RESUMEN:

En el presente ensayo se realiza un análisis de los datos personales y la protección jurídica que tienen los sujetos titulares de estos derechos. Con el fin de llegar a este objetivo se revisó varios temas, entre ellos, qué son los datos, la protección que se les debe dar, cómo se clasifican, sus principios y derechos; ya que debemos recordar que con el avance tecnológico se vuelve relevante para el derecho el estudio de este tema porque no puede ser solamente estudiado desde la visión informática, dejando de lado la parte jurídica.

Además se realizó una revisión sucinta de casos en los que está implicado la protección de datos y las tecnologías de la información y comunicación (TICs), específicamente en cuanto a los datos considerados especialmente protegidos (salud), el *spam, phishing*, redes sociales, motores de búsquedas, el secreto de las comunicaciones y la seguridad informática.

INDICE:

UNIVERSIDAD DE CUENCA

FACULTAD DE JURISPRUDENCIA Y CIENCIAS POLÍTICAS Y SOCIALES

ESCUELA DE DERECHO

Maestría en Derecho Informático

Titulo del ensayo:
Las tecnologías de la información y comunicación y la protección de datos personales

Ensayo previo a la obtención del Diplomado en Derecho Informático

Autora: María Cristina León Carvajal

Cuenca, enero de 2010

Los planteamientos que se exponen a continuación son de exclusiva responsabilidad de la autora.

María Cristina León Carvajal
Autora

INTRODUCCIÓN:

En nuestro país, en la actualidad se carece específicamente de una ley que regule la protección de datos personales, sin embargo, debemos aclarar que existe un gran avance en este tema, ya que la Constitución Política de la República, aprobada en el año 2008, en el artículo sesenta y seis; reconoce y garantiza a las personas "el derecho a 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"[1]. Además existen varias normas supletorias como la Ley de Garantías y Control Constitucional aprobada en julio de 2009 y la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos que se refieren brevemente al tema.

Dentro del presente ensayo se hará una revisión de varias situaciones producidas por la recolección de datos personales dentro de las actividades que realizamos, datos recolectados por personas naturales o jurídicas, a través de diferentes medios; sin conocer el fin específico para ello. Esto puede darse en cualquier momento, por ejemplo cuando nos inscribimos un curso o al alquilar determinado bien, para lo cual se nos solicita nuestros datos. Otra situación que puede presentarse, es que los datos ya se encuentren registrados en bancos de datos sin nuestro conocimiento, en este caso se debe garantizar un adecuado manejo y utilización, además se debe respetar derechos como el del honor de las personas, su intimidad y privacidad, garantizando la utilización debida de los datos, estos derechos

[1] Asamblea Nacional Constituyente, *Constitución Política de la República del Ecuador*, Ciudad Alfaro, 2008. http://www.asambleanacional.gov.ec/documentos-asamblea-nacional/constituciones/constitucion-de-2008/constitucion-2008.pdf. Registro Oficial No. 449 del 20 de Octubre de 2008

que gozamos conforme la Declaración Universal de los Derechos Humanos en el artículo doce[2].

De las situaciones antes mencionadas, se desprende la siguiente interrogante: ¿Cómo hacer exigible los derechos enunciados, sin la existencia de una regulación expresa? En este caso, la norma suprema declara el principio, pero actualmente no existe una norma que objetivase el derecho. En consecuencia, es necesario analizar la situación de la protección de datos, que con la revolución y auge de las tecnologías de la información y comunicación – TICs, han evolucionado la sociedad; desprendiéndose la necesidad de una ley que garantice de manera efectiva los derechos mencionados anteriormente.

Así mismo, es necesario analizar algunas de las situaciones que se pueden presentar actualmente por el avance tecnológico, y como este puede afectar a los datos personales; como protegerlos y cuál es el alcance e implicaciones que tiene el usos de las nuevas tecnologías de la información y comunicación.

[2] Declaración Universal de los Derechos Humanos, Art. 12 http://www.un.org/es/documents/udhr/

CAPITULO 1: LOS DATOS PERSONALES

1.1 Antecedentes:

Dentro de la “Sociedad de la Información” (término que se ha comenzado a utilizar para dar un nombre a la sociedad que trabaja de forma importante con la información dentro de sus actividades), la concurrencia entre la informática y las telecomunicaciones, ha dado como resultado cambios muy drásticos en los ámbitos tecnológico, social, laboral, político, económico, entre otros; de manera que existe un creciente nivel de informatización y automatización de procesos que se llevan adelante; ya sea por el incremento a fuentes de información a través de Internet, por las nuevas relaciones interpersonales que se ha creado, o por la información personal que se maneja en la red. De esto se desprende justamente como una amenaza, el riesgo que determinados derechos puedan ser sensibles a las nuevas formas de delincuencia, atentando el derecho a la libertad, la intimidad y privacidad de las personas.

Los sistemas normativos, tanto internacionales como nacionales, no cuentan con una adecuada solución a varios problemas que pueden suscitarse; ya sea porque estos sistemas legislativos envejecen rápidamente para el ritmo en que evolucionan las tecnologías; o, porque como en el caso de Ecuador existe una regulación epidérmica. Un ejemplo de lo que puede suceder con los datos personales es su manipulación, que se convierte en una vulneración a los derechos o perdida de ciertas libertades; se puede llegar a la identificación de personas y de su situación patrimonial o crediticia. Otra situación que puede suscitarse es la gran capacidad de almacenamiento de

datos que tienen los motores de búsqueda como por ejemplo Google o Yahoo; sin olvidarlos del molestoso *spam* que llega todos los días a nuestros correos.

El criterio del Dr. Pablo Yánez[3], nos ayuda a ejemplificar que es lo que sucede con el manejo inadecuado de los datos personales, expresando que se pueden presentar los siguientes casos:

a. Tomar decisiones que afectan negativamente a los sujetos, sin que estos tengan conocimiento de porque se resuelve de una forma perjudicial en determinados casos;
b. Elaboración o creación de un perfil del individuo, con interconexión a ficheros que permite controlar sus actividades;
c. Efectuar una simulación de las relaciones o comportamientos futuros del individuo, fundamentándose para ello en sus datos; y,
d. Actuar negligentemente, sin actualizar, borrando o completando los datos registrados.

Por otro lado, personas jurídicas como empresas pueden también ocupar esos datos o captarlos sin que sean percibidos, ya que pueden ser considerados intrascendentes, obteniéndose sin el consentimiento necesario o que se omita información sobre que se hará con los mismo; afectando de esta manera a la autodeterminación que tenemos las personas para saber si entregamos o no los datos. De estas afirmaciones podemos colegir que el objetivo de la protección de datos personales; es tutelar la información personal que se encuentra dentro de bancos de datos o en archivos, con la intención de que esta sea fidedigna, reservada y cumpla con el fin para el que fue obtenida.

[3] YÁNEZ, Pablo. Introducción al Estudio del Derecho Informático e Informática Jurídica. Quito: Escuela Politécnica Javeriana del Ecuador, 1999.

1.2 Los datos

Comenzaremos definiendo el término dato, el Diccionario de la Real Academia Española nos dice: "(Del lat. *datum*, lo que se da). Antecedente necesario para llegar al conocimiento exacto de algo o para deducir las consecuencias legítimas de un hecho"[4]; para Miguel Elías[5] es: "una representación de una porción de la realidad expresada en términos que forman parte de un código preestablecido de manera que pueda ser interpretado, y que está destinado a dar esa información a un receptor (de allí el origen de la palabra, "*datum*", que en latín significa "*dado*", participio del verbo "*dar*")". Un interesante y simple concepto que podemos encontrar es el que expresa Molina Quiroga, citado por Miguel Elías dentro del mismo artículo, diciendo que se debe entender al dato como la "mínima unidad de información (…) que puede consistir ya sea en un punto, una frase, un número, una cifra, un articulo de un código, una nota musical, una imagen, etc.".

De lo anotado anteriormente, podemos concluir que los datos serían las unidades mínimas de información, almacenadas en soportes físicos o lógicos, sin un fin específico, y que aislados carecen de un contenido. Por consiguiente, si estos datos, cuentan con un tratamiento o sirven para un fin se puede convertir en información; palabra que según el diccionario de la Real Academia Española[6] viene de: "(Del lat. *informatĭo, -ōnis*). 1. Acción y efecto de informar. 2. Averiguación jurídica y legal de un hecho o delito. 3. Comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada. 4. Conocimientos así comunicados o adquiridos". Es decir, el dato es un

[4]Diccionario de la Real Academia Española http://buscon.rae.es/draeI/SrvltGUIBusUsual?TIPO_HTML=2&TIPO_BUS=3&LEMA=dato

[5] Elías, Miguel. *Situación legal de los datos de carácter personal frente a las nuevas tecnologías* 2001. http://www.alfa-redi.org/rdi-articulo.shtml?x=638

[6]Diccionario de la Real Academia Española. Diccionario de la Real Academia Española. 20 de diciembre de 2009 <http://buscon.rae.es/draeI/SrvltGUIBusUsual?TIPO_HTML=2&TIPO_BUS=3&LEMA=informaci%C3%B3n >

antecedente para una investigación y el momento en el que sirve para un fin o soluciona un problema, es información.

Por último, debemos hablar de otros términos que se desprenden de los anteriores, es así que la documentación es un conjunto de datos, y por su parte la información que ha sido recabada nace el conocimiento.

1.3 La protección de datos personales

Como hemos enunciado inicialmente, con el uso de las TICs se puede realizar el tratamiento, almacenamiento y transmisión de información que en muchos casos puede ser sensible, dando como resultado convertirse en un instrumento de presión y control; como por ejemplo si cae en manos de los poderes públicos en el caso de que exista algún tipo de persecución; o, con las empresas privadas al convertirse en una herramienta de promoción comercial, como sucede con el correo electrónico no deseado.

Cabe anotar que con el fin de que exista una convivencia entre todos los sujetos que interactuamos dentro de la sociedad, es necesario que algunos datos sean proporcionados, para preservar el bien común; es aquí donde la protección de datos debe tener como objeto el limitar la utilización de dichos datos para que no agreda la intimidad de los sujetos y coartar el ejercicio de sus derechos[7], pero a su vez dar seguridad jurídica a la comunidad.

