UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
CARRERA DE DERECHO

TESIS DE GRADO

"DEFENSA DEL DERECHO A LA INTIMIDAD FRENTE AL PODER INFORMÁTICO"

Postulante : **Paulette Fernández Mendoza**

Tutor : **Dr. Marcelo Fernandes Irahola**

La Paz – Bolivia
2009

Dedicatoria

El presente trabajo de investigación esta dedicado con muchisimo cariño y agradecimiento a nuestro Creador y mi madre, ejemplo de virtudes incontables, por su constante apoyo y cariño, quien siempre me otorga el privilegio de su gran amor.

“DEFENSA DEL DERECHO A LA INTIMIDAD FRENTE AL PODER INFORMÁTICO”

DISEÑO DE INVESTIGACIÓN

Enunciado del titulo del tema

“DEFENSA DEL DERECHO A LA INTIMIDAD FRENTE AL PODER INFORMÁTICO”.

Identificación del problema

La falta de una normativa jurídica específica que regule el área de la informática que proteja los datos personales, puede atentar al derecho a la intimidad ya que con el avance de la tecnología, el uso de los datos personales pueden causar daños económicos y morales.

Problematización

¿En nuestro país existe un vació jurídico en cuanto a la protección de los datos personales?

¿Por qué no se protege el uso de los datos personales?

¿Existe la necesidad de crear una normativa de protección de datos personales adecuada en nuestro país?

¿Por que en Bolivia la protección de datos personales no se ha actualizado frente a otros países?

¿Será que la falta de legislación que regule el área de la informática trae como consecuencia el atentado a la protección de datos personales?

¿Será necesario crear medios de protección de los datos personales en el ámbito informático?

Delimitación de la investigación

Delimitación Temática

En el presente trabajo se realizó un análisis sobre los conceptos de intimidad frente al avance tecnológico de la informática, la defensa del derecho a la intimidad reconocido e incorporado en la declaración de derechos Humanos, ya que la misma protege la protección de los datos personales, actualmente el derecho a la privacidad se encuentra reconocida en nuestra Constitución; asimismo en el Código Civil como un derecho de la personalidad, por tanto está dentro del campo jurídico y social.

Delimitación Temporal

El presente trabajo se estudió desde el año 2006 hasta nuestros días, por el gran avance jurídico tecnológico.

Delimitación Espacial

El campo de trabajo que se tomó en cuenta es el centro de la ciudad de La Paz.

Fundamentación e importancia de la investigación

La intimidad constituye un bien personal al que no puede renunciar el individuo sin resentirse en su dignidad humana; el ser humano es social por naturaleza, pese a ello no deja de sentir la necesidad de realizar una vida interior, ajena a las relaciones que mantiene con otros individuos, y que le permite identificarse como ser humano. El derecho a la intimidad es un derecho fundamental reconocido dentro de los derechos humanos, asimismo por nuestra Constitución y el Código Civil, en nuestro país.

Con el desarrollo de la informática se crean registros, almacenes y bases de información automatizadas mucho más sofisticadas, a partir de éstos la información es fácilmente manipulable, de allí que una de sus características es la facilidad de su manejo, ello permite intercambiar información de manera instantánea entre diferentes bases, almacenes o registros de información, de allí, que en la actualidad la información puede ser triangulizada y comparada con otra información obtenida, con lo que se puede saber mucho más de una persona de lo que se cree.

El derecho a la intimidad reconoce al ser humano, el derecho de reservarse para sí o para un grupo reducido de personas ciertos hechos, situaciones e información personal. Con el avance de la tecnología y la creación de sofisticados sistemas de bases, almacenes y registros de información, el derecho a la privacidad en la actualidad, también reconoce y faculta a los titulares de esta información el de poder ejercer ciertos derechos sobre la información personal que ha sido entregada a terceros por razones de orden legal o social como: derecho a la autodeterminación informativa, derecho al anonimato, derecho de acceso, derecho de oposición de registro, derecho de cancelación.

En nuestro país se protege el derecho a la intimidad personal, imagen, honor y reputación, pero no es especifica en la protección de datos personales, causando una laguna jurídica por lo que es necesario que exista una norma especifica para proteger los datos personales.

Objetivos a los que se ha arribado en la investigación

Objetivo General.-

- Proponer una norma que garantice y proteja íntegramente los datos personales de las personas naturales o jurídicas asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, tanto públicos como privados destinados a dar informes, para garantizar el derecho a la intimidad de las personas.

Objetivos Específicos.-

- Establecer la falta de protección de los datos personales en la legislación boliviana.
- Conocer el avance jurídico de España, por que su legislación es utilizada como norma base en las demás legislaciones; Argentina, como único representante de América latina con autorización de transferencia de datos hacia la Unión Europea; México y Uruguay con respecto a la protección de los datos personales.
- Determinar el vació jurídico que existe en nuestro país, en cuanto a una normativa especifica que proteja los datos personales vulnerando así el derecho a la intimidad.

Marco de referencia

Histórico

Las primeras grandes declaraciones de derechos humanos se produjeron en las colonias inglesas de Norteamérica, impulsadas por sus conflictos con la corona inglesa: en junio de 1776 se proclamó la Declaración de Derechos de Virginia y en julio la Declaración de Independencia de los Estados Unidos. La Declaración de Independencia, redactada por Thomas Jefferson, afirmaba lo siguiente: "Sostenemos como verdaderas evidencias que todos los hombres nacen iguales, que están dotados por su Creador de ciertos derechos inalienables, entre los cuales se encuentra el derecho a la vida, a la libertad y a la búsqueda de la felicidad...".

Una década más tarde, en Europa, en los tiempos agitados de la Revolución Francesa, en 1789 se proclama en París la Declaración de los Derechos del Hombre y del Ciudadano. A esta declaración, le siguió en 1793 una segunda más radical.

Durante el siglo XVIII fueron fundamentales las ideas de Montesquieu y Rousseau. Montesquieu (1689-1755), criticó severamente los abusos de la Iglesia y del Estado, al estudiar las instituciones y costumbres francesas de la época, dio formas precisas a la teoría del gobierno democrático parlamentario con la separación de los tres poderes, legislativo, ejecutivo y judicial, como mecanismo de control recíproco entre los mismos, acabando teóricamente con la concentración del poder en una misma

persona y los consecuentes abusos y atropellos que históricamente había producido el irrestricto poder del monarca en contra de los seres humanos.

El siglo XVIII fue un siglo de logros importantes y al mismo tiempo de considerables limitaciones. Dos ejemplos: 1) Las declaraciones hablan de los "Derechos de los Hombres" (las mujeres quedaban excluidas). 2) Frecuentemente eran "compatibles" con la esclavitud. En Estados Unidos no se abolió la esclavitud hasta la Guerra de Secesión, en 1865. En España, se abolió en 1814, aunque se permitió que continuara en las colonias (concretamente en Cuba, hasta 1880).

Los movimientos obreros emprenden la defensa de los derechos humanos desde una perspectiva colectiva, de manera más amplia, es el momento en el que los trabajadores exigen sus reivindicaciones. Ya en el siglo XX, las revoluciones mexicana y rusa de 1917 constituyen hechos históricos determinantes para la consagración jurídica de estos derechos colectivos, los derechos económicos y sociales.

A la Primera Guerra Mundial siguió la creación de la Sociedad de Naciones, que aunque no fue capaz de evitar la segunda guerra mundial, sí tuvo el mérito de ser el precedente de una organización supranacional de carácter vinculante. Otros logros de la Sociedad de Naciones fueron la creación del Tribunal Internacional de la Haya, la firma del "Convenio internacional para la supresión de la esclavitud" (firmado en 1926 y completado y ratificado por las NNUU en 1956) o la creación de la Organización Internacional del Trabajo.

A la Segunda Guerra Mundial siguió la creación de las Naciones Unidas. Los horrores de la guerra y los juicios de Nuremberg y Tokio contra los altos responsables nazis y japoneses, acusados de crímenes de guerra y genocidios, mostraban la necesidad de regular de forma precisa el concepto de derechos humanos y, sobre todo, de establecer claramente cuáles eran. El resultado fue la aprobación, en 1948, de la Declaración Universal de los Derechos Humanos. Con el paso de los años, la Declaración Universal, que como tal no es de carácter vinculante, se ha ido completando con una serie de convenios, convenciones y pactos, estos sí vinculantes, que van desarrollando, y en algunos casos ampliando, los contenidos de la Declaración Universal. El objetivo además es que estos derechos lleguen a formar parte del derecho positivo de todas las naciones, lo que en muchos casos ya ha sucedido (otra cosa es que luego sean respetados).

Las normas y principios empezados a promulgar hace siglos de forma fragmentada y difusa en distintos entornos culturales (con una incidencia en general limitada

sobre la vida cotidiana de los ciudadanos de las correspondientes épocas históricas), con el paso del tiempo se han ido consolidando y difundiendo: por un lado, detallando cada vez con más precisión los distintos derechos y, por otro lado, construyendo sociedades dotadas de los mecanismos necesarios para velar por el respeto efectivo de estos derechos.

