UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS JURÍDICAS

ESCUELA DE DERECHO

TITULO: EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y LA SEGURIDAD INFORMÁTICA.

TRABAJO DE GRADUACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADA DE LOS TRIBUNALES DE LA REPÚBLICA DEL ECUADOR

AUTORA: MARÍA CRISTINA LEÓN CARVAJAL

DIRECTOR: DR. ANTONIO MARTÍNEZ BORRERO

CUENCA, ECUADOR

2009

Índice de Contenidos:

Resumen:

En la presente monografía se realizará un análisis fundamentalmente de la situación actual de la protección de datos personales y de la seguridad informática dentro del ordenamiento jurídico ecuatoriano, ya que con el avance tecnológico se vuelve relevante para el derecho, porque no puede ser solamente estudiado desde la visión informática, dejando de lado la parte jurídica.

Es por ello que se estudiará la legislación ecuatoriana que desarrolla el tema, la diferencia entre intimidad y privacidad como bienes jurídicos protegidos, el hábeas data entre otros temas. Además haremos una revisión sucinta de la seguridad informática y algunos casos donde los datos personales son propensos a ser vulnerados

Abstract:

This paper is intended to make a basic analysis of the current state of data protection and computer security within the Ecuadorian legal system, since technological advancement issues have become relevant to the law, because it cannot be studied only from the computer point of view, ignoring the law.

INTRODUCCIÓN:

Actualmente en nuestro país carecemos de una ley específica que regule la protección de datos personales, sin embargo, cabe mencionar que la Constitución Política de la República del Ecuador[1] redactada en el año 2008, señala en el artículo sesenta y seis que: "se reconoce y garantizará a las personas:", numeral diez y nueve: "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". Así también tenemos normas supletorias como la Ley de Control Constitucional y la Ley de comercio electrónico, firmas electrónicas y mensajes de datos que hablan brevemente sobre este tema.

El problema que va a ser objeto de estudio dentro de esta monografía surge cuando los datos personales de un individuo dentro del quehacer diario son recolectados por personas naturales o jurídicas, a través de medios electrónicos o almacenados en estos; desconociendo el fin para el que se recaba esta información. Esto sucede en cualquier momento, por ejemplo, cuando realizamos actividades comunes como inscribirnos en un curso o alquilar una película, donde nos solicitan nuestros datos personales. Por otro lado, muchos de estos datos ya se encuentran en registros, bancos de datos, archivos u otros medios técnicos, y son de carácter sensible, por lo cual, se debe garantizar un adecuado manejo y utilización, al mismo tiempo que se debe respetar derechos como el del honor de las personas y la intimidad, derechos que gozamos conforme la Declaración Universal de los

[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

Derechos Humanos que expresa en el artículo doce: "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(…)"[2].

Con estos antecedentes se desprende la siguiente interrogante: ¿Cómo podemos hacer exigible los derechos que hemos enunciado si no existe regulación expresa sobre el tema? La norma suprema del país declara el principio, pero no existe una norma que objetivase el derecho. Para ejemplificar la problemática que con lleva esta situación tenemos el caso de la ausencia de normativa para las personas que viven con VIH/SIDA (PVVS), a quienes el Estado garantiza conforme la Constitución Política en su artículo sesenta y seis numeral once: "El derecho a guardar reserva sobre sus convicciones. Nadie podrá ser obligado a declarar sobre las mismas. En ningún caso se podrá exigir o utilizar sin autorización del titular o de sus legítimos representantes, la información personal o de terceros sobre sus creencias religiosas, filiación o pensamiento político; ni sobre datos referentes a su salud y vida sexual, salvo por necesidades de atención médica" [3]. Es decir, la confidencialidad sobre su estado de salud es un dato sensible que no puede ser divulgado con excepción por expresa autorización de la persona y solamente en circunstancias específicas; lo que se busca es proteger a las PVVS de toda forma de discriminación.

A partir de este ejemplo pueden surgir nuevas interrogantes como: ¿dónde se encuentran alojadas actualmente todos los datos sobre la salud? Y, ¿Quién garantiza que dichos datos no sean manipulados de forma dolosa o que causen un perjuicio a sus titulares? Por consiguiente, es de suma importancia analizar el tema de la protección de datos, ya que con el auge y revolución de las tecnologías de la información y comunicación (TIC's), el

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

[3] 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

mundo se encuentra inmerso dentro del movimiento de la Sociedad de la Información. Por ello, es indispensable que por medio de la ley, se garantice efectivamente los derechos consagrados por la Constitución, creando los instrumentos jurídicos necesarios para respaldar lo consagrado en la carta magna y lograr el manejo adecuado estos datos, tanto en la recolección como en su tratamiento, y como resultado respetar los principios reconocidos internacionalmente.

Por último, la presente monografía en su capítulo final tratará otro punto neurálgico, a saber: la seguridad informática; ya que es indispensable saber que sucede con los datos que nos solicitan en el momento que ingresamos a una página web, por ejemplo, al llenar un formulario o realizar una compra vía la Internet, así como, cual es la cadena de custodia que tiene determinada información reservada o confidencial dentro de una empresa o institución, ya que al momento no podemos estar seguros de cuál es el tratamiento que reciben nuestros datos, ni quién garantiza que sean utilizados de conformidad para lo que fueron creados, o que no seamos víctimas de una estafa vía on line, es decir cuando ingresamos nuestros datos en una página falsa.

CAPITULO 1: GENERALIDADES

1.1 Antecedentes:

Los cambios que se dan actualmente como resultado de la concurrencia de la informática y las telecomunicaciones, son muy drásticas sobre todo en los ámbitos político, económico, tecnológico, laboral y social; en el presente, es creciente el nivel de informatización y automatización que ha sufrido la sociedad, por el incremento vertiginoso en el acceso a fuentes de información; las relaciones interpersonales que actualmente se dan a distancia y el tratamiento de la información personal que se maneja por la Internet.

Estas consideraciones desencadenan como amenaza que algunos derechos fundamentales pueden ser vulnerados por nuevas formas de delincuencia, derechos que tienen origen en la dignidad humana, como es la libertad; que va de la mano del poder de decisión que tenemos las personas; dando como resultado a la intimidad y la necesidad de ser protegida jurídicamente. El sistema normativo con el que se cuenta tanto a nivel nacional como internacional no concede las soluciones adecuadas al problema planteado, en el caso de la normativa nacional porque existe un vacío legal especifico que delimite este problema y traiga su solución, existiendo solamente una regulación epidérmica y a nivel internacional la regulación existente envejece rápidamente, sin poder ser actualizada conforme la necesidad, produciendo de esta manera lagunas normativas peligrosas.

En la actualidad en cada momento se recolecta varios datos personales, convirtiéndose en una posible vulneración a los derechos fundamentales, o una pérdida de ciertas libertades; esto en razón que algunos de estos datos pueden servir para identificar a las personas y hasta su situación patrimonial. Así mismo, el peligro surge en el momento en que esto se convierte en una invasión a nuestra privacidad y/o intimidad (términos que serán analizados posteriormente); y que se da por la creciente capacidad que tienen los motores de búsqueda y a su vez, la facilidad para el almacenamiento de los nuevos sistemas informáticos.

Para ejemplificar a continuación encontramos algunas situaciones que pueden suscitarse, tomadas del libro Introducción al Estudio del Derecho Informático e Informática Jurídica de Pablo Yánez[4]:

1. Se puede tomar decisiones que afectan negativamente a los sujetos, sin que estos tengan conocimiento de porque se resuelve de una forma perjudicial;
2. Elaboración de un perfil del individuo, con interconexión a ficheros que permite controlar sus actividades;
3. Efectuar una simulación de las relaciones o comportamientos futuros del individuo, fundamentándose para ello en sus datos; y,
4. Actuar negligentemente, sin actualizar, borrando o completando los datos registrados.

Por su parte, las empresas con estos mismos datos pueden realizar diversos tratamientos, algunos no perceptibles para el usuario, ya que se puede captar, almacenar, relacionar y hasta transmitir datos que a simple vista se consideran intrascendentes; obtenerlos sin consentimiento o como dijimos anteriormente a través de omisiones de información que afectan la autodeterminación de las personas. Es por eso que el derecho a la protección de datos tiene por objetivo que los ciudadanos puedan tutelar

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

la información personal que se encuentra dentro de bancos de datos o archivos automatizados, que esta información sea fidedigna, reservada y cumpla con el fin para el cual fue recabada; caso contrario violaría derechos como el de la igualdad de las personas ante la sociedad en la que se desenvuelve, puede lesionaría la imagen del individuo y por ultimo invadir la vida privada.

1.2 Los datos

Antes de entrar en detalle sobre la protección de datos personales, es necesario definir lo que son los datos, y su implicación con otros términos como información, documentación y conocimiento, con el fin de distinguir estos términos y sus diferencias. La acepción que encontramos dentro del Diccionario de la Real Academia Española para el dato 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"[5].

Miguel Elías[6] se refiere de la siguiente manera: "El dato 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*")". Sin embargo, es interesante entender al dato como la "mínima unidad de información" conforme lo dice Molina Quiroga citado por Miguel Elías dentro del mismo artículo; diciendo "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.". Podemos llegar a la conclusión que los datos son unidades mínimas de información que pueden estar

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

[6] Sumer, 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

almacenadas en soportes físicos o lógicos, no tienen un fin específico, se encuentran aislados por lo que son palabras que carecen de un contenido como por ejemplo información.

Por consiguiente, los datos que se encuentran en un soporte físico o lógico y que tienen un tratamiento específico o algún tipo de adecuación con el fin de servir a un objetivo específico se convierten en información. La información según el diccionario de la Real Academia Española[7] es: (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 antecedente para una investigación y el momento en el que sirve para un fin o soluciona un problema, es información.

La documentación es un conjunto de datos, y el conocimiento surge de la información recabada; según el diccionario de la Real Academia Española, conocimiento[8] es a: 1. Acción y efecto de conocer. 2. Entendimiento, inteligencia, razón natural. 3. Noción, ciencia, sabiduría.

Me permito citar un ejemplo de la sutileza entre lo estos conceptos, según el Dr. Jesús Rivero Laguna[9] nos ilustra con el siguiente ejemplo:

> "El dato <<17 de febrero>>, así como el del <<22 de diciembre>>, probablemente no les diga nada a ustedes, salvo que tuviera que ver con una determinada celebración o recordatorio que les

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

[8]Diccionario de la Real Academia Española. Diccionario de la Real Academia Española. 20 de junio de 2009 <http://buscon.rae.es/drael/SrvltGUIBusUsual?TIPO_HTML=2&TIPO_BUS=3&LEMA=conocimiento >

[9] RIVERO LAGUNA, Jesús. Del Peso Navarro, Emilio. Ley de Protección de Datos, La nueva LORTAD. s.f.

afecte o interese. Aunque los anteriores datos se perfeccionasen con un año – lo que restringiría el ámbito de aplicación precedente, aumentando por el contrario su <<valor>>-, puede que siguieran sin despertar su interés.

Así, concretar el dato del 17 de febrero, al 1836, o concretar el dato del 22 de diciembre, al año 1870, sigue sin aportarnos nada probablemente, y puede que menos que antes, a nuestra sana curiosidad. Aparentemente, sería irrelevante que ambos <<datos>> formasen parte de un determinado fichero, estuviese o no automatizado.

Permítanme otros ejemplos de ficheros con datos de carácter personal: fichero <<A>>, que contiene, entre otros, el dato del primer apellido de personas españolas, como por ejemplo <<Domínguez>>, que si desean en línea anterior de presentación podríamos perfeccionar con el segundo apellido <<Bastida>>; y el fichero <<B>>, que contiene, entre otros, el dato del famoso poeta español precitado <<Bécquer>>.

¿Dónde quiero llegar? Muy sencillo.

Ficheros con datos personales, aparentemente inocuos e inconexos, pueden aportarnos sabrosas informaciones. Así, si sabemos que los ficheros A y B antes citados contienen datos relacionados, podríamos deducir, por ejemplo, que <<Gustavo Adolfo Bécquer se llamaba, en realidad, Gustavo Adolfo Domínguez Bastida>>.

Igualmente, si de estos últimos ficheros sabemos cómo se relacionan con los primitivos de datos de fechas, podríamos concluir relevantes informaciones (cuando menos para ganar en esta ocasión un premio en algún Concurso de Literatura, o <<prestigio personal>> en una partida de Trivial): <<Bécquer o Domínguez Bastida, nació el 17 de febrero de 1836 y murió el 22 de diciembre de 1870>>.