De acuerdo al diccionario de la Real Academia Española, la protección de datos se entiende como: "**1.** f. Sistema legal que garantiza la confidencialidad de los datos personales en poder de las administraciones

[7] Davara Rodríguez, M. A. (1997). *Manual de Derecho Informático.* Navarra: Editorial Aranzadi, SA.

públicas u otras organizaciones. Agencia de protección de datos"[8]. Para Miguel Davara, es "el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad"[9].

Del párrafo anterior se desprenden los siguientes puntos a considerar:

1. Se intenta proteger a las personas del manejo o manipulación de sus datos personales susceptibles de tratamiento automatizado o el soporte en el que se encuentran sea susceptible a este tipo de tratamiento.
2. Posibilidad de identificar al titular con el resultado del tratamiento de los datos; incluso con la probabilidad de conocer nuevas características como consecuencia del tratamiento de datos.
3. El manejo de los datos sin el consentimiento de su titular o para fines diferentes a los que el titular autorizó o se vio obligado a dar los datos.

La protección de datos gira sobre varios principios, el más importante de ellos el consentimiento: la manifestación de voluntad, donde el titular de los datos autoriza su tratamiento. Para Miguel Davara[10] el ciudadano es el único que decide cuándo, dónde y cómo se presentan sus datos al exterior, o si se dan a conocer a terceros; esto es, el afectado tiene que otorgar su consentimiento para que se pueda realizar un tratamiento automatizado; dicho de otra forma, no se pueden tratar datos de carácter personal sin consentimiento de su titular.

[8] Diccionario de la Real Academia Española. Diccionario de la Real Academia Española. 20 de diciembre de 2009 <http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=proteccion>
[9] Davara Rodríguez, M. A. (1997). *Manual de Derecho Informático.* Navarra: Editorial Aranzadi, SA.
[10] Davara & Davara Asesores Jurídicos. (2001). *Factbook Comericio Electrónico.* Navarra: Aranzadi .

La naturaleza jurídica de la protección de datos personales está basada en los principios de dignidad e integridad de las personas, y su función social es la de garantizar que cada persona pueda controlar sus datos personales, en el uso y destino, con el propósito de impedir su tráfico ilícito y una potencial vulneración de su dignidad. Por último, debemos aclarar que la expresión "protección de datos" podría dar a entender equívocamente que el objeto de protección será el dato, cuando el fin que tiene este derecho es proteger al sujeto titular de los datos; siendo la expresión correcta: Protección jurídica de los individuos con relación al tratamiento automatizado de los datos de carácter personal.

1.4 Clasificación de los datos personales:

Los datos pueden ser de diversa naturaleza: históricos como una fecha, geográficos como un lugar, climáticos como las temperaturas máximas y mínimas de un lugar, o personales como un nombre, entre otros. Para el presente estudio nos concentraremos en los relativos a las personas, por los derechos que desprenden; "Los datos pueden ser los nombres, apellidos, fecha de nacimiento, el número de teléfono, los datos biométricos o los médicos, información sobre la carrera profesional, etc."[11]. Por consiguiente, son los que contienen características identificadoras de personas o que se les puede imputar. Según Pablo Yánez dentro de la obra citada, los datos personales son: "Todo dato acerca de una persona, identificada o identificable de forma directa o indirecta, en particular mediante un número de identificación. La acepción "identificada o identificable" hace relación al conjunto de derechos de orden subjetivo que la persona de la cual existen datos tiene sobre ellos" [12].

[11] Supervisor europeo de protección de datos. (s.f.). *Supervisor europeo de protección de datos.* Recuperado el 21 de junio de 2009, de www.edps.europa.eu: http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Brochures/brochure_guide_es.pdf

[12] YÁNEZ, Pablo. Introducción al Estudio del Derecho Informático e Informática Jurídica. Quito: Escuela Politécnica Javeriana del Ecuador, 1999

A continuación realizaremos una clasificación construida a partir de la opinión de los tratadistas Miguel Davara, Miguel Elías, y Pablo Yánez, que tiene como punto de partida el grado de confidencialidad, entendido como el mayor o menor nivel de secreto con el que se van a guardar y tratar los datos personales, recordemos que pertenecen al individuo, afectan su vida privada; es decir, a su intimidad, por lo que se les eleva a la calidad de datos personalísimos, siendo su titular el único que tiene el poder de disposición y decisión.

a. **Datos públicos (o que pueden tener alcance público)**: Aquellos datos conocidos por varias personas o por la comunidad en general, sin que su titular, pueda impedir su difusión dentro de los límites de respeto y de convivencia social. Muchos de estos datos constan en registros públicos y privados, como por ejemplo la guía telefónica. Entre los datos públicos podemos enumerar: nombres, apellidos, edad y profesión.
b. **Datos privados:** Su titular tiene la facultad para decidir si difunde a terceros, dependiendo de las circunstancias en que la persona se ve obligada a proporcionarlos o ponerlos en conocimiento; como por ejemplo si están regulado por la Ley. De todas maneras en cuanto a estos datos la conciencia social puede en algunos casos puede impedir que se realice su difusión para respetar la voluntad del secreto.

La diferencia básica entre los datos públicos y privados se basa en el grado de secreto, que es sometido a la conciencia social y depende del dato del que se trate.

Los datos privados se clasifican en datos íntimos y secretos:

a. **Datos íntimos:** Se refieren a datos de un sujeto individualizado y relativo a su fuero interno o íntimo, sin llegar a información puramente sensible. Son datos que el individuo puede proteger su difusión, salvo que tenga que proporcionarlos periódica y regularmente cumpliendo

con un fin o de conformidad a la Ley. Por ejemplo son datos que identifican su personalidad, creencias e ideologías, pensamientos, sentimientos y salud. El problema se puede desencadenar si existe una asociación entre ellos y se llegare a crear un perfil inexacto o arbitrario; con el cual se puede causar un daño al titular o convertirse en datos secretos.

b. **Datos secretos:** El individuo no está obligado a dar a nadie, salvo casos excepcionales contemplados de forma tácita por la Ley; pero es necesario la existencia de una regulación detallada que proteja correctamente la difusión. Por ejemplo, datos relativos a la salud, en personas portadoras de VIH/SIDA.

   Los datos secretos se clasifican a su vez en profundos y reservados:

   i. **Datos profundos:** Son aquellos que bajo ningún concepto el individuo está obligado a proporcionarlos, salvo su voluntad.
   ii. **Datos reservados:** Llamados también sensibles, sensibilísimos o de sensibilidad especial. Son aquellos que no admiten excepción alguna para darlas a conocer, ni siquiera la voluntad del individuo.

1.5 Características de la protección de datos

Según Pablo Yánez[13], los datos personales para ser considerados objeto de protección por parte del derecho deben ser lícitos, determinados, pertinentes, actualizados, temporalizados, accesibles, rectificables, cancelables, consentidos, identificables, seguros y secretos; a continuación describimos el alcance de cada uno de estas características:

a. Lícitos: Tanto en el momento de recolección como en su uso, no se utilicen criterios o conductas determinadas como ilícitas por la Ley;
b. Determinados: Los datos no pueden ser utilizados para fines distintos para los que fueron recogidos;

[13] YÁNEZ, Pablo. Introducción al Estudio del Derecho Informático e Informática Jurídica. Pág. 174. Quito: Escuela Politécnica Javeriana del Ecuador, 1999

c. Pertinentes: Los datos serán exactos y completos en relación a su titular;
d. Actualizados: Deben ser puestos al día de forma que respondan con veracidad a la situación real de su titular;
e. Temporalizados: Los datos serán conservados solamente por el periodo necesario para los fines en base a los cuales fueron recabados o registrados;
f. Accesibles: Su almacenamiento debe permitir el acceso por parte del titular;
g. Rectificables: Al ser automatizados los datos, deben admitir la posibilidad de rectificación;
h. Cancelables: Los datos deben tener la posibilidad de ser borrados físicamente, siendo cual sea el soporte en el que se encuentre;
i. Consentidos: Debe existir por parte del titular la voluntad para entregar los datos, con la facultad de reservarse la información considerada como secreta o íntima;
j. Identificables: Los datos procesados emitirán la identidad y dirección del responsable de su manejo;
k. Seguros: Los responsables del manejo responderán por su alteración, pérdida, tratamiento o acceso no autorizado; y,
l. Secretos: Los responsables del tratamiento automatizado y quienes intervengan en cualquier fase, están obligados al secreto profesional respecto de los mismos y al deber de guardarlos; obligaciones que subsistirán aún después de finalizar sus relaciones con el titular del fichero, o en su caso, con el responsable del mismo.

En el caso de la creación de una Ley de Protección de Datos, sería necesario delimitar los momentos[14] que se protegerá dentro del tratamiento de datos, a saber:

a. Momento de la toma de los datos
b. Momento del tratamiento automatizado: donde se puede también cruzar y relacionar datos de diferentes bases con el fin de crear un nuevo perfil.

[14] Davara Rodríguez, M. A. (1997). *Manual de Derecho Informático.* Navarra: Editorial Aranzadi, SA.

c. Momento de la utilización: llamada cesión de datos, donde se da a conocer o se comunican los resultados.

Esto tiene su importancia ya que dependiendo del momento se fijará los principios de la protección de datos, los derechos de los ciudadanos y los procedimientos que permitirán ejercer estos derechos. Además depende del momento, ya que según eso cambia las circunstancias, por ejemplo, no se dan los mismos acontecimientos en el momento de su recolección, que en el tratamiento donde se puede afectar a la privacidad de las personas, y en el último momento podría existir una agresión a los derechos de las personas.

