarios de internet autentificarse frente a otros usuarios, los cuales actúan como pasaportes electrónicos vinculando a un usuario de firma digital con su clave pública. 33

Las propiedades de la criptografía de clave pública, plasmada principalmente a través de la firma digital, garantiza en forma óptima el servicio de la autenticación de usuarios, a fin de asegurar la identidad de los mismos como signatarios de documentos o para garantizar el acceso a servicios distribuidos en la red, el no repudio una vez firmado un documento por parte del signatario no será posible que este se retracte, la integridad de la información a fin de evitar modificación de

32http://es.wikipedia.org consultado el consultado el 24 de julio del 2008 a las 13:00am
33http://enciclopedia.us.es/index.php/Infraestructura_de_clave_p%C3%BAblica consultado el 21/01/2010 a las 12:00pm.

los datos firmados, la auditabilidad para identificar y rastrear las operaciones especialmente en el estampillado de tiempo, y el acuerdo de claves secretas para garantizar la confidencialidad de la información intercambiada. 34

2.2 Estructura y Funciones del PKI.

En la infraestructura de clave publica la principal diferencia que existe en relación a la clave secreta, es la asimetría pues el sistema asimétrico es un sistema de cifrado de clave pública, en la qué las claves para cifrar y descifrar son distintas, e imposible de obtener una a partir de otra, por lo que si no se conoce la segunda clave es imposible descifrar el mensaje, logrando incluso verificar la integridad del mensaje, es decir si ha sido modificado, alterado, mutilado, etc. pues el criptograma no se descifrará de forma adecuada, demostrando que el mismo fue alterado o sustituido.35

Hasta hoy el sistema de clave asimétrica constituye el único método capaz de brindar la seguridad requerida por el ordenamiento jurídico para equiparar la firma digital a la firma ológrafa, y desde este punto de vista puede ser opuesta a terceros, ya que es posible no solo mantener la integralidad e inalterabilidad del documento sino además establecer con exactitud la persona del emisor sin que este pueda repudiar.36

En las operaciones criptográficas de clave pública, se utilizan algoritmos de cifrado que son conocidos y accesibles, razón por la cual la seguridad que brinda el PKI, está ligada a la privacidad de la clave privada y Políticas de seguridad que son muy importantes.

Generalmente, los componentes y participantes de la infraestructura de clave pública son:

- La autoridad de certificación que es la entidad de confianza que está facultada para emitir certificados en relación con las firmas digitales de las

34http://www.iec.csic.es/criptonomicon/susurros/susurros11.html consultado el 21/01/2010 a las 12:40pm.
35http://www.fundaciondike.org.ar/seguridad/firmadigital.html consultado el 27 junio del 2009 a las 13:00pm
36http://www.foroabogadossanjuan.org.ar/Doctrina_Provincial/articulo_doctrina_olivares280501.htm consultado el 12 de julio del 2009 a las 13:00pm.

personas, además ofrece o facilita los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumple otras funciones relativas a las comunicaciones basadas en las firmas digitales, a más de emitir y revocar certificados.

- La autoridad de registro la cual es responsable de verificar el enlace entre los certificados y la identidad de sus titulares.
- La autoridad de validación es la encargada de comprobar la validez de los certificados digitales.
- Los repositorios que son las estructuras encargadas de almacenar la información relativa al PKI. El repositorio de certificados y el repositorio de listas de revocación de certificados que incluye todos los certificados que por algún motivo han dejado de ser válidos antes de la fecha.
- La autoridad de sellado de tiempo, es la encargada de firmar documentos con el propósito de probar que existían antes de un tiempo determinado.
- Los usuarios y entidades finales son aquellos, que tienen un par de claves (pública y privada) y un certificado asociado a su clave pública, haciendo uso de la tecnología PKI (para validar firmar digitales, cifrar documentos para otros usuarios, etc.) 37

En nuestra realidad tomando en consideración la infraestructura del Banco Central del Ecuador, podemos manifestar que:

El Banco Central del Ecuador constituye hasta el momento la única entidad de certificación habilitada por CONATEL (Consejo Nacional de Telecomunicaciones) para operar en el país la cual goza de confianza y se encuentra facultada para emitir y revocar certificados digitales respecto de las firmas electrónicas que otorga, así mismo es responsable de verificar el enlace entre los certificados y la identidad de sus titulares, de igual forma comprueba la validez de los certificados digitales.

El Banco Central como entidad de certificación almacena toda la información referente a los certificados digitales que emite, permitiendo a través de

37*www.seguridaddigital.info/index.php?option=com_content&task=view&id=118&Itemid=26 consultado el 21 de enero del 2010 a las 16:30*

mecanismos automáticos el acceso público a las listas de certificados que se encuentran revocados o suspendidos.

Los usuarios de firmas electrónicas en el Ecuador pueden ser personas naturales o jurídicas del ámbito privado así como instituciones del sector público teniendo en consideración que en este último caso, la firma electrónica se proporcionará a través del representante de la institución a fin de poder establecer en el futuro las responsabilidades pertinentes.

Usos de la tecnología PKI

La tecnología PKI puede ser empleada en los siguientes casos:

1.- En Autenticación de usuarios y sistemas (login),

2.- En Identificación del interlocutor, cifrado y firmado de datos digitales, y

3.- Para asegurar las comunicaciones y garantizar el no repudio (negar la realización de una transacción).

De acuerdo a la realidad de la infraestructura del Banco Central del Ecuador, a través del empleo de la tecnología PKI, se puede realizar las siguientes funciones como: autenticación de los usuarios a través del uso de la firma electrónica, cifrado y firmado de datos digitales.

2.3 Generalidades y antecedentes.

La firma tiene la función esencial de acreditar la autoría de un documento, y tiene por objeto, representar formalmente el consentimiento y la aceptación del autor de un documento, por ende el acto de firmar da origen al nacimiento de derechos y obligaciones.

Julio Cesar Rivera manifiesta que: "La firma está compuesta por trazos que forman el modo habitual que tiene la persona de escribir su nombre con la finalidad de manifestar la adhesión de su voluntad al texto a cuyo pie la pone." 38

38Rivera Julio Cesar, Instituciones de Derecho Civil, Tomo II, pág. 730, Edit. Abeledo Perrot. http://www.foroabogadossanjuan.org.ar/Doctrina_Provincial/articulo_doctrina_olivares280501.htm consultado el 12 de julio del 2008 a las 11:50am

En la actualidad, la firma manuscrita "certifica el reconocimiento o el acuerdo de voluntades sobre un documento por parte de cada firmante, por lo tanto el acto de firmar denota una gran importancia desde el punto de vista legal, pues es relevante, y sólo puede ser realizada por una persona y comprobada por otra con la ayuda de una muestra de la misma. 39 No obstante la firma manuscrita puede ser falsificada u obtenida con: engaño, coacciones u otro ilícito proceder perdiendo legalmente su validez.

ANTECEDENTES

En Roma los documentos en los tiempos antiguos no llevaban firma, sino que existía una ceremonia llamada manufirmatio, por lo que luego de la lectura del documento por parte del autor, o por el notarius, dicho documento era desplegado sobre una mesa, y se le pasaba la mano por el pergamino, de tal forma que este acto significaba la aceptación por parte del autor del documento sobre el contenido del mismo, y solo después de cumplida esta ceremonia se estampaba el nombre del autor del documento.

En el Sistema Jurídico Visigodo, las leyes otorgaban mucha importancia, a las formalidades documentales, regularizando las suscripciones, signos y comprobaciones de las escrituras, la presencia de testigos era un requisito fundamental pues ellos al tocar con sus manos, signar, o suscribir el documento, daban la confirmación de que el documento en realidad existencia.
Habían dos elementos la "subscripto" que representaba el nombre del signante y la fecha, y el "signum", que significaba un rasgo que sustituía en el caso de que la persona, no supiera o pudiera escribir, la "subscripto" daba pleno valor probatorio al documento y el "signum" debía ser completado con el juramento de la veracidad por parte de uno de los testigos si faltaba la firma y el signo del autor del documento, él documento era inoperante.

39http://www.delitosinformaticos.com/firmaelectronica/analisis.shtml autor del artículo Hugo Daniel Carrión consultado el 26 de junio del 2008 a las 12.00am.

En la Edad Media se da la aparición del sello real, que tuvo una labor importante, ya que garantizaba la autenticidad del documento.

2.4 Definición de Firma

La Firma etimológicamente, proviene del latín "firmare" que significa: "afirmar, dar fuerza".40

La Real Academia Española de la Lengua, define a la firma como: "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 o para obligarse a lo que en él se dice".

En el Vocabulario Jurídico a la firma se la define como: "Trazado gráfico, conteniendo habitualmente el nombre, los apellidos y la rúbrica de una persona, con el cual se suscriben los documentos para darles autoría y virtualidad y obligarse en lo que en ellos se dice.