Además, podemos generar conocimiento a partir de las información precedentes, deduciendo importantes conclusiones:

años de vida, etc., y extrapolando estadísticas relativas a las personas cuyos datos poseemos en nuestros ficheros.

Ésta es la cara y la cruz de la moneda de oro que tenemos en nuestras manos: según se utilice puede generar riqueza añadida, o introducir abusos ilegítimos. El <<dato>> en sí mismo puede ser irrelevante, no así su <<información>> asociada, y desde luego determinante el <<conocimiento>> que puede llegar a generar."

1.3 La protección de datos personales

Como hemos revisado anteriormente, a través de las nuevas tecnologías de la información y comunicación, se puede realizar el tratamiento, almacenamiento y transmisión de la información lo que hace posible que se controle la información con la que se cuenta y como consecuencia convertirse en un instrumento de presión y control social; ya que debemos recordar que la información es la base del conocimiento y a su vez el conocimiento es una garantía del bienestar[10] , como por ejemplo, cuando la información está en manos de los poderes públicos, o en el caso de las empresas privadas, pueden estos datos convertirse en una herramienta comercial, como sucede actualmente con todos los correos electrónicos que nos llegan con información sobre empresas y servicios.

Por otro lado, en la sociedad en la cual estamos viviendo es imperativo proporcionar de una forma más o menos voluntaria, determinados datos con el fin de preservar el bien común; pero, estos datos a su vez deben estar protegidos contra el acceso de personas no autorizadas, es decir, la protección de datos tiene como objetivo limitar la utilización de la

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

informática ante el temor de que pueda agredir a la intimidad de los ciudadanos y coartar el ejercicio de sus derechos.[11]

El diccionario de la Real Academia Española, nos da un concepto específico para lo que es la protección de datos y se refiere en los siguientes términos: 1. f. Sistema legal que garantiza la confidencialidad de los datos personales en poder de las administraciones públicas u otras organizaciones. *Agencia de protección de datos.*[12]

Según Miguel Davara: se entiende a la protección de datos como: "el amparo debido a los ciudadanos contra la posible utilización por terneros, 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"[13] De esta frase se desprende los siguientes puntos a considerar:

1. Se intenta proteger a las personas ante el 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.

[11] Davara Rodríguez, M. A. (1997). *Manual de Derecho Informático*. Navarra: Editorial Aranzadi, SA.
[12]Diccionario de la Real Academia Española. Diccionario de la Real Academia Española. 20 de junio de 2009 <http://buscon.rae.es/drael/SrvltConsulta?TIPO_BUS=3&LEMA=proteccion>
[13] Davara Rodríguez, M. A. (1997). *Manual de Derecho Informático*. Navarra: Editorial Aranzadi, SA.

A modo de conclusión, podemos decir que la naturaleza jurídica de la protección de datos personales está basada en los principios constitucionales de la dignidad e integridad de las personas, y su función social es la de garantizar que cada persona posea el poder de control sobre sus datos personales, en el uso y destino, con el propósito de impedir su tráfico ilícito y una potencial vulneración de la dignidad del titular del dato.

Debemos aclarar que la expresión "protección de datos" da a entender equívocamente que el objeto de protección será el dato, cuando **en realidad el fin que tiene este derecho es proteger al sujeto titular de los datos.** Sin embargo, positivamente a la expresión anterior podemos decir que este término encasilla el estudio en los datos y la incidencia en el bien jurídico protegido y los intereses que puede afectar. De todas maneras es conveniente afirmar la expresión correcta sería: **Protección jurídica de los individuos con relación al tratamiento automatizado de los datos de carácter personal.**

1.4 Clasificación de los datos personales:

Existe una gran variedad de datos, los cuales pueden ser de toda índole: geográficos, históricos, animales, climáticos, personales entre otros, de los cuales los relativos a las personas tienen una importante relevancia debido a los derechos que de ellos se desprende. Los datos personales por ejemplo pueden ser apellidos, fecha de nacimiento, número de teléfono, datos biométricos o médicos, información sobre la carrera profesional, etc."[14]. Son los que contienen características identificadoras de personas o que se les puede imputar.

[14]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

Una acepción que se puede dar de Datos Personales es: "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."[15]

La clasificación con la que trabajaremos será una construida a partir de varios tratadistas entre ellos Miguel Davara, Miguel Elías, y Pablo Yánez, que concuerdan en tener como línea de partida la confidencialidad, entendida como el mayor o menor grado 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**: Son aquellos conocidos por un número cuantioso de personas, o por la comunidad en general, sin que su titular, aunque no esté obligado a proporcionarlos si fuesen demandados puede impedir su difusión dentro de los límites de respeto y de convivencia social. Muchas veces constan en numerosos registros públicos o privados Ejemplo: nombres, apellidos, edad, profesión.

b. **Datos privados:** Son aquellos que su titular tiene la facultad para ponerlos en conocimiento de terceros, dependiendo de las situaciones o circunstancias en que la persona se ve obligada a proporcionarlos o ponerlos en conocimiento de terceros como por

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

ejemplo si están regulado por la ley. Sin embargo, aquí la conciencia social puede favorecer para impedir que se realice su difusión y respetar la voluntad del secreto.

Como conclusión se desprende que la diferencia 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:

a. **Datos íntimos:** Son datos que se refieren a un sujeto individualizado y relativos a su fuero interno o íntimo sin llegar a información puramente sensible. Son aquellos datos que el individuo puede protegerlos de su difusión, salvo que tenga que proporcionarlos periódica y regularmente y siempre que vayan a cumplir un determinado fin cívico o de conformidad con la Ley. Estamos hablando por ejemplo de datos que identifican su personalidad, creencias e ideologías, pensamientos, sentimientos y salud.

   El problema que desencadena estos datos, se da en función de existir una asociación entre varios de ellos, y llegar a crear un perfil inexacto o arbitrario y con el cual se puede causar un daño al titular o convertirse en datos secretos.

b. **Datos secretos:** Son aquellos que el individuo no está obligado a dar a nadie, salvo casos excepcionales contemplados de forma tácita por la Ley; pero que en forma correlativa es necesario la existencia de una regulación detallada que

proteja correctamente la difusión. Por ejemplo, datos relativos a la salud, en el caso específicos de personas portadoras de VIH/SIDA. Debemos recordar que una de las facetas de la intimidad como parte de la libertad es el derecho al secreto, que se entiende como la facultad que tenemos los individuos para reservarse ideas, sentimientos o conocimientos. Los datos secretos se clasifican en profundos y reservados:

i. **Datos profundos:** Son aquellos que bajo ningún concepto el individuo está obligado a proporcionarlos, salvo el caso de 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 Legislación Ecuatoriana referente al tema

El Ecuador, hasta el momento no cuenta con una ley específica sobre esta temática de protección de datos informáticos así como tiene España a través de la Ley Orgánica 15/199, del 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y Argentina con la ley 25.326 de Protección de Datos Personales. Esta situación causa muchos vacios al momento de tratar de resolver o buscar una solución a determinado problema referente a este tema de análisis, situación por la que debemos recurrir a otras leyes que tienen vinculación con este derecho como son:

1. **Constitución de la República del Ecuador (2008)[16]:** se encuentra vigente actualmente hace un importante avance en cuanto a lo que es la protección de datos, ya que reconoce expresamente su existencia en el artículo sesenta y seis sobre los derechos de libertad en su numeral décimo noveno donde manifiesta: "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." A su vez dentro del mismo artículo en el numeral vigésimo reconoce el derecho a la intimidad personal y familiar.

   Así también, en la sección quinta sobre la acción del hábeas data del capítulo tercero, título III nos manifiesta de manera mucho más completa que la Constitución de 1998 en qué consiste esta garantía al expresar en el artículo noventa y dos:
   "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 datos sensibles,

[16] 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

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, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados".

2. **Constitución Política de la República de 1998[17]:** Tenía varios artículos pertinentes a nuestro estudio, por ejemplo el artículo veinte y tres al referirse a los derechos que el Estado reconocerá y garantizará a las personas, dentro del numeral octavo enuncia: "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"; así mismo el numeral vigésimo primero del mencionado artículo nos dice que: "El derecho a guardar reserva sobre sus convicciones políticas y religiosas. Nadie podrá ser obligado a declarar sobre ellas. En ningún caso se podrá utilizar la información personal de terceros sobre sus creencias religiosas y filiación política, ni sobre datos referentes a salud y vida sexual, salvo para satisfacer necesidades de atención médica"

   Por su parte dentro en la sección segunda del capítulo sexto del Título III declara la garantía del hábeas data, conforme al artículo noventa y cuatro enuncia que "Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio,

[17]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>.

el afectado podrá demandar indemnización. La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional" Por último el artículo doscientos setenta y seis da como competencia del Tribunal Constitucional en el párrafo tercero el conocer las resoluciones que denieguen del hábeas data entre otros recursos.

3. **Ley de Control Constitucional[18]:** tiene un capítulo específico para el Hábeas Data como Garantía de los derechos de las personas, y enuncia se puede interponer este recurso en el caso de desear tener acceso a documentos, bancos de datos e informes que sobre sí mismas o sus bienes, así como conocer el uso y finalidad que se les haya dado o se les esté por dar.

El objeto del hábeas data conforme el artículo treinta y cinco es:

a) Obtener del poseedor de la información que éste la proporcione al recurrente, en forma completa, clara y verídica,
b) Obtener el acceso directo a la información;
c) Obtener de la persona que posee la información que la rectifique, elimine o no la divulgue a terceros; y,
d) Obtener certificaciones o verificaciones sobre que la persona poseedora de la información la ha rectificado, eliminado, o no la ha divulgado.

El hábeas data no es aplicable en el caso que afecte al sigilo profesional, para obstruir la acción de la justicia o cuando los documentos que se soliciten tengan carácter de reservados por razones de Seguridad Nacional. Por último, no se puede solicitar la

[18]—. Tribunal Constitucional. 20 de junio de 2009 <http://www.tribunalconstitucional.gov.ec/documentos/Ley%20de%20Control%20Constitucional.pdf>.

eliminación de datos o informaciones cuando por ley deben mantenerse en archivos o registros públicos o privados.

4. **Proyecto de Ley de Garantías y Control Constitucional[19]:** El 10 de junio de este año el Presidente de la República envió a la Comisión Legislativa el Proyecto de Ley Orgánica, en el mismo que cuenta con las siguientes particularidades en cuanto al Habeas data:
   a. En el objeto amplía el ámbito de aplicación a los datos genéticos, además de ya hablar que estos datos pueden encontrarse en soporte material o electrónico.
   b. Se cambia el objeto del hábeas data por el ámbito de protección, enunciando que esta acción se puede interponer en los casos en que se niegue 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, además de cuando se niegue la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten sus derechos; y por ultimo cuando se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de jueza o juez competente.
   c. Sin embargo, este proyecto suprime toda la regulación en cuanto al proceso, que si cuenta la actual ley.

5. **Ley de comercio electrónico, firmas electrónicas y mensajes de datos[20]:** En el artículo nueve se pronuncia sobre la protección de datos al expresar lo siguiente:

[19]Presidencia de la República del Ecuador. Asamblea Nacional. junio de 2009. 21 de junio de 2009 <http://www.asambleanacional.gov.ec/index.php?option=com_docman&task=doc_download&gid=544&Itemid=188>.

[20]—. Conatel. 20 de junio de 2009 <http://www.conatel.gov.ec/site_conatel/index.php?option=com_docman&task=doc_download&gid=1775&Itemid=>.

a. 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
b. 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 la referida ley. Los datos personales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.
c. No es preciso el consentimiento para recopilar datos en los siguientes casos:
    i. Cuando se haga de fuentes accesibles al público,
    ii. Cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y;
    iii. 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.
d. Es consentimiento pude ser revocado a criterio del titular, pero no con efecto retroactivo.

6. **Reglamento general a la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos[21]:** Dentro del artículo veinte y uno sobre la seguridad en la prestación de servicios electrónicos manifiesta que se consideran datos sensibles los datos personales, información financiera de cualquier tipo como por ejemplo números

[21]—. Conatel. 21 de junio de 2009 <http://www.conatel.gov.ec/site_conatel/index.php?option=com_docman&task=doc_download&gid=1776&Itemid>

de tarjetas de crédito, o datos similares que puedan involucrar la transferencia de dinero, o se pueda cometer fraudes o ilícitos.