1.6 Principios y derechos de la protección de datos

Principios: De los principios que se enumerarán a continuación se derivan una serie de derechos que deben estar consagrados dentro de una ley como es el caso de la Ley Española de Protección de Datos[15]; **e**l listado que se expone a continuación fue elaborada a partir de las clasificaciones de Miguel Davara[16], Emilio del Peso Navarro y Miguel Ángel Ramos[17] dentro de sus obras:

a. Principio de proporcionalidad: Los datos que se incorpora deben ser congruentes, suficientes y no excesivos; para el fin que justifica la existente del fichero.
b. Principio de vinculación al fin: Debe existir un fin para el cual un fichero de datos sea creado, en este caso antes de su creación debe conocerse el fin del mismo. Este principio engloba a su vez el principio de pertenencia y el de utilización no abusiva.

[15] Del Peso Navarro, Emilio. Ley de Protección de Datos La Nueva Lortad. Madrid: Ediciones Días de Santos, S.A., 2000.
[16] Davara Rodríguez, Miguel Angel. Manual de Derecho Informático. Navarra: Editorial Aranzadi, SA., 1997.
[17] Del Peso Navarro, Emilio y Miguel Angel Ramos González. LORTAD Análisis de la Ley. Madrid: Ediciones Días de Santos, S.A., 1998.

- Principio de pertinencia: Los datos deben ser pertinentes, es decir, estar relacionados con el fin perseguido al crearse el fichero y no excesivos.
- Principio de utilización no abusiva: Los datos recogidos no deben ser utilizados para finalidades incompatibles con aquellas para las que fueron recogidos.

c. Principio de exactitud: El responsable deberá poner los medios necesarios para comprobar la exactitud de los datos registrados y asegurar que estén actualizados en todo momento.
d. Principio de secreto del responsable: El responsable del fichero deberá adoptar las medidas necesarias de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal.
e. Principio de acceso individual: Cualquier persona tendrá derecho a solicitar y obtener de forma gratuita información sobre sus datos de carácter personal sometidos a tratamiento, el origen primario de dichos datos, y las sesiones realizadas o que se pretendan hacer.
f. Principio de transparencia hacia los afectados o publicidad: Es necesario que exista un registro público en el que figuren los ficheros de datos de carácter personal tanto los de titularidad pública como privada.

Principios singulares: Se los llama así porque afectan en diferentes momentos

a. Principio de recogida: necesidad de informar al afectado del alcance de los datos que se recogen.
b. Principio de tratamiento: Debe existir consentimiento o por medio de una ley
c. Principio de cesión: Con consentimiento expreso del titular, además de que debe existir la libre revocabilidad del consentimiento para ceder los datos.

Principios especiales: Son los que afectan a los datos sensibles como la ideología, religión o creencias, salud, raza o vida sexual.

a. Principio de pertinencia de los datos: Conforme al ámbito y la finalidad para lo que fueron obtenidos
    - Principio de derecho al olvido:

      Los datos deberán desaparecer del fichero una vez se haya cumplido el fin para el que fueron recabados. La forma de almacenamiento no puede impedir el ejercicio del derecho de acceso.
b. Principio de exactitud y actualización: Los datos deben reflejar con veracidad la situación del titular.
c. Principio de congruencia y racionalidad: Es la necesidad de garantizar que los datos no pueden ser tratados ni utilizados salvo los casos que sean necesarios y conforme a la finalidad para la cual fueron tomados.
d. Principio de consentimiento: El principio enuncia que el interesado debe otorgar su consentimiento libre, expreso y escrito; previo en todos los casos para que sus datos sean tratados o cedidos. Además debemos puntualizar que el consentimiento puede ser revocable y su excepción se funda en la ley. Dentro de este principio se encuentra el principio de lealtad, el que nos asevera que los datos no pueden ser recolectados por medios fraudulentos, ilícitos o desleales.

Derechos[18]: Es necesario que los principios arriba enunciados tengan un reconocimiento para conseguir una protección idónea, a saber:

a. Derecho a la autodeterminación: Es la facultad de controlar y conocer los datos que se encuentran en soportes informáticos o susceptibles de tratamiento automatizados.
b. Derecho de información y acceso: El interesado tiene derecho a tener conocimiento de una serie de circunstancias sobre la forma en que van a ser tratados sus datos de carácter personal, cuando considere necesario.

[18] Davara Rodríguez, M. A. (1997). *Manual de Derecho Informático.* Navarra: Editorial Aranzadi, SA.

c. Derecho de rectificación y cancelación: En caso de que los datos son inexactos o dejado de ser necesarios, el titular puede solicitar su rectificación o cancelación.
d. Derecho de impugnación: Se da en determinados actos, cuando su fundamento sea un tratamiento automatizado de sus datos de carácter personal.
e. Derecho a exigir una responsabilidad por los daños que a sus bienes o derechos se le haya causado: por el tratamiento de los datos erróneamente introducidos en el fichero.

Por último, debemos anotar que estos derechos deben estar concebidos a través de un procedimiento, por ejemplo, en el caso de nuestra legislación el "habeas data" es el instrumento que permite facilitar un camino mediante para que el ciudadano pueda encontrar una defensa para los derechos que pretende proteger.

1.7 La intimidad y la privacidad

La intimidad es un pilar fundamental para la protección de la individualidad de la persona, se entiende que se relaciona con la protección que se da a aquel ámbito que no desea hacer público: sentimientos, pensamientos o hábitos propios de una persona, familia o colectividad[19]; este es un derecho fundamental consagrado en la Constitución Política de la República e internacionalmente reconocido a través de las convenciones relativas a los Derechos Humanos, teniendo sus raíces en la dignidad, el respeto y la inviolabilidad de la persona.

[19] Caceres, María Paulina. Taller de Protección de Datos. Cuenca, enero de 2008.

Sin embargo, actualmente con la Sociedad de la Información ha adquirido una nueva dimensión, mayormente por el tratamiento automatizado de la información y su transmisión telemática, ya que puede llegar a atentar contra la personalidad como característica del individuo, sobretodo en el ámbito de su libertad al entrar en el campo de la intimidad y que según Davara[20] esto es lo que se ha dado en llamar la "privacidad". Lo que se busca es un equilibrio entre la libertad de expresión (dentro de la cual se encuentra la libertad de opinión y la libertad de recibir o comunicar información) y la protección de la esfera privada de los individuos a través del tratamiento de sus datos en ejercicio del derecho de obtener y difundir libremente información.

Su desarrollo histórico ha sido conforme a la normativa de cada país al que pertenecen, en este caso tenemos la tradición del *Common Law* que se rige para los países anglosajones y el derecho continental que rige a países como Ecuador, de Latinoamérica y países como España y Francia.

Para la corriente anglosajona[21], los derechos de privacidad abarcan los siguientes principios o derechos:

a. El derecho de libertad: se definía una zona de decisión personal en la que el Estado no podía intervenir;
b. La prevención y protección contra los totalitarismos: La protección de la privacidad como de los datos personales buscan proteger del conocimiento profundo e individualizado de las personas a estructuras estatales y en el caso de persecuciones estatales, la privacidad sería la mejor protección de grupos minoritarios y disidentes, y;
c. El derecho a ser dejado solo.

[20] Davara & Davara Asesores Jurídicos. (2001). *Factbook Comericio Electrónico*. Navarra: Aranzadi .
[21] Gregorio, C. G., Greco, S., & Baliosian, J. (s.f.). *Facultad Latioamericana de Estudios Sociales*. Recuperado el 2 de 12 de 2008, de Flacso: http://www.flacso.org.ec/docs/sfintgregorio.pdf

Por su parte en la tradición continental están relacionados a la evolución de la defensa del honor. En el año 81 a.C. se da la primera manifestación de protección de la intimidad a través de la *Lex Comelia de Iniuris*[22]*,* entendida como la inviolabilidad de domicilio. Actualmente es considerado como un derecho fundamental, parte de los derechos de la personalidad.

Una noción moderna de intimidad la define como un atributo entre la libertad y la autonomía; la intimidad es simultáneamente condición de la personalidad individual y de la personalidad social[23]. En cuanto a la evolución del derecho a la intimidad se dice que es "un derecho reciente cuyo origen se remonta al conocido artículo *The Right to Privacy* de S. Warren y L. Brandeis, en donde exponían la inquietud sobre la necesidad de que el derecho a la intimidad o los acontecimientos de la vida privada de un individuo recibiesen una protección adecuada frente a la injerencia de los medios de comunicación. En ese momento, los juristas se refirieron a un derecho de exclusión (*the right to be let alone*) como una reafirmación de la intimidad y la individualidad.[24]"

En el derecho anglosajón su evolución se ha dado a través de cuatro periodos:

a. Desde los orígenes del *Common Law* hasta 1890 cuando se publica el artículo *The Right to Privacy.*
b. Desde 1890 hasta 1960 donde se publica un ensayo de William Prosser referido a los problemas que se suscita entre la privacidad y la prensa.

[22] Comisión de transparencia y acceso a la información del Estado de Nuevo León. «Comisión de Transparencia y acceso a la Información del Estado de Nuevo León.» enero de 2008. www.ctainl.org.mx. 20 de junio de 2009 <http://www.ctainl.org.mx/revista_8/elementos/fundamentojuridicopd.pdf>.
[23] Gregorio, C. G., Greco, S., & Baliosian, J. (s.f.). *Facultad Latioamericana de Estudios Sociales*. Recuperado el 2 de 12 de 2008, de Flacso: http://www.flacso.org.ec/docs/sfintgregorio.pdf
[24] CASTRO BONILLA, Alejandra. «Alfa Redi.» 20 de agosto de 2008 <http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/castro.pdf>

c. De 1960 a 1969 en Inglaterra se comienza a trabajar en el proyecto de ley que se enfoca en los conflictos entre la privacidad y los medios masivos de comunicación.
d. Desde 1969 donde se empieza con el proyecto de ley de Walden, donde aparece el problema de la tutela de los datos personales memorizados por ordenadores.

En la jurisprudencia de los Estados Unidos de América, el derecho de la privacidad busca proteger los sentimientos y sensibilidades de las personas; no su propiedad o intereses pecuniarios, por lo cual es un derecho personal que termina con la muerte. Es así que los registros penales de los menores pueden ser abiertos si la persona fallece, situación que en el derecho continental no sucede ya que la intimidad y privacidad está ligada al honor de las personas[25].