Planiol y Ripert definen a la firma como: "una inscripción manuscrita que indica el nombre de una persona que entiende hacer suyas las declaraciones del acto**"**41

Guillermo Cabanellas la define como: "Nombre y apellido o título, que se pone al pie del escrito, para acreditar que procede de quien lo escribe, para autorizar lo allí manifestado u obligarse a lo declarado en el documento"42.

2.5 Clases de firmas Manuscrita, Electrónica, Digital.

Acorde a un análisis jurídico realizado por el Doctor José Luis Barzallo, presenta los siguientes tipos de firmas:

1) La Firma Manuscrita

Es la firma propia del signatario, por medio de la que se lo identifica. La firma manuscrita certifica el reconocimiento, o el acuerdo de voluntades sobre un

40 MANTILLA MOLINA, Roberto L. Citado por: ABASCAL ZAMORA, José María, En: Diccionario Jurídico Mexicano, "Firma", Instituto de Investigaciones Jurídicas, UNAM, T-D-H, 2ª edición, Porrúa, México, 1987, pág. 1453.
41 PLANIOL y RIPERT, Traité Practiqué De Droit Civil Français, VII, núm. 1458. Citado por REVIDATTI, Gustavo Adolfo En: Enciclopedia Jurídica Omeba, "Firma" Ob. Cit., pág. 290.
42 CABANELLAS, Guillermo, Diccionario Enciclopédico de Derecho Usual, T- A-E, 20ª edición, Heliasta, Argentina, 1981. pág. 76.

documento por parte de cada firmante, por lo que el acto de firmar denota importancia desde el punto de vista legal. No obstante la firma puede ser realizada por una persona y comprobada por cualquier otra con una muestra de la misma. La firma tiene características propias, lo que permite que su elaboración, sea sencilla y su comprobación sea vinculante con quien la realizo 43

Gabriel Campoli articulista de la revista virtual Alfa-redi unifica criterios en torno a la definición de Firma no ológrafa manifestando que: "es toda aquella realizada por cualquier otro medio que no sea la inscripción manual de los rasgos que identifican a una persona." En esta categoría podemos incluir a la firma digital, electrónica y cualquier otra realizada por medios técnicos o de cualquier otra especie"44.

2) La Firma a Ruego

Es aquella generada cuando una persona ya sea por qué no puede o no sabe firmar recurre a está, la cual sirve para defender los bienes de los socios del negocio, presentándose por lo general en las relaciones profesionales de derecho.

3) Firma Autorizada

Es aquella en la que un tercero autoriza mediante cualquier acto permitido por la ley como por ejemplo, en el caso de las personas jurídicas.

4) Rúbrica

La Real Academia de la lengua define a la rúbrica como "Rasgo o conjunto de rasgos de figura determinada, que como parte de la firma pone cada cual después de su nombre o título".

En la rúbrica generalmente se utiliza signos o símbolos para identificarse como un individuo determinado, no necesariamente irá acompañado del nombre o apellido,

---

43 www.delitosinformaticos.com/firmaelectronica/analisis.shtml articulista Hugo Daniel Carrión consultado el 26 de junio del 2008 a las 12.00pm

44 Campoli, Gabriel. Firma Ológrafa y no ológrafa. Revista Alfa-redi en www.alfa-redi.org consultado el 21 de julio del 2008 a las 13:15pm

no obstante es un requisito importante pues identifica de mejor manera a una persona, en todos los actos tanto públicos como privados, en que la utilice.

La rúbrica constituye un valor agregado para la firma, pues consiste en un rasgo que al añadirla al nombre y apellido de una persona proporciona cierto nivel o especie de seguridad, dificultando su falsificación debiendo para ello mantenerse siempre de igual forma el trazado de la misma.
Dentro de la categoría de firmas se destacan otro tipo de firmas, que se encuentran diseñadas a través de medios tecnológicos como:

a) La Firma Electrónica

Es aquella que emplea tecnología de alta seguridad, y puede ser utilizada para firmar todo tipo de documento, pues al emplearla dejamos constancia de la voluntad de identificarnos y obligarnos con lo que firmemos.

La Ley Modelo de **UNCITRAL** define a la firma electrónica como: "datos en forma electrónica consignados en un mensaje de datos, o 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 la información contenida en el mensaje de datos."

A su vez dentro del género de firma electrónica podemos encontrar otro tipo de firmas como:

La Firma Digital

El Dr. José Luis Barzallo la define como: "un tipo de firma electrónica basada en criptografía de clave pública y clave privada, la cual se respalda con certificados electrónicos"

La Firma Biométrica

Los sistemas biométricos son aquellos que se basan en las características físicas del usuario para comprobar su identidad, los sistemas de reconocimiento del

rostro, toman una instantánea digital de la cara y la confrontan con una base de datos, probando la identidad antes de admitirle cualquier transacción u actividad.
La biometría cada día avanza y se relaciona con el hardware y software para equipos, como por ejemplo en el caso de los periféricos "inteligentes" que pueden detectar si una persona se encuentra autorizada para utilizar cierto dispositivo.

Por último los sistemas de lápiz óptico, permiten "firmar" un soporte electrónico y pueden programarse para que reconozcan los "comportamientos de una firma", incluyendo la presión, la velocidad al firmar y la forma en la que se realizan los trazos de los caracteres45.

2.6 Generalidades de la Firma Digital

Si queremos realizar negocios en línea es imprescindible que los usuarios tengamos confianza, y seguridad para interactuar y ejecutar transacciones por medio del Internet, conviniendo utilizar para ello la "Firma Digital".

José Luis Barzallo define a la firma Digital como: "un tipo de firma electrónica basada en criptografía de clave pública y clave privada, la cual se respalda con certificados electrónicos"

Renato Javier Jijena Leiva manifiesta que **"t**ratándose de comercio electrónico, la firma digital es el sustituto tecnológico de la firma manuscrita u "ológrafa", y quien la use, junto con acreditar fehacientemente su identidad y con la imposibilidad de posteriormente repudiar el envío de un mensaje, jurídicamente hablando está manifestando su voluntad en orden a realizar una determinada transacción electrónica con un determinado "contratante", con una gran diferencia " la firma digital es mucho más segura."

La Firma Digital es un mecanismo técnico de seguridad, utilizado en las comunicaciones que se generan a través de medios electrónicos como el correo electrónico, y necesariamente útil en las transacciones de índole comercial a

45 José Luis Barzallo autor del trabajó presentado en el I Congreso Mundial de Derecho Informático. Organizado por la Comunidad Alfa-Redi y la OMDI en Quito-Ecuador. Del 15 al 18 de Octubre de 2.001

través de la red al no existir contacto físico entre las partes, constituyendo este tipo de firma una herramienta jurídica de identificación.

La Ley Modelo de la **UNCITRAL** otorga a la Firma Digital el principio de la equivalencia funcional en relación a la Firma Manuscrita, por tanto tendrán los mismos efectos y finalidades como:

a) atribuir la autoría de un documento a la persona que lo realizo; y
b) la aceptación del contenido del documento por parte de quien lo realizo.

Es necesario que este tipo de firma cumpla con los requisitos de la firma manuscrita, para que pueda obtener la misma validez y efectos jurídicos de la misma.

No obstante la Firma Digital es un mecanismo técnico que permite la transformación, de un mensaje utilizando métodos de encriptación, de tal forma que la persona que reciba el mensaje lo recepta encriptado con la clave privada del firmante, y solamente podrá leerlo sí posee la clave pública46.
En concreto la Firma Digital sirve para "la Identificación Indubitable de una persona que emite un mensaje, transacción o documento en medios electrónicos" la misma que busca evitar vicios del consentimiento que puedan generarse en los contratos a través de Internet. En el ciberespacio la verificación y constatación, de dicha firma lo realizará una entidad certificadora legalmente autorizada para operar, creadora de la Firma Digital. 47

2.7 Definiciones de Firma Digital.

El tratadista ecuatoriano José Luis Barzallo define a la firma Digital como: "un tipo de firma electrónica basada en criptografía de clave pública y clave privada, la cual se respalda con certificados electrónicos"

Renato Javier Jijena Leiva manifiesta que **"**Tratándose de comercio electrónico, la firma digital es el sustituto tecnológico de la firma manuscrita u "ológrafa", y quien

46 Trabajó presentado en el I Congreso Mundial de Derecho Informático. Organizado por la Comunidad Alfa-Redi y la OMDI en Quito-Ecuador. Del 15 al 18 de Octubre de 2.001
47 http://www.fundaciondike.org.ar/seguridad/firmadigital.html consultado el 27 de julio del 2008 a la 13:00pm

la use, junto con acreditar fehacientemente su identidad y con la imposibilidad de posteriormente repudiar el envío de un mensaje, jurídicamente hablando está manifestando su voluntad en orden a realizar una determinada transacción electrónica con un también determinado "contratante" pero con una gran diferencia la firma digital es mucho más segura.

Otros autores manifiestan que la firma digital, es un proceso criptológico que permite asegurar la identidad del autor del documento, y la inalterabilidad del contenido del mimo luego de haber sido confirmado, además de expresar la hora y fecha de dicha firma.48

En la **legislación Ecuatoriana** en el CAPITULO I SECCION DE LAS FIRMAS ELECTRONICAS no existe una definición de Firma Digital, si no que más bien encontramos la definición de firma electrónica:

Art. 13.- Firma electrónica.-"Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que pueden ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos."