7. **Código Orgánico de la Función Judicial[22]**: en el artículo trece enuncia que se prohíbe a las juezas y jueces dar trámite a informaciones sumarias o diligencias previas que atenten a la honra y dignidad de las personas o a su intimidad.

8. **Ley especial de Telecomunicaciones[23]**: En el artículo catorce de las disipaciones fundamentales declara que el Estado garantizara el derecho al secreto y privacidad de las telecomunicaciones

9. **Código de Procedimiento Penal[24]:** especifica que uno de los derechos del ofendido es a que se proteja su persona e intimidad conforme el artículo sesenta y nueve

10. **Ley General de Instituciones del Sistema Financiero[25]**: en el capítulo III sobre el sigilo y reserva bancaria perteneciente al título VIII tiene una referencia especial a este tema, que consta desde el artículo ochenta y ocho al noventa y cuatro; menciona sobre lo que es el sigilo bancario, en el que las instituciones financieras no podrán proporcionar información relativa a las operaciones sino solo al titular

[22]Registro Oficial. Derecho Ecuador. 20 de junio de 2009 <http://www.derechoecuador.com/index.php?option=com_content&task=view&id=4874&Itemid=526>.

[23] Congreso Nacional del Ecuador. Conatel. 20 de junio de 2009 <http://www.conatel.gov.ec/site_conatel/index.php?option=com_docman&task=doc_download&gid=1774&Itemid=>.

[24]—. Lexis. 20 de junio de 2009 <http://www.lexis.com.ec/lexis/novedadesDescargas/CodigosLeyes/CODIGO%20DE%20PROCEDIMIENTO%20PENAL.htm>.

[25]—. Superintendencia de Bancos del Ecuador. 20 de junio de 2009 <http://www.superban.gov.ec/medios/PORTALDOCS/downloads/normativa/Ley_gral_inst_sist_financiero_ene_2009.pdf>.

o su representante. Por otro lado los informes de inspección y análisis que emita la Superintendencia, en el ejercicio de las funciones de control y vigilancia, serán escritos y reservados, estos informes no se divulgarán a terceros, en todo ni en parte, por la Superintendencia, ni por la institución examinada, ni por ninguna persona que actúe por ellos, salvo casos específicos determinados en la misma ley.

1.6 La intimidad y la privacidad

El pilar fundamental de la protección a la individualidad de la persona es el derecho a la intimidad, preliminarmente se puede entender que se relaciona con la protección del hombre a aquel ámbito que no desea hacer público o sentimientos, pensamientos o hábitos propios de una persona, familia o colectividad[26]; es un derecho fundamental consagrado en la Constitución como norma suprema del Estado e internacionalmente a través de las convenciones relativas a los derechos humanos, pero que actualmente ha adquirido una nueva dimensión dentro de la Sociedad de la Información por la posibilidad del tratamiento automatizado de la información y su transmisión telemática. Es decir, es necesario que el derecho a la intimidad tenga raíces profundas en la dignidad, el respeto y sobretodo la inviolabilidad de la persona.

En la actualidad un tratamiento automatizado de los datos de carácter personal 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[27] 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

[26] Caceres, María Paulina. Taller de Protección de Datos. Cuenca, enero de 2008.
[27] Davara & Davara Asesores Jurídicos. (2001). *Factbook Comericio Electrónico*. Navarra: Aranzadi .

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.

1.6.1 Desarrollo histórico:

Los derechos de intimidad y privacidad se han desarrollado conforme la normativa a la cual pertenece, en este caso tenemos la tradición del *Common Law* que se rige para los países anglosajones y el derecho continental que es el que nos rige a países como Ecuador, a toda Latinoamérica y a países como España y Francia.

Según el derecho anglosajón los derechos de privacidad abarcan un área más amplia en engloba:

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.

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*[28], entendida como la inviolabilidad de domicilio.

[28] 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.

Actualmente es considerado como un derecho fundamental, derecho de la personalidad. La noción moderna de intimidad es entendida como un atributo entre la libertad y la autonomía; la intimidad es simultáneamente condición de la personalidad individual y de la personalidad social[29].

"El derecho a la intimidad 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.[30]"

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.
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.

---

www.ctainl.org.mx. 20 de junio de 2009 <http://www.ctainl.org.mx/revista_8/elementos/fundamentojuridicopd.pdf>.

[29] 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

[30] CASTRO BONILLA, Alejandra. «Alfa Redi.» 20 de agosto de 2008 <http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/9507fc6773bf8321fcad954b7a344761/castro.pdf>

Dentro de la jurisprudencia de los Estados Unidos el derecho de la privacidad busca proteger los sentimientos y sensibilidades de las personas, no su propiedad o intereses pecuniarios, de donde se desprende que es un derecho personal que termina con la muerte. Un caso que es interesante mencionar es el caso de 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[31].

Dentro de la doctrina alemana, que sigue la corriente continental, la intimidad se entiende desde tres esferas, conforme lo señala el artículo "El fundamento jurídico de la protección de datos"[32]:

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.

1.6.2 Diferencia entre intimidad y privacidad.

[31]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

[32]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>.

Según el Diccionario de la Real Academia Española en la edición vigésima segunda nos indica al referirse por intimidad[33] en su segunda acepción se entiende como: "Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia". Por su parte la privacidad[34] 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 por ejemplo.

Por su parte para 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 revisar libros consultados, películas vistas, asociaciones a las que se pertenece, entre otras. Debemos recordar además que un elemento fundamental y materia para que exista la privacidad e intimidad son los datos personales, ya que todos estos datos son susceptibles de protección, cada individuo decide en qué esfera colocar su información y aunque no todos son íntimos o privados es más, los asuntos íntimos son privados, pero no todos los asuntos privados son íntimos.

1.7 El Hábeas Data:

El impacto que las TIC en la actualidad se ve reflejado a través de las formas de acceso a la información con todas las opciones que se pueden dar, entre las que se encuentra en el caso de que la información sea de acceso público o restringido, que el titular de la misma pueda tener acceso a ella

[33] http://buscon.rae.es/draeI/SrvltGUIBusUsual?TIPO_HTML=2&TIPO_BUS=3&LEMA=intimidad
[34] Diccionario de la Real Academia Española. Diccionario de la Real Academia Española. 20 de junio de 2009 <http://buscon.rae.es/draeI/SrvltGUIBusUsual?LEMA=privacidad>

con la posibilidad de actualizarla o corregirla si es del caso. El hábeas data es la institución encargada de este propósito.

El habeas data puede ser clasificado en función del bien jurídico protegido de la siguiente manera:

- Hábeas data propio: Destinado a tutelar el derecho a la autodeterminación informativa, los principios de igualdad, dignidad y libertad; los derechos del honor, reputación, intimidad e imagen; que pueden ser vulnerados a través del tratamiento de la información. Este sería el necesario para nuestros fines.
- Hábeas data impropio: Protege el derecho al acceso a la información pública. En este caso, este hábeas data se encuentra dentro de la LOTAIP (Ley orgánica de transparencia y acceso a la información pública)

Clasificación del Habeas data[35]:

a. **Informativo:** Persigue el acceso a un registro con el fin de indagar sobre la información que se encuentra en el.
    a. **Exhibitorio:** Su fin es conocer los datos propios registrados e información pública, es decir se habla del derecho al libre acceso a las fuentes de información, incluida la libertad de prensa o expresión. Sin embargo, vale aclarar que es un derecho limitado que se contrapone al derecho de seguridad del Estado.
    b. **Finalista:** Se entiende que busca conocer la finalidad por la cual se recogió el dato.
    c. **Autoral:** Saber quien obtuvo el dato.
b. **Aditivo:** busca que se agregue un dato que al ser omitido afecta al titular o en su defecto que se aclare. Un ejemplo de esto puede darse

[35]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

en cuanto a las bases de datos crediticias en cuanto al garante y deudor principal.

c. **Correctivo:** Lo que se intenta es que se corrijan datos falsos, inexactos, imprecisos o ambiguos que se puede llevar a interpretar erróneamente alguna situación.
d. **Reservador:** Se da en el caso de datos confidenciales para que no sea conocidos por cualquiera, por ejemplo en el caso de datos sensibles.
e. **Cancelatorio:** Busca la eliminación del dato dentro del archivo ya que no se puede garantizar que el dato se encuentre con la reserva y confidencialidad necesaria o cuando simplemente es un dato que ya no trae ningún beneficio.

Por su parte para la jurisprudencia de varios países de América existen otros tipos de habeas data, a saber:

- Impugnativo: busca cambiar una valoración equivoca de la información
- Bloqueador: de forma precautelatoria hasta que se decida si se cancela o de mantiene un dato.
- Disociador: con el fin de que se transforme el dato a fin de que no se reconozca al sujeto.
- Asegurador: A fin de que el juez evalúe si se utilizaron los medios técnicos idóneos para evitar la utilización del dato por quienes no están autorizados.
- Reparador: es la acción que se entabla para que se ordene indemnizar el daño causado.

1.8 *La intimidad de las personas jurídicas*

Para entrar en el tema de la intimidad de las personas jurídicas es necesarios hablar de quien es el sujeto activo, es decir, la persona física o las personas jurídicas. Se dice comúnmente que las personas jurídicas no tienen

intimidad, pero la pregunta que se hace en este caso es que si son titulares de derechos fundamentales las personas jurídica. El problema surge en el hecho que a las personas naturales se les protege la intimidad y privacidad, pero en el caso de las jurídicas solo se les podría proteger exclusivamente la situación económica.

Existen diferentes corrientes al respecto, España, Alemania, Francia e Irlanda excluyen la protección a las personas jurídicas, por su parte Suiza, Australia, Dinamarca, Luxemburgo y Noruega lo admiten en el aspecto económico que hacíamos referencia. Por su parte las Naciones Unidas permiten que los Estados contratantes apliquen la protección a las personas jurídicas. En el caso del derecho continental por ejemplo, para Venezuela no cabria esta situación conforme a lo declarado por el Tribunal Superior de Justicia en *Inversora Bohemia II C.A y Valores H.B*; mientras que en Trinidad y Tobago si, como se demuestra en el caso *Collymore y cotro c. General Attorney el Privy Council*[36].

Lo que puede suceder para que se dé cabida a la existencia de esta figura, es que las personas jurídicas se vean afectadas por las conductas que protegen la intimidad de las personas naturales, es decir, cuando existe una violación a sus derechos no se tienen un mecanismo para que se puedan defender.

Como lo expone Orozco Pardo, dentro del libro de Peso Navarro[37] nos dice que esto no supone que las personas jurídicas pasen a ser titulares de derechos y facultades, que por esencia no es posible, pero que, con el

[36] 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

[37] DEL PESO NAVARRO, Emilio. Ley de protección de datos. La nueva LORTAD. . Madrid: Diez de Santos, 2000.

ánimo de impedir su indefensión, cabe extender la protección de la Ley a tales entidades.

CAPÍTULO 2: LA PROTECCIÓN DE DATOS:

2.1 *Aspectos generales:*

La protección de datos puede girar sobre varios principios, los más importantes tienen que ver con el consentimiento, entendido como la manifestación de voluntad, mediante la cual el interesado autoriza en este caso el tratamiento de sus datos personales. Según Davara[38] el ciudadano es el único que decide cuándo, dónde y cómo se presentan sus datos al exterior, o se dan a conocer sus datos a terceros; esto es, el afectado tiene que otorgar su consentimiento para que se pueda realizar un tratamiento automatizado de sus datos de carácter personal; dicho de otra forma, no se pueden tratar datos de carácter personal sin consentimiento de su titular (del titular de los datos).

2.2 *Características*

Según Pablo Yanes en la obra citada, los datos personales para ser considerados objetos de protección por parte del derecho deben ser[39]:

- **a. Lícitos:** que tanto en su recogimiento o en su uso, no se utilicen criterios o conductas determinadas como ilícitas por la ley.
- **b. Determinados**: los datos de carácter personal objeto de tratamiento automatizado no podrán usarse para finalidades distintas de aquellas para las que los datos hubieran sido recogidos.

[38] Davara & Davara Asesores Jurídicos. (2001). *Factbook Comericio Electrónico*. Navarra: Aranzadi .