Dentro de la doctrina alemana (parte de la corriente continental), la intimidad se entiende desde tres esferas, conforme lo señala el artículo "El fundamento jurídico de la protección de datos"[26]:

a. La esfera privada: comprende todo aquello que la persona desea excluir del conocimiento público. Abarca su imagen y su comportamiento, aún el exterior de su domicilio que sólo deben conocer quienes se encuentran en contacto con él.
b. La esfera confidencial: comprende la información que la persona participa a otros sujetos de confianza, y;
c. Esfera del secreto: corresponde a los hechos y noticias de carácter extremadamente reservado que han de quedar inaccesibles a todos los demás.

[25]Gregorio, C. G., Greco, S., & Baliosian, J. (s.f.). *Facultad Latioamericana de Estudios Sociales*. Recuperado el 2 de 12 de 2008, de Flacso: http://www.flacso.org.ec/docs/sfintgregorio.pdf
[26]Comisión de transparencia y acceso a la información del Estado de Nuevo León. «Comisión de Transparencia y acceso a la Información del Estado de Nuevo León.» enero de 2008. www.ctainl.org.mx. 20 de junio de 2009 <http://www.ctainl.org.mx/revista_8/elementos/fundamentojuridicopd.pdf>.

Diferencia entre intimidad y privacidad.

En el diccionario de la Real Academia Española se refiere a la intimidad[27] como: "Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia"; y por su parte la privacidad[28] es entendida como: "Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión". De forma extensiva el término intimidad puede ser entendido como lo más íntimo de una persona, dentro ella se encuentran todos los sentimientos, creencias tanto políticas como religiosas, e información sobre su salud.

En cambio dentro de la privacidad existe información que puede no ser relevante, pero, al ser analizada dentro de un determinado contexto puede ayudar a la construcción de un perfil muy fiable del individuo. Esta situación se podría dar al momento de revisar la conducta de la persona, por ejemplo lo libros consultados, películas vistas, asociaciones a las que se pertenece, entre otras.

De lo anotado anteriormente debemos anotar que el elemento fundamental y materia para que exista la privacidad e intimidad son los datos personales, y cada individuo decide en qué esfera colocar su información y aunque no todos los datos son íntimos o privados, los asuntos íntimos son privados, pero no todos los asuntos privados son íntimos.

[27] Diccionario de la Real Academia Española. Diccionario de la Real Academia Española. 20 de noviembre de 2009 http://buscon.rae.es/draeI/SrvltGUIBusUsual?TIPO_HTML=2&TIPO_BUS=3&LEMA=intimidad

[28] Diccionario de la Real Academia Española. Diccionario de la Real Academia Española. 20 de noviembre de 2009 <http://buscon.rae.es/draeI/SrvltGUIBusUsual?LEMA=privacidad>

CAPÍTULO 2: CASOS DE IMPLICACIONES ENTRE LA PROTECCIÓN DE DATOS Y LAS TICS

2.1 Datos considerados especialmente protegidos - salud:

Para algunas personas existen datos que predominan en la lista de los que deben ser protegidos, en razón que están dentro de la esfera de lo íntimo, y no pueden estar en manos de cualquier persona y menos ser divulgados, como es el caso de datos que tienen que ver con la salud, el trabajo, convicciones políticas y religiosas. Así como hemos analizado anteriormente, es necesario que toda persona pueda proteger sus datos de salud para que no sean utilizados de forma indebida y exista una tutela efectiva de este derecho.

Dentro de la sociedad en la que estamos viviendo, la tecnología ha transformado el mundo médico, dejando la puerta abierta para que los datos personales puedan estar en manos de cualquier persona. Es verdad que algunos datos son necesarios para que exista un estudio y un desarrollo científico, sobre todo para determinar los signos y síntomas dentro de una enfermedad. Sin embargo, los datos también pueden convertirse en un bien a ser explotado dentro de una mafia donde están asociados médicos, casas farmacéuticas y farmacias.

El proceso de los datos personales terapéuticos, ha estado latente y con el descubrimiento del genoma humano se ha dado un gran avance, pasando de una medicina generalizada a una específica y personalizada; que depende del diagnostico que se dé a cada persona. Para esto es necesario

que los datos sean protegidos en su manejo y utilización. El dato terapéutico es en sí la unión de la historia clínica, genética y fármaco terapéutica de una persona; con el fin de tener una información completa, actualizada y sobretodo de acuerdo a cada individuo.

Para Francisco Almodóvar[29] dentro del artículo "El dato personal terapéutico", es *"*aquélla información concerniente a personas físicas identificadas o identificables, que necesitan los agentes que intervienen en la vida del medicamento, para llevar a cabo una información terapéutica adecuada, veraz, actualizada y responsable*".*

De estos conceptos se desprende, como hemos afirmado anteriormente, la necesidad que el sujeto titular de los datos este informado sobre el tratamiento que se dé a estos, con el fin de que pueda dar su consentimiento, proceso que tiene varias etapas y mayormente necesita que sea homologado a nivel internacional; de esta manera se puede cumplir con el fin de realizar una investigación científica con grandes cantidades de información personalizada. Por lo cual, se observa la necesidad de la existencia de un órgano que controle y supervise los datos con el fin de que cumplan con las características de adecuados, pertinentes y no excesivos; además de crear todo el aparataje necesario para crear responsables, accesos, actualización entre otros.

2.2 El *Spam*

El *Spam* es el correo que se envía de forma masiva con el fin de publicitar determinado producto, es un término inglés utilizado para llamar un tipo de

[29]Almodóvar, Francisco. «Alfa Redi.» 2005. www.alfa-redi.com. 19 de junio de 2009 <http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/cfbae8c34623d555c3da02c5242bd118/viewalmodovar.pdf>.

carne enlatada comercializada en los Estados Unidos, que fue poco a poco divulgándose hasta contar con el termino al que hoy hacemos referencia.

"Se entiende que es el correo electrónico no deseado, no solicitado, no consentido[30]". En este sentido es necesario recalcar que un correo puede ser enviado a una cantidad importante de direcciones, que si la lista de distribución es recabada previamente y bajo el consentimiento de los destinatarios, no se consideraría *Spam;* pero así mismo, puede existir consentimiento para un fin determinado y al no ser respetada y los datos son utilizados con otro fin se puede interpretar como correo no deseado. Aquí lo importante para ponerle en la categoría de deseado o no deseado; es decir, que el correo sea con consentimiento consciente, informado y aplicable al correo. Estamos hablando en este caso de una autorización para una finalidad específica, por ejemplo si dejo mis datos para que se me envíe una información determinada y se utiliza en cambio para promocionar bienes y servicios de una empresa.

La motivación para que exista este tipo de correos es sobre todo por ser una actividad económicamente rentable, ya que son medios de bajo costo y con buenos resultados. Sin embargo, para las personas que reciben el correo sus consecuencias son totalmente diferentes, ya que en primer lugar se atenta contra la privacidad de los ciudadanos, ya que en muchos de los casos se crean perfiles inexactos de las personas a través del rastreo en Internet de todas sus actividades. Además se ha convertido a nivel internacional en un problema de seguridad, de comunicaciones, de falta de confianza en la red, entre otros; ya que existe un abuso del fin para el cual se le ocupa sobretodo en el caso del correo electrónico.

[30] Brian Nougreres, Ana. «Informática y Derecho.» Informática y Derecho; Memorias del X Congreso Iberoamericano de Derecho e Informática. Santiago de Chile: LOM ediciones, 2004. 273- 284.

2.3 El *phishing*:

Es un nuevo tipo de delito que en nuestro país se está poniendo en auge, causando perjuicio a las personas; ocurre cuando se ingresa datos en páginas Web que son falsas, replicas exactas de otras; en las cuales se ingresa información confidencial de carácter crediticio o personal, incluyendo claves para realizar transferencias electrónicas. El *phishing* es un delito que se puede clasificar dentro de las estafas, ya que se comete utilizando un engaño, a saber la ingeniería social, que tiene con fin intentar conseguir información confidencial de una persona de forma fraudulenta.

Un ejemplo de *phishing* es el caso de suplantación del sitio web del Grupo Financiero Produbanco: En este caso llega a nuestro correo electrónico un mensaje informándonos que se necesita actualizar los datos de una cuenta (Anexo 1), dándonos como opción un link que nos llevará a la página falsa. Estos dos links nos direccionan a paginas suplantadas, a saber el primer link nos envía a http://www.thermapower.com.tw/incluides/actualizacion/produbanco/persona/produbancopersona.htm y el segundo a la página que tiene por dirección: http://www.thermapower.com.tw/incluides/actualizacion/produbanco/empresa/produbancoempresa.htm; ninguna de estas dos son paginas del Grupo Financiero Produbanco, aunque su parecido es similar, la página verdadera para hacer este tipo de transacciones es: www.produbanco.com/GFPNetseguro (Anexo 2).

Lo que se pretende es que una vez que se ingrese los datos crediticios de una tarjeta, por ejemplo el número de cédula y la clave, queden registrados en la base de datos de los estafadores, para después ingresar a la verdadera página y realizar varias transacciones, perjudicando al usuario del servicio. Para completar con la suplantación, una vez que hemos

ingresados los datos nos dice que ha existido un error en la página, situación que no es real, lo que sucede es que como ya se realizo el ilícito el usuario es enviado a una página que muestra el error (anexo 3).

2.4 Las redes sociales

Son un nuevo tipo de organización social con un impacto inimaginable en cuanto a las personas que buscan hacer amigos, comparten información o necesitan publicitarse. Su evolución se da desde un servicio de acceso a la red ofrecido por alguna entidad, hasta hacerse la unidad de varios conglomerados sociales, buscando potenciar las sociedades a través del Internet. Los sitios más conocidos son www.facebook.com; www.hi5.com; www.twitter.com, entre otros. El problema que debemos llevar a colación se da por el manejo indebido de los datos y casos de suplantación de identidad. Todas estas páginas, poseen una política de privacidad, en la cual nos hablan sobre el control que se da a los datos personales que son ingresados, y como esta información es compartida con otros individuos usuarios del servicio.