La Declaración Universal es la culminación, hasta el momento, de este afán de universalización y concreción de los derechos de las personas.

Historia del Derecho a la Intimidad.

La noción de intimidad o privacidad está ligada al nacimiento del llamado Estado Liberal, y se desarrolla por primera vez con el llamado constitucionalismo inglés. En esta rama del Derecho anglosajón se dieron las primeras discusiones sobre el tema de la libertad y la autonomía.

Lo que hoy en día conocemos como derecho a la privacidad tiene sus orígenes en los Estados Unidos, donde por primera vez es tratado como categoría independiente de derechos. A finales del siglo XIX, en un artículo titulado “The Right for Privacy”, Samuel D. Warren y Louis Brandeis, se basaron en los principios del common law para intentar establecer un límite jurídico con fundamento en el cual se pudieran prohibir las intromisiones de la prensa en la vida privada y doméstica.

Marco teórico que sustenta la investigación

El Derecho Informático y los derechos humanos

El primer libro que se publica en el mundo con ese título, data de 1950, dos años antes, el 10 de diciembre de 1948, la Organización de las Naciones Unidas promulga la Declaración de Derechos Humanos y en su artículo 19 se describe por primera vez en la historia normativa, el derecho humano a la información.

Algunos autores adjudican el origen histórico de los derechos humanos al ius naturalismo racionalista, a la Ilustración y la Revolución francesa, aunque según Desantes (1990), sin negar esa influencia, la naturaleza jurídica de los derechos humanos tiene su origen en la consideración cristiana de los hombres como hijos de Dios.

La localización histórica de los derechos humanos influyo en la consideración jurídica de su naturaleza. Existen dos tendencias, la positividad, según la cual los derechos humanos existen en tanto están concedidos por la ley, principalmente por la ley constitucional. La otra corriente es la ius naturalista, según la cual, radican en

la naturaleza del hombre, en tanto que son necesarios para existir conforme a su naturaleza personal y social del hombre mismo, por eso, la ley no los concede, sino que los reconoce y los garantiza. Y son los hombres que obtienen su perfil racionalmente, a medida que avanzan culturalmente.

Y por muy extensa que resulte su relación, siempre se advertirá algún derecho nuevo en cuanto surja una nueva necesidad o posibilidad humana.

El derecho a la intimidad

En un principio, en Europa se desarrolla el concepto de derechos de la personalidad, algunos países, como Alemania, habían rechazado la existencia de estos derechos, y sólo los reconoce a partir de la ley fundamental de 1949. Por otra parte, los juristas franceses estaban más avanzados en el tema, pues ya habían desarrollado estos conceptos y pusieron en vigencia la ley del 17 de julio de 1970, que tenía una parte destinada a la protección de la vida privada (Monreal, 1997). El primer texto constitucional en Europa que recogió de forma expresa el derecho a la privacidad fue la Constitución portuguesa de 1986 (artículo 33.1), a la cual le sigue la Constitución española de 1978 (artículo 18).

Estados Unidos de Norte América por su parte, concibe al derecho a la privacidad como: El derecho de ser dejado sólo (the right to be let alone) o el derecho a la privacidad (the rigth of privacy) se origina en 1873 formulado por el Juez Thomas A. Cooley. Más tarde, este concepto fue formulado orgánicamente por primera vez en un artículo publicado en 1890 por dos jóvenes abogados Warren y Louis D. Brandeis.

En Bolivia, los antecedentes más antiguos nacionales son: Constitución Política del Estado de 1831 artículo 158, la de 1834 artículo 160 y la de 1871 artículo 13, que disponen que las acciones privadas que no ofenden al orden público ni perjudican a un tercero están reservadas a Dios y exentas de toda autoridad (Morales Guillen; 1994).

El proyecto de Angel Osorio consagra especialmente el derecho a la privacidad en los siguientes términos. " ...todas las personas tienen derecho a que sea respetada su vida íntima. El que, aun sin culpa ni dolo, se entrometiere en la vida ajena, publicando retratos, divulgando secretos, difundiendo correspondencia, mortificando a otros en sus costumbres o perturbando de cualquier modo su intimidad, será obligado a cesar en tales actividades y a indemnizar al agraviado. Los tribunales regularan libremente, con arreglo a las circunstancias del caso, el modo de aplicar estas dos sanciones". Según Ferreira (1982), se trata de una de las fuentes más directas del artículo 1071 bis de la

Ley Argentina destinada a la protección del derecho a la privacidad.

El término apropiado, en un correcto castellano sería vida privada. Según el comentario que realiza la Comisión Andina de Justicia, la mayoría de las legislaciones trata del derecho a la privacidad, el mismo que hace referencia al poder que tiene toda persona de excluir a los demás del conocimiento de los actos y actividades personales (Lete del Rio, 1991). Protege a la persona y a su familia, y comprende la libertad del individuo para conducirse en determinados espacios y tiempo libre de perturbaciones ocasionadas por terceros.

Esta misma institución, considera que el derecho a la privacidad se proyecta en dos dimensiones: Primero, como secreto, atenta contra ella todas las divulgaciones ilegítimas de hechos relacionados con la vida privada o familiar, o las investigaciones también ilegítimas de acontecimientos propios de dicha vida, donde el ser humano no puede ejercer un control autónomo sobre él. Segundo, como libertad individual, trasciende y se realiza en el derecho de toda persona a tomar por sí sola decisiones que conciernen a la esfera de su vida privada.

El derecho a la intimidad debe cumplir una serie de requisitos, los mismos que sirven para no confundirlo con otros derechos de la personalidad, entre los que se encuentran:

a) La veracidad de los hechos.- Los hechos deben reflejar la realidad, porque sólo en lo real puede entrometerse alguien (Ferreira, 1982). Esta veracidad elimina una serie de conductas que consiste en atribuir hechos falsos a las víctimas.
b) Los hechos deben ser desconocidos- Es el carácter secreto u oculto de la información. Pues son "manifestaciones que quedan sustraídos al conocimiento de extraños o cuando menos ajenos al circulo familiar del sujeto (Monreal, 1997: 49) Pero, es necesario recalcar que el "hecho de que un grupo reducido de personas conozca aspectos de la vida privada de otra no le quita a dicha información el carácter de reservados" (Ferreira, 1982: 104).
c) El conocimiento de la información debe ser dañoso, el daño puede ser moral o patrimonial. Además se debe conocer que la vida privada está conformada de alegrías y tristeza y ambas quedan protegidas (Ferreira, 1982). Monreal excluye al daño patrimonial, pues considera que debe provocar moralmente al sujeto una turbación moral en razón de ver afectado su sentido del pudor o de recato cayendo en subjetivismo, pues mide lo moral de acuerdo a la reacción promedio de un hombre común y obviando que también pueden existir daños patrimoniales. (Monreal, 1997)

d) La voluntad del sujeto, pues éste no debe desear que otros tomen conocimiento de esos hechos, este elemento ha sido obviado por Rubio Ferreira, sin embargo Monreal lo rescata, ya que el consentimiento de la persona elimina la sustancia antijurídica. El consentimiento puede ser expreso o tácito, pero en todo caso inequívoco. Es principalmente circunstanciado esto quiere decir, que será de aplicación sólo al supuesto para que ha sido otorgado. En este sentido afirma Monreal (1997) que "la voluntad del sujeto solamente puede excluir de la reserva propia de la vida privada aquello a que ella va referida y en la forma que aquel lo señala".

Con la utilización de redes en las que circula libremente información con contenidos personales y entre otras tecnologías, la implantación de nuevas técnicas de recolección de información, se considera que se tendrá como resultado sociedades altamente informatizadas. En la actualidad la sociedad es un panóptico, compara la vigilancia de prisiones donde todas las conductas de los prisioneros son observadas y registradas por un vigilante o inspector quien controla a cada uno de los prisioneros, los cuales no lo pueden verlo ni podían ver a otros prisioneros. Cada sociedad informatizada cada acto que se realice dejará una huella indeleble, siendo imposible evitar la estigmatización y el consiguiente encasillamiento.

Las personas deben ser informados acerca de la colecta, uso, almacenamiento y tratamiento de la información. La información que se desea recolectar y tratar debe ser obtenida legal y lícitamente, además de ser registrada únicamente para finalidades determinadas, sin que puedan ser utilizadas de manera incompatible con esas finalidades. Asimismo, la información debe ser adecuada, pertinente y no excesiva en relación a la finalidad. Del mismo modo, la información debe ser exacta y puesta al día por lo que se debe reconocer el derecho de acceso y rectificación al titular de los mismos. Limitar el uso de la informática no significa otra cosa que restringir el derecho a la libertad de expresión, lo cual se justifica únicamente en aras de la protección de otros derechos fundamentales como es el derecho a la privacidad de todos y cada uno de los seres humanos del mundo.

Principios generales para proteger la información personal

- Principio de autodeterminación informativa

Desde esta perspectiva, el primer derecho que fue invocado y debe ser invocado siempre, es el derecho a ser informado acerca de las características, facultades, derechos y obligaciones de los quienes almacenan información. Esto en Europa se

denomina autodeterminación informativa, que significa la posibilidad de saber quién, qué, cuándo, y con qué motivo se sabe algo sobre mi.