[39] 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 al titular de los mismos.
d. **Actualizados:** debe ser puestos al día de forma que respondan con veracidad a la situación real de su titular
e. **Temporalizados:** no serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.
f. **Accesibles:** Serán almacenados de forma que permitan el ejercicio del derecho de acceso por parte de su titular.
g. **Rectificables:** los datos, al ser automatizados, admitirán la posibilidad de rectificación.
h. **Cancelables:** los datos, se encuentren en el soporte que se encuentre, admitirán la posibilidad de borrarlos físicamente
i. **Consentidos:** su entrega nacerá de la voluntad expresa del titular, 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 de su manejo responderán por su alteración, pérdida, tratamiento o acceso no autorizado, había cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural
l. **Secretos:** los responsables de su tratamiento automatizado y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal 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 automatizado, o en su caso, con el responsable del mismo.

Nuestra legislación debería recoger los siguientes elementos: en primer lugar se debe hacer los lineamientos sobre los momentos que se protegerán dentro del tratamiento de datos:

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

Esto tiene su importancia porque dependiendo del momento se fijará los principios de la protección de datos, los derechos de los ciudadanos y los procedimientos que permitirán ejercer los derechos. Además que 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.

2.3 Principios de la protección de datos

Principios generales:

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.

- **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: Porque 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 dato deben reflejar con veracidad la situación del titular.
c. **Principio de congruencia y racionalidad:** 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 previo en todos los casos para que sus datos sean tratados o cedidos. Dicho consentimiento debe tener como características que debe ser libre, expreso, escrito e. 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.

2.4 Derechos:

Es necesario que los principios arriba enunciados tengan un reconocimiento para que se pueda conseguir una protección idónea, a saber:

a. **Derecho a la autodeterminación:** Es la facultad de controlar y conocer los datos que sobre ella 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 estos le sean requeridos.
c. **Derecho de rectificación y cancelación:** En caso de que los datos son inexactos o dejado de ser necesarios, el titular puede solicitar estos derechos.
d. **Derecho de impugnación:** En el caso de 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.

2.5 Datos especialmente protegidos:

Existen datos que deben ser protegidos por sus titulares o personas detentoras, ya que entran en la esfera de lo intimo, 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..

Entramos a analizar esta situación ya que toda persona nace con el derecho de que sus datos personales sean protegidos, lo que conlleva a

que en el caso de los datos sobre la salud, no sean utilizados de forma indebida, es decir, debe existir una tutela a este derecho. Actualmente en la Sociedad de la Información, cada vez más la tecnológica ha transformado el mundo medico y existe una serie de datos personales que están en manos de cualquier persona dentro de este fructífero negocio. No podemos negar que son datos necesarios para el desarrollo científico, sobretodo en cuanto a los signos y síntomas que tiene una persona al desarrollar determinada enfermedad, pero también esto puede convertirse en una especie de mafia donde están asociados médicos, casas farmacéuticas y farmacias.

Es un proceso que ha estado latente desde hace mucho tiempo, sin embargo, con el descubrimiento del genoma humano se ha dado un gran avance, ya que se ha pasado de una medicina colectiva a una personalizada, es decir, depende el diagnóstico según la persona; lo que conlleva a una medicina con responsabilidad en el manejo, utilización y protección de los datos dependiendo de cada ser humano para su diagnostico. Sin embargo, esta medicina desprende la responsabilidad de utilizar y proteger los datos personales.

De aquí nace lo que se llama el dato terapéutico, que es 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. Según Francisco Almodóvar[40] dentro de su artículo "El dato personal terapéutico", al dar un concepto nos dice que 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".

[40]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>.

Como hemos dicho anteriormente, cada uno de los ciudadanos tiene que ser informado sobre cuál será el tratamiento que se dé a sus datos, para que este dé su consentimiento. Este es un proceso de sumo cuidado, tiene varias etapas dentro de un proceso, que debe ser homologado a nivel internacional con el fin de cumplir su objetivo. Esta información es de suma importancia para poder llegar al objetivo de realizar investigación científica, ya que se necesita grandes cantidades de información personalizada.

En este sentido, se ve la necesidad de que exista un órgano que controle y supervise los datos recolectados, con el fin de que sean adecuados, pertinentes y sobretodo no sean excesivos, además de que se deben crear estándares de actuación en relación a quién accede a los datos, por qué, para qué, si está autorizado, como actualizar los datos, y las responsabilidades entre otros criterios. Otro problema que podemos traer a colación es que son varias las personas que tienen acceso al dato terapéutico, por ejemplo, en este caso el prescriptor, para ofrecer una información eficaz, es decir para crear un sistema de seguimiento fármaco terapéutico con el fin de tener una educación en salud preventiva.

CAPÍTULO 3: SEGURIDAD DE LA INFORMACIÓN

3.1 Introducción:

Para entrar en el tema de la seguridad informática, es necesario dar un concepto de seguridad[41], según el Diccionario de la Real Academia Española, es "cualidad de seguro" y seguro[42] se entiende que es: "libre y exento de todo peligro, daño o riesgo". Debemos recordar que en la actualidad, la información cada día tiene un rol más importante dentro de la esfera de lo público y privado, es un recurso del cual no se puede prescindir, por lo tanto, es imperativo que sea fiable, es uno de los activos más importantes de las empresas, por lo que, la seguridad de esta también tiene una importancia relevante.

El objetivo primordial de la seguridad de la información es garantizar la continuidad de la organización, minimizar el daño que puede ser causado por varios agentes que serán descritos más adelante y en caso de que esto suceda, tener los respaldos necesarios para poder regresar al estado anterior de las cosas. La información puede estar en diversos estados, como por ejemplo de forma escrita o impresa en un papel, se puede encontrar en una imagen o expuesta en una conversación, almacenada o transmitida en un medio electrónico, es decir, debemos entender que existen diversas formas en que la información se adquiere, distribuye y/o almacena.

---

[41] Diccionario de la Real Academia Española. Diccionario de la Real Academia Española. 20 de junio de 2009 <http://buscon.rae.es/drael/SrvltGUIBusUsual?TIPO_HTML=2&TIPO_BUS=3&LEMA=seguridad>

[42] Diccionario de la Real Academia Española. Diccionario de la Real Academia Española. 20 de junio de 2009 <http://buscon.rae.es/drael/SrvltGUIBusUsual?TIPO_HTML=2&TIPO_BUS=3&LEMA=seguro>

La seguridad informática: "No se trata simplemente de asegurar que los tratamientos automatizados de una máquina se efectúen correctamente, es decir, de manera fiable: se trata de asegurar que a través de esas redes que cubren el mundo entero, ninguna información, se pierda de forma voluntaria o fortuita, en dirección a terceros no autorizados, se convierta en inaccesible para sus legítimos poseedores o sea modificada"[43].

En resumen, la seguridad informática es el conjunto de sistemas y procedimientos que garantizan la confidencialidad, integridad y disponibilidad de la información, que se logra a través de implementar un sistema adecuado de controles, que va desde políticas, prácticas, procedimientos, estructuras organizacionales y funciones de software.

3.2 Justificación

Es necesario que exista seguridad en la información, en función que es un recurso importante de la empresa, marca la diferencia con respecto a otras en el tema de ventaja competitiva, rentabilidad, imagen comercial; así como mantiene el flujo de fondos y el cumplimiento de la ley y normas. Actualmente los sistemas de información están siendo amenazados de varias formas por ejemplo: espionaje, sabotaje, fraudes, vandalismo, incendios, inundaciones, daños mediante virus, denegación de servicios y a través de "hacking". Dichos sistemas de información son vulnerables dentro de la interconexión de las redes públicas y privadas, así como por el uso compartido de los recursos de información.

La seguridad informática no se logra solamente a través de medios técnicos, sino es necesario que sea respaldado a través de una gestión y

[43] DEL PESO NAVARRO, Emilio. Ley de protección de datos. La nueva LORTAD. . Madrid: Diez de Santos, 2000.

procedimientos adecuados, que deben ser efectuados por medio de una planificación minuciosa por parte de todo el personal de una institución.

3.3 Clasificación de la información:

Se utiliza como herramienta la clasificación de la información con el fin de facilitar la seguridad de los recursos y los datos, para de esta forma saber qué tipo de protección se requieren dependiendo de la información que va a ser protegida.

La propiedad de la información juega un papel importante para determinar la responsabilidad, el propietario de los datos o recursos es el responsable de su utilización y disposición, es decir, se debe identificar al responsable de los recursos y datos de los sistemas de información en las organizaciones. En esta persona recaerá la responsabilidad de la clasificación y de aprobar quiénes van a ser los usuarios autorizados y los privilegios de accesos especiales. Se puede clasificar la información por niveles, categorías o en forma combinada.

- **Niveles:** Es una clasificación jerárquica donde el nivel más bajo es no clasificado y el mayor es alto secreto. Por ejemplo, en el caso de dependencias militares, los niveles son separados por datos y usuarios.
- **Categorías:** se utiliza para grupos independientes de datos y recursos que necesitan procedimientos similares de protección, cada categoría no tiene relación ni dependencia entre ellas, se asignan a usuarios y a datos. Por ejemplo, si el usuario no tiene la misma categoría que los datos, el acceso es denegado.
- **Combinada:** Es la unión de las dos clasificaciones anteriores, siendo la más segura por su combinación.

Los criterios para clasificar la información debe ser en base al riesgo de los datos y los recursos, por ejemplo una clasificación en base a su sensibilidad seria:

a. **Destrucción:** Se entiende como borrar o no tener disponible los recursos, datos o programas, y que la información es necesaria para la continuidad del negocio. Este tipo de sensibilidad afecta a la disponibilidad de la información
b. **Modificación:** Se refiere al cambio de datos o programas, situación que puede pasar en empresas que manejan datos sensibles, y atentan contra una la integridad de los datos o programas.
c. **Difusión:** Se considera como el conocimiento que se adquiere a través de los datos obtenidos, tiene que ver con el valor de los datos y afecta a la confidencialidad.

El esquema de clasificación por niveles jerárquicos con criterio de sensibilidad a la difusión sería:

a. **Datos confidenciales:** difusión no autorizada y su uso puede suponer un importante daño a la organización
b. **Datos restringidos:** Difusión no autorizada y su utilización iría contra los intereses de la organización y/o clientes por ejemplo datos de producción, programas, software o datos del personal.
c. **Datos de uso interno:** No necesitan ningún grado de protección para la difusión por ejemplo organigramas, listados de teléfonos, etc.
d. **Datos no clasificados**: no necesitan ningún grado de protección para difusión por ejemplo informes anuales que la empresa pública.

Un dato que debe ser protegido son los de carácter personal, aquellos que puedan atentar contra la intimidad de las personas. Debemos recordar que cuando se adoptan medidas de seguridad no se debe olvidar la proporcionalidad entre los costos, medias y procedimientos de seguridad y el grado de dependencia respecto a los datos, la gravedad de los perjuicios que podría existir.

3.4 Tipos de seguridad de la información:

La referida seguridad de la información se logra a través de la implementación de un conjunto adecuado de controles, para lo cual es esencial que una organización identifique los requerimientos que tiene en cuanto a seguridad. En primer lugar, se debe evaluar los riesgos físicos a los cuales la organización es vulnerable, su probabilidad de ocurrencia y el impacto que tendría; este tipo de amenazas pueden proceder de la naturaleza o del hombre. Ejemplo: inundaciones, fuego, cortes de electricidad, robos, hurtos, entre otros, a esto se conoce como seguridad física.

Además es necesario implementar la seguridad lógica, que sirve para proteger el patrimonio informacional, es decir, las aplicaciones informáticas como el contenido de ficheros y bases de datos. Se puede realizar a través de contraseñas lógicas, biométricas, firmas digitales, utilización de criptografía y con respaldos de la información. Otro recurso a efectuar es el organizativo – administrativo, complementario seguridad física y lógica, que se entiende como los requisitos normativos, legales, reglamentarios que se realizan a través de políticas como de seguridad, personal, contratación, un análisis de riesgos y planes de contingencia.

Por último, contamos con el recurso jurídico, el cual se entiende como la aprobación de normas legales, un marco jurídico para proteger los bienes informáticos, por ejemplo la Ley de protección de datos, Ley de Propiedad Intelectual, Código Penal, etc.