Existen datos públicos recabados, por ejemplo el nombre, dirección de correo electrónico, número telefónico, entre otros; así también, se recopila información según como se vaya usando o interactuando en el sitio web, como por ejemplo, el tipo de navegador que se utiliza y la dirección IP desde la cual se conecta, con el fin de ver la preferencia de los usuarios. Además se utilizan las *cookies*, que son para: “Llevar el control de usuarios: cuando un usuario introduce su nombre de usuario y contraseña, se almacena una *cookie* para que no tenga que estar introduciéndolas para cada página del servidor. Sin embargo una cookie no identifica a una persona, sino a una combinación de computador y navegador, y para, conseguir información sobre los hábitos de navegación del usuario, e intentos de *spyware*, por

parte de agencias de publicidad y otros (…)"[31]. Función que es posible desactivarla.

La información publicada en las redes sociales son bajo la responsabilidad del usuario, por lo que, estos servicios no garantizan que dicha información sea vista exclusivamente por personas autorizadas por nosotros, situación que se puede dar por ejemplo cuando se violan la seguridad de la contraseña de inicio de sesión. En el momento que exista una de estas violaciones deben ser informadas inmediatamente al administrador del servicio para que se pueda tomar las acciones correspondientes. Sin embargo, cabe traer a colación que por ejemplo en la red social *Facebook,* cambiaron actualmente los perfiles de seguridad, dejando al mínimo y existiendo la posibilidad que cualquier persona tenga acceso a nuestra información.

En cuanto a información confidencial como contraseñas y números de tarjeta de crédito, según la política de privacidad, es encriptado conforme a protocolos establecidos, sin embargo, se solicita que mediante correos electrónicos y servicios de mensajería no se envíe esta información sensible. Además en cuanto a los contenidos que subimos a estos servicios, están protegido por los derechos de propiedad intelectual, y por adhesión debemos sujetarnos a sus condiciones de uso y política de privacidad, es decir, conforme el texto que se encuentra en el sitio web[32] concedemos una licencia general, transferible, entre otras cualidades para que se utilice el contenido de publiquemos; y que terminará en el momento cuando se elimina dichos contenidos. Sin embargo, debemos tener presente que la información que subimos a estos medios electrónicos puede ser difundida a millones de usuarios, ya que existe la posibilidad de copiar y difundir a través de otros medios electrónicos.

[31] Wikipedia. «Wikipedia.» www.wikipedia.org. 1 de septiembre de 2009 <http://es.wikipedia.org/wiki/Cookie>.
[32] Facebook. facebook.com. 1 de septiembre de 2009 http://www.facebook.com/terms.php>.

Como expresa Pablo Fernández Burgueño[33] dentro de su artículo "Nuevas Tecnologías – El peligro de las redes sociales y sus principales consecuencias jurídicas nos dice que el uso no responsable de las redes sociales puede acarrear lo siguiente:

- Publicación de fotografías que puede llevar a perder el control de la privacidad
- El anonimato da lugar a un uso constante y repetido por organizaciones criminales de pederastas y terroristas
- No existe la certeza que la persona con la que unos e comunica a través de la red social es a quien dice ser en la vida real
- Existe suplantaciones de identidad
- Puede dar lugar a ruptura de parejas, robos y despidos por la información que está inmersa
- Los menores de edad son propensos a que su información e intimidad sea publicada a través de estos medios.

En el caso de existir abusos por parte de otros usuarios, se puede hacer una denuncia tanto en el caso de una cuenta ficticia (identidad falsa) o cuenta impostora (suplantación de personalidad), así como cuando exista contenido pornográfico o censurable. En el caso de la suplantación de identidad, es un proceso que puede darse sin que los otros contactos se den cuenta, ya que no se puede saber a ciencia cierta que la persona con al cual estamos comunicándonos es quien dice ser. Igual caso sucede en la suplantación de personalidad en un correo electrónico, en este caso, se debe contactar al soporte técnico del servicio que estemos utilizando y ellos nos darán una solución oportuna según el caso, como por ejemplo, el que se encuentra en el (anexo 4).

[33] Fernández Burgueño, Pablo. «Pablo F Burgueño.» 1 de septiembre de 2009 <http://www.pabloburgueno.com/wp-content/uploads/2009/06/El-peligro-de-las-redes.pdf>.

2.5 Los motores de búsquedas

En la actualidad, Google Inc., ha convertido en una de las empresas con mayor presencia en Internet, gracias a los servicios que presta a sus usuarios, como por ejemplo correo electrónico, buscador, mapas, navegador web, blog de notas, directorio, calendario, entre otros. No obstante, al contar con tantos servicios, también maneja varios datos de sus usuarios, sobre todo en lo que se refiere a información personal; que según su política de privacidad[34] se divide dicha información recopilada en diferentes niveles, a continuación hablaremos de los más importantes:

- Información proporcionada por uno mismo al momento de registrarse en los servicios de Google: nombre, dirección de correo electrónico y contraseña. En algunos casos, para determinados servicios se solicita un número de tarjeta de crédito o información bancaria, misma que es encriptado por seguridad.
- *Cookies*: Como pudimos observar en el caso de las Redes Sociales, en Google también existen *cookies.* De igual manera nos informa que esta herramienta es ocupada para mejorar el servicio que presta.
- Información de registro: Datos que se incluye son la dirección IP, el idioma, el tipo de navegador entre otras.
- Comunicaciones de usuarios: En el caso de utilizar el correo electrónico, es necesario que estos datos sean alojados en un *hosting* con el fin de poder realizar consultas y responder peticiones.
- Datos de ubicación: Google puede recibir información sobre la ubicación de las personas en caso de utilizar el servicio de google *maps*. Dentro de este punto, es necesario hablar de Google *Latitude*, un servicio que afecta la privacidad de las personas, ya que compartimos nuestra ubicación con familiares y amigos. En muchos casos puede resultar una ayuda, por ejemplo en el caso de una persona secuestrada y tenga

[34]Google Inc. Google. 1 de septiembre de 2009 <http://www.google.com/privacypolicy.html>.

activado el servicio, se puede dar con el paradero de la misma, pero a su vez, puede atentar contra nuestra privacidad cuando alguna persona quiera controlar las acciones que hacemos y el lugar en el que nos encontramos.

En caso de utilizar los datos proporcionados para otro fin de aquellos para los cuales fueron recabados, son informados para que se dé el consentimiento por parte del usuario. Ante lo cual se puede manifestar la oposición y Google esta en la obligación de no recopilar ni utilizar dicha información.

De lo anotado anteriormente, cabe recalcar que uno de los problemas que se destacan en la Web, se dan porque los datos personales que se registran en los buscadores como Google, en muchos casos quedan en ellos por más tiempo del debido, por ejemplo puede existir información sobre delitos cometidos por personas hace mucho tiempo atrás y que violan el derecho de intimidad de estas, ante lo cual existen dos posiciones:

a. Por parte de Google, consideran que ellos no tienen ninguna responsabilidad ya que la información del buscador esta alojada en páginas web de terceros.
b. Por su parte la Agencia Española de Protección de Datos (AGPD), a través de una resolución determino que Google debía eliminar los datos personales.

   En este ejemplo, cabe la interrogante si es ilegal que un buscador muestre los datos que un gobierno determinado, en este caso el español ha registrado sobre hechos y actos públicos, mismo que son multiplicados a través de otras páginas; o en su defecto, si es necesario que existan controles sobre la información que se publica en Internet, para que no puedan ser indizados por los buscadores. Una analogía que considero grafica esta situación es la siguiente: “Demandar a Google por esto, podría ser equivalente a demandar a

> una empresa de binoculares por que algunas personas usan binoculares para espiar a sus vecinos, Google no es más que un reflejo de la web, es básicamente un gran binocular que nos permite encontrar información en un caos de datos, pero no es el que genera realmente dichos datos (…)"[35]

A criterio de Joaquín Muñoz[36], en estos casos lo que se debe hacer es solicitar el bloqueo de estas publicaciones, siempre y cuando la información no sea de interés general, hecho noticioso, y exista como motivo el respeto a la dignidad o el derecho al honor entre otros. Otra solución que se puede dar es a través de una herramienta para *webmasters* que se encuentra en un de los módulos de Google[37], es posible eliminar páginas web obsoletas, inexistentes, eliminar información o imagines e informar sobre un contenido inapropiado que aparezca en el buscador.

2.6 El secreto de las comunicaciones

Tema discutido por el ser humano desde muchos años atrás, ya que uno de los anhelos es el conocer el contenido de las comunicaciones de otras personas. Ante lo cual el artículo doce de la Declaración Universal de los Derechos del Hombre expresa que "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación (…)"[38]; en el mismo sentido el artículo diez y siete del Pacto Internacional de Derechos Civiles y Políticos protege el secreto en las comunicaciones.

---

[35] Mourguiart, Marcel. CHW. 1 de septiembre de 2009 <http://www.chw.net/2009/05/google-sentenciado-a-eliminar-datos-personales/>.

[36] Muñoz, Joaquín. Joaquín Muñoz - Protección de Datos y Nuevas Tecnologías. 1 de septiembre de 2009 <http://www.joaquinmunoz.com/2009/03/08/borrar-datos-personales-de-google/>.

[37] Google Inc. Google - Herramientas para Webmasters. 1 de septiembre de 2009 <https://www.google.com/accounts/ServiceLogin?service=sitemaps&passive=true&nui=1&continue=https://www.google.com/webmasters/tools/removals%3Fhl%3Des%26action%3Dcreate%26type%3Dot%26next%3DSiguiente%2B%25C2%25BB&followup=https://www.google.com/webmasters/t>.

[38] Declaración Universal de los Derechos Humanos, Art. 12 http://www.un.org/es/documents/udhr/

La comunicación es entendida como: “un proceso de transmisión de mensajes, un proceso en cuyo curso se hacen llegar a otro expresiones del propio pensamiento articuladas en signos no meramente convencionales”; conforme lo expresa Jiménez Campo dentro del texto de Rebollo Delgado[39]; de este concepto se desprende que ya no se habla de conversaciones directas o en persona, sino que estamos hablando de comunicaciones donde ya interviene determinado medio técnico por ejemplo el Internet o el teléfono. En este caso, el derecho que se protege, es en conjunto todo el proceso de la comunicación, es decir se tutela la libre comunicación, siendo el secreto un elemento esencial de la inviolabilidad de las comunicaciones; que se expresa como uno de los derechos de libertad e intimidad. Es por ello que el secreto de las comunicaciones es un instrumento para proteger la intimidad de las personas.