- Principio de calidad de información

La información sólo podrá ser tratada y sometida a tratamiento cuando cumpla con las características de: pertinencia, adecuación y límite en relación con el ámbito, la finalidad determinada y legítima para la que fueron recogidos. Se habla de información adecuada, a la justificación legal y/o social que debe existir para la colecta, tratamiento y almacenamiento, lo que implica que la recolección de información puede realizarse siempre y cuando exista uno de los dos fundamentos enunciados a continuación:

a) Un fundamento legal, es decir, que la ley lo debe establecer así
b) Un fundamento social, pues la colecta debe ser en virtud de un interés general, por lo que debe estar al servicio de cada ciudadano.

Se habla de información pertinente pues sólo se puede solicitar y recolectar la información necesaria para el objetivo, no permitiendo preguntar más de lo debido. Toda información recolectada tiene debe tener dos límites claramente establecidos: objetivo y tiempo. Y recolectada para la finalidad, y que esta no podrá ser utilizada con fines para los cuales no haya sido acopiada. Esta finalidad previamente justificada debe ser cumplida en un tiempo también determinado, por lo que la misma información debe ser almacenada mientras se cumpla el fin y sea útil. Una vez que se hayan alcanzado los límites estos serán cancelados, pues habrán dejado de ser necesarios y pertinentes.

La información recolectada debe ser exacta y puesta al día de forma que responda con veracidad a la situación actual del titular de la misma, pues para que exista vulneración del derecho a la privacidad debe existir entrometimiento en hechos reales de la vida (Ferreira, 1982).

- Principio de justificación social

La recolección de datos debe tener un propósito general y usos específicos socialmente aceptables.

- Principio de la limitación de la recolección

Debe ser restringida al mínimo necesario; los datos no pueden ser obtenidos por medios ilícitos o de mala fe y deben serlo con conocimiento y consentimiento del interesado o con autorización legal.

- Principio de la especificación el propósito o finalidad

Deben estar especificados los fines al momento de la recolección, y el uso debe quedar limitado a ellos.

- Principio de la confidencialidad

No deben ser revelados sin consentimiento del interesado (o autorización legal). De salvaguarda de la seguridad Protección adecuada a los datos (para prevenir pérdidas, destrucciones o acceso ilegal).

- Principio de política de apertura

Debe haber una política de apertura con respecto al desarrollo, práctica y métodos concernientes a los datos personales, y el público interesado debe conocerlos, su propósito y los usos y métodos de operación de los sistemas de datos personales.

- Principio de limitación en el tiempo

Los datos deben destruirse cuando terminan los fines que los originaron.

- Principio de control

Debe haber un órgano responsable legalmente de la efectividad de los principios contenidos en la legislación.

- Principio de participación individual

El titular debe tener derecho a acceder a sus datos, con información del centro de datos y del responsable; debe ser informado en tiempo y forma de cualquier dato referido a su persona; puede oponerse a cualquier dato que le concierne, y debe quedar registrada su oposición, debiendo tener derecho a la supresión en caso de que prospere; en su caso debe ser informado de las razones por las que no prospera su acceso o por la que su pedido no prospera en tiempo y forma.

- Principio de consentimiento del Afectado

Se debe cumplir con el principio de licitud en la captura, ello significa una permisión como principio, lo que supone el conocimiento y consentimiento del afectado.

Información especialmente protegida

Las legislaciones mundiales, en general, diferencian el tratamiento de información sensible y la no sensible: La primera está vinculada con la intimidad del sujeto, esta información se concreta en dos grupos fundamentales: ideologías, religión o creencias y el origen racial, salud o vida sexual. La segunda se refiere a otras circunstancias de la vida como: profesión, estudios, estado civil y otros.

La regla general debería establecer la prohibición en el tratamiento de información sensible, porque reviste características específicas que la hacen merecedoras de una protección más profunda que las otras.

Seguridad de la información conferida y deber de confidencialidad

La información recolectada y almacenada genera, en quien la recolecta y almacena, el deber de mantener en reserva la información que conoce en atribución al ejercicio de sus actividades. Asimismo, se debe establecer que para que sea efectivo es necesario, además, tener sistemas de seguridad informática. Esta seguridad informática se refiere a las técnicas desarrolladas para proteger los equipos informáticos conectados en una red frente a daños accidentales o intencionados, que deberán adaptarse con relación: al estado de la tecnología, a la naturaleza de la información almacenada y a los riesgos a los que está expuesta.

Principio de acceso

Este principio implica la facultad que tienen los usuarios de acceder a las bases de información para conocer qué información suya está siendo almacenada o recolectada, para que el mismo pueda darse cuenta de los posibles errores que la misma contenga y que la ayudaran a rectificarla o pedir que se la rectifiquen. Del mismo modo ha de cancelarse la información que ya no es útil. La cancelación, así mismo, implica que se borre la información del soporte que la contiene, impidiendo su regeneración.

Hipótesis de trabajo

La ausencia de una normativa que proteja los datos personales en nuestro país trae como consecuencia la vulneración del derecho a la intimidad.

Variables

Variable independiente

La ausencia de una normativa que proteja los datos personales en nuestro país.

Variable dependiente

La vulneración del derecho a la intimidad

Unidades de análisis

País

Nexo lógico

Traer.

Métodos y técnicas que fueron utilizados en la investigación

Métodos generales

En el presente trabajo, se utilizo el método deductivo, para efectuar un análisis de la realidad y las leyes aplicando desde lo general a lo particular, asimismo se considero la historia con referencia al tema como legislación comparada y la doctrina.

Métodos Específicos

Los métodos utilizados fueron el dogmático Jurídico y el método comparativo para resolver el problema de investigación se acudió al mismo ordenamiento jurídico, pues se investigaron las normas jurídicas vigentes, al mismo tiempo, se analizo leyes de otros países para realizar estudios comparativos.

Técnicas a utilizadas en la investigación

Se utilizo para el análisis de la parte teórica jurídica-doctrinal de las categorías conceptuales refiriéndonos a la Constitución Política del Estado vigente, todas las normas y las concepciones jurídicas relacionadas con el derecho a la protección de datos personales y derecho a la intimidad en Bolivia, visión comparada en Latinoamérica dicha información se obtuvo de fuentes internas y externas.

Fuentes internas

Se refiere a la información y a los datos que se encontraron en la legislación vigente de nuestro país.

Fuentes externas

Se refiere a los datos que se obtuvieron como bibliografía, revisión de textos, archivos, trabajos y documentos de Internet.

CAPITULO I.

MARCO TEÓRICO REFERENCIAL

EL DERECHO

La defensa de la intimidad frente al poder informático, es de suma importancia y utilidad por la actualidad del contenido; empecemos con el estudio de los derechos personalísimos, no solo por que, todo estudioso de la ciencia jurídica debe tener un profundo y completo conocimiento del objeto central que motiva nuestra ciencia, sino por que debemos empezar por los conceptos básicos que están indisolublemente concatenados con el presente tema de investigación.

1.1. DEFINICIÓN

La palabra derecho puede tomarse en tres acepciones distintas[1];

En primer lugar, la designada como el conjunto de normas o reglas que rigen la actividad humana en la sociedad, cuya inobservancia está sancionada; es decir el derecho objetivo

En segundo lugar, a la facultad que pertenece al individuo, como un poder del individuo; es decir el derecho subjetivo.

En tercer lugar, el derecho como equivalente a justicia, como portador del valor justicia.

El derecho incorpora unos valores a la sociedad, valores que fundamentalmente son dos: la justicia y la seguridad jurídica.

Para Fernando de Castro, *"el derecho es la forma que reviste la garantía de las condiciones de vida de la sociedad, fundada sobre el poder coercitivo del Estado."* [2]

Por su parte el Doctor Eduardo García Maynez dice que el: *"Derecho es un orden concreto, instituido, por el hombre para la realización de valores colectivos, cuyas normas integrantes de un sistema que regula la conducta de manera bilateral, externa y coercible, y en caso de inobservancia, aplicadas o impuestas por los órganos del poder público"*[3].

Por lo que, podemos definir al derecho como un producto cultural en un conjunto de normas jurídicas sistematizadas inspiradas en los valores como la justicia,

[1] De Castro, Fernando.: Derecho Civil en España, Vol. I. Madrid, 1955.
[2] De Castro, Fernando.: Derecho Civil en España, Vol. I. Madrid, 1955.
[3] García Maynez, Eduardo, "Filosofía del Derecho", Ed. Porrúa.

seguridad, orden que regulan la vida de las personas en sociedad en caso de quebrantamiento, pueden aplicarse normas jurídicas por los órganos del poder público.

1.2 DERECHO OBJETIVO Y SUBJETIVO

1.2.1 Derecho objetivo

El Dr. Héctor Ramón Peñaranda define al derecho objetivo como: *"El conjunto de normas por las que se rige una sociedad Para establecer un concepto de derecho más elaborado hay que determinar los elementos que caracterizan estas normas que llamamos jurídicas".*[4]

Por lo que, podemos definir al derecho objetivo como el conjunto de normas que forman nuestro ordenamiento jurídico, es aquel conjunto de reglas de conducta que en una sociedad determinada van a gobernar las relaciones de los individuos entre ellos mediante las normas jurídicas.