3.5 Características de la seguridad de la información

Lo que se busca a través de la implementación de estas seguridades es que la información cumpla con las siguientes características:

a. **Confidencialidad:** Garantizar que la información es conocida de forma exclusiva por los usuarios autorizados en forma y tiempo que ha sido determinado.
b. **Integridad:** La información sea creada, modificada o borrada sólo por los usuarios autorizados; se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
c. **Disponibilidad:** La información se pueda utilizar cuándo y cómo lo requieran los usuarios autorizados.
d. **Autenticación:** Se acredite que el remitente del mensaje es quien dice ser y no otra persona.
e. **No repudio:** Tanto de origen como de destino, esto es que no se pueda alegar que el remitente o destinatario puedan alegar que no se envió o recibió determinado dato.
f. **Control de accesos:** para limitar que los usuarios que no se encuentran autorizados accedan a los recursos telemáticos.

3.6 La seguridad informática y el derecho

El objetivo que se busca es impedir que se den infracciones y violaciones de las leyes, así como de obligaciones establecidas en los estatutos o normas y reglamentos de la empresa, para ello los controles desde el puto de vista legal comprenden los siguientes:

a. **La protección de datos y la confidencialidad de la información personal:** Con la actual tendencia en cuanto a la Internet y las tecnologías de la información y comunicación (Tics), varios países han incluido leyes dentro de sus ordenamientos jurídicos con el fin de controlar el procesamiento y transmisión de datos personales, esto

motivado para imponer responsabilidades a las personas que recopilan, procesan y divulgan información personal almacenada en bases de datos.

Por ello que se debe designar un responsable de la protección de datos, para que oriente a cualquier persona detentora de datos personales de sus responsabilidades individuales y de los procedimientos específicos.

b. **Protección de registros y documentos de la organización:** Existen registros que son importantes para la organización, los cuales deben ser protegidos contra la pérdida, destrucción y falsificación. Algunos por ejemplo tienen como objetivo 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:** Es necesario que se implemente procedimientos que garanticen la propiedad intelectual, propiedad industrial y 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 en el comercio electrónico:** Debemos entender que el comercio electrónico abarca el intercambio electrónico de datos, el correo electrónico y las transacciones en línea a través de Internet; es aquí donde se puede ser vulnerable a diversas amenazas, por lo que es necesario que se apliquen controles. Entre las consideraciones más importantes tenemos:

a. **Autentificaciones:** Estamos hablando de la identidad de las partes, tanto del comerciante como del cliente, ya que debe existir una confianza recíproca para poder realizar el negocio.
b. **Autorización:** Se debe designar una persona para fijar precios, emitir o firmar documentos.
c. **Procesos de oferta y contratación:** Debe existir protocolos para la confidencialidad, integridad y prueba de envío y recepción de documentos claves, con el fin de que no exista repudio de contratos.
d. **Información sobre fijación de precios:** Esto tiene que ver con la seguridad sobre la información, es decir, el nivel de confianza ante el listado de precios publicados y en los descuentos
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:** Se necesita verificar que la información de pago que suministra el cliente es la correcta e irrefutable.
g. **Cierre de la transacción:** Se debe establecer la forma de pago que sea 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 se puede resolver con técnicas criptográficas como las que veremos a continuación:

1. **Política de utilizar controles criptográficos:** El objetivo de la política es maximizar beneficios y minimizar los riesgos que ocasiona el uso de técnicas criptográficas, evitar 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. Lo que se hace es evaluar 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 cuento 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, por ejemplo 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. La firma electrónica dependiendo la legislación del país puede ser legalmente vinculante.
4. **Servicios de no repudio:** Este se utiliza cuando se necesita resolver una disputa en cuanto a si un evento o acción ocurrió o no, es el caso 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. 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.

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.

3.7 El phishing:

El problema se desprende por el ingreso de datos, en páginas verdaderas o replicas falsificadas con el fin de causar un perjuicio; el nombre de este delito es *phishing*, que tiene como fin perjudicar a las personas incautas que no se dan cuenta de su falsedad. El perjuicio en si se produce porque se pide ingresar ciertos datos de carácter crediticio o personal, incluyendo claves para realizar transferencias electrónicas.

El *phishing* es una nueva forma de delito que se ha creado, se puede clasificar dentro de las estafa ya que se comete utilizando la ingeniería social, que tiene con fin intentar conseguir información confidencial de una persona de forma fraudulenta, por ejemplo al querer conocer una contraseña o información detallada sobre cuentas bancarias.

Para ejemplificar lo que sucede con el *phishing* podemos traer a colación el caso de suplantación de página que últimamente ha sufrido el Grupo Financiero Produbanco: Nos llega a nuestro correo electrónico la información que necesitamos actualizar nuestros datos personales de una cuenta; correo electrónico que se envía aleatoriamente a un conglomerado, el texto es el siguiente: (Anexo 1)

"SOLO PARA CLIENTES DEL PRODUBANCO

Estimado cliente del Produbanco:

Produbanco siempre a hecho todo lo posible para 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 cuenta estos 3 puntos importantes:

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

Además próximamente 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 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_personas/login.asp?yes=empresas

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

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 casi igual, la página verdadera para hacer este tipo de transacciones es: www.produbanco.com/GFPNetseguro

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 (anexo 3), se 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 4).

3.8 Las redes sociales

Las redes sociales son un nuevo tipo de organización que se encuentra en auge y tienen un impacto inimaginable en cuanto a las personas que buscan hacer amigos y por ello, comparten información personal. Su evolución comenzó desde un simple servicio de acceso a la red ofrecido por alguna entidad, hasta el momento de 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. Sin embargo, en estas redes existen problemas relativos al manejo indebido de los datos y casos de suplantación de identidad. Todas estas páginas, por ejemplo tienen 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 varios datos recabados, algunos los que denominamos datos públicos, es decir, los que se revelan de forma consiente como 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 según nos dice el sitio web de Wikipedia[44] 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 (…)". Sin embargo, vale la pena anunciar que es posible desactivar esta función.

Estos servicios de redes sociales nos explican que la información que ha sido publicada esta bajo la responsabilidad del usuario, por lo que, estos servicios no garantizan que dicha información sea vista exclusivamente por personas que nosotros autorizamos, situación que se puede dar por ejemplo cuando se violan las condiciones de seguridad de la contraseña de inicio de sesión. En el momento que exista una de estas violaciones deben ser informadas

[44] Wikipedia. «Wikipedia.» www.wikipedia.org. 1 de septiembre de 2009 <http://es.wikipedia.org/wiki/Cookie>.

inmediatamente al administrador del servicio para que se pueda tomar las acciones correspondientes.

En cuanto a información confidencial como contraseñas y números de tarjeta de crédito, esta es encriptada conforme a protocolos establecidos, sin embargo, se solicita que mediante correos electrónicos y servicios de mensajería no se envíe información privada.

Los contenidos que subimos a estos servicios, como en *Facebook*, está protegido por los derechos de propiedad intelectual, y por adhesión debemos sujetarnos a sus condiciones de uso y a su política de privacidad, es decir, conforme el texto que se encuentra en el sitio web [45] 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.

Como expresa Pablo Fernández Burgueño[46] 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

[45] Facebook. facebook.com. 1 de septiembre de 2009 http://www.facebook.com/terms.php>.

[46] 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>.

- 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 esta 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 5.

3.9 El Caso de Google y los datos personales

Google Inc., se ha convertido en una de las empresas con mayor presencia en el Internet, gracias a todos los servicios que presta, como por ejemplo correo electrónico, buscador, mapas, navegador web, blog de notas, directorio, calendario, entre otros. Sin embargo, justamente al tener tantos servicios, maneja varios datos de sus usuarios sobretodo información personal; que según su política de privacidad[47] se divide dicha información recopilada en diferentes niveles, a continuación hablaremos de los mas importantes:

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

a. Información proporcionada por uno mismo al momento de registrarse en los servicios de Google, estos datos puede ser 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 encriptada por seguridad.
b. *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.
c. Información de registro: Datos que se incluye son la dirección IP, el idioma, el tipo de navegador entre otras.
d. 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
e. 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 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 de el consentimiento. Ante lo cual se puede manifestar la oposición y Google esta en la obligación de no recopilar ni utilizar dicha información.

Uno de los problemas que se destacan en la web, son los datos personales que se registran en los buscadores como Google, en muchos casos, 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 el 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 (…)"[48]

A criterio de Joaquín Muñoz[49], dentro de su blog, en estos casos lo que podríamos hacer es solicitar el bloqueo de estas publicaciones, siempre y cuando la información no sea un de interés general, hecho noticioso, y exista como motivo el respeto a la dignidad o el derecho al honor entre

[48]Mourguiart, Marcel. CHW. 1 de septiembre de 2009 <http://www.chw.net/2009/05/google-sentenciado-a-eliminar-datos-personales/>.
[49] 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/>.

otros. A través de una herramienta para webmasters que se encuentra en un de los módulos de Google[50], es posible eliminar paginas web obsoletas, inexistentes, eliminar información o imagines e informar sobre un contenido inapropiado que aparezca en el buscador.

3.10 El secreto de las comunicaciones

Este es un tema que desde muchos años atrás el hombre ha discutido, es así que una de las pretensiones que siempre ha existido es el conocer el contenido de las comunicaciones de otra persona. Es por ello que 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 (…)"[51]; en el mismo sentido el artículo diez y siete del Pacto Internacional de Derechos Civiles y Políticos protege este derecho.

Según Jiménez Campo dentro del texto de Rebollo Delgado[52], se entiende a la comunicación que "es 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". Esto se entiende 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 la Internet o el teléfono.

---

[50] 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>.

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

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

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.

3.11 Legislación internacional respecto al tema:

La protección de datos debe ser considerada como una garantía, los derechos de privacidad e intimidad a nivel de instrumentos internacionales están expresados en varios documentos, sin embargo hemos priorizado los más relevantes para el presente estudio:[53]

- Declaración Universal de los Derechos Humanos de 1948, que establece la protección en contra de la injerencia arbitraria en la vida privada de las personas conforme el artículo doce, y el derecho a la libertad de opinión y expresión según el artículo diez y nueve
- Dentro de la Declaración sobre la utilización del progreso científico y tecnológico en interés de la paz y en beneficio de la humanidad[54] proclamado en 1975, dentro de la proclamación sexta dice: Todos los Estados adoptarán medidas tendientes a extender a todos los estratos de la población los beneficios de la ciencia y la tecnología y a protegerlos, (…) de las posibles consecuencias negativas del uso indebido del progreso científico y tecnológico, incluso su utilización indebida para infringir los derechos del individuo o del grupo, en particular en relación con el respeto de la vida privada y la protección de la persona humana y su integridad física e intelectual.

[53]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

[54] Asamblea General de las Naciones Unidas. «Oficina del Alto Comisionado para los Derechos Humanos.» 10 de noviembre de 1975. www.unhchr.ch. 18 de junio de 2009 < http://www.unhchr.ch/spanish/html/menu3/b/70_sp.htm >.

- Dentro de la convención sobre los Derechos del Niño[55] de 1989 en el artículo diez y seis numeral primero expresa que: Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y a su reputación.
- La Convención Americana sobre Derechos Humanos[56] - Pacto de San José de Costa Rica de 1969 contiene varias normas respecto al tema tratado, sin embargo el artículo once sobre la protección de la honra y de la dignidad, numeral dos expresa: Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación; y el numeral tres que dice: toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.
- Directrices de la Organización de Cooperación y Desarrollo Económico OCDE para la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales de 1980[57]: "Las directrices de privacidad suponen la unanimidad internacional sobre las guías generales para la recogida y gestión de información personal. Los principios establecidos en las directrices de privacidad se caracterizan por su claridad y flexibilidad de aplicación, y por su formulación, que es lo suficientemente general para permitir su adaptación a los cambios tecnológicos. Los principios abarcan todos los medios del procesamiento informático de datos sobre individuos (desde computadoras locales a redes con complejas ramificaciones nacionales e internacionales), todos los tipos de procesamiento de datos personales (desde la administración de personal hasta la compilación de perfiles de consumidores) y todas las categorías de datos (desde datos de tráfico hasta datos de contenidos, desde el

[55] Asamblea General de las Naciones Unidas. «Alto Comisionado para los Derechos Humanos.» 20 de noviembre de 1989. www.unhchr.ch. 18 de junio de 2009 <http://www.unhchr.ch/spanish/html/menu3/b/k2crc_sp.htm>.