La Ley Peruana No. 27269 define a la Firma Digital en el artículo 3 como "aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves únicas; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave pública."

2.8 Características de la Firma

La Ley Modelo de la **UNCITRAL** (United Nations Commission on International Trade Law/CNUDMI Comisión de las Naciones Unidas para el Derecho Mercantil Internacional) aplica el principio de la equivalencia funcional para la Firma Digital en relación a la Firma Manuscrita, por ende estas dos clases de firmas buscan los

48http://www.espaciosjuridicos.com.ar/datos/AREAS%20TEMATICAS/ECONOMICO/firmadigital.htm consultado el 30 de julio del 2008.

mismos efectos y finalidades, en virtud de que atribuyen autoría de un documento a la persona que lo realizó, y la aceptación del contenido del documento por parte de la misma.

Para ello será necesario que la Firma Digital cumpla con los requisitos de la firma manuscrita, a fin de que obtenga la misma validez y efectos jurídicos consecuentemente el objetivo de la Firma Digital será el brindar seguridad en los negocios que se generan a través de Internet.

Existen reglas importantes para la administración de la Firma Digital, por lo cual dicha firma identificará únicamente al signatario, y será solo él quien deba mantenerla bajo su control exclusivo, debiendo la firma contar para su validez con el certificado digital.

La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional *CNUDMI* en el artículo siete de la Ley Modelo establece los principios, que debe contener una firma para ser considerada como válida en el comercio electrónico.

Art. 7 (Ley Modelo) Firma.- Cuando la Ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos:

a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos; y

b) Si ese método es tan fiable como sea aprobado para los fines para los que se generó o comunicó el mensaje de datos, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo pertinente.

2). El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que no exista una firma. 49,

A demás podemos encontrar otras características de la Firma Digital como las siguientes:

49 Comisión de las Naciones Unidas para el Derecho Mercantil Internacional será interpretada por las siglas en inglés: UNCITRAL

a) La Firma Digital otorga certeza de la integridad del documento.

   Es decir que cuando se cambia algún dato, la firma queda inválida, pues mediante un procedimiento técnico conocido como hashing, que tiene semejanza con una pericia grafo técnica, verifica que la firma sea válida y pertenezca al firmante.

b) La Firma Digital es perfectamente susceptible de generar los mismos efectos de una firma manuscrita.

c) Pretende emular imitar y mejorar las funciones que cumple la firma manuscrita para los documentos tradicionales y como la firma digital es única, no puede negar que le pertenece.50

Nuestra legislación de Comercio electrónico, Firmas y Mensaje de Datos en cuanto a los requisitos legales para la validez de la firma digital exige:

Art. 15.- Requisitos de la firma electrónica.- Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

a) Ser individual y estar vinculada exclusivamente a su titular,

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

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

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

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

En cuanto a los requisitos teóricos tenemos: Identidad e Integridad, no obstante existen otros requisitos importantes como: la Autenticidad, Autoría, y no Repudio.

50 -LA FIRMA DIGITAL COMO MEDIO DE SEGURIDAD EN TRANSACCIONES ELECTRÓNICAS Y SU IMPLICANCIA JURÍDICA Autor Ing. Roberto Nina Ale Ingeniero en Informática y Sistemas, Corte Superior de Justicia de Tacna y Moquegua, Poder Judicial del Perú

1. **Identidad.-** la firma garantiza que los intervinientes son quienes dicen ser.

2. **Integridad.-** garantiza que ningún documento o información enviada entre vendedor o comprador pueda sustituirse, alterarse, o modificarse de modo malicioso e intencionado.

3. **Autenticidad** el documento o mensaje firmado, pertenece a un individuo determinado y como respaldo de ello la entidad certificadora se encarga de certificar o autentificar **reconociendo** el origen del mensaje (esto es válido incluso cuando no tenemos a la persona identificada, pues la garantía de identidad la ofrece el propio certificado, no la firma).

4. **Autoría** ninguna de las partes puede negar su participación activa, lo cual significa que en lo posterior las partes no pueden repudiar nada que hayan manifestado.

5. **No Repudio** significa el no rechazo, no negación por parte de la persona que ha firmado el documento.

6. **Confidencialidad e**s decir que la información ha sido cifrada y la voluntad del emisor, solo permitirá conocer el contenido de la información al receptor que él determine pueda descifrarla. 51

2.9 Diferencia entre Cifrar y Firmar

Cuando se **firma un documento** y no se lo cifra, el mensaje enviado es susceptible de ser interceptado, y leído por cualquier persona entonces: tendremos certeza de quién lo envía, pero no de la confidencialidad del mensaje y de su integridad.

Cuando **ciframos un documento**, tendremos la garantía de que el documento que ha sido enviado, goza de confidencialidad, requisito

51http://www.fundaciondike.org.ar/seguridad/firmadigital.html consultado el 27 de julio del 2009 a las 13:00pm

importante para que se desarrollen las relaciones comerciales a través de la red.

Sin embargo gracias a la firma electrónica y a su regulación legal en nuestro cuerpo normativo, se podrá realizar operaciones confiables y seguras como las que se efectúan mediante los documentos físicos. 52

2.10 Firma Digital versus Firma Manuscrita

La Firma digital constituye el equivalente a la firma de puño y letra en el mundo digital y goza del mismo valor jurídico que la manuscrita, sin embargo existe la importancia de diferenciar entre la Firma digital y la Firma digitalizada, ya que esta última es el resultado de pasar la firma manuscrita a través del scanner, quedando en claro que la firma digitalizada no es una firma digital.53

La equivalencia funcional entre firma electrónica y firma autógrafa, se cumple en Internet siempre y cuando la Firma electrónica cumpla con los siguientes requisitos:

1.- Que la Firma electrónica tenga una clave secreta que sólo posee el firmante.

2.- Que la Firma Electrónica tenga una clave pública que conoce todo el mundo,

3.- Que la Firma haya sido creada por un programa que sea capaz de comprobarla en lo posterior; y

4.- que tenga un certificado digital que asegure y garantice, que el poseedor de la clave secreta perteneciente a una clave pública es una persona concreta.

En nuestra legislación ecuatoriana con respecto a la validez y efectos de la firma digital en la Ley de Comercio Electrónico, Firma y Mensaje de Datos manifiesta lo siguiente:

Art. 14.- Efectos de la firma electrónica.- La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a la firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba.

52-LA FIRMA DIGITAL COMO MEDIO DE SEGURIDAD EN TRANSACCIONES ELECTRÓNICAS Y SU IMPLICANCIA JURÍDICA Autor Ing. Roberto Nina Ale Ingeniero en Informática y Sistemas, Corte Superior de Justicia de Tacna y Moquegua, Poder Judicial del Perú

53http://www.lasasesorias.com/es/publica/firmaelectronica/lafirmaelectronica.html consultado el 01 de agosto del 2008 a las 9:00am

Por ende para que la firma digital tenga la misma validez y eficacia probatoria que una firma de puño y letra, debe cumplir también con requisitos técnicos como mecanismos de seguridad, con la finalidad de garantizar a las partes contratantes que los datos utilizados para la elaboración del documento electrónico, son seguros y confiables, siendo importante que la firma garantice que no puede ser falsificada con la tecnología que existe a su expedición.

La Legislación Venezolana en cuanto a la Validez y eficacia probatoria, equipara la firma electrónica a la firma autógrafa y manifiesta lo siguiente:

> **"Artículo 16.** La Firma Electrónica que permita vincular al Signatario con el Mensaje de Datos y atribuir la autoría de éste tendrá la misma validez y eficacia probatoria que la ley otorga a la firma autógrafa. A tal efecto, salvo que las partes dispongan otra cosa,....."

Adicionalmente la Ley venezolana establece que la firma electrónica deberá cumplir con los siguientes aspectos:

- Garantizar confidencialidad, ofrecer seguridad de que no pueda ser falsificada, entre otras, y manifiesta que la Firma Electrónica podrá formar parte integrante del Mensaje del Mensaje de Datos o estar asociada a este, enviarse o no en un mismo acto"

Por tanto la Firma Electrónica goza de reconocimiento legal en virtud de tener equivalencia funcional, es decir que un documento electrónico firmado puede ser presentado como prueba "documental" en un procedimiento judicial o extrajudicial cuyo objetivo sea resolver una controversia sobre un hecho documentado a través de los medios electrónicos.

2.11 Las funciones de la Firma Electrónica

1. **Identificación de las partes o parte firmante:** la firma garantiza que los intervinientes son quienes dicen ser.

2. **Autenticación del contenido,** el contenido del mensaje se recibe íntegramente y sin modificación alguna, por tanto el contenido del documento electrónico firmado no puede ser alterado.

3. **Confidencialidad,** el contenido al estar cifrado sólo puede ser conocido por el firmante o por aquellos a quien el firmante autorice acceder al documento firmado.