1.2.2 Derecho subjetivo

El Dr. Héctor Ramón Peñaranda define como: *"el conjunto de facultades y poderes concretos atribuidos a un titular, que puede ejercer libremente, (los derechos), estos van a estar constituidos por aquellas prerrogativas que el Derecho objetivo reconoce a los individuos o reconoce a un grupo de individuos".*[5]

Es la facultad, es el poder que nos otorga el Derecho Objetivo para reclamar ante la autoridad competente el cumplimiento de un deber jurídico contraído por otra persona. Por eso los actos humanos, los productos de espíritu y las cosas del mundo exterior son entidades que pueden ser objeto de derecho subjetivo.

Cuando se habla de sujeto de derecho, se habla de una persona que disfruta de determinada prerrogativa. Las personas no son objeto de derecho, objeto de derecho son las cosas y animales. Cuando se habla de sujeto de derecho, se habla de una persona que disfruta de determinada prerrogativa; las personas no son objeto de derecho, objeto de derecho son las cosas y animales.

Por lo que, podemos definir que el derecho objetivo, o norma, nace el derecho subjetivo como facultad, que se expresa cuando se dice, que derecho es aquello que me es lícito o permitido hacer; que no es sino expresión refinada del deseo de

[4] Peñaranda Quintero Héctor Ramon, Derecho Civil I: Personas Y Familia, Maracaibo, 12 De Junio De 2001
[5] Peñaranda Quintero Héctor Ramon, Derecho Civil I: Personas y Familia, Maracaibo, 12 De Junio De 2001

apropiación, que pretende excluir a los demás de algo que pensamos o queremos que nos pertenezca.

1.3 DERECHOS PERSONALÍSIMOS

Los derechos subjetivos esenciales han recibido la denominación de derechos de la personalidad por cuanto pertenecen a la persona por su sola condición de tal. Dichos derechos aluden a un conjunto de facultades fundamentales que atienden a la más eficaz protección y defensa de la persona individual y de sus atributos.

Los derechos de la personalidad también denominados derechos personalísimos como lo define el Dr. Juan Espinoza Espinoza: "*corresponden innatamente a toda persona, desde antes de su nacimiento y hasta su muerte, y que le garantizan el íntegro ejercicio y desenvolvimiento de sus atributos esenciales para así poder desarrollarse plenamente en su humanidad*"[6].

Los derechos personalísimos o derechos de la personalidad, reconoce el derecho de la vida, la libertad, aspectos referidos al honor, etc., insertada en la legislación y la doctrina universal en el siglo XIX, en la que se tradujeron en un reconocimiento embrionario pero aislado y no metódico hasta que, en el siglo XX, se produce su consagración sistemática, fundamentalmente a través de normas de carácter internacional como la Declaración Universal de los derechos Humanos (1948) o el Pacto de San José de Costa Rica (1969), que se tradujeron en tratados, pactos y convenciones que redondean un verdadero derecho internacional tuitivo de los derechos de la personalidad, que obliga a los adherentes a adecuar sus legislaciones locales.

1.3.1 CARACTERÍSTICAS DE LOS DERECHOS PERSONALÍSIMOS

Luis Prieto nos dice que las características de los derechos personalísimos son las siguientes[7] :

- Absolutos**: se da erga ommes**
- Innatos, inherentes y necesarios**: Porque surgen en el origen de la persona por su solo carácter de su ser individual, existe una unión inseparable entre el sujeto y el objeto del derecho.**

[6] Espinoza Espinoza Juan, Derecho de las Personas, 4ª Edición, Palestra, Lima, 2004
[7] Prieto Sanchis, Luis. Estudios de Derechos Fundamentales. Ed. Debate, Madrid, 1990.

- Vitalicios**: Durante toda la vida de la persona, con algunas excepciones referidas a supuestos que se dan luego del fallecimiento de ellas que se trasladan a los herederos.**
- **Inalienables**: estos derechos están fuera del comercio, no pueden ser objeto de cesión o transferencia.
- **Extrapatrimoniales**: pero tienen repercusión económica o patrimonial en caso de su violación; ergo, de darse su lesión, surge a favor de la víctima un crédito indemnizatorio y la facultad de exigir judicialmente el cese de la acción lesiva si continuara.
- **Autónomos**: las características propias de estos derechos subjetivos, que los llevan a diferenciarse de los demás, constituyendo una categoría particular, "inconfundible".

1.3.2 DERECHOS INHERENTES A LA PERSONALIDAD: HONOR, INTIMIDAD E IMAGEN

HONOR

German Bidart nos dice que: ***"El honor es la apreciación y la valoración que hacen los demás de las cualidades ético-sociales de una persona. Es la buena reputación de que se disfruta; es el buen nombre es un patrimonio de elevada estimación, pero solamente adquiere sentido en la estimación de los otros"***[8]**.**

Para Miguel Alegre el derecho al honor "es el derecho al decoro, entendido de acuerdo a las costumbres imperantes en la sociedad, el derecho al honor está protegido por las normas penales que establecen los delitos de difamación o injurias" [9].

Miguel Angel Alegre nos dice que ***"el mayor número de personas a las cuales fue comunicado el ataque contra el honor, aumenta la cantidad natural de la infracción de la misma manera que el mayor número de monedas robadas aumenta la cantidad del delito de hurto***"[10]**.**

Por lo que podemos definir como honor, el aprecio y estima que una persona recibe de la sociedad en la que vive; es un derecho íntimamente relacionado con la dignidad personal. Las personas jurídicas poseen lo que se denominaría reputación que sin problema alguno se protege de toda difamación de injurias que de algún modo u otro pudieran repercutir negativamente; sin embargo, el grado de protección

[8] Bidart Campos, Germán. 1994. La Interpretación de los Derechos Humanos, Buenos Aires, Ed. Ediar.
[9] Alegre Martínez, Miguel Ángel. El Derecho a la Propia Imagen. Ed. Tecnos, Madrid, España. 1997
[10] Alegre Martínez, Miguel Ángel. El Derecho a la Propia Imagen. Ed. Tecnos, Madrid, España. 1997

sería algo menor que en el caso de las personas físicas. Los atentados más graves contra el honor personal son los delitos de injurias y calumnias para los cuales nuestro ordenamiento reserva la protección penal.

PROPIA IMAGEN

Para Luis Prieto el derecho a la imagen es *"la representación gráfica de la figura humana mediante un procedimiento mecánico o técnico de reproducción y, en sentido jurídico es la facultad exclusiva del interesado a difundir o publicar su propia imagen, y por ende el derecho a evitar su reproducción"*[11]

Miguel Angel Alegre dice que el derecho a la imagen personal es *"La facultad que el Ordenamiento Jurídico concede a la persona para decidir cuándo, por quién y de*

***qué forma pueden ser captados, reproducidos o publicados sus rasgos fisonómicos reconocibles"*[12].**

Por lo que, podemos definir que el derecho a la propia imagen protege frente a la captación, reproducción y publicación de la imagen en forma reconocible y visible. Cada persona dispone de la facultad exclusiva de determinar cuando, como, por quién y en que forma quiere que se capten, reproduzcan o publiquen sus rasgos fisonómicos, controlando el uso de dicha imagen por terceros, impidiendo así su captación, reproducción y publicación por cualquier procedimiento mecánico o tecnológico, sin su consentimiento expreso.

INTIMIDAD

Para Luis Prieto la intimidad es: "*el reconocimiento de que cada persona tenga un ámbito de desarrollo y expresión de su manera de ser que le esté reservado, del cual pueda excluir a los extraños y donde tenga derecho a no ser importunado por la indebida curiosidad ajena"*[13].

Lucrecio Rebollo dice que hablar de "*intimidad es hablar de sentimientos, de creencias (políticas, religiosas), pensamientos o de una información, o la relativa a la vida*

[11] Prieto Sanchis, Luis. Estudios de Derechos Fundamentales. Ed. Debate, Madrid, 1990.
[12] Alegre Martínez, Miguel Ángel. El Derecho a la Propia Imagen. Ed. Tecnos, Madrid, España. 1997
[13] Prieto Sanchis, Luis. Estudios de Derechos Fundamentales. Ed. Debate, Madrid, 1990.

sexual, cuya difusión puede producir ciertas reservas al individuo"[14].

Por lo que podemos definir que la Intimidad, es elegir libremente el ámbito de nuestra propia soledad, nace como consecuencia de los derechos del hombre y del ciudadano como un derecho de protección vinculado básicamente a las injerencias arbitrarias a su vida privada, familia, domicilio y correspondencia.

La esfera de intimidad de la persona reconoce por una parte, una proyección hacia el exterior del individuo que conduce a la protección de valores como la inviolabilidad del domicilio, de la correspondencia, de la documentación personal, y en general de las comunicaciones privadas, dentro de las cuales debe entenderse un cuidado extensivo a bienes materiales pertenecientes a la persona; de otra parte, existe una proyección hacia el interior del ser humano que se traduce en la protección de bienes propiamente inmateriales como lo son el honor, la honra, la propia imagen.