[56] Asamblea General de la Organizacion Interamericana de Derechos Humanos. «Organización de Estados Americanos.» 7 al 22 de noviembre de 1969. www.oas.org. 18 de junio de 2009 <http://www.oas.org/Juridico/spanish/tratados/b-32.html>.

[57] Resumen Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales http://www.oecd.org/dataoecd/16/51/15590267.pdf

más trivial al más delicado). Los principios se pueden aplicar en los ámbitos nacional e internacional. A lo largo de los años se han utilizado en gran número de instrumentos de regulación nacional o de autorregulación y todavía se usan ampliamente en los sectores público y privado."

- La Directiva 95/46/CE[58] del Parlamento Europeo es el texto de referencia en materia de protección de datos personales para Europa. Crea el marco regulador destinado a establecer un equilibrio entre la protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea. En esta se fija límites estrictos para recoger y utilizar los datos personales y solicita la creación de un organismo nacional independiente encargado de la protección de los mencionados datos.

  Se aplica en los datos que se encuentran en medios automatizados o los contenidos en ficheros no automatizados. El objetivo que busca esta directiva es proteger los derechos y las libertades de las personas en lo que respecta al tratamiento de datos personales, estableciendo principios de orientación para determinar la licitud de dicho tratamiento. Dichos principios se refieren a:

  - **La calidad de los datos:** los datos personales serán tratados de manera leal y lícita, y recogidos con fines determinados, explícitos y legítimos. Deben ser exactos y, en caso de ser necesario, actualizados.
  - **La legitimación del tratamiento**: Debe existir el consentimiento del titular de los datos o si el tratamiento es necesario para: a. ejecutar un contrato en el que el interesado es parte, b. para el cumplimiento de una obligación jurídica a la que este sujeto el responsable del tratamiento, c. para proteger el interés vital del interesado, d. para el cumplimiento de una misión de interés público, e. la satisfacción del interés legítimo perseguido por el responsable del tratamiento.

[58]Unión Europea. «Europa - Sintesis de la Legislación de la UE.» 1995. www.europa.eu. 13 de mayo de 2009 <http://europa.eu/legislation_summaries/information_society/l14012_es.htm>.

- **Categorías:** Se deberá prohibir el tratamiento de datos personales que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas y pertenencia a sindicatos, así como datos relativos a la salud o vida sexual. Salvo en el caso de que sean necesarios para salvaguardar el interés vital del interesado o para la prevención o el diagnóstico médico.
- **Información:** el responsable del tratamiento deberá facilitar información por ejemplo identidad del responsable del tratamiento, fines del tratamiento, destinatarios de los datos, entre otros, a la persona de quien se recaben los datos.
- **Derecho de acceso:** Todos los interesados deberán tener el derecho a:
    - Obtener la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen y la comunicación de los datos objeto de los tratamientos;
    - La rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos, así como la notificación a los terceros a quienes se hayan comunicado los datos de dichas modificaciones.
- **Excepciones y limitaciones**: se podrá limitar el alcance de los principios relativos a la calidad de los datos, la información del interesado, el derecho de acceso y publicidad de los tratamientos con objeto de salvaguardar la seguridad del Estado, la defensa, la seguridad pública, la represión de infracciones penales, un interés económico y financiero importante de un Estado miembro o de la UE o la protección del interesado.
- **Derecho del interesado a oponerse al tratamiento:** el interesado deberá tener derecho a oponerse, a que los datos que le conciernen sean objeto de tratamiento. Deberá ser informado antes de que los datos se comuniquen a terceros a efectos de prospección y tendrá derecho a oponerse a dicha comunicación.

- **Confidencialidad y seguridad del tratamiento**: las personas que actúen bajo la autoridad del responsable o del encargado del tratamiento, sólo podrán tratar datos personales a los que tengan acceso. Se debe aplicar las medidas adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental, la alteración, la difusión o el acceso no autorizados.
- **Notificación del tratamiento a la autoridad de control**: el responsable efectuará una notificación a la autoridad de control con anterioridad a la realización de un tratamiento.

Además prevé que las legislaciones nacionales deben tener un recurso para el caso de que el responsable del tratamiento de datos no respete los derechos de los interesados; las personas que sufran un perjuicio tendrán derecho a obtener la reparación del perjuicio sufrido.

CONCLUSIONES:

Con esta monografía se ha efectuado un análisis jurídico del impacto de las TICS, profundizando en la materia de los datos personales; y, los preceptos constitucionales sobre la intimidad y privacidad, como potestades inherentes a los seres humanos. Además de los mecanismos legales, judiciales y técnicos existentes para proteger estos derechos. La evolución tecnológica en la que vivimos ha producido un desarrollo total en cuanto a las formas de intercambio o transacciones mercantiles de bienes y servicios, revolucionando el comercio, y a su vez la forma de conseguir información sobre la necesidad de los potenciales consumidores, creando de esta manera recolectores de datos, con el fin de conocer gustos y necesidades de las personas. Sin embargo, los buscadores de información pueden vulnerar la confidencialidad de los seres humanos, y el derecho a la intimidad y privacidad, ambos requisitos fundamentales para vivir en una sociedad libre.

Actualmente es difícil limitar la creación de perfiles dentro de la red, en base de la información que ingresamos a los navegadores; por lo cual, se hace necesario procurar la protección de esta información sensible minimizando los efectos que se pueden producir, por medio de una adecuada normativa que limite las solicitudes inescrupulosas que vulneran nuestras garantías constitucionales. Del mismo modo, el derecho a la intimidad a través de los tiempos ha evolucionado, pasando por el derecho a ser dejado solo, representando una de las libertades individuales más importantes que tenemos y que actualmente se refleja en el derecho al control sobre nuestros datos que se encuentran en diferentes soportes, tanto lógicos como físicos. 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 ello, que dentro de un estado constitucional de derechos y justicia ciertamente la subsunción normativa desaparece, obligándose a ponderar los preceptos constitucionales; para garantizar lo establecido en el artículo 66 numeral 20 "el derecho a la intimidad personal y familiar", situación que no genera discusión ni malestar. Desarrollar de este precepto, a fin de responder a su espíritu y tenor, es necesario, ya que la normativa inferior debe generar mecanismos objetivos para garantizarlo, en aras de alcanzar tanto para administradores como administrados elementos ciertos, que den oportunamente protección a tan trascendental materia y aseguren certidumbre, es decir, seguridad jurídica.

Como preámbulo de esta necesidad, la ley de comercio electrónico, firmas electrónicas y mensajes de datos, 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, existe las necesidad de completar con una regulación expresa, la normativa existente, desarrollando y completando la protección de datos personales; así como, para tener derecho a que sean actualizados, aclarados, modificados o borrados conforme el caso. En cuanto al habeas data, este 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.

Una vez que se cree todo un sistema jurídico de ser el caso, se deberá crear una autoridad que regule el uso de las bases de datos, como existe en otros países, por ejemplo la Agencia Española de Protección de Datos, ente publico autónomo cuya finalidad es velar por el cumplimento de la legislación en cuanto as esta materia. Colocar a tan delicada materias en

instituciones que responden a intereses políticos o de otra índole, seria debilitar y desconocer el espiritu de la norma constitucional. La institución que administre datos personales debe poseer autonomía administrativa y financiera, con lo cual blindamos la posibilidad de manejos ajenos a la técnica y registre con elementos esenciales como imparcialidad, celeridad, oportunidad, acceso físico y electrónico, entre otros.

Por ejemplo, en el caso de España, la Agencia tiene como deber velar por el cumplimiento de la legislación vigente en cuanto as los derechos de información, acceso, rectificación, oposición y cancelación de datos. Mantener a una entidad creada ara el efecto dentro del manejo técnico, es fundamental para garantizar a todos y todas una efectiva administración de datos personales.

REFERENCIAS:

GLOSARIO:

- **Ingeniería social**[59]: 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**[60]: 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 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.

[59] Wikipedia. «Wikipedia.» www.wikipedia.org. 21 de junio de 2009 <http://es.wikipedia.org/wiki/Ingeniería_social_(seguridad_informática)>.
[60] Wikipedia. «Wikipedia.» www.wikipedia.org. 20 de junio de 2009 <http://es.wikipedia.org/wiki/Algoritmo_de_cifrado>.

- 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>.
- Asamblea General de la Organizacion Interamericana de Derechos Humanos. «Organización de Estados Americanos.» 7 al 22 de noviembre de 1969. www.oas.org. 18 de junio de 2009 <http://www.oas.org/Juridico/spanish/tratados/b-32.html>.
- Asamblea General de las Naciones Unidas. «Alto Comisionado para los Derechos Humanos.» 20 de noviembre de 1989. www.unhchr.ch. 18 de junio de 2009 <http://www.unhchr.ch/spanish/html/menu3/b/k2crc_sp.htm>.
- —. «Oficina del Alto Comisionado para los Derechos Humanos.» 10 de noviembre de 1975. www.unhchr.ch. 18 de junio de 2009 < http://www.unhchr.ch/spanish/html/menu3/b/70_sp.htm>.
- Asamblea Nacional Constituyente. «Asamblea Nacional.» 26 de julio de 2008. www.asambleanacional.gov.ec. 21 de junio de 2009 <http://www.asambleanacional.gov.ec/documentos-asamblea-nacional/constituciones/constitucion-de-2008/constitucion-2008.pdf>.
- 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 >.
- Castro Fernandez, Juan Diego. «El Habeas Data en Costa Rica.» Informática y Derecho 5. Mérida: Aranzadi, 1994. 1313 - 1318.

- 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>.
- Congreso Nacional del Ecuador. Conatel. 20 de junio de 2009 <http://www.conatel.gov.ec/site_conatel/index.php?option=com_docman&task=doc_download&gid=1774&Itemid=>.
- —. Conatel. 20 de junio de 2009 <http://www.conatel.gov.ec/site_conatel/index.php?option=com_docman&task=doc_download&gid=1775&Itemid=>.
- —. Conatel. 21 de junio de 2009 <http://www.conatel.gov.ec/site_conatel/index.php?option=com_docman&task=doc_download&gid=1776&Itemid>.
- —. Lexis. 20 de junio de 2009 <http://www.lexis.com.ec/lexis/novedadesDescargas/CodigosLeyes/CODIGO%20DE%20PROCEDIMIENTO%20PENAL.htm>.
- —. Superintendencia de Bancos del Ecuador. 20 de junio de 2009 <http://www.superban.gov.ec/medios/PORTALDOCS/downloads/normativa/Ley_gral_inst_sist_financiero_ene_2009.pdf>.
- —. Tribunal Constitucional. 20 de junio de 2009 <http://www.tribunalconstitucional.gov.ec/documentos/Ley%20de%20Control%20Constitucional.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 junio de 2009 <http://buscon.rae.es/draeI/SrvltGUIBusUsual?TIPO_HTML=2&TIPO_BUS=3&LEMA=dato>.
- Elías, Miguel Sumer. «Alfa-redi.» 21 de junio de 2009 <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>.
- Maxi. «Comisión de Transparecnia y acceso a la Información del EStado de Nuevo León.» www.ctainl.org.mx. 21 de junio de 2009

<http://www.ctainl.org.mx/revista_8/elementos/fundamentojuridicopd.pdf>.

- 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/>.
- OCDE. «OCDE.» www.oecd.org. 20 de junio de 2009 <http://www.oecd.org/dataoecd/16/51/15590267.pdf>.
- Organización de las Naciones Unidas. «Naciones Unidas.» 21 de junio de 2009 <http://www.un.org/es/documents/udhr/>.
- Pierini, Alicia, Valentín Lorences y María Ines Tornabene. Hábeas Data. Buenos Aires: Editorial Universidad, 1999.
- Presidencia de la República del Ecuador. Asamblea Nacional. junio de 2009. 21 de junio de 2009 <http://www.asambleanacional.gov.ec/index.php?option=com_docman&task=doc_download&gid=544&Itemid=188>.
- Rebollo Delgado, Lucrecio. Derechos Fundamentales y Protección de Datos. Madrid: Dykinson, S.L., 2004.
- Registro Oficial. Derecho Ecuador. 20 de junio de 2009 <http://www.derechoecuador.com/index.php?option=com_content&task=view&id=4874&Itemid=526>.
- 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>.