4. **No repudio entre las partes,** garantiza que el firmante o las partes firmantes son quienes dicen ser, y por lo tanto ninguna de las partes puede negar haber firmado, enviado o recibido el mensaje. 54

El uso de la firma electrónica proporciona las siguientes ventajas:

1. **Independencia del momento en que se produce la firma:** podemos continuar la tramitación de un expediente sin necesidad de hacerlo desde el despacho, tampoco hay limitación horaria.
2. **Inmediatez de la acción**: cuando firmamos un documento, éste es transferido al responsable de hacer las siguientes gestiones para la tramitación.
3. **Rapidez:** no se necesita que el documento esté impreso para poder firmar el documento.
4. **Perdurabilidad y seguridad:** el documento electrónico está custodiado y protegido dentro del gestor documental, garantizando que existen copias de seguridad remotas. 55

En la Ley de Mensaje de Datos ecuatoriana en el CAPITULO I SECCION DE LAS FIRMAS ELECTRONICAS encontramos referencias atinentes a:

---

54 http://www.lasasesorias.com/es/publica/firmaelectronica/lafirmaelectronica.html consultado el 01 de agosto del 2008 a las 9:00am

http://www.entornoempresarial.com/?ed=18&pag=articulos&id=1211 articulista Dr. Leoncio Landáez Otazo *consultado el 05 de agosto del 2008 a las 10.00am*

55http://www.netfocus.es/es/EMPRESA/SALA_DE_PRENSA/ENTREVISTA_FIRMA_ELECTRONICA/ consultado el 10 de agosto del 2008 a las 12:30pm

Duración de la Firma

En el Art. 18 la Duración de la firma electrónica.- Las firmas electrónicas tendrán duración indefinida. Podrán ser revocadas, anuladas o suspendidas de conformidad con lo que el reglamento a esta ley señale.

Extinción de la Firma

Art. 19.- Extinción de la firma electrónica.- La firma electrónica se extinguirá por:
a) Voluntad de su titular,
b) Fallecimiento o incapacidad de su titular;

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

d) Por causa judicialmente declarada.

La extinción de la firma electrónica no exime a su titular de las obligaciones previamente contraídas derivadas de su uso.

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

En esta ley también encontramos, algunos deberes y responsabilidades que devienen del uso de la firma digital como:

Art. 17.- Obligaciones del titular de la firma electrónica.- El titular de la firma electrónica deberá:

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

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

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

d) Verificar la exactitud de sus declaraciones;

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

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

g) Las demás señaladas en la ley y sus reglamentos**.**

Desde el punto de vista jurídico la Firma Digital tiene funciones legales las cuales dependerán, del ordenamiento jurídico interno de cada país, al no existir normativa supranacional en torno al tema de las firmas electrónicas.

Consentimiento.- Cuando el titular firma un documento electrónico o mensaje, demuestra que conoce el contenido del mismo manifestando su voluntad. En el caso de las personas jurídicas se aplica la representación, por parte de los funcionarios para lo cual ellos deberán ser autorizados para actuar en nombre de la misma.

Nuestra Ley de Comercio Electrónico, Firmas y Mensaje de Datos, manifiesta:

Art. 13.- **Firma electrónica.-** Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que pueden ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos

Prueba.- Nuestra Ley de Comercio Electrónico, Firmas y Mensaje de Datos, manifiesta:

Art. 14 **Efectos de la firma electrónica.-** La firma electrónica tendrá igual validez y se le reconocerá los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida en prueba en juicio.

Vigencia de la firma.- la firma debe tener un período de vigencia para ser utilizada, será la entidad de certificación quien maneje los datos, y verifique los mismos existiendo un tiempo por el cual puede afirmar su certeza y veracidad. No obstante dichos datos son tomados en cuenta por terceros que se vinculan con el titular de la firma, siendo importante su conocimiento respecto del plazo durante el cual pueden confiar en que la firma otorga plenos efectos vinculantes respecto al titular.

La Ley de Comercio Electrónico, en él Art. 18 **Extinción de la firma electrónica.- "**las firmas electrónicas tendrá duración indefinida y podrán ser revocadas, anuladas o suspendidas de conformidad con lo que la ley señale."

Relación al titular: .- el Art. 15 de la referida ley manifiesta: **Requisitos de la firma electrónica.-**

Literal a) Ser individual y estar vinculada exclusivamente a su titular.

Oponibilidad frente a terceros.- los datos consignados en la firma electrónica son tomados en cuenta por terceros que se vinculan con el titular de la firma

Integridad.- La firma digital otorga certeza de la integridad del documento es decir que, no puede modificarse con posterioridad

Verificable.-

Literal b) que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta ley y sus reglamentos. 56

Nuestra ley de comercio electrónico regla aspectos muy importantes atinentes a: los requisitos, adquisición, uso, derechos, obligaciones, validez, extinción y efectos

56 http://www.entornoempresarial.com/?ed=18&pag=articulos&id=1211 autor Dr. Leoncio Landáez Otazo *consultado 05 de agosto del 2008 a las 9.00am*
http://www.netfocus.es/es/EMPRESA/SALA_DE_PRENSA/ENTREVISTA_FIRMA_ELECTRONICA/

que produce la firma electrónica, que de acuerdo a mi criterio se encuentran también encaminados a cumplir un objetivo principal que es la protección y no divulgación de datos de carácter personal que se trasmiten a través de la red, salvaguardando, el derecho a la intimidad, privacidad, y confidencialidad prevista en la Constitución del estado.

2.12 Diferencia teórica entre la Firma Electrónica y Firma Digital

Antes de establecer las diferencias entre estas clases de firmas, daremos las siguientes definiciones:

Apolonia Martínez Nadal define a la **Firma Electrónica** como "simplemente cualquier método o símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención actual de vincularse o autenticar un documento, cumpliendo todas o algunas de las funciones características de una firma manuscrita."57.

Otros autores la definen como "todo método derivado del desarrollo y del estado de la técnica electrónica u otra análoga, que por el uso de determinados sistemas técnicos, permite proteger bienes de naturaleza inmaterial e identificar el cumplimiento de los principios de integridad, autenticidad, disponibilidad, aceptación y validación;"58.

El tratadista José Luis Barzallo define a la firma Digital como: "un tipo de firma electrónica basada en criptografía de clave pública y clave privada, la cual se respalda con certificados electrónicos".

1.- Por tanto la Firma Digital constituye una especie de Firma Electrónica.

2.- La Firma Digital requiere la utilización de criptografía en clave pública, y por tanto es una secuencia de caracteres alfanuméricos que contiene los elementos que identifican al remitente. 59

---

57 Martínez Nadal, Apolonia. Comercio electrónica, firma digital y autoridades de certificación. Edit. Civitas. Segunda edición. 1.999. Pág. 39.
58 Espinoza Céspedes, Francisco. Contratación electrónica, medidas de seguridad y derecho informático. Editora RAO. 2.000. Pág. 125.
59 (Blanco, M. "Firma electrónica vs. Firma digital". Diario "El Universal". p. A/4. Caracas, 09.12.2000)

3.- La Firma Digital está ligada íntimamente al concepto de criptografía, asimétrica o clave pública, mientras que la firma electrónica es cualquier tipo de método que se utilice con la intención de firmar algún dato electrónico. 60

4.- La firma electrónica no es 100% segura como la Firma Digital, sin embargo se encuentra a ella ligada dos principios rectores como: la equivalencia funcional y la neutralidad tecnológica.

5.- "La firma digital a diferencia de la firma electrónica confiere seguridad jurídica.

6.- La firma o rúbrica digital constituye una versión legal de la firma manuscrita y por ende no hay dos iguales.

2.13 Los Certificados Digitales

Uno de los principales inconvenientes que surgen en Internet es el relacionado con la identificación de las personas o entidades, siendo una solución la utilización de certificados digitales que equivalen a una licencia de conducir, o cualquier otra forma de identidad, la cual es empleada conjuntamente con un sistema de cifrado de clave pública. 61

Un Certificado Digital es un Documento Electrónico, a través del cual un tercero confiable (autoridad de certificación ejemplo VeriSign) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública, dicho certificado contiene los datos de los algoritmos utilizados y del usuario, firmado digitalmente por la Autoridad de Certificación donde consta la Clave Pública del usuario constituyendo un fichero digital que no es modificable e intransferible. 62

Las entidades emisoras de certificados, tienen la responsabilidad de confirmar la identidad del titular del certificado, y ofrecer garantía al visitante de que el sitio web es confiable, a demás es importante que el emisor se encuentre acreditado, para que dicho certificado tenga valor y sea conocido por quienes interactúen con el propietario del certificado.