Eduardo Novoa Monreal define al derecho a la intimidad como: "*un sector personal reservado a fin de hacer inaccesible al publico, sin voluntad del interesado, eso que constituye lo esencial de la personalidad*"[15].

Por lo que definimos que la intimidad, es la parte reservada o más particular de los pensamientos, afectos o asuntos interiores de una persona, familia colectividad, es fácil deducir que a esa información, solo tendremos acceso con la autorización de su titular por el valor moral, social, político o de otro tipo que guarda determinada información.

La intimidad constituye un bien personal al que no puede renunciar el individuo sin resentirse en su dignidad humana; el ser humano es social por naturaleza, pese a ello no deja de sentir la necesidad de realizar una vida interior, ajena a las

[14] Rebollo Delgado, Lucrecio. El Derecho Fundamental a la Intimidad. Segunda Edición Actualizada, Ed. Dykinson, S.L. Madrid, 2005

[15] Novoa Monreal Eduardo, "Derecho a la Vida Privada y la Libertad de Información", 5ta Edición Siglo Veintiuno Argentina Editores, 1997

relaciones que mantiene con otros individuos, y que le permite identificarse como ser humano.

El derecho a la intimidad es un derecho fundamental reconocido dentro de los derechos humanos, asimismo por la Constitución Política del Estado, Código Civil, y Código Penal en nuestro país.

> Art. 18 Código Civil **Nadie puede perturbar ni divulgar la vida intima de una persona. Se tendrá en cuenta la condición de ella. Se salvan los casos previstos por ley.**

Requisitos

1) Perturbación de la intimidad.

2) Arbitrariedad de la perturbación, pues este derecho está limitado por los intereses públicos, y así no sería arbitraria, por ejemplo:

a) la reproducción de fotos criminales;
b) la investigación de hombres públicos, por tratarse de sucesos de repercusión social donde juega también la libertad de informar;
c) cuando lo piden las propias personas o prestan su consentimiento a la intromisión;
d) el control de la intimidad de los incapaces por sus padres o curadores;

3) En los juicios de divorcio invocar y probar el adulterio del cónyuge.

4) Que el hecho no sea un delito penal.

La afectación al Derecho a la Intimidad de fisgoneo de lugares privados como; vigilancia electrónica intervención de teléfonos, grabadores en recintos privados.

La protección jurídica del derecho al honor, a la intimidad y a la propia imagen, está regulada en el Derecho Internacional, como podemos apreciar en las siguientes declaraciones: Declaración Universal de Derechos Humanos, aprobada en Nueva York el 10 de diciembre de 1948 por la Organización de las Naciones Unidas, como lo expresa en su artículo 12: *"nadie será*

objeto de injerencia arbitraria en su vida privada, su familia, su domicilio o correspondencia, ni de ataques a su honra ni a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". **Esta Declaración es una muestra de protección universal de estos derechos, protege ante vulneraciones y lesiones a los derechos inherentes a la personalidad en la esfera moral, existiendo la igualdad ante la ley, pues se le reconoce a toda persona el derecho a recibir protección jurídica.**

La Declaración Americana de los Derechos y Deberes del Hombre, aprobada en la Novena Conferencia Internacional Americana en Bogotá, Colombia; expresa en su artículo 5: *"Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar."* En este precepto se alude al derecho que poseen las personas de proteger su honor, su intimidad y privacidad. En dicha Declaración se preceptúa en su artículo 9: "Toda persona tiene derecho a la inviolabilidad de su domicilio y en el artículo 10: *"Toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia"*. Los derechos preceptuados son manifestaciones del derecho a la intimidad.

1.4 DERECHOS FUNDAMENTALES

Es frecuente el uso indistinto de la expresión derechos humanos y derechos fundamentales; por lo que es necesario diferenciarlos de la siguiente manera:

EL Dr. Willman Duran Ribera, nos dice que: *"una vez que los derechos humanos, se positivizan, adquieren la categoría de verdaderos derechos protegidos procesalmente y pasan a ser derechos fundamentales, en un determinado ordenamiento jurídico; o lo que es lo mismo: los derechos fundamentales son derechos humanos positivados"*[16].

Por lo que, podemos definir que los derechos fundamentales, son el conjunto de derechos subjetivos y garantías reconocidos en la Constitución como propios de las personas y que tienen como finalidad prioritaria garantizar la dignidad de la persona, la libertad, la igualdad, la participación política y social, el pluralismo o cualquier otro

[16] Duran Ribera Willman "Los Derechos Fundamentales como contenido esencial del estado de derecho", [en línea]: http://www.tribunalconstitucional.gov.bo/search_res.html, [consulta: 06/11/08]

aspecto fundamental que afecte al desarrollo integral de la persona en una comunidad de hombres libres. El titular del derecho tiene la facultad de exigir su respeto y observancia, pudiendo acudir para ello al órgano jurisdiccional competente para reclamar, a través de los recursos que establece el respectivo orden jurídico, la protección de tales derechos y su reparación del daño sufrido; se designa a los derechos garantizados por la Constitución y que en cambio, la denominación derechos humanos, hace referencia a derechos garantizados por normas internacionales.

Los derechos fundamentales tienen como fuente de creación al legislador constituyente y los derechos humanos, a los Estados y organismos internacionales. El Dr. Wiliam Duran Ribera en su articulo titulado los Derechos Fundamentales como contenido esencial del estado de derecho hace referencia a Luigi Ferrajoli, que conceptualiza como derechos fundamentales a "*todos aquellos derechos subjetivos que corresponden universalmente a todos lo seres humanos dotados del status de personas,; entendiendo por derecho subjetivo cualquier expectativa positiva (de prestaciones) o negativa (de no sufrir lesiones)adscrita a un sujeto por una norma jurídica...* "[17]

1.4.1. GARANTÍAS DE LOS DERECHOS FUNDAMENTALES

Los derechos fundamentales son y valen lo que valen sus garantías; si no existe un sistema, un conjunto de instrumentos de protección de los derechos fundamentales que sean eficientes, encargados a órganos independientes e imparciales, las declaraciones de derechos son pura retórica, son declaraciones de buenas intenciones.[18]

La Declaración de Derechos del Hombre y del Ciudadano de 1789 en el Art. 16 dice "*toda sociedad en la cual la garantía de los derechos no esté asegurada no existe Constitución, porque sin garantía los derechos fundamentales nos son derechos*"[19], sin garantías eficaces no existe derecho.

Los principales rasgos de este sistema de garantías son[20]:

---

[17] Duran Ribera Willman "Los Derechos Fundamentales como contenido esencial del estado de derecho", [en línea]: http://www.tribunalconstitucional.gov.bo/search_res.html, [consulta: 06/11/08]

[18] Fundación de Derechos Humanos, "Declaración Americana de los Derechos y Deberes del Hombre", Serie Cuadernos Divulgativos. Fundación Sánchez Editores. Caracas, 1993.

[19] Conferencia Internacional Americana, Ix,"Declaración Americana de los Derechos y Deberes del Hombre", Bogotá, Mayo de 1948

[20] Conferencia Internacional Americana, Ix,"Declaración Americana de los Derechos y Deberes del Hombre", Bogotá, Mayo de 1948

1) El sistema garantiza la vinculación de los derechos fundamentales frente a todos los poderes públicos y en menor medida en las relaciones entre particulares, esto se concreta en la aplicación directa de la Constitución.
2) Un segundo rasgo es que es un sistema que no deja resquicios, no deja entrada a la impunidad del poder; esto quiere decir que cabe reaccionar frente a cualquier hecho lesivo de los derechos fundamentales, cualquiera que sea el productor del mismo. No existen esferas de inmunidad.
3) Es un sistema que establece pluralidad de procedimientos y órganos de garantía sin olvidar que los cimientos del sistema están asentados en la tutela judicial efectiva y en los órganos jurisdiccionales.

1.4.2 JURISDICCIÓN

Según el diccionario Enciclopédico de derecho usual la jurisdicción es "la función del Estado que tiene por fin la actuación de la voluntad concreta de la ley mediante la substitución de la actividad individual por la de los órganos públicos, sea para afirmar la existencia de una actividad legal, sea para ejecutarla ulteriormente" [21]

Por su parte Eduardo Garcia nos dice que la jurisdicción es *"la función pública realizada por órgano competente del Estado, con las formas requeridas por ley, en*

virtud del cual. Por acto de juicio y la participación de sujetos procesales, se determina el derecho de partes, con el objeto de dirimir sus conflictos de relevancia jurídica, mediante decisiones con autoridad de cosa juzgada, eventualmente factibles de ejecución" [22]

Por lo que, concluimos que jurisdicción es la potestad encargada a un órgano estatal, el Poder Judicial y al encomendar al Poder Judicial esa actividad privativa del Estado emerge la Potestad Jurisdiccional, no es mas que la cesión al Poder Judicial, a través de la ley de organización judicial, del deber de realizar esa actividad jurisdiccional; es decir, de imponer la norma jurídica para resolver un conflicto particular cuyo objetivo final es lograr la convivencia jurídica o restaurar el orden quebrantado.