2.7 La seguridad informática

Su objetivo es impedir que se den a través de medios electrónicos nuevas formas de infracciones y violaciones a la Ley, así como que se cumplan dentro de una empresa las obligaciones establecidas en estatutos, reglamentos y normas, para lo cual es necesario realizar varios controles entre los que podemos enumerar los siguientes:

a. **La protección de datos y la confidencialidad de la información personal:** Como hemos visto dentro de todo este ensayo, gracias a la tendencia actual en cuanto a las telecomunicaciones y TICs, se ha incluido en varios países leyes con el fin de controlar el procesamiento y transmisión de los datos personales, poniendo responsabilidades a las

[39] Rebollo Delgado, Lucrecio. Derechos Fundamentales y Protección de Datos. Madrid: Dykinson, S.L., 2004.

personas que recopilan, procesan y divulgan información personal o que se encuentra almacenada en un medio telemático. De lo cual se desprende que en cada una de las empresas que maneje datos de esta índole es necesario que se designe un responsable, mismo que responderá por sus acciones.

b. **Protección de registros y documentos de la organización:** En cada organización existen registros y documentos que son de suma importancia, a los cuales se les debe proteger contra la pérdida, destrucción y falsificación, a través de sistemas lógicos; para en el caso de que suceda algún tipo de inconveniente, se pueda regresar al estado anterior de las cosas sin sufrir un perjuicio por la pérdida irrecuperable de datos. Por ejemplo, se debe respaldar las actividades esenciales del negocio, puede servir de evidencia de que la organización opera conforme la ley, con el fin de garantizar una defensa contra acciones civiles o penales, o; para validar el estado financiero de esta organización. Estos registros se clasifican en diferentes grupos, para ejemplificar tenemos registros contables, de bases de datos, de transacciones.

c. **Derechos de propiedad intelectual:** Se debe implementar procedimientos que garanticen la propiedad industrial, intelectual y las marcas registradas. La violación de estos derechos puede dar como resultado acciones legales que pueden derivar hasta en demandas de orden penal. Por ejemplo, varios requisitos de carácter legal pueden poner restricciones al uso de determinado material o software, poner restricciones a la copia de material que constituya propiedad de una determinada empresa. Además de los derechos de propiedad intelectual de software, ya que estos se constituyen propiedad de la empresa conforme al acuerdo de licencia que limita su uso.

d. **Seguridad aplicada a las actividades de comercio electrónico:** El comercio electrónico abarca el intercambio electrónico de datos, el correo

electrónico y las transacciones en línea a través de Internet; existiendo actualmente una vulnerabilidad a amenazas de diversa índole, por lo que se considera necesario aplicar ciertos controles como los detallados a continuación:

a. **Autentificaciones:** Es un proceso en el cual se hace una identificación de las partes que actúan dentro del proceso de comercio electrónico, a saber el cliente y el comerciante; de esta forma existe confianza recíproca para realizar determinado negocio.
b. **Autorización:** Debe ser designada una persona para fijar precios, emitir o firmar documentos.
c. **Procesos de oferta y contratación:** Se debe crear y estandarizar los protocolos para la confidencialidad, integridad y prueba de envío y recepción de documentos claves, con el fin de que no exista repudio de contratos de comercio electrónico.
d. **Información sobre fijación de precios:** Los precios publicados y descuentos deben ser exactos, no se existir un cambio, por lo que se necesita un nivel de confianza en cuanto a los listados.
e. **Transacciones de compra:** Punto neurálgico del comercio electrónico, tiene que ver con los datos que son suministrados en el momento de realizar una compra, la confidencialidad e integridad con respecto a pagos, direcciones de entrega, confirmación de la recepción.
f. **Verificación:** Dentro de este proceso es imperativo verificar que la información de pago que suministra el cliente es correcta e irrefutable.
g. **Cierre de la transacción:** Se debe establecer la forma de pago adecuada con el fin de evitar fraudes; por ejemplo a través de tarjetas de crédito o transferencias bancarias.
h. **Órdenes de compra**: Establecer los criterios de protección que se requiere para mantener la confidencialidad e integridad de la información sobre órdenes de compra y para evitar la pérdida o duplicación de transacciones.

i. **Responsabilidad**: Determinar quién asume el riesgo de eventuales transacciones fraudulentas.

Algunas de estas consideraciones pueden ser resueltas a través de técnicas criptográficas como las que veremos a continuación:

1. **Política de utilizar controles criptográficos:** Con esta política se busca maximizar beneficios y minimizar los riesgos que ocasiona el uso de técnicas criptográficas, evitando el uso inadecuado o incorrecto. El procedimiento es buscar el control criptográfico óptimo a ser aplicado, ver cuál es su propósito y el proceso que se necesita para ser implementado (ver si el control criptográfico sería la solución apropiada para proteger la información).

2. **Cifrado:** Es una técnica criptográfica con el fin de proteger la confidencialidad de la información sensible o crítica. Se evalúa los riesgos que puede tener dicha información, tomando en cuenta el tipo y la calidad del algoritmo de cifrado a utilizar y la longitud de las claves criptográficas. Al ser implementado una política de este tipo se debe tener en cuenta la normativa vigente, ya que en diferentes partes del mundo existe legislación en cuanto a los controles aplicables a la exportación e importación de tecnología criptográfica.

3. **Firma Digital:** Proporciona un medio de protección de la autenticidad e integridad de documentos electrónicos, dentro del comercio electrónico con el fin de verificar quien firma el documento y si su contenido ha sido o no modificado. Se puede aplicar para firmar pagos, transferencias de fondos, contratos y convenios electrónicos. Dependiendo del país la firma electrónica puede ser legalmente vinculante.

4. **Servicios de no repudio:** Se utiliza para resolver una disputa en cuanto a si un evento o acción ocurrió o no, por ejemplo cuando se objeta haber

enviado una instrucción firmada digitalmente a través de correo electrónico.

5. **Administración de claves:** Es esencial con el fin de utilizar de manera eficaz las técnicas criptográficas a las que nos hemos referido anteriormente, su objetivo es que la información sea confidencial, autentica e integra. Se debe implementar un sistema de administración de claves con el fin de respaldar el uso de las técnicas criptográficas por parte de la organización. Todas las claves deben ser protegidas contra modificación y destrucción; mientras que las claves secretas y privadas deben ser protegidas contra la divulgación no autorizada.

   Existen dos tipos de técnicas:

   a) **Técnicas de clave secreta:** Se da cuando dos o más partes interesadas comparten una clave y esta se utiliza para cifrar y descifrar información. El riesgo es que esta clave debe mantenerse en secreto, caso contrario se podría descifrar toda la información o introducir información no autorizada;

   b) **Técnicas de clave pública:** En este caso cada usuario tiene dos claves: una clave pública (que puede ser revelada a cualquier persona) y una clave privada (que debe mantenerse en secreto). Esta técnica se utiliza para crear firmas digitales como anotamos anteriormente.

CONCLUSIONES:

En el presente ensayo se ha revisado el impacto que ha tenido las tecnologías de la información y comunicación en nuestros días, sobretodo en cuanto la protección jurídica de los individuos con la relación al tratamiento automatizado de los datos de carácter personal. Se ha examinado las características que deben tener los datos para ser considerados objeto de protección de este derecho, así como cuales son los principios y derechos que se desprenden. El proceso tecnológico en el que vivimos ha desarrollado las nuevas formas de transacciones mercantiles de bienes y servicios, cambiando las antiguas practicas del comercio, y a su vez la forma de conseguir información sobre la necesidad de los potenciales consumidores, creando recolectores de datos, para conocer gustos y necesidades de las personas. Aunque en muchos de los casos estos buscadores de información pueden vulnerar la confidencialidad de los seres humanos, así como el derecho a la intimidad y privacidad, requisitos fundamentales para vivir en una sociedad libre.

En la actualidad se vuelve casi imposible limitar a las personas la creación de perfiles por medio de la red, ya que se elaboran con la información que se obtiene al navegar en la Web; siendo necesario procurar que exista una protección de esta información. Así también, la tecnológica evoluciona rápidamente existiendo la posibilidad de que los datos personales puedan ser manipulados; y el derecho no debe ni puede quedarse atrás con el fin de buscar el bien común de las personas.

Es por esto que también el derecho a la intimidad y privacidad ha evolucionado, ya no es considerado como el derecho a ser dejado solo, o una limitación para el Estado, ahora se ha convertido en una de las libertades individuales que se busca proteger, reflejado en el derecho al control sobre nuestros datos alojados en diversos soportes, tanto lógicos como físicos. Por ejemplo, se debe garantizar el tratamiento de datos considerados sensibles como los de la salud a los cuales nos hemos referido anteriormente.

Aquí se desprende la necesidad que dentro de un estado constitucional de derechos y justicia como en el que actualmente nos encontramos, es necesario ponderar los preceptos constitucionales; para garantizar lo establecido en el artículo sesenta y seis numeral vigésimo segundo “el derecho a la intimidad personal y familiar”. Es necesario desarrollar este precepto, a fin de responder a su espíritu y tenor, ya que actualmente no existe una normativa inferior que genere los mecanismos objetivos para garantizar el derecho, con el fin de alcanzar una oportuna protección en la materia generando seguridad jurídica. La ley de comercio electrónico, firmas electrónicas y mensajes de datos, como preámbulo protege los datos personales, introduciendo la necesidad de contar con una autorización por parte del titular para que estos sean tratados y se pueda garantizar la autodeterminación de los sujetos. Por ello encaja la necesidad de completar la regulación en esta materia. Cabe aclarar que el hábeas data es un mecanismo efectivo de acceso en forma posterior a los datos, es decir, a los ya existentes; pero deja abierta la posibilidad de la manipulación anterior, situación que apoya la necesidad de otra ley.