---

60 Apuntes en clases Maestría Derecho Informático Universidad de Cuenca.

61 http://www.iec.csic.es/criptonomicon/articulos/expertos51.html artículo publicado en internet por *Fernando Martínez consultado el día 22 de enero del 2010 el 15:00pm*

62 http://www.biocom.com/informatica_medica/legalrec_firma_digital.html *consultado el 22 d enero del 2010 a las 16:00pm*

En América Latina existen entidades facultadas para autorizar la creación de una autoridad de certificación o prestador de servicios como por ejemplo:

- En Chile, el Ministerio de Economía;
- En Colombia, la Sociedad Cameral de Certificación Digital Certicámara y GSE Gestión de Seguridad Electrónica;
- En Ecuador, el Banco Central del Ecuador;
- En España: la Fábrica Nacional de Moneda y Timbre, el Ministerio de Industria, Turismo y Comercio, la Agència Catalana de Certificació, la Autoritat de Certificació de la Comunitat Valenciana, etc.;
- En Guatemala, el Ministerio de Economía;
- En México, la Secretaría de Economía;
- En Perú, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual;
- En la República Dominicana el Instituto Dominicano de las Telecomunicaciones;
- En Venezuela, la Superintendencia de Servicios de Certificación Electrónica. 63

El formato de un certificado digital debidamente autorizado, debe contener por lo menos la siguiente información:

- Nombre, dirección y domicilio del suscriptor.
- Identificación del suscriptor nombrado en el certificado.
- El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
- La clave pública del usuario.
- La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
- El número de serie del certificado.
- Fecha de emisión y expiración del certificado.

63 http://es.wikipedia.org/wiki/Certificado_digital consultado el día 22 de enero del 2010 el 15:00pm

Dentro de las principales funciones que tienen los certificados digitales se puede destacar las siguientes: certificar que el sitio web y los recursos de red tales como servidores y routers son confiables, además de brindar protección a los datos intercambiados, de la manipulación o suplantación de identidad.

2.14 Generalidades de las Entidades Certificadoras.

La Ley de Comercio Electrónico ecuatoriana estable la regulación de las Entidades Certificadoras señalando desde el Art. 29 al 35 cuales son los requerimientos para que una empresa pueda constituirse como Entidad Certificadora, sus obligaciones, y responsabilidades, la garantía de la protección datos, la prestación de sus servicios, la terminación contractual entre el suscriptor del servicio o usuario y la entidad certificadora, así como la notificación de la cesación de sus actividades como entidad.

2.15 La legislación ecuatoriana y la confianza basada en los Certificados Digitales

El Certificado Digital es un documento electrónico, firmado digitalmente por la Autoridad de Certificación, donde consta la clave pública del usuario al que hace referencia, incluyendo los datos del usuario y los Algoritmos utilizados.64
En Internet a diario se constituyen miles de relaciones comerciales, basadas en la confianza al pesar de que las partes físicamente no se encuentren presentes y solo se comuniquen a través de la red, a la cual tienen acceso todas las personas, siendo lo normal que cada individuo adopte y manifieste la personalidad virtual que quiera.

Los certificados deben cumplir con los requisitos legales y técnicos, para ser certificados reconocidos, es decir que tiene respaldo o valor legal, los cuales promueven la confianza necesaria a los intervinientes para operar a través de la red la cual se traduce en documento electrónico original, denominándolo confianza digital. 65

---

64 www.certificadodigital.com.ar consultado el 20 de agosto del 2008 a las 14:00am
***65** AR: Revista de Derecho Informático ISSN 1681-5726Edita: Alfa-Redí No. 013 - Agosto del 1999 Confianza digital basada en certificados Por Ignacio Alamillo*

No obstante el requisito legal más importante que deben cumplir las Entidades de Certificación acreditadas es responder civilmente por daños y perjuicios por el incumplimiento de sus obligaciones respecto de los suscriptores.

A continuación me permitiré transcribir algunos de los artículos de la Ley de Comercio electrónico ecuatoriana:

"Art. 30 Son obligaciones de las entidades de certificación de información acreditadas: literal h) Contar con una garantía de responsabilidad para cubrir daños y perjuicios que se ocasionaren por el incumplimiento de las obligaciones previstas en la presente ley, y hasta por culpa leve en el desempeño de sus obligaciones. Cuando certifiquen límites sobre responsabilidades o valores económicos, esta garantía será al menos del 5% del monto total de las operaciones que garanticen sus certificados, de la misma forma el Art. 31 de la misma ley en mención manifiesta cual es la responsabilidad de las entidades Certificadoras:**"**

"Art. 31.- Responsabilidades de las entidades de certificación de información acreditadas.- Las entidades de certificación de información serán responsables hasta de culpa leve y responderán por los daños y perjuicios que causen a cualquier persona natural o jurídica, en el ejercicio de su actividad, cuando incumplan las obligaciones que les impone esta ley o actúen con negligencia, sin perjuicio de las sanciones previstas en la Ley Orgánica de Defensa del Consumidor. Serán también responsables por el uso indebido del certificado de firma electrónica acreditado, cuando éstas no hayan consignado en dichos certificados, de forma clara, el límite de su uso y del importe de las transacciones válidas que pueda realizar. Para la aplicación de este artículo, la carga de la prueba le corresponderá a la entidad de certificación de información.**"**

La ley de Comercio electrónico es clara en manifestar cuales son las principales obligaciones y facultades que la ley otorga a las entidades de certificación, resaltando como responsabilidad trascendental, el responder por daños y perjuicios causados a las personas por el incumplimiento o negligencia en el

desempeño de sus obligaciones, garantizando y precautelando de acuerdo a la ley el derecho a la confidencialidad y reserva de datos de carácter personal de los usuarios, pues deben ser resguardados, recibiendo un servicio de óptima calidad sin perjuicio de las sanciones establecidas en las leyes pertinentes, lo cual genera confianza en las personas para operar en internet a través del uso de la firma electrónica, pues cuenta con certificados digitales reconocidos los mismos que tienen valor legal.

Los contratos con los usuarios deberán incluir una cláusula de responsabilidad que reproduzca lo que señala el primer inciso, cuando la garantía constituida por las entidades de certificación de información acreditadas no cubra las indemnizaciones por daños y perjuicios, aquellas responderán aun con su propio patrimonio.

Los certificados reconocidos o acreditados tienen el valor agregado, como la integridad, autenticación, el no repudio legal, y la confidencialidad.

Existen certificados, denominados ordinarios los cuales no cumplen con los requisitos exigidos por la ley, por tal razón no respalda a la firma, y solamente acreditan un valor técnico a la misma.

La confianza basada en los certificados descansa en las garantías que ofrecen las entidades de certificación a los suscriptores o terceros en razón de que los certificados digitales constituyen estructuras de datos cuyo objetivo es, transmitir la identidad de una persona y su clave pública, así como determinar las manifestaciones del usuario en forma segura, y confiable, gracias a la firma que emite la entidad. 66

Desde mi personal punto de vista el uso de la firma electrónica en la actualidad, a través de las transacciones en el comercio electrónico y en las comunicaciones en general que se realizan a través del internet, es muy importante en virtud de que se precautela la seguridad de datos de índole personal, evitando que sean fácilmente interceptados por terceras personas, que pudieran utilizarlos en forma

66 AR: Revista de Derecho Informático ISSN 1681-5726Edita: Alfa-Redi No. 013 - Agosto del 1999Confianza digital basada en certificados Por Ignacio Alamillo

maliciosa e ilícita garantizando el derecho a la privacidad e intimidad personal. La firma electrónica al encontrarse respaldada por un documento electrónico llamado certificado digital, otorgado por una entidad certificadora legalmente acreditada, nos produce seguridad a los usuarios para operar a través de la red. Solamente por medio de la utilización de la firma asimétrica se puede precautelar todo tipo de información transmitida pues está basada en técnicas de criptografía que permite transformar un mensaje de datos o texto original en un texto indescifrable, garantizando que solamente el destinatario podrá descifrar el mensaje aplicando la clave publica del emisor.

CAPITULO III

MECANISMOS DE SEGURIDAD EN EL PAGO ELECTRONICO RESPECTO DE LA PROTECCIÓN DE DATOS PERSONALES

En la actualidad el comercio electrónico constituye un nuevo paradigma, dentro de las negociaciones, pues ha ido revolucionando las antiguas modalidades y costumbres dentro del comercio tradicional.

Hoy es frecuente que a través, de Internet adquiramos un sin número de artículos, bienes o servicios, por medio de la ejecución de transacciones, debiendo proporcionar para ello nuestros datos personales, de manera confiada sin tener la certeza de que si en verdad el vendedor será en realidad quien dice ser.

Sin embargo con el desarrollo tecnológico, todos estos obstáculos han ido quedando atrás en razón del aparecimiento de mecanismos tecnológicos que nos otorgan seguridad, permitiendo precautelar nuestros datos personales, a la hora de realizar transacciones a través de los medios de pago electrónicos, los mismos que producen confianza para operar en Internet.

3.1Generalidades

El realizar transacciones electrónicas de pago a través de Internet constituye un gran riesgo creándose, para ello mecanismos informáticos eficaces con el fin de garantizar la seguridad a través de los medios electrónicos de pago67.