Uno de los principales rasgos de la potestad jurisdiccional es su carácter irrevocable y definitivo, capaz de producir en la actuación del derecho lo que técnicamente se denomina cosa juzgada.

---

[21] Cabanellas, Guillermo, Diccionario Enciclopédico de Derecho Usual, Buenos Aires, Argentina, Editorial Heliasta, 1996,
[22] García Maynez Eduardo, Filosofía Del Derecho, Ed. Porrúa, 1999

En sentido coloquial, la palabra "jurisdicción" es utilizada para designar el territorio (estado, provincia, municipio, región, país, etc.) sobre el cual esta potestad es ejercida. Del mismo modo, por extensión, es utilizada para designar el área geográfica de ejercicio de las atribuciones y facultades de una autoridad o las materias que se encuentran dentro de su competencia; y, en general, para designar el territorio sobre el cual un Estado ejerce su soberanía.

1.5. DERECHOS HUMANOS

No podemos olvidar que el derecho a la intimidad esta reconocido como un derecho humano; por lo que es preciso que desentrañemos su concepto y sus características.

El Dr. Willman Duran define como derechos humanos: *"al conjunto de derechos de que gozan las personas y que no pueden ser restringidos ni violados, esencialmente, por los gobernantes"*.[23]

En su primer desarrollo los derechos humanos fueron denominados "derechos individuales" "derechos fundamentales","libertades individuales",etc. Esto por que los derechos de los individuos se los consideraba aisladamente. Posteriormente fue necesario observar determinados derechos que el individuo tenía en tanto sujeto social que forma categorías o grupos. Allí surgieron los derechos sociales. Por ese motivo, la denominación "derechos individuales" no abarcaba al conjunto ahora considerado.

1.5.1 CARACTERÍSTICAS DE LOS DERECHOS HUMANOS

Entre las características de los derechos humanos tenemos:

***La universalidad** de los derechos humanos que surgió ya en la Edad Moderna, superados algunas desigualdades de la Edad Media, con las Revoluciones Americana y Francesa y con el posterior desarrollo del derecho constitucional en América Latina durante el siglo XIX y en Europa en el siglo XX. El carácter universal de los derechos humanos alcanza su mayor apogeo luego de la creación de las Naciones*

[23] Duran Ribera Willman "Los Derechos Fundamentales como contenido esencial del estado de derecho", [en línea]: http://www.tribunalconstitucional.gov.bo/search_res.html, [consulta: 06/11/08]

Unidas y la adopción de la Declaración Universal de los Derechos Humanos al culminar la segunda Guerra Mundial.
Kofi Annan, Secretario General de la ONU subraya a este respecto: "Los derechos humanos son la base de la existencia humana y de la coexistencia y son universales, indivisibles e interdependientes. Los derechos humanos son los que nos hacen humanos. Son los principios con los cuales creamos la morada sagrada de la dignidad humana. [24]

Imperatividad *de los derechos humanos, es decir, que son universalmente obligatorios para todos (erga omnes), bajo cualquier punto de vista e* incluso en aquellos casos en que no haya sanción expresa ante su incumplimiento, nos lleva a retomar el debate entre el carácter absoluto y relativo de los derechos humanos.

Se ha concluido ya que aún cuando no haya un consenso total sobre el tema,

existen ciertos derechos que gozarían de cierta **absolutidad** y que no podrían ser suspendidos bajo ninguna circunstancia, como el derecho a la vida, la integridad física y moral de las personas, la prohibición de la esclavitud y servidumbre, las normas del debido proceso, y la libertad de pensamiento, de conciencia y de religión. Es decir, son aquellas normas que estarían en el marco del ius cogens, que no son susceptibles de derogación bajo ninguna circunstancia.

Los complejos fenómenos que enfrenta actualmente la humanidad, particularmente en lo que respecta al incremento de la pobreza, de los conflictos internos, la xenofobia y las prácticas de racismo y otras formas de intolerancia, hacen vislumbrar que la humanidad deberá asumir una evolución cada vez más vertiginosa de los derechos humanos y de su adecuado cumplimiento.

1.5.2. NATURALEZA DE LOS DERECHOS HUMANOS

Las declaraciones de derechos humanos, sean ellas universales, regionales o internacionales o internas de un país determinado, tienen el carácter de un postulado básico de convivencia social que se

[24] Kofi Anna, Mensaje en el Cincuentenario de La Declaración Universal de los Derechos Comisión Internacional de Juristas, Edición Especial, 1968

propone como premisa política de una vida en sociedad. Su origen es una concepción política de lo que debe ser una comunidad humana que sea grata al hombre y respetuosa de su dignidad, se vincula a ideas de justicia y ética.

Por si mismas no tienen efecto normativo ni valen para imponer a un estado determinado el reconocimiento o el respeto de los derechos de quienes viven en su territorio; en cambio, desde el momento en que su contenido se vacía dentro de la legislación positiva de un estado, adquieren un carácter jurídico y pasan a integrar la legislación positiva de un estado; con ello, los derechos humanos se convierten en instituciones jurídicas, conforme al alcance que el texto legal les consigne.

Generalmente los derechos humanos se incorporan a las constituciones políticas de los diversos países y dentro de ellas se transforman en limitaciones que la carta fundamental pone a las atribuciones de los poderes públicos y en especial del poder legislativo. Esto significa que las leyes o las ordenes de autoridades de ese estado habrán de respetar el marco inviolable de la constitución asigna a
estos derechos.

Los textos constitucionales sobre reconocimiento de derechos del hombre tienen por principal finalidad amparar a los ciudadanos contra excesos o arbitrariedades de la autoridad o de los poderes públicos, empero, para que tales reglas constitucionales impongan también el deber jurídico dictado por el mas alto nivel normativo, para que todos los hombres respeten esos derechos.

Ella opera cuando un estado celebra un pacto o un tratado jurídicamente vinculante con otro o con otros estados, en los que se reconozca obligado a respetar esos derechos.

1.5.3. GENERACIONES

Las generaciones de los derechos fundamentales responden al devenir histórico de los pueblos y a los cambios culturales propios de las transformaciones sociales emanadas de la evolución a nivel político, social, económico y hasta tecnológico: Existen 4 generaciones que son las siguientes[25]:

1. Derechos de primera generación: son los derechos civiles y políticos, estos derechos se distinguen pues su titularidad y ejercicio no es colectivo sino que suele ser individual y por ende derivados de la persona humana de forma directa en virtud de su condición, por lo que reciben el nombre originario de derechos humanos.
Dentro de la gama de derechos podemos citar los siguientes: igualdad, dignidad, libertad, vida (integridad física, psíquica y moral), seguridad personal, derecho a la no tortura o tratos degradantes, la no esclavitud, la justicia, la personalidad jurídica, el derecho a no ser arrestado arbitrariamente defendido por el recurso de habeas corpus defensa y principios que componen el debido proceso, presunción de inocencia, intimidad y privacidad, honor, imagen, integridad moral, libertad de circulación, libertad de domicilio, asilo, nacionalidad, matrimonio y familia, propiedad privada, pensamiento, conciencia, religión, libertad de opinión, libertad de expresión, reunión y asociación y participación política a través del sufragio.

2. Derechos de segunda generación: son derechos sociales, económicos y culturales, son derechos modernos cuyo ejercicio es individual pero la titularidad no sólo puede ser individual pero también colectiva al tratarse además de libertades positivas que reclaman una acción pública o Estatal para su defensa. Efectivamente si los derechos de primera generación procuraban proteger al individuo frente al poder estatal, en la segunda generación se evoluciona hacia una exigencia del estado de garantizar la protección de los bienes sociales que amparan al individuo. Entre estos derechos podemos citar el derecho al trabajo, el derecho a la equidad, la dignidad, la seguridad e higiene, el derecho a la asociación sindical, el derecho a la protección de madres y menores trabajadores, la garantía de la igualdad laboral y la solidaridad humana, derecho a la seguridad social, derecho a la salud, derecho a la educación y el derecho a la cultura, al arte y la ciencia.

[25] Castro Bonilla, Alejandra, [en línea] Derechos Fundamentales, http://www.hacienda.go.cr/centro/datos/Articulo/Los%20Derechos%20Fundamentales%20en%20Internet.doc, [consulta: 06/11/08]

3. Derechos de tercera generación: son derechos colectivos de los pueblos, dentro de esta generación de derechos, que en su mayoría aún están siendo codificados, se pretenden proteger derechos o bienes comunes de los pueblos.

Se suelen denominar también derechos de la solidaridad y se han defendido por presión política y discursos ideológicos que defienden y agrupan derechos colectivos y de los pueblos. Esta categoría los conforman el derecho al orden internacional apto para el desarrollo de los derechos humanos, el derecho a la libre determinación de los pueblos y la disposición de sus riquezas, el derecho de las minorías, el derecho de los migrantes, el derecho al medio ambiente sano y el derecho de los apátridas.