Existe la experiencia de países que se encuentran adelantados en el tema de protección de datos, que una vez creado el sistema jurídico, es necesario la creación de una autoridad que regule el uso de las bases de datos, como por ejemplo la Agencia Española de Protección de Datos, ente público

autónomo cuya finalidad es velar por el cumplimento de la legislación en cuanto a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

Es necesario hacer alusión a los casos y ejemplos tratados, en los que por medio de las TICs se puede vulnerar los datos personales. A saber el *Spam*, correo no deseado que se envía con fines comerciales donde utilizan nuestros datos con el fin de promocionar bienes y servicios, es perjudicial por el tiempo que se pierde la revisar cada correo no solicitado. Por su parte el *phishing* en nuestro país está en boga, son muchos los incautos que han sido víctimas de este tipo de estafa, sobre todo personas que utilizan los servicios del sistema financiero a través de medios electrónicos, evidenciándose la necesidad de contar con mejores controles y una capacitación a los clientes de estos servicios.

Las redes sociales y los motores de búsquedas, eminentemente servicios nuevos que presta la red, también son un lugar en el cual podemos sufrir algún tipo de vulneración en cuanto a nuestros datos personales y actividades que realizamos. Lastimosamente a través de las redes sociales estamos transparentando todas las actividades que realizamos, sin darnos cuenta que implícitamente estamos compartiendo datos sensibles y que no deben estar al alcance de cualquier persona; minimizando nuestra privacidad a la mínima expresión, ya una persona se puede enterar que realizó otra persona el fin de semana por medio de revisar por ejemplo el *Facebook*.

Ante todas estas consideraciones en el caso de ser una empresa o institución es necesario implementar todo un sistema de seguridad informática con el fin de garantizar la continuidad de la organización, minimizar el daño que puede ser causado por varios agentes; en este caso

se logra a través de medios técnicos respaldado por una gestión y procedimientos adecuados, que deben ser efectuados por medio de una planificación minuciosa por parte de todo el personal de una institución.

REFERENCIAS:

GLOSARIO:

- **Dirección IP**[40]: es un número que identifica de manera lógica y jerárquica a una interfaz de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (*Internet Protocol*), que corresponde al nivel de red del protocolo TCP/IP.
- **Hosting**[41]**:** El **alojamiento web** (en inglés *web hosting*) es el servicio que provee a los usuarios de Internet un sistema para poder almacenar información, imágenes, vídeo, o cualquier contenido accesible vía Web. Los Web Host son compañías que proporcionan espacio de un servidor a sus clientes.
- **Ingeniería social**[42]: es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.
- **Algoritmo de cifrado**[43]: En la jerga de la criptografía, la información original que debe protegerse se denomina *texto en claro* o texto plano. El *cifrado* es el proceso de convertir el *texto plano* en un galimatías ilegible, denominado *texto cifrado* o *criptograma*. Por lo general, la aplicación concreta del *algoritmo de cifrado* (también llamado *cifra*) se basa en la existencia de una *clave*: información

[40]Wikipedia. «Wikipedia.» www.wikipedia.org. 21 de junio de 2009 <http://es.wikipedia.org/wiki/Dirección_IP>
[41]Wikipedia. «Wikipedia.» www.wikipedia.org. 21 de junio de 2009 < http://es.wikipedia.org/wiki/Hosting>
[42] Wikipedia. «Wikipedia.» www.wikipedia.org. 21 de junio de 2009 <http://es.wikipedia.org/wiki/Ingeniería_social_(seguridad_informática)>.
[43]Wikipedia. «Wikipedia.» www.wikipedia.org. 20 de junio de 2009 <http://es.wikipedia.org/wiki/Algoritmo_de_cifrado>.

secreta que adapta el *algoritmo de cifrado* para cada uso distinto.

BIBLIOGRAFÍA:

- Aced Felaez, Emilio y y otros. ¿Seguridad, privacidad, confidencialidad? El desafío de la protección de datos personales. Montevideo: Ediciones Trilce, 2004.
- Almodóvar, Francisco. «Alfa Redi.» 2005. www.alfa-redi.com. 19 de junio de 2009 <http://www.alfa-redi.com//apc-aa-alfaredi/img_upload/cfbae8c34623d555c3da02c5242bd118/viewalmodovar.pdf>.
- Asamblea Constituyente. «Asamblea Nacional.» www.asambleanacional.gov.ec. 21 de junio de 2009 <http://www.asambleanacional.gov.ec/documentos-asamblea-nacional/constituciones/constitucion-de-1998/1998-Documento-original.pdf>.
- Brian Nougreres, Ana. «Informática y Derecho.» Informática y Derecho; Memorias del X Congreso Iberoamericano de Derecho e Informática. Santiago de Chile: LOM ediciones, 2004. 273- 284.
- Cabanellas de las Cuevas, Guillermo y otros. Derecho de Internet. Buenos Aires: Editorial Heliasta S.R.L., 2004.
- Caceres, María Paulina. Taller de Protección de Datos. Cuenca, enero de 2008.
- Castro Bonilla, Alejandra. 20 de agosto de 2008. Alfa Redi. <http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/castro.pdf> .
- Comisión de transparencia y acceso a la información del Estado de Nuevo León. «Comisión de Transparencia y acceso a la Información del Estado de Nuevo León.» enero de 2008. www.ctainl.org.mx. 20 de junio de 2009 <http://www.ctainl.org.mx/revista_8/elementos/fundamentojuridicopd.pdf>.
- Davara & Davara Asesores Jurídicos. Factbook Comericio Electrónico. Navarra: Aranzadi , 2001.
- Davara Rodríguez, Miguel Angel. Manual de Derecho Informático. Navarra: Editorial Aranzadi, SA., 1997.
- De los Reyes Corrpio Gil, María y Lorenzo Delgado. El tratamiento de los datos de carácter personal y la protección de la intiidad en el sector de las telecomunicaciones. Madrid: Agencia de protección de Datos, 2001.

- De Quinto Zumárraga, Francisco. Protección de Datos Personales. Barcelona: Il lustre Consell de Col.legis Oficials de Graduats Socials de Catalunya, 2001.
- Del Peso Navarro, Emilio. Ley de Protección de Datos La Nueva Lortad. Madrid: Ediciones Días de Santos, S.A., 2000.
- Del Peso Navarro, Emilio y Miguel Angel Ramos González. LORTAD Análisis de la Ley. Madrid: Ediciones Días de Santos, S.A., 1998.
- Devoto, Mauricio. Comercio Electrónico y Firma Digital. La regulación del ciberespacio y las estrategias globales. Buenos Aires, 2001.
- Diccionario de la Real Academia Española. Diccionario de la Real Academia Española. 20 de diciembre de 2009 <http://buscon.rae.es/draeI/SrvltGUIBusUsual?TIPO_HTML=2&TIPO_BUS=3&LEMA=dato>.
- Elías, Miguel. *Situación legal de los datos de carácter personal frente a las nuevas tecnologías* 2001. http://www.alfa-redi.org/rdi-articulo.shtml?x=638
- Facebook. facebook.com. 1 de septiembre de 2009 <http://www.facebook.com/terms.php>.
- Fernández Burgueño, Pablo. «Pablo F Burgueño.» 1 de septiembre de 2009 <http://www.pabloburgueno.com/wp-content/uploads/2009/06/El-peligro-de-las-redes.pdf>.
- Gregorio, Carlos G., Silvana Greco y Javier Baliosian. «Facultad Latioamericana de Estudios Sociales.» Flacso. 2 de 12 de 2008 <http://www.flacso.org.ec/docs/sfintgregorio.pdf>.
- Google Inc. Google. 1 de septiembre de 2009 <http://www.google.com/privacypolicy.html>.
- Google Inc. Google - Herramientas para Webmasters. 1 de septiembre de 2009 <https://www.google.com/accounts/ServiceLogin?service=sitemaps&passive=true&nui=1&continue=https://www.google.com/webmasters/tools/removals%3Fhl%3Des%26action%3Dcreate%26type%3Dot%26next%3DSiguiente%2B%25C2%25BB&followup=https://www.google.com/webmasters/t>.
- Mourguiart, Marcel. CHW. 1 de septiembre de 2009 <http://www.chw.net/2009/05/google-sentenciado-a-eliminar-datos-personales/>.
- Muñoz, Joaquín. Joaquín Muñoz - Protección de Datos y Nuevas Tecnologías. 1 de septiembre de 2009 <http://www.joaquinmunoz.com/2009/03/08/borrar-datos-personales-de-google/>.
- Organización de las Naciones Unidas. «Naciones Unidas.» 21 de junio de 2009 <http://www.un.org/es/documents/udhr/>.
- Rebollo Delgado, Lucrecio. Derechos Fundamentales y Protección de Datos. Madrid: Dykinson, S.L., 2004.
- Rivera Llano, Abelardo. Dimensiones de la informáticaen el Derecho. Bogotá: Jurídica Radar, 1995.

- Rivero Laguna, Jesus. Del Peso Navarro, Emilio. Ley de Protección de Datos, La nueva LORTAD. Madrid: Editorial Diaz de Santos, 2000. 23 - 24.
- Suñe Llinás, Emilio. Tratado de Derecho Informático Vol. 1. Madrid: A Gráficas y Encuadernaciones RC, 2000.
- Supervisor europeo de protección de datos. «Supervisor europeo de protección de datos.» www.edps.europa.eu. 21 de junio de 2009 <http://www.edps.europa.eu/EDPSWEB/webdav/shared/Documents/EDPS/Publications/Brochures/brochure_guide_es.pdf>.
- Wikipedia. «Wikipedia.» www.wikipedia.org. 20 de junio de 2009 <http://es.wikipedia.org/wiki/Algoritmo_de_cifrado>.
- Wikipedia. «Wikipedia.» www.wikipedia.org. 21 de junio de 2009 <http://es.wikipedia.org/wiki/Ingeniería_social_(seguridad_informática)>.
- Wikipedia. «Wikipedia.» www.wikipedia.org. 1 de septiembre de 2009 <http://es.wikipedia.org/wiki/Cookie>.
- Yánez, Pablo. Introducción al Estudio del Derecho Informático e Informática Jurídica. Quito: Escuela Politécnica Javeriana del Ecuador, 1999.