Existen protocolos como el **SET** (SECURE ELECTRONIC TRANSACTION) que se ha desarrollado para la utilización en los pagos electrónicos y que además proporciona Autenticación y Privacidad sobre la información trasmitida, no obstante los riesgos de seguridad no residen en los protocolos utilizados sino en cómo se utilizan, siendo los diversos métodos de pago los que han de determinar los protocolos a utilizarse y el modo de hacerlo.

67- Los Medios de Electrónicos de Pago, Los Mecanismos de Seguridad en el Pago Electrónico por Mercedes Martínez González Capitulo I.

Los sistemas de pago deben contar con requisitos de seguridad esenciales y estar escoltados de técnicas criptográficas, con el fin de certificar que las transacciones electrónicas sean confiables, siendo el pilar fundamental de protección de datos en el comercio electrónico al momento de realizar los pagos la "Autentificación de las partes."

3.2 Los Métodos de pago en el Comercio electrónico.

Existen diversos métodos de pago electrónicos por ejemplo:
1.- Pagos con presentación de tarjeta sea de crédito o debito
Pagos sin la presentación de tarjeta
Pagos realizados a través de Internet
Pagos realizados utilizando teléfonos móviles
2.- Pagos realizados utilizando dinero electrónico
Digicash
3.- Sistema debito directo
En Internet
Mediante teléfono móvil
4.- Sistema de cuenta centralizada
Ejemplo PayPal, eBay
5.- Banca electrónica.-
6.- Sistema de cuenta telefónica.-
7.- Sistema de micro pagos
Ejemplo: Millicent y Payword

Pagos con tarjeta de crédito.- Debe existir una línea de crédito asociada a una tarjeta de cualquier marca. En una transacción, al momento de efectuar el pago se presenta la tarjeta y tanto el vendedor como comprador están físicamente presentes, efectuándose la autentificación mediante comprobación de la firma del cliente en la orden, respecto de la firma que consta en la tarjeta aplicando el **principio de Algo que se hace con el principio de Algo que se tiene** el cual se cumple con la presentación de la tarjeta de crédito.

No obstante el utilizar este tipo de sistema trae consigo riesgo como la clonación de la tarjeta, falsificación de la firma y no verificación de la misma por parte del vendedor.

Pagos sin la presentación de tarjeta o las llamadas transacciones MOTO (mail order/telephone order) utilizadas en situaciones en las que el cliente y el comerciante no se encuentran físicamente presentes, ejemplo: reservar habitaciones en hoteles, el método de autentificación utilizado se basa en **el principio Algo que el usuario conoce**, en este caso el tenedor o poseedor de la tarjeta proporcionará información relacionada con los números y fecha de expiración de la misma no obstante a fin de aumentar la seguridad se podrá solicitar información adicional que solo el usuario conoce como nombre, fecha de nacimiento, dirección, teléfono, etc.

Los pagos que se efectúan a través correo electrónico no son lo suficientemente seguros y por tal razón se utilizarán protocolos de comunicación como el **SMTP** mismo que no garantizará confidencialidad ni seguridad con la probabilidad de que ocurra suplantación de identidad. Existen otros canales de comunicación como las páginas web, en que las partes al no encontrarse físicamente presentes, el método de autentificación a utilizarse será idénticamente al aplicado en el método de pago anterior.

En el caso de los servidores web la solución a los problemas de confidencialidad y autentificación se remedian, mediante el uso de protocolos **SSL** por lo que el URL tendrá una ligera variante respecto de la habitual, garantizando la seguridad en la comunicación y la autentificación del servidor.
En el caso de utilizar los teléfonos móviles para la compra y pago de artículos existe una gran ventaja, al no requerir que el cliente ingrese sus datos confidenciales como número de tarjeta, pues el principio de autentificación fundamental aplicado en este sistema de pago será Algo que se tiene es decir el teléfono móvil debe estar en posesión del cliente y asociado con alguna tarjeta financiera suya. Los teléfonos móviles utilizan el protocolo USSD que garantiza la seguridad de los mensajes transmitidos, razón por la cual medios de servicios

como Mobipay (es un sistema que permite realizar pagos a través del teléfono móvil en tiempo real y de forma totalmente segura, dirigido especialmente a titulares de tarjetas) tiene ventaja sobre otros basados en un intermediario pues el comprador nunca facilita sus datos bancarios al vendedor, con lo que evita el riesgo de que dichos datos consignados sean almacenados en servidores in seguros.

Los riesgos más trascendentes en cuanto a la seguridad en los pagos con tarjeta son los siguientes:

- Autentificación inadecuada del cliente
- Canal inseguro (aquella vía de comunicación como por ejemplo internet, a través del cual, la información que trasmitimos puede ser fácilmente interceptada por un tercero, al no estar protegido con las medidas técnicas de seguridad que lo resguarden ante posibles ataques)
- Almacenamiento de datos personales o confidenciales en servidores poco o nada seguros, (es decir que cuando dichos servidores no se encuentren protegidos mediante el uso de corta fuegos, que denieguen el acceso a personas no autorizadas hacia la red privada, terceras personas en forma maliciosa, fácilmente pudieran sustraer o manipular dichos datos.)
- El dinero, monederos, y cheques electrónicos se caracterizan por no basarse en ningún tipo de cuenta, ya que este sistema de pago emula el dinero físico, utilizando un software que el usuario debe instalar en su ordenador procediendo abrir una cuenta en una institución capacitada para emitir y validar dinero electrónico, y consiste en cupones o unidades monetarias que no están asociadas a ninguna cuenta bancaria, pues bastaría que el usuarios solicite dinero electrónico en su cuenta o tarjeta, garantizándose el anonimato, seguridad y privacidad de datos, no siendo posible que el comerciante obtenga un perfil del usuario a partir de las compras que realice.

Dentro del sistema de debito directo, el usuario debe dar un permiso al comerciante o vendedor para retirar dinero de su cuenta bancaria, ejemplo: para pagar cuentas de teléfono, luz, etc., no obstante dicho debito se puede efectuar a través de internet o teléfono móvil, sin embargo este ultimo será el más conveniente en virtud de que un intermediario ejemplo Paybox estará facultado por el usuario para debitar de su cuenta la cantidad de dinero necesaria para realizar el pago de sus compras, debiendo asignarle un PIN al usuario para que pueda identificarse durante cada pago precautelando la privacidad y seguridad del mismo.

En la práctica este sistema funciona de la siguiente manera:
1.- El cliente escoge en la página web del vendedor la opción Paybox, luego el usuario deberá ingresar su número de teléfono en dicha página y solicitar que lo llamen, activándose una contestadora automática en la cual le pedirán que confirme la compra

tecleando su PIN de usuario, ratificando inequívocamente su voluntad de comprar, enviándole luego un mensaje de confirmación por parte de Paybox y será este quien se encargará de completar el cobro del pago con el banco del comprador.

En el sistema de cuenta centralizada en Internet el usuario deberá abrir una cuenta con una entidad intermediadora de pagos ejemplo Paypal recibiendo un password que le permitirá identificarse y autentificarse cada vez que realice un pago admitiendo incluso transacciones entre particulares (P2P), para esto se combinará el uso de pagina web y correo electrónico, una vez efectuada la autorización de pago por parte del pagador en la página web del intermediario este notificará un mensaje al receptor del pago debiendo este remitirse a la página web para confirmar dicha información, este sistema actúa como pasarela entre cliente y comerciante por lo cual, datos confidenciales estarán seguros garantizando seguridad y privacidad.

En el caso de Banca electrónica como el que aplica Instituciones financieras en nuestro país se tomará en consideración el canal que se empleará ejemplo

internet, celular, o teléfono convencional, empleando protocolo de seguridad en las comunicaciones. Ejemplo en internet se aplicará el protocolo SSL y un método de autentificación que estará relacionado con **Algo que se sabe** un password o con **Algo que se tiene** ya sea esta una tarjeta, dispositivo inteligente etc.

Sistemas Micro pagos es aquel utilizado para pagos muy pequeños donde el coste de la transacción es mayor que el del pago, debiendo destacar que utilizan cifrados muy débiles ejemplo de ello es Millecent, Payword, etc.

Por último los sistemas de cuenta telefónica, a los que se carga los pagos cuenta con un intermediario operador de la telefonía y que a diferencia de otros sistemas con intermediario no admite pago entre P2P, previamente debiendo el cliente firmar un contrato con el operador del servicio telefónico, para que le asigne un número especial y poder operar. En otros países este sistema no ha sido utilizado con el fin de trasmitir información confidencial, pero se han cometido muchas estafa

3.3 Requisitos de seguridad

Al momento de realizar pagos electrónicos a través de Internet se puede incurrir en diversos fraudes y estafas siendo determinante el método de pago empleado y la tecnología utilizada.