Se citan como calificación de esta categoría, aunque en muchos países por situaciones políticas, sociales o económicas, aún no han sido reconocidos de forma expresa, pese a que existe la convicción de su categoría como derechos humanos, el derecho al medio ambiente, a la cultura, al ocio, a la paz, a la regulación de la informática, etc., son algunos de los derechos que el hombre moderno considera indispensables para una vida digna en nuestros días.[26]

4. Derechos de cuarta generación: son derechos de la sociedad del conocimiento, son en realidad los nuevos derechos de futuras generaciones, derivados de la revolución tecnológica a los que denomina Derechos en la Sociedad del Conocimiento.

Estamos ante una nueva sociedad de cambios; en el ámbito político internacional, el orden cosmopolita al que alude, ha logrado introducir innovaciones que obligan a las sociedades a adoptar nuevas medidas para la convivencia mundial a través incluso de la ampliación de los límites de la acción internacional; los problemas del mundo ya no afectan a un sector de la sociedad sino que nos afectan a todos, e incluso la amenaza de la guerra se ha globalizado.

1.5.4 LOS DERECHOS HUMANOS Y LAS NUEVAS TECNOLOGÍAS

En el plano de los derechos humanos, las nuevas Tecnologías de la Información y la Comunicación (TIC) han introducido amenazas comunes que obligan a la ampliación de la protección de los derechos del ser humano, la interacción entre la

[26] De Esteban, Jorge y Pedro González-Trevijano. Curso de Derecho Constitucional Español I. Primera edición, Servicio de publicaciones de la Facultad de Derecho, Universidad Complutense de Madrid, Madrid, 1992

comunicación y la telemática en esta nueva era, ha posibilitado un mundo de información en tiempo real, de transmisión masiva y asimilación simultánea de esa información. Esta dinámica ha generado cambios en el plano jurídico, social y político que exigen respuestas universales y no aisladas.

La invención de nuevas tecnologías ha introducido medios de comunicación inéditos cuya implementación pone en incompatibilidad la aplicación de la legislación que antes era utilizada para el mundo analógico, en lo que respecta a la protección de derechos como la intimidad personal, la inviolabilidad de las comunicaciones y el derecho de la propiedad intelectual, entre otros.

La Declaración Universal de Derechos Humanos del Ciberespacio,[27] escrita por Robert Gelman el 12 de noviembre de 1997 sostiene la existencia de nuevos derechos humanos a raíz de la existencia de una sociedad que ya no se basa en bienes privados de propiedad sino que el bien es la información.

Existe una nueva pretensión internacional que apoya por la protección y defensa de derechos humanos que puedan verse menoscabados ante el desarrollo tecnológico.

Dentro de esta gama de derechos podríamos citar el derecho de acceso a la informática, el derecho a acceder al espacio que supone la nueva sociedad de la información en condiciones de igualdad y de no discriminación, el derecho a acceder a la línea o punto de conexión (línea, satélite, cable...), el derecho de acceder a hardware o equipo físico, el derecho de acceder a un Software (condiciones técnicas que derecho a gozar de educación, información y cultura, el derecho a la autodeterminación informativa (en la manipulación de los datos personales, intimidad e imagen en el ciberespacio), el derecho al Habeas Data, el derecho a la limitación del uso de la informática para garantizar los derechos fundamentales y la seguridad digital (en defensa de bienes personales, morales y patrimoniales); asimismo la defensa contra el terrorismo digital o informático (desde la actividad de hackers, crackers, hasta la utilización de nuevas formas de invasión de la persona a través de la informática).

Luis Otero nos dice que el desarrollo de las nuevas tecnologías de la información vinculadas a la revolución de las telecomunicaciones del último tercio del siglo XX,

[27] Gelman, Robert. La Declaración Universal de Derechos Humanos del Ciberespacio. http://www.arnal.es/free/info/declaracion/html

en el que Internet, ha generado importantes reflexiones sobre el alcance de dichos cambios y sobre el respeto y salvaguardia de los derechos humanos.[28]

En términos generales, lo que se denomina la sociedad de la información está caracterizada, entre otros factores, por la aparición de una serie de medios técnicos de transmisión y de información que provocan numerosos efectos sobre el comportamiento individual y colectivo y sobre la formación de hábitos culturales.

Además, tras este fenómeno se esconden también otros factores de influencia generalizada, como su papel democratizador, la relevancia creciente de la tecnología y del lenguaje, o la función social de la formación en el mundo moderno[29].

Este cambio señala que el interesado posee la autodeterminación informativa como una facultad para el resguardo del derecho a la intimidad, haciendo especial hincapié en la necesidad de evitar la elaboración de un perfil de la persona a partir de la interacción de archivos que resguardan distintos datos personales del individuo; por tanto, el concepto de derecho a la intimidad ha sufrido una importante variante, pues evoluciona de ser un simple derecho de exclusión en el que el individuo reafirmaba su derecho a la privacidad o "derecho a estar solo" para adquirir una nueva dimensión como derecho facultativo que le permite ejercer acciones en defensa de su vida privada.

Otro derecho que adquiere más que un nuevo cambio de acción, una variante sustancial y de fondo, es el derecho a la seguridad. Este derecho en el marco de las TIC se denomina seguridad digital y surge como un principio de la nueva sociedad de la información que permite el resguardo preventivo de los bienes propiedad de los agentes (individuales o colectivos) que intervienen en la convergencia de las tecnologías y los medios de comunicación, y que puedan verse vulnerados con los avances tecnológicos.

Por ejemplo, hablamos de tomar medidas para evitar la irrupción de hackers y crackers o de terrorismo digital en los sistemas informáticos del Estado o de un usuario individual, evitar la alteración o eliminación de documentos públicos por parte de terceros a través de la informática o bien la violación de la correspondencia privada constante en un correo electrónico adscrito como cuenta de un servidor

---

[28] Otero Carvajal, Luis Enrique. Derechos Humanos y sociedad de la información. Nuevas formas de acción social. En http://www.ucm.es.../la%20sociedad%20informacional%20y%20los%20derechos%20humanos.html

[29] Escobar de la Serna, Luis. Sociedad, Información y Constitución. XX Aniversario de la Constitución. Editorial Universitas S. A., Madrid, 1999

privado, y hasta la suplantación de la personalidad en materia de comercio electrónico.

La seguridad digital puede proteger la información que se resguarda en formato digital ya sea en línea (en la Web) o en ordenadores públicos o privados, mediante mecanismos técnicos y normas de seguridad empresariales o institucionales que protejan los bienes y la información sensible o en trámite; elevar este derecho a la categoría de un derecho fundamental, le permite al individuo recibir las facilidades de acceso a sistemas de protección derivados de la propia tecnología, en una época en la cual la tecnología está condicionando al derecho.

CAPITULO II

INFORMÁTICA Y DATOS PERSONALES

2.1 DEFINICIÓN DE DERECHO INFORMÁTICO

Julio Téllez define al derecho informático como: *"el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informatica*[30]*"*.

Por otra parte Delpiazzo, nos dice que pueden distinguirse en ese término, dos acepciones: "*el Derecho Informático como una rama del Derecho integrada por las normas y principios que se refieren a la actividad informática y por otro, una ciencia que tiene por objeto el estudio del sector jurídico"*[31].

Por lo que, podemos definir como derecho informático, al conjunto de normas jurídicas que regulan las acciones, procesos, productos y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones, tiene por objeto la información.

2.2 INFORMÁTICA E INTIMIDAD

La magia que brindan las nuevas tecnologías de la información, también presentan costados obscuros, como cuando representan un riesgo para la intimidad.

Gilberto Alcala establece cuatro categorías a) una invasión a la zona de privacidad, b) la difusión de hechos privados embarazosos, c) una publicidad que coloque a la persona en falsas posiciones ante los ojos de los ciudadanos y d) indebida apropiación del nombre o apariencia de una persona[32].

Por otro lado, el avance de la tecnología ha hecho posible la existencia eficiente de bancos de datos, antes existían pero sus alcances eran limitados; en uno de los aspectos más específicos, alude a las centrales de riesgo crediticio, desde que nació la informática y el almacenaje y procesamiento de datos, comenzó la preocupación sobre su uso. Algunas legislaciones se ocuparon y llegaron a la distinción en lo que se denominaron datos sensibles de una persona, la posibilidad de registrar un sin fin de datos personales, permite reconstruir hasta los detalles más recónditos de la vida.

---

[30] Tellez Valdes Julio, Derecho Informatico, Ed. Mc. Graw Hill, México, D.F. 1996

[31] Delpiazzo, Carlos, E, "Protección De Los Datos Personales en los Tiempos de Internet, El Nuevo Rostro de la Intimidad",

[32] Alcala, Gilberto, "Proyecto de Ley Sobre la Vida Privada y su Incidencia en el Derecho a la Información"

Linch afirma que un ciudadano estadounidense genera diariamente 150 registros digitales[33]; si se repara en que éstos almacenan tales contactos y todos ellos podrían concentrarse en una base de datos, a partir de allí es factible conocer hasta los detalles más recónditos de la vida de la persona; siempre han existido datos aunque no en la cantidad y calidad que ahora y la posibilidad teórica de reunirlos.