- Unión Europea. «Europa - Sintesis de la Legislación de la UE.» 1995. www.europa.eu. 13 de mayo de 2009 <http://europa.eu/legislation_summaries/information_society/l14012_es.htm>.
- 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: Textos completos de leyes referidas

Constitución Política de la República de Ecuador

TÍTULO II
DERECHOS
Capítulo sexto
Derechos de libertad

Art. 66.- Se reconoce y garantizará a las personas:
19. 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.
20. El derecho a la intimidad personal y familiar.

TÍTULO III
GARANTÍAS CONSTITUCIONALES
Capítulo tercero
Garantías jurisdiccionales
Sección quinta
Acción de hábeas data
Art. 92 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 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, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.

Constitución Política de la República de Ecuador de 1998

CAPITULO 2 DE LOS DERECHOS CIVILES
TITULO III
DE LOS DERECHOS, GARANTIAS Y DEBERES
Art. 23.- 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.

21. El derecho a guardar reserva sobre sus convicciones políticas y religiosas. Nadie podrá ser obligado a declarar sobre ellas. En ningún caso se podrá

utilizar la información personal de terceros sobre sus creencias religiosas y filiación política, ni sobre datos referentes a salud y vida sexual, salvo para satisfacer necesidades de atención médica.

TITULO III

DE LOS DERECHOS, GARANTIAS Y DEBERES

CAPITULO 6 DE LAS GARANTIAS DE LOS DERECHOS

Sección segunda

Del hábeas data

Art. 94.- Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito.

Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos.
Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización.

La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional.

TÍTULO XIII

DE LA SUPREMACÍA, DEL CONTROL Y DE LA REFORMA DE LA CONSTITUCIÓN

CAPITULO 2

Del Tribunal Constitucional

Art. 276.- Competerá al Tribunal Constitucional:

Conocer y resolver las demandas de inconstitucionalidad, de fondo o de forma, que se presenten sobre leyes orgánicas y ordinarias, decretos-leyes,

decretos, ordenanzas; estatutos, reglamentos y resoluciones, emitidos por órganos de las instituciones del Estado, y suspender total o parcialmente sus efectos.

Conocer y resolver sobre la inconstitucionalidad de los actos administrativos de toda autoridad pública. La declaratoria de inconstitucionalidad conlleva la revocatoria del acto, sin perjuicio de que el órgano administrativo adopte las medidas necesarias para preservar el respeto a las normas constitucionales.

Conocer las resoluciones que denieguen el hábeas corpus, el hábeas data y el amparo, y los casos de apelación previstos en la acción de amparo.
Dictaminar sobre las objeciones de inconstitucionalidad que haya hecho el Presidente de la República, en el proceso de formación de las leyes.

Dictaminar de conformidad con la Constitución, tratados o convenios internacionales previo a su aprobación por el Congreso Nacional.

Dirimir conflictos de competencia o de atribuciones asignadas por la Constitución.

Ejercer las demás atribuciones que le confieran la Constitución y las leyes.
Las providencias de la Función Judicial no serán susceptibles de control por parte del Tribunal Constitucional.

Ley de Control Constitucional - artículos 34 al 45

TITULO II
DE LAS GARANTIAS DE LOS DERECHOS DE LAS PERSONAS
CAPITULO II
DEL HABEAS DATA

Art. 34.- Las personas naturales o jurídicas, nacionales o extranjeras, que deseen tener acceso a documentos, bancos de datos e informes que sobre sí mismas o sus bienes están en poder de entidades públicas, de personas naturales o jurídicas privadas, así como conocer el uso y finalidad que se les haya dado o se les esté por dar, podrán interponer el recurso de hábeas data para requerir las respuestas y exigir el cumplimiento de las medidas tutelares prescritas en esta Ley, por parte de las personas que posean tales datos o informaciones.

Art. 35.- El hábeas data tendrá por objeto:

1. Obtener del poseedor de la información que éste la proporcione al recurrente, en forma completa, clara y verídica,
2. Obtener el acceso directo a la información;
3. Obtener de la persona que posee la información que la rectifique, elimine o no la divulgue a terceros; y,
4. Obtener certificaciones o verificaciones sobre que la persona poseedora de la información la ha rectificado, eliminado, o no la ha divulgado.

Art. 36.- No es aplicable el hábeas data cuando afecte al sigilo profesional; o cuando pueda obstruir la acción de la justicia; o cuando los documentos que se soliciten tengan el carácter de reservados por razones de Seguridad Nacional.

No podrá solicitarse la eliminación de datos o informaciones cuando por disposición de la Ley deben mantenerse en archivo o registros públicos o privados.

Art. 37.- La acción de hábeas data deberá interponerse ante cualquier juez o tribunal de primera instancia del domicilio del poseedor de la información o datos requeridos. Los jueces o magistrados, evocarán conocimiento de inmediato, sin que exista causa alguna que justifique su inhibición, salvo

cuando entre estos y el peticionario existan incompatibilidades de parentesco u otros señalados en la Ley.

Art. 38.- El juez o tribunal en el día hábil siguiente al de la presentación de la demanda convocará a las partes a audiencia, que se realizará dentro de un plazo, de ocho días, diligencia de la cual se dejará constancia escrita.

La respectiva resolución deberá dictarse en el término máximo de dos días, contados desde la fecha en que tuvo lugar la audiencia, aún si el demandado no asistiere a ella.

Art. 39.- Declarado con lugar el recurso, las entidades o personas requeridas entregarán, dentro del plazo de ocho días toda la información y, bajo juramento, una explicación detallada que incluya por lo menos, lo siguiente:

1. Las razones y fundamentos legales que amparen la información recopilada;
2. La fecha desde la cual tienen esa información;
3. El uso dado y el que se pretenderá dar a ella,
4. Las personas o entidades a quienes se les haya suministrado los referidos datos, la fecha del suministro y las razones para hacerlo;
5. El tipo de tecnología que se utiliza para almacenar la información; y,
6. Las medidas de seguridad aplicadas para precautelar dicha información.

Art. 40.- De considerarse insuficiente la respuesta, podrá solicitarse al juez que disponga la verificación directa, para la cual, se facilitara el acceso del interesado a las fuentes de información, proveyéndose el asesoramiento de peritos si así se solicitare.

Art. 41.- Si de la información obtenida el interesado considera que uno o más datos deben ser eliminados, rectificados, o no darse a conocer a terceros, pedirá al juez que ordene al poseedor de la información que así proceda.

El juez ordenará tales medidas, salvo cuando claramente se establezca que la información no puede afectar el honor, la buena reputación, la intimidad o irrogar daño moral al solicitante.

El depositario de la información dará estricto cumplimiento a lo ordenado por el juez, lo cual certificará bajo juramento, sin perjuicio de que ello se verifique por parte del propio interesado, solo o acompañado de peritos, previa autorización del juez del trámite.

La resolución que niegue el hábeas data, será susceptible de apelación ante el Tribunal Constitucional, en el término de ocho días a partir de la notificación de la misma.

Art. 42.- Los representantes legales de las personas jurídicas de derecho privado o las naturales que incumplieren las resoluciones expedidas por jueces o Tribunales que concedan el hábeas data, no podrán ejercer ni directa ni indirectamente, las actividades que venían desarrollando y que dieron lugar al hábeas data, por el lapso de un año.

Esta disposición será comunicada a los órganos de control y demás entidades públicas y privadas que sean del caso.

Art. 43.- Los funcionarios públicos de libre remoción que se nieguen a cumplir con las resoluciones que expidan los jueces o tribunales dentro del procedimiento de hábeas data serán destituidos inmediatamente de su cargo o empleo, sin más trámite, por el respectivo juez o tribunal, salvo cuando se trate de los funcionarios elegidos por el Congreso Nacional, quienes deberán ser destituidos por éste, a pedido fundamentado del juez o tribunal y previo el correspondiente juicio político.

La sanción de destitución se comunicará inmediatamente a la Contraloría General del Estado y a la autoridad nominadora correspondiente.

Art. 44.- Las sanciones antes señaladas se impondrán sin perjuicio de las respectivas responsabilidades civiles y penales a que hubiere lugar.

Art. 45.- Están legitimados para iniciar y continuar los procedimientos previstos en esta sección, no solo las personas natural o jurídico que consideren tener derecho a ello, sino también los padres, tutores y curadores en nombre de sus representados.

Proyecto de Ley de Garantías y Control Constitucional: Artículos 49 al 51

Capítulo VI

Acción de hábeas data

Artículo 49.- Objeto: La acción de hábeas data tiene por objeto garantizar judicialmente a toda persona el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre si misma, o sobres sus bienes, estén en poder de entidades públicas o de personas naturales o jurídicas privadas, en soporte material o electrónico. Así mismo, toda persona tiene derecho a conocer el uso que se haga a dicha información, su finalidad, el origen y destino de la misma y el tiempo de vigencia del archivo o banco de datos.

El titular de los datos podrá solicitar al responsable del archivo o banco de datos, el acceso sin costo a la información antes referida, así como la actualización de los datos, su rectificación, eliminación o anulación. No podrá solicitarse la eliminación de datos personales que por disposición de la Ley deben mantenerse en archivos públicos.

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

Artículo 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, salvo cuando exista orden de jueza o juez competente.

Artículo 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.

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

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.

Reglamento general a la Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos.

Art. 21.- De la seguridad en la prestación de servicios electrónicos.- La prestación de servicios electrónicos que impliquen el envío por parte del usuario de información personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de prestación de dichos servicio. Es obligación de quien presta los servicios, informar en detalle a los usuarios sobre el tipo de seguridad que utiliza, sus alcances y limitaciones, así como sobre los requisitos de seguridad exigidos legalmente y si el sistema puesto a disposición del usuario cumple con los mismo. En caso de no contar con seguridades se deberá informar a los usuarios de este hecho en forma clara y anticipada previo el acceso a los sistemas o a la información e instruir claramente sobre los posibles riesgos en que puede incurrir pro al falta de dichas seguridades.

Se consideran datos sensibles del consumidor sus datos personales, información financiera de cualquier tipo como números de tarjetas de crédito, o similares que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten.

Por el incumplimiento de las disposiciones contenidas en el presente artículo o por falta de veracidad o exactitud en la información sobre seguridades, certificaciones o mecanismos para garantizar la confiabilidad de las transacciones o intercambio de datos ofrecida al consumidor o usuario, el

organismo de control podrá exigir al proveedor de los servicios electrónicos la rectificación necesaria y en caso de reiterarse el incumplimiento o la publicación de información falsa o inexacta, podrá ordenar la suspensión del acceso al sitio con la dirección electrónica del proveedor de servicios electrónicos mientras se mantengan dichas condiciones.

Código Orgánico de la Función Judicial

Art. 13.- PRINCIPIO DE PUBLICIDAD.- Las actuaciones o diligencias judiciales serán públicas, salvo los casos en que la ley prescriba que sean reservadas. De acuerdo a las circunstancias de cada causa, los miembros de los tribunales colegiados podrán decidir que las deliberaciones para la adopción de resoluciones se lleven a cabo privadamente.

No podrán realizase grabaciones en video de las actuaciones judiciales.

Se prohíbe a las juezas y a los jueces dar trámite a informaciones sumarias o diligencias previas que atenten a la honra y dignidad de las personas o a su intimidad.

Ley Especial de Telecomunicaciones (Ley Nro. 184) - Artículo 14

CAPITULO I
Disposiciones Fundamentales

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.

Código de Procedimiento Penal - Artículo 69 numeral 6

TITULO III
LOS SUJETOS PROCESALES
CAPITULO II
EL OFENDIDO

Art. 69.- Derechos del ofendido.- El ofendido tiene derecho:

6. A que se proteja su persona y su intimidad, y a exigir que la policía, el Fiscal, el juez y el tribunal adopten para ello los arbitrios necesarios, sin menoscabo de los derechos del imputado;

Ley General de Instituciones del Sistema Financiero - artículos 88 a 94

TITULO VIII
DE LA INFORMACION
CAPITULO III
SIGILO Y RESERVA BANCARIA

Art. 88. - Los depósitos y demás captaciones de cualquier índole que se realicen en las instituciones del sistema financiero, estarán sujetos a sigilo bancario, por lo cual las instituciones financieras receptoras de los depósitos y captaciones, sus administradores, funcionarios y empleados no podrán proporcionar información relativa a dichas operaciones sino a su titular o a quien lo represente legalmente.