Uno de los principales riesgos en los pagos electrónicos suele ser la suplantación de identidad de una de las partes involucradas en la transacción, así como la exposición de datos personales o confidenciales al alcance de hackers, crackers, estafadores, espías e intrusos en la comunicación, dado por lo general a la escuálida protección del servidor que almacena la información, utilizado en el momento de la transacción como canal de comunicación entre las partes.

a) Suplantación del comprador: ocurrirá cuando un sujeto, tomando la calidad de impostor realice pagos electrónicas al vendedor por compras, con tarjetas de crédito, debito o cuenta bancaria que no le pertenecen y que no es autentico poseedor.
b) Suplantación del vendedor: en este caso el estafador buscará suplantar la identidad del vendedor utilizando trucos informáticos ejemplo clonando los servidores web de: entidades de pago, instituciones bancarias o paginas de

comercio con apariencia del sitio original, pues serán propicias para lograr sus objetivos consiguiendo que el incauto comprador caiga en su trampa a través del phising (término informático que denomina un tipo de delito dentro del ámbito de las estafas cibernéticas, caracterizado por intentar adquirir información confidencial de forma fraudulenta), con el fin de obtener datos confidenciales: números de tarjetas de crédito o cuenta bancaria, a fin de suplantarlo posteriormente en compras fraudulentas, no obstante la aplicación de la ingeniería social (la cual constituye la práctica de obtener información confidencial, a través de la manipulación de los usuarios de internet, para obtener acceso o privilegios en sistemas de información que les permitan realizar algún acto ilícito que perjudique o exponga a la persona a riesgo, siendo utilizada principalmente por los hackers o delincuentes cibernéticos) estará enfocada al envió de correo electrónico o spam, pues los estafadores incitarán al individuo a conectarse con su página web por medio de un enlace web que ellos mismos facilitarán a la víctima, bajo pretextos de: actualizar sus datos de tarjeta o cuenta bancaria, etc. a través de la pagina.

c) **Datos almacenados en servidores poco seguros**: sucede cuando el vendedor cuenta con servidores que no están protegidos ante eventuales ataques de hackers, en el que almacenan datos personales de los clientes, como números de tarjetas de crédito, cuentas bancarias, etc. en forma temporal hasta gestionar el proceso de pago con la institución bancaria convirtiéndose en un riesgo informático que afecta e incide en forma directa en el pago electrónico. Habitualmente **estos** riesgos **los** sufren las entidades financieras o servicio de pago, las cuales protegen sus servidores mediante firewalls (más conocidos como corta fuegos, son la parte de una red diseñada para bloquear el acceso a los usuarios a redes privadas conectadas a Internet. Todos los mensajes que entren o salgan de la intranet pasan a través del corta fuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados).

d) **Escuchas e intrusiones en la comunicación**: existe situaciones en que embusteros puedan escuchar la comunicación al momento de intercambiar

datos confidenciales entre comprador y vendedor para posteriormente realizar compras o actos fraudulentos en la red.

Los riesgos de seguridad dependerán del canal de comunicación empleado entre las partes ejemplo: internet, teléfonos móviles, etc. existiendo requisitos que deben cumplir los métodos de pago como la: **Autenticidad** la cual garantiza la no suplantación de las partes. **Integridad** garantizando que ningún documento o información enviada entre vendedor o comprador pueda sustituirse, alterarse, o modificarse de modo malicioso e intencionado. C**onfidencialidad**, que garantizará el no acceso de escuchas o intrusos en la comunicación dependiendo siempre del canal utilizado así como de los protocolos o mecanismos criptográficos empleados para obtener mayor seguridad.

3.4 La autenticidad de la identidad

La Autenticación es la fase más importante en el proceso de pago electrónico y consiste en "probar de modo interactivo la identidad ante un interlocutor". En el proceso de autenticación es común utilizar certificados digitales cuando los servidores se encuentran protegidos por protocolos de seguridad pues los certificados digitales serán otorgados y avalados por terceros de confianza, que gozan de reconocimiento y credibilidad. Otro de los mecanismos empleado para garantizar la autenticación es la firma digital, constituida por técnicas criptográficas, y funciones resúmenes garantizando de forma especial al comprador la no suplantación de identidad por parte del vendedor con la certeza, de con quien cree dialogar en verdad lo es.

El vendedor, no tendrá el riesgo de que el cliente repudie una compra, causándole perjuicios económicos.

En una tradicional transacción electrónica encontramos al comprador o cliente quién constituye sujeto principal de pago, ya sea por sí mismo o por interpuesta persona, seguido del vendedor o comerciante que es quién oferta y comercializa sus productos o servicios mediante la red siendo receptor del pago efectuado por el comprador, su banco o intermediario de pagos. En último lugar tenemos a las Entidades y Servicios Financieros quienes previa autorización del cliente efectúan

los pagos al vendedor, encargándose del movimiento de dinero entre cliente y vendedor. Aquí se cuenta con el Banco del comprador y vendedor, la pasarela de pagos de la tarjeta sea de crédito o debito y el mediador quien gestiona el servicio de pago. Las Entidades de Certificación, son las únicas instituciones que a través de la firma digital garantizará la validez de los documentos utilizados en las transacciones.

Principios fundamentales de la Autentificación

La Autentificación es la base de protección de datos en el comercio electrónico, la cual se fundamenta en los siguientes principios:

Algo que se sabe: en este caso se pregunta al usuario una información personal que solo él sabe ejemplo el **PIN** (número de identificación personal)

Algo que se tiene: es decir que el usuario es el tenedor y poseedor de un objeto físico especifico necesario, ejemplo teléfono móvil o tarjeta inteligente (chip con información de autentificación).

Algo que se es: este principio se encuentra íntimamente vinculado con referencias biológicas del usuario escáner de retina o de iris del ojo, voz etc.

Algo que se hace: es decir algo que reproduce el usuario como puede ser la voz o muestra de su escritura como la firma etc.

Existen medios a través de los cuales se realiza la Autentificación. En el tema de las Tarjetas magnéticas se utiliza la firma manuscrita del usuario, cuando se encuentra presente siendo la comprobación de la Autentificación visual, cuando las compras se realizan mediante vía telefónica y no se presente la tarjeta se consignan datos como: tipo de tarjeta, número de la misma, y fecha de caducidad, no obstante requieren de información adicional de cuatro dígitos que solo el usuario la conoce y que consta al reverso de la tarjeta de crédito.

Existen tarjetas inteligentes que están conformadas por chips que contienen toda la información referente al usuario, más seguras que las tarjetas magnéticas pero con la posibilidad de que la información contenida sea modificada, realizándose la comprobación de la misma con un número pin que solo el verdadero usuario conoce.

La Autentificación Biométrica considerada como el mecanismo más seguro, consiste en reconocer patrones o características biológicas del usuario, ejemplo huellas dactilares, patrones faciales, análisis del iris, y retina, etc.

La Autentificación en Internet se la realiza mediante el uso de protocolos como el SET y SSL que aplican firmas y certificados digitales, que regulan las transacciones electrónicas, autentificación realizada con antelación a que las partes intercambien información, en los pagos móviles siendo necesario que el comprador este en tenencia del teléfono (tarjeta SIM) y conozca el Pin de usuario, combinándose dos principios de la autentificación, algo que se tiene con algo que se sabe

3.5 Justificabilidad de la Firma Digital en las transacciones electrónicas dentro del E- Commerce

Las comunicaciones a través de la red se encuentran en constante peligro, pues múltiples son los ataques que efectúan los hackers, con la mala intención de interferir en las mismas y así obtener la información deseada, siendo necesario optar por medidas de seguridad como: la firma digital a fin de evitar daños, siendo justificable el uso de la misma en el momento en que se celebran contratos, o efectúan transacciones, on-line, a través de la red de libre acceso.

La Firma Digital surge para garantizar confidencialidad en las comunicaciones, y constituye el único medio tecnológico que satisface aspectos de seguridad como:

Integridad de la información: que constituye garantía contra la modificación de datos en forma intencional o accidental.

Autenticidad del origen del mensaje: garantiza al receptor que el mismo ha sido generado por la parte identificada en el documento como emisor, sin posibilidad de suplantar al sistema.

No repudio del origen: protege al receptor del mensaje respecto de la negación realizada por el emisor, pues no podrá negar que ha generado dicho mensaje, convirtiéndose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

Imposibilidad de suplantación: el hecho de que la firma sea creada por el signatario mediante medios que conserva bajo su control asegura la imposibilidad de suplantación por parte de otro individuo.

Auditabilidad: permite identificar y rastrear las operaciones efectuadas por el usuario dentro del sistema informático cuyo acceso se ejecuta mediante la presentación de certificados" 68

68- http://www.delitosinformaticos.com/firmaelectronica/analisis.shtml Articulista: Hugo Daniel Carrión consultado el 20 de julio del 2009.

CONCLUSIONES

Frente al progreso acelerado que la tecnología ha obtenido y a la dependencia que esta ha llegado a generar en los seres humanos, a tal punto de influir de manera determinante en nuestra forma de vida, remplazando costumbres y tradiciones por nuevos hábitos y modalidades a través del uso del Internet, el cual se ha producido por la globalización tecnológica.

En la actualidad observamos que través de Internet, millones de personas realizan a diario, compras, comunicaciones, trasmisión de datos, y comercio electrónico observando que este último ha remplazado a la antigua modalidad de hacer comercio, convirtiéndose en una tendencia mundial en la era de la globalización produciendo una indudable revolución en las transacciones comerciales, la misma que ha significado un cambio cultural y un nuevo paradigma en las negociaciones.