ANEXOS

ANEXO 1:

PRODUBANCO : actualice sus datos de ingreso y su clave maestra

De: **PRODUBANCO** (seguridad@produbanco.com.ec)
Enviado: miércoles, 08 de abril de 2009 11:50:36
Para: crisle4@hotmail.com

SOLO PARA CLIENTES DEL PRODUBANCO

Estimado cliente del produbanco:

Produbanco siempre a hecho todo lo posible por salvaguardar la información confidencial de sus clientes.Por lo tanto quiere hacerle saber que los servidores del produbanco han sido actualizados, incorporando estas mejoras a disposición del cliente:tenga en cuentas estos 3 puntos importantes:

- Después de 5 minutos de inactividad, la sesión caducará.
- Tu password unicamente lo podrás teclear desde nuestro teclado en linea.
- Ahora contamos con los mejores consultores de seguridad del mundo.

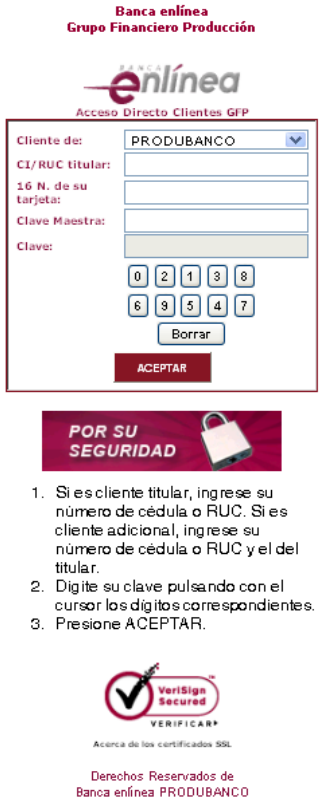
Además proximamente contará con un sistema de cifrado de datos nuevo, el cual permitirá que sus movimientos sean más veloces y seguros. Por lo que le recomienda, que ingrese en su cuenta bancaria a través de estos enlaces para asegurar la buena funcionabilidad de las nuevas mejoras:

Para Personas: actualización/produbanco_personas/login.asp?yes=personas

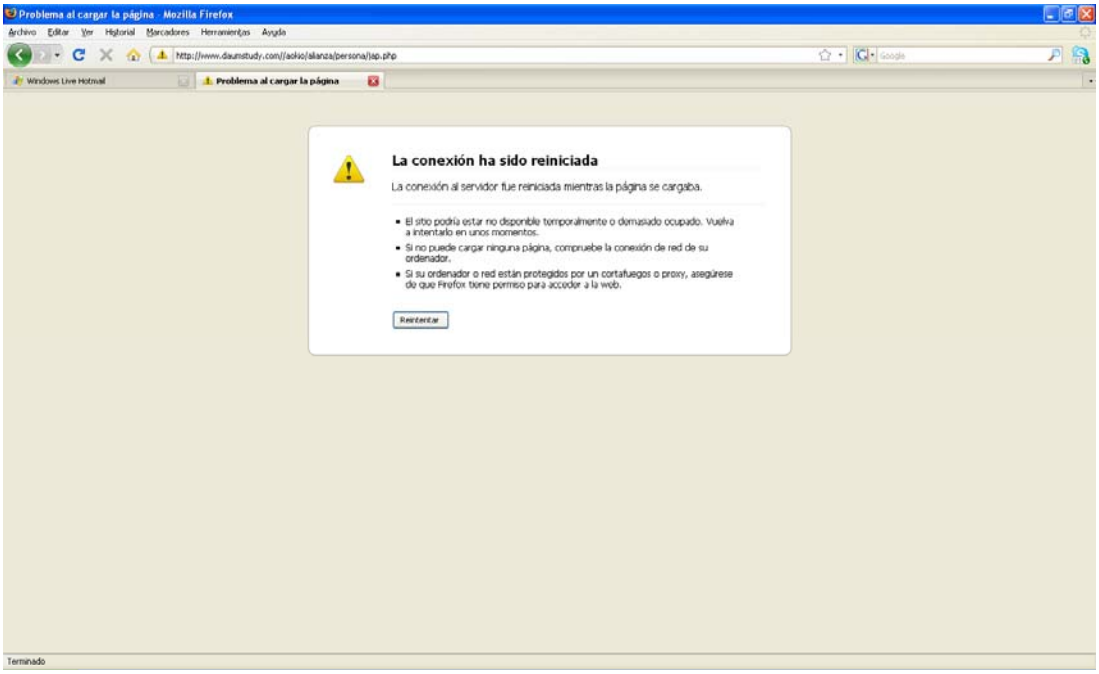
Para Empresas: actualización/produbanco_empresa/login.asp?yes=empresas

Gracias por su atención, Atte. Produbanco S.A.

ANEXO 2:



ANEXO 3:



ANEXO 4:

From: Microsoft Customer Support
Sent: Tuesday, January 08, 2008 10:41 PM
To: crisle4@hotmail.com
Subject: RE: SRX1055037783ID - Windows Live ID: Necesito saber una cosa.: Notificar un problema de :Otro

Estimada Cristina:

Gracias por contactarnos. Tu correo fue transferido del Soporte de Windows Live ID al Soporte de Windows Live Hotmail. Apreciamos tu interés y confianza en nuestros servicios.

De acuerdo con tu correo, comprendemos que presentas inconvenientes ya que nos comentas que un usuario se hace pasar por tu identidad con otra cuenta. Estamos en la mejor disponibilidad para ayudarte.

Si crees que tu nombre está siendo utilizado en una cuenta de MSN Hotmail, que no creaste, necesitamos una declaración tuya negando tu participación en la cuenta y con la persona que registró la cuenta.

Necesitamos prueba documentada de la falsificación o equivocación de tu identidad en MSN Hotmail (por ejemplo, un mensaje enviado por la persona que falsificó tu identidad, haciendo prueba de que la persona está falsificando tu identidad). Si no tienes un mensaje de correo electrónico sobre la falsificación de tu identidad, por favor envíanos una explicación escrita detallada de tus razones para creer que tu identidad está siendo falsificada.

Si tu identidad está siendo falsificada en un foro de conversación o en un grupo de noticias, necesitamos copia del mensaje utilizado en el foro de conversación o en el grupo de noticias, el nombre de MSN Hotmail utilizado en el mensaje y una explicación sobre la falsificación de tu identidad.

Por favor envía por fax tu reclamo, incluyendo el texto "Yo no creé la cuenta (nombre de la cuenta). Esta cuenta está siendo utilizada para falsificar mi identidad. No tengo conocimiento de la persona que creó esta cuenta."

Envía el fax al número 1 (425)-936-7329, con las siguientes instrucciones:
A: "Atención-MSNABUSE"

Por favor incluye una copia de tu identificación personal con foto y toda la documentación solicitada anteriormente.

Si no tienes acceso a un fax, por favor envía la información a:

Attn: MSNABUSE
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Lamentamos los inconvenientes que esto pudiera ocasionarte y a la vez agradecemos tu paciencia.

Ten en cuenta que Windows Live Hotmail también proporciona una completa ayuda en línea; simplemente ve a la siguiente dirección:

http://help.live.com//help.aspx?project=MailFull&market=es-es

Atentamente,

Pablo Sanchez
Soporte de Windows Live Hotmail

--- Original Message ---
From: crisle4@hotmail.com
Sent: Tuesday, January 08, 2008 8:24:33 PM UTC
To: LV_ID.WNLV.WW.00.ES.MSF.SEA.TS.T01.RTG.00.EM
Subject: Windows Live ID: Necesito saber una cosa.: Notificar un problema de: Otro
Servicio: [Service:]
Windows Live ID
Tipo de problema: [What type of problem do you have?]
Necesito saber una cosa. [Necesito saber una cosa.]
Notificar un problema de seguridad [Notificar un problema de seguridad]
Otro [Otro]
Nombre completo: [Full Name:]
Ma. Cristina León
¿En qué dirección de correo deseas recibir una respuesta? [What e-mail address would you like a response sent to?]
crisle4@hotmail.com
Dirección de correo electrónico principal o Id. de usuario asociado con la cuenta motivo de su solicitud. [Primary e-mail address/member ID associated with the account you are inquiring about:]
crisle4@hotmail.com
Para asegurarte de obtener una resolución rápida, proporciona tantos detalles como sea posible, incluyendo la fecha y la hora en que se produjo el problema, los pasos que seguiste antes de encontrarte con el problema para que podamos reproducirlo y los datos sobre cualquier mensaje de error que hayas recibido. [Be specific when describing your problem. The details that you include enable us to promptly send you the most likely solution to your issue.]
El problema que necesito averiguar es como se hace si han clonado mi cuenta de correo, es decir, en vez de ser @hotmail.com es @hotmail.es, y

desde esta están enviando información fraudulenta que me perjudica ya que aparecen mis datos.
Frecuencia del problema: [Frequency of the issue:]
Primera vez [First time]
¿Cómo obtiene acceso a su cuenta? [How do you access your account?]
Equipo [Computer]
Tipo de conexión a Internet: [Type of Internet connection:]
T1 o superior, o LAN corporativa [T1 or faster, or company LAN]
¿Ha instalado recientemente un programa nuevo? (Si ha seleccionado sí, agregue sus comentarios en el cuadro de texto de más arriba) ? [Have you recently installed any new software (if you enter yes please add more comments in the text box above)?]
No [No]
¿Qué sistema operativo utilizas?Windows Vista: Mozilla/5.0 (Windows; U; Windows NT 6.0; es-ES; rv:1.8.1.11) Gecko/20071127 Firefox/2.0.0.11 [Which operating system are you using?]
¿Qué explorador utilizas?: Firefox2.0.0.11 [Which browser are you using]
Ubicación: es-co - Español (Colombia) [Location: es-co - Spanish (Colombia)]
Tipo de soporte: Soporte de correo electrónico
Type of Support: E-mail Support
Browser Default Language: es-es,es;q=0.8,en-us;q=0.5,en;q=0.3