Las instituciones del sistema financiero con el objeto de facilitar procesos de conciliación, darán acceso al conocimiento detallado de las operaciones anteriores y sus antecedentes a la firma de auditoría externa contratada por la institución, que también quedará sometida al sigilo bancario.

Las instituciones del sistema financiero podrán dar a conocer las operaciones anteriores, en términos globales, no personalizados ni parcializados, solo para fines estadísticos o de información.

Podrán también proporcionar información general respecto del comportamiento de clientes en particular, para fines de evaluación' de crédito a requerimiento de otra institución del sistema financiero o de establecimientos comerciales autorizados por aquellos, sin que ello implique la facultad de revelar transacciones individualizadas.

Art. 89. - Las instituciones del sistema financiero están obligadas a mantener sistemas de control interno que permitan una adecuada identificación de las personas que efectúan transacciones con la institución.

Asimismo, tendrán la obligación de proporcionar a la Superintendencia la información sobre las operaciones que determinadas por ésta, por su naturaleza y monto, requieran de un informe especial. La Superintendencia proporcionará esta información a otras autoridades que por disposición legal expresa, previa determinación sobre su causa y fines, puedan requerirla, quienes también estarán sujetas al sigilo bancario hasta que se utilice la información en los fines para los cuales se la requirió. Tratándose de operaciones de cambio de moneda extranjera o de cualquier mecanismo de captación en moneda nacional o extranjera, en los montos que determine la Superintendencia, ésta establecerá los requisitos que permitan investigar el origen y procedencia de los recursos.

Art. 90. - Los informes de inspección y análisis que emitan los funcionarios y empleados de la Superintendencia, en el ejercicio de las funciones de control y vigilancia, serán escritos y reservados. La Superintendencia, de creerlo del caso y de haber observaciones, los trasladará a conocimiento de las autoridades correspondientes de la institución examinada. Estos informes no se divulgarán a terceros, en todo ni en parte, por la Superintendencia, ni por la institución examinada, ni por ninguna persona

que actúe por ellos, salvo el caso previsto en el artículo 93 de esta ley o, cuando se trate de auditorías integrales dispuestas por la Junta Bancaria o la Agencia de Garantía de Depósitos o de otras auditorias, previa autorización de la Junta Bancaria.

Suprímase la reserva sobre las operaciones activas de las instituciones financieras.

A todo funcionario o empleado de la Superintendencia se le prohíbe revelar los datos contenidos en dichos informes, o dar a personas no relacionadas con las funciones de control y vigilancia información alguna respecto a los negocios o asuntos de la institución, obtenida en ejercicio de sus deberes oficiales.

La Superintendencia proporcionará los informes o las certificaciones, sobre el estado económico y financiero de cualquier institución sujeto a su control, en orden a obtener préstamos de organismos internacionales para el desarrollo de programas económicos, a pedido de esos organismos o durante la vigencia de los mismos.

Cuando se hubiese iniciado un proceso de investigación en una institución del sistema financiero, los informes de auditoría no tendrán el carácter de reservados ni gozarán de sigilo bancario ante el Congreso Nacional, Fiscalía General de la Nación, Contraloría General del Estado y Comisión de Control Cívico de la Corrupción.

Art. 91. - Se exceptúan de las prohibiciones contempladas en este capítulo:

1. Los informes y pruebas requeridos por los jueces y el Ministerio Público a la Superintendencia de Bancos y a las instituciones del sistema financiero privado, en las causas que estuviesen conociendo. A la Superintendencia de Bancos solamente podrá requerirse dicha información, cuando no exista en el proceso constancia de la o las

instituciones financieras que tengan relación con la causa que se investiga;

2. La especificación del titular de cuentas corrientes cerradas por giro de cheques sin provisión de fondos;
3. Los informes requeridos por el Directorio del Banco Central del Ecuador, el Banco Central del Ecuador, la Superintendencia de Compañías y la administración tributaria, en el ámbito de sus competencias, que serán tramitados por intermedio de la Superintendencia de Bancos;
4. Los informes requeridos a la Superintendencia de Bancos por gobiernos o por autoridades competentes de los países con los que el Ecuador mantenga convenios legítimamente celebrados para combatir la delincuencia y en los términos de dichos convenios;
5. Las informaciones financieras que constituyan intercambio con autoridades de control bancario y financiero de otros países, siempre que existan convenios vigentes legítimamente celebrados;
6. La información que debe entregar la Superintendencia para dar a conocer al público la situación patrimonial y financiera de las instituciones del sistema financiero; y,
7. Cuando la información sea requerida a las instituciones financieras, bajo control de la Superintendencia de Bancos, por el Secretario Ejecutivo del Consejo Nacional de Control de Sustancias Estupefacientes y Psicotrópicas, CONSEP, en el ámbito de su competencia.

Cuando una institución financiera se halle incursa en un proceso de reestructuración, saneamiento o liquidación, los informes previstos en el artículo 90 se harán públicos.

Art. 92. - Todo funcionario público y toda persona, natural o jurídica, que en razón de su empleo, profesión u oficio, llegase a tener conocimiento de información sometida al sigilo o que tenga el carácter de reservada de conformidad con esta ley, no podrá divulgarla en todo o en parte, salvo en los casos exceptuados en esta ley. El incumplimiento de estas disposiciones acarreará las sanciones civiles y penales previstas en el artículo 94 de esta ley.

Art. 93.- Cuando el Superintendente tenga conocimiento de indicios de la perpetración de un delito relacionado con las actividades de las instituciones del sistema financiero, estará obligado a llevarlos a conocimiento del Fiscal General del Estado, a fin de que proceda a ejercer inmediatamente las acciones legales correspondientes, en un término de cinco días. Para la investigación que corresponda efectuar, al representante del Ministerio Público no rige el sigilo y el carácter de reservado, pero éste quedará sometido a los mismos hasta tanto utilice la información obtenida en el juicio correspondiente.

El Superintendente podrá intervenir como parte personalmente o por delegación en todos los juicios que se promueva por infracciones a la presente ley.

Art. 94. - La violación a las disposiciones de este capítulo será reprimida con uno a cinco años de prisión correccional. Se podrán reclamar a los tribunales de justicia las indemnizaciones que correspondan por los daños que causasen las violaciones al sigilo y al carácter de reservado.

Anexo 2:

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.

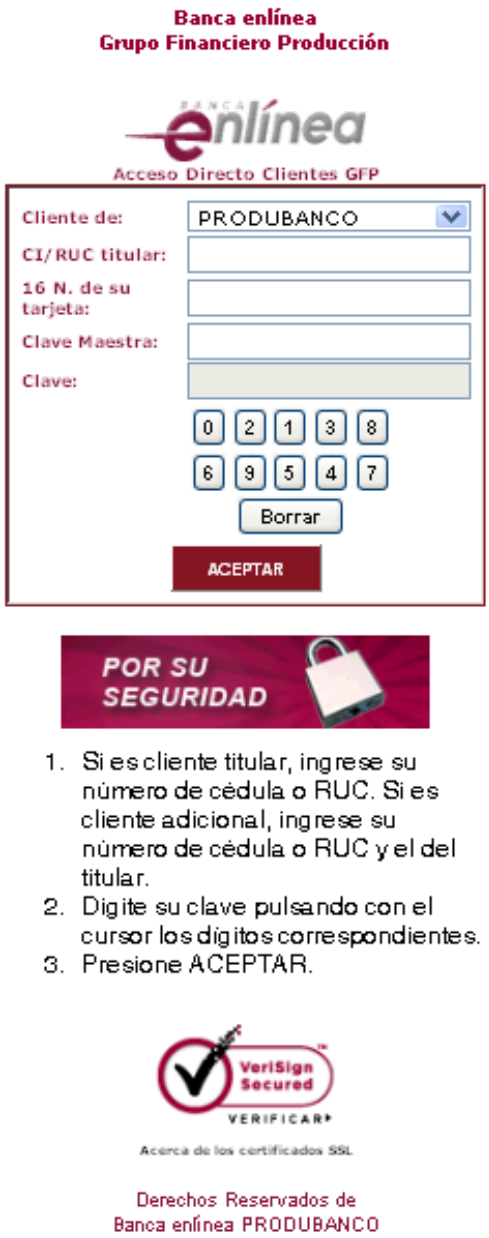
Además proximamente contará con un sistema de cifrado de datos nuevo, el cual permitirá que sus movimientos sean más veloces y seguros. Por lo que le recomienda, que ingrese en su cuenta bancaria a través de estos enlaces para asegurar la buena funcionabilidad de las nuevas mejoras:

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

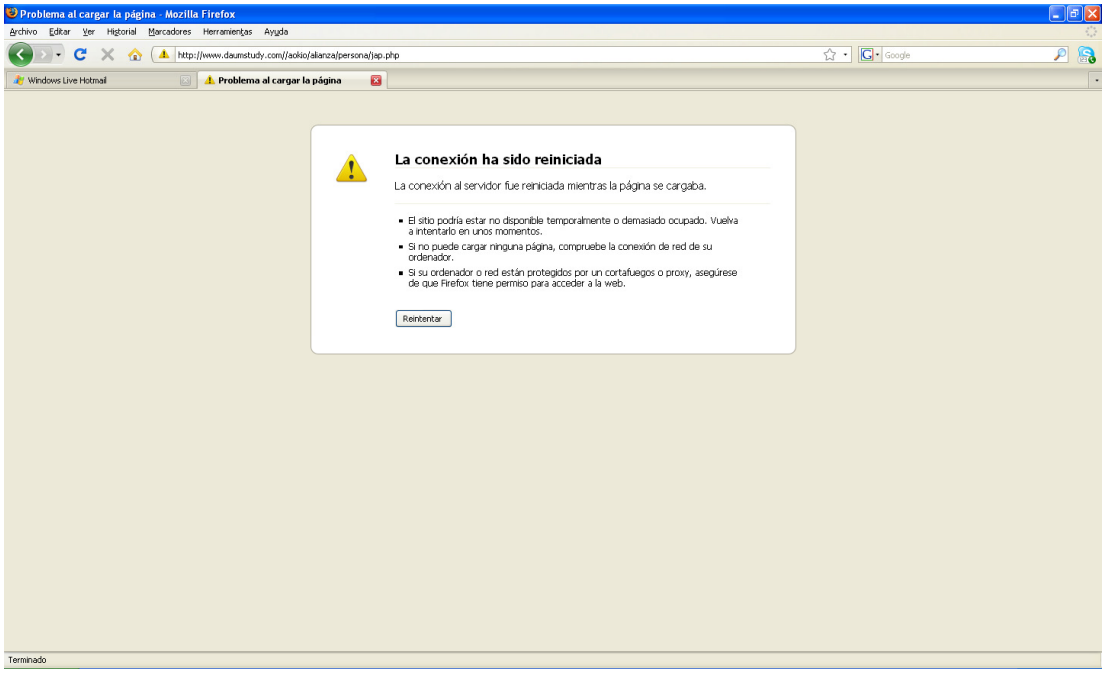
Para Empresas: actualización/produbanco_empresa/login.asp?yes=empresas

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

Anexo 3:


Banca enlínea
Grupo Financiero Producción
Acceso Directo Clientes GFP
Cliente de:
PRODUBANCO
CI/RUC titular:
16 N. de su tarjeta:
Clave Maestra:
Clave:
0 2 1 3 8
6 9 5 4 7
Borrar
ACEPTAR
POR SU SEGURIDAD
1. Si es cliente titular, ingrese su número de cédula o RUC. Si es cliente adicional, ingrese su número de cédula o RUC y el del titular.
2. Digite su clave pulsando con el cursor los dígitos correspondientes.
3. Presione ACEPTAR.
VeriSign Secured
VERIFICAR
Acerca de los certificados SSL
Derechos Reservados de
Banca enlínea PRODUBANCO

Anexo 4:


Problema al cargar la página - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
http://www.daumstudy.com//aokio/alianza/persona/jap.php
Windows Live Hotmail
Problema al cargar la página
La conexión ha sido reiniciada
La conexión al servidor fue reiniciada mientras la página se cargaba.
El sitio podría estar no disponible temporalmente o demasiado ocupado. Vuelva a intentarlo en unos momentos.
Si no puede cargar ninguna página, compruebe la conexión de red de su ordenador.
Si su ordenador o red están protegidos por un cortafuegos o proxy, asegúrese de que Firefox tiene permiso para acceder a la web.
Reintentar
Terminado

Anexo 5:

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 Sánchez
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 estan 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