Sin embargo alrededor del mundo observamos que diariamente se producen delitos e infracciones electrónicas, que perjudican a miles de personas que operan a través de Internet, al momento de realizar comunicaciones, transferencias, comercio electrónico por medio de las cuales se trasmite datos principalmente de índole personal tales como nombres, direcciones, números de tarjetas de crédito, teléfonos, edad entre otras, cuyos titulares no toman las medidas técnicas de seguridad, en algunos casos por desconocimiento, dando como resultado la consecución de estafas, intercepción de mensajes, suplantación de identidades, sustracción y manipulación de la información entre otras, situaciones que con el tiempo han demostrado a los usuarios de Internet la necesidad de utilizar la firma electrónica a fin de precautelar sus datos trasmitidos, en razón que la información en la actualidad se ha convertido en el cuarto factor económico a nivel mundial superando a las materias primas, trabajo y capital.

Es por ello que la firma electrónica, por medio de la criptografía nos permite realizar contratos y transacciones, a través de Internet con seguridad y confianza sin el futuro temor de enfrentar repudio, rechazo o suplantación de identidad en un mensaje de datos, pues la firma electrónica ha reportado alrededor del mundo importantes efectos en cuanto al crecimiento del correo electrónico, pues dicha

firma se encuentra respaldada por certificados digitales otorgados por terceros de confianza, otorgando seguridad para operar en Internet.

Por tanto la firma electrónica tienen un papel protagónico muy importante ya que salvaguarda en forma efectiva Datos Personales trasmitidos a través de la red, demostrando la reducción considerable de incidentes e infracciones informáticas, tornándose más seguras las comunicaciones que se realizan a través de Internet.

RECOMENDACIONES

De acuerdo a las estadísticas, lamentablemente en el Ecuador el Comercio Electrónico no ha despertado en forma masiva, debido principalmente a la falta de información respecto de la seguridad o mecanismos tecnológicos, para salvaguardar nuestra información que la trasmitimos por medio de la red, pero sobre todo por la desconfianza que nos ha generado Internet, pues al no existir en nuestro país un marco regulatorio especifico que garantice la privacidad, confidencialidad, e intimidad personal de Datos Personales que trasmitimos a través de la red de redes, imperará el miedo y rechazo a realizar transacciones en razón de no existir garantías para la protección y respeto del Derecho a la intimidad informática.

Es por ello que como recomendación propongo:

1. Que el Ecuador a través del Banco Central del Ecuador en calidad de Entidad Certificadora realice boletines, talleres, seminarios, y cursos gratuitos en forma permanente en colegios, universidades, escuelas, instituciones públicas y privadas a fin de sociabilizar los beneficios y usos de la Firma Electrónica.
2. Que se determine la obligatoriedad del uso de la firma electrónica para la emisión de disposiciones, resoluciones, y dictámenes al interior de las instituciones públicas a fin de que se generalice el uso de la misma, en virtud que debe reestructurarse en primera instancia el proceso de gestión organizativa al interior de las instituciones públicas, a fin de agilitar los tramites y llegar hacia la etapa de oficina sin papeles.
3. La creación de una Ley Orgánica de Protección de Datos Personales que tanta falta le hace a nuestro país en virtud de la necesidad de garantías, que existen en cuanto a la privacidad, confidencialidad, e intimidad personal respecto de los datos personales, pues considero desde mi personal punto de vista que resulta insuficiente las escasas disposiciones que el legislador ha implementado en diversos cuerpos normativos, pues con la implementación de una ley específica de Protección de Datos y la

complementación de la firma electrónica como mecanismo de seguridad técnica se logrará garantizar la protección al Derecho de la intimidad informática, generando en los usuarios ecuatorianos de Internet la seguridad de realizar transacciones por medio del comercio electrónico.

BIBLIOGRAFIA:

- Francisco de Quinto Zumárraga, Protección de Datos Personales, Edit. Illustre Consell de Col-legis Oficials de Graduats Socials de Catalunya España, Marzo 2001
- Martínez Nadal Apolonia. Comercio electrónico, firma digital y autoridades de certificación. Edit. Civitas. Segunda edición. 1.999. Pág. 39.
- Martínez Nadal Apolonia, La ley de firma electrónica, Edit. Civitas, Madrid, Año 2000.
- Los Medios Electrónicos de Pago, Problemas Jurídicos, Director Ricardo M. Mata y Martin Coordinador Antonio Ma. Javato Martin Edit. Comares, España, Año 2005.
- Régimen Jurídico de Internet, Colección Derecho de las Telecomunicaciones, coordinadores Javier Cremades., Miguel Ángel Fernández- Ordoñez, Rafael Illescas, Edit. Temis, Colombia, Enero del 2002.
- Ricardo Luis Lorenzetti, Carlos Alberto Soto Coaguila, Comercio Electrónico Tomo 3, Edit. TEMIS S.A., Bogotá – Colombia, Año 2003.
- Carlos Ruiz Miguel, La configuración constitucional del derecho a la intimidad, Edit. Tecnos, Madrid, Año 1995.
- Valentín Carrascosa López, Informática y Derecho 5, Edit. ARAZANDI, Mérida España, Septiembre 1992.

Normativa Nacional:

- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos No. 67 del 2002 Publicada en Registro Oficial Suplemento No. 557 de fecha 17 de Abril de 2002.
- Constitución Política del Ecuador 2008 Publicada en Registro Oficial N0. 449 de fecha 20 de Octubre del 2008.

- Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional.
- Ley Orgánica de Defensa al Consumidor
- Ley de Propiedad Intelectual
- Ley de Telecomunicaciones

Normativa Internacional:

- CE Constitución Española
- DPCCD Directiva 97/7/CE, del Parlamento Europeo y del Consejo, de 20 de mayo de 1997, relativa a la protección de los consumidores en materia de contratos a distancia

- DPDP Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

- DPDPIT Directiva 97/66/CE, del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.

- DFE Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

- LGTel Ley 11/1998, de 24 de abril, General de Telecomunicaciones

- LODHI: Ley Orgánica 1/1982, de 5 de mayo, de protección del derecho al honor, a la intimidad personal y familiar, y la propia imagen

- LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- PCDCE Posición común nº 22/2000, aprobada por el Consejo el 28 de febrero de 2.000, con vistas a la adopción de la Directiva sobre el Comercio Electrónico.
- RDLFE Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.

Compilación de Documentos:

- Compilación documentos otorgados por la Dra. Sofía Espinoza Coloma en la cátedra de Sociedad de la Información.
- Compilación documentos otorgados por el Dr. Diego Ponce Vásquez en la cátedra.
- Compilación documentos otorgados por el Dr. José Luis Barsallo Sacoto en la cátedra de Mensaje de Datos y Firma Digital.
- Compilación documentos otorgados por el Dr. Miguel Summer Elías en la cátedra de Protección de Datos.
- Compilación documentos otorgados por el Dr. Ariel Agramont Loza "Los Últimos avances de la Tecnología SSL" Documento técnico de VeriSign.

Bibliografía Virtual:

http://web.usc.es/~ruizmi/pdf/e~com.pdf
http://derin.uninet.edu/cgi-bin/derin/vertrabajo?id=16
http://es.wikipedia.org/wiki/Criptograf%C3%ADa
http://www.delitosinformaticos.com/firmaelectronica/analisis.shtml por Hugo Daniel Carrión
http://www.foroabogadossanjuan.org.ar/Doctrina_Provincial/articulo_doctrina_olivares280501.htm
http://www.entornoempresarial.com/?ed=18&pag=articulos&id=1211 por *Dr. Leoncio Landáez Otazo*
http://enciclopedia.us.es/index.php/Infraestructura_de_clave_p%C3%BAblica
http://www.iec.csic.es/criptonomicon/susurros/susurros11.html

http://www.fundaciondike.org.ar/seguridad/firmadigital.html

http://www.seguridaddigital.info/index.php?option=com_content&task=view&id=118&Itemid=26

http://www.espaciosjuridicos.com.ar/datos/AREAS%20TEMATICAS/ECONOMICO/firmadigital.htm

http://www.lasasesorias.com/es/publica/firmaelectronica/lafirmaelectronica.html

http://www.netfocus.es/es/EMPRESA/SALA_DE_PRENSA/ENTREVISTA_FIRMA_ELECTRONICA/

http://www.biocom.com/informatica_medica/legalrec_firma_digital.html

http://www.certificadodigital.com.ar

www.vlex.com/vid/123967

http://derin.uninet.edu/cgi-bin/derin/vertrabajo?id=16

http://web.usc.es/~ruizmi/pdf/e~com.pdf

http://www.alfa-redi.orgCampoli, Gabriel. Firma Ológrafa y no ológrafa. Revista Alfa-Redi

http://www.alfa-redi.orgFernando Ramos Suárez, Contratación Electrónica Revista Alfa-Redi Núm. 19, Septiembre 2001.