Pero la informática ha permitido el salto potencial de acceder casi de inmediato a todos esos datos, clasificarlos, ordenados, permite también formular programas de interpretación de tales datos; a partir de allí la vida del usuario queda expuesta. Aproximadamente en los años '60 la atención se centró en el uso de la información personal y se fue expandiendo contemporáneamente con la proliferación de las computadoras. En los últimos años se ha producido una espiral de utilización de información personal que se consolida con la difusión de internet; esto significa el acceso de millones de personas, que hoy se estiman en más de 50 millones, en un mismo espacio virtual y así se multiplican las posibilidades de invasión a la intimidad en el Internet.

La utilización exponencial de medios digitales multiplica obviamente la información almacenada y las bases de datos; por lo que genera una nueva masa de información personal expuesta al público; cuando las bases de datos eran pocas o cuando se generaban deliberadamente, era más fácil controlarlas. La Internet agrega elementos delusorios de la intimidad: es que si tendrá tanta incidencia en la vida de las personas, y bajos índices de seguridad, la vida de la persona quedará más expuesta que antes.

La simple selección de temas de información preferidos, puede brindar información de sumo interés; como las consultas médicas, los tipos de estudios realizados, permiten elaborar un perfil ideológico, sanitario o intelectual de cada persona, el desafío es mejorar la seguridad de la utilización de los datos personales.

Los estudios sobre la interferencia de la informática en la intimidad no son nuevos, pues ya tienen más de dos décadas; sin embargo, el ingreso en la Era Digital provoco una explosión del problema, el principal medio Internet y una sus funciones como el correo electrónico tiene serios problemas de seguridad en la protección de datos personales en nuestro país.

En tanto comienzan a intercambiar datos más de 50 millones de usuarios dispersos en el mundo, proliferan los mercados electrónicos, las publicaciones en línea, los

[33] Lynch, Horacio María, Notas sobre el derecho en la Era Digital, En La Ley, Año Lx, Nro 93, 15/Mayo/96

requerimientos de información, los requerimientos de servicios, la actividad del teletrabajo, las interconsultas médicas, las video conferencia, los mensajes personales enviados y recibidos, abre un amplio campo de riesgo para la intimidad. Es necesario una mayor protección de la intimidad, un agravamiento y ampliación de las figuras protectoras, mayores exigencias de seguridad para quienes almacenan los datos personales.

2.3 DATOS PERSONALES

Rubén Flores Nos dice que: *"dato personal, es la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables"* [34].

La Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre, en su artículo 2°, letra b) los define como: toda información sobre una persona física identificada o identificable. Se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social".

En cuanto a las personas jurídicas, no rige respecto de ellas el concepto de privacidad de sus datos personales, por lo que sus datos podrán ser siempre conocidos, por primacía del derecho a la información, sin perjuicio de lo relativo al secreto comercial o industrial, o lo referente a los derechos autorales o industriales respectivos.

Por lo expuesto dato personal, es toda información que permitiere la identificación directa o indirecta de las personas a las cuales se emplean, es información de una persona como el nombre, sexo, nacionalidad, domicilio, estado civil, atención médica, número de afiliado a la seguridad social, voz, fotografía, huella digital, número de placa de vehículos, números de nuestros teléfonos fijo o celular y otros.

[34] Flores Dapkevicius, Ruben : Amparo, Hábeas Corpus, Hábeas Data, Editorial B De F, Buenos Aires 2004

2.3.1 DATOS SENSIBLES

Para Eduardo Novoa se consideran como datos sensibles *"*los antecedentes policiales, datos de salud, información de seguridad nacional, creencia religiosa y comportamiento sexual, información financiera"[35].

Horacio V. Lynch, nos dice que: "los llamados datos sensibles, afectan con particular incidencia la esfera personal del individuo, desde que la sumatoria de datos sensibles se puede revelar, inclinaciones o tendencias"[36].

Por lo que, podemos definir como datos sensibles, los que revelan origen racial y étnico, opiniones políticas, convicciones religiosas filosóficas o morales, afiliación sindical e información referente a la salud o vida sexual, padecer determinada enfermedad; por ello las personas no están obligadas a informarlos.

La simple idea que el entrecruzamiento de datos genera nueva información, esta idea es básica para entender el problema, si se cruza información sobre determinados actos mecánicamente cumplidos por una persona, es posible que de tales datos se deduzcan tendencias o inclinaciones ignoradas hasta por el propio actor de los actos. Como norma general los datos de ideología, creencias, religión o afiliación sindical no pueden ser tratados ni almacenados en ficheros, sólo pueden ser objeto de tratamiento con el consentimiento expreso y por escrito del afectado. Los datos sensibles pueden ser objeto de tratamiento, si resulta necesario para la prevención o para el diagnóstico médicos, para la prestación de asistencia sanitaria o de un tratamiento médico o para la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario[37].

2.3.2 DATOS PÚBLICOS

Alberto Arteaga nos dice que: *"los datos públicos son aquellos datos que no tienen mayor trascendencia y que son de fácil obtención, es decir que se encuentran casi*

---

[35] Eduardo Novoa Monreal, "Derecho a la vida Privada y la Libertad de Información", Siglo Veintiuno Editores, Quinta Edición, 1997

[36] V. Lynch, Horacio María, Notas Sobre El Derecho en la era digital, En La Ley, Año Lx, Nro 93, 15/Mayo/96.

[37] Piñar Mañas, José Luis, Protección de datos personales, [en línea]: http://74.125.93.132/search?q=cache:rgPkBQAZoaEJ:www.agpd.es/upload/FOLLETO.PDF+derecho+a+la+proteccion+de+datos+personales&cd=37&hl=es&ct=clnk&gl=bo, [consulta: 26/01/09]

a disposición de todos como por ejemplo: nombre, domicilio, numero de cedula de identidad, etc"[38].

Veamos un ejemplo la existencia de personas que, por las responsabilidades que ejercen tienen derecho a una protección mayor que el resto de las personas si, por ejemplo, un juez tiene que tener su vida privada más reservada que una persona sin similares responsabilidades. Hemos puesto el ejemplo de un magistrado porque entonces en su caso se advierte hasta qué punto puede verse cuestionada o deteriorada una investidura si sus acciones privadas quedan expuestas a la consideración de los litigantes y abogados.

2.4 TITULARIDAD DE LOS DATOS PERSONALES

Maria Linch nos dice que *"la titularidad de los datos corresponde a quien pertenece la información, entonces el titular de la información para defender esa facultad de dar o no a conocer tales datos"*[39]

Por lo que, podemos definir que los titulares de los datos personales, es de quien pertenece la información. Tiene ciertos derechos nombraremos los siguientes:

Acceso a los datos propios, esta es la facultad que tiene el individuo de saber acerca de sus datos registrados en una base de datos o archivos y la utilización que se les puede dar; de este derecho prácticamente se desprenden los demás respecto de la titularidad de la información frente a la administración de la misma.

Corrección y actualización de la información, al tener el individuo el derecho de acceder a su información, también tiene el derecho de rectificar la veracidad de los datos y en su caso exigir la corrección, así como la actualización de tales datos.

Confidencialidad y exclusión, en algunas bases de datos se registran datos "sensibles" o información reservada, tratándose de este tipo de registros el titular tiene todo el derecho de exigir al administrador de los comunicados la mas estricta confidencialidad en relación con sus datos y en caso de transgredir esta facultad, el titular tiene el poder jurídico suficiente para exigir la exclusión de su información de

[38] Arteaga Sanchez, Alberto,"La Intercepción, interrupción, impedimento o Revelación de comunicaciones privadas ajenas"
[39] V. Lynch, Horacio María, Notas Sobre El Derecho en la era Digital, En La Ley, Año Lx, Nro 93, 15/Mayo/96.

la base de datos o archivo respectivo, independientemente de la acción judicial que tendrá por los perjuicios que le cause la revelación de su información “sensible”.

2.5 TRANSFERENCIA INTERNACIONAL DE DATOS

La transferencia internacional de datos personales de un Estado a otro se ven seriamente amenazados, si no se establece un control que marque límites de garantía y seguridad en la transmisión telemática o en la transferencia de los datos personales cruzando fronteras; por ello, la regulación de los límites a la transferencia de datos se encuentra, en el origen de las normas nacionales e internacionales reguladoras de la protección de datos.

Las normas internacionales que regulan la materia tienen por objeto establecer un núcleo básico de principios de protección de datos, que permita considerar uniforme el régimen aplicable en los Estados signatarios, permitiendo así el flujo de información hacia los mismos e impidiendo su transmisión a quienes no cumplan esos principios.[40]

2.6. RED IBEROAMERICANA DE PROTECCIÓN DE DATOS

El habeas data es un recurso constitucional que defiende la autodeterminación informativa del ciudadano y es prácticamente un desarrollo que se ha dado tan solo en América Latina y el caribe. Este derecho constitucional presenta importantes avances en el tema de Habeas Data en la región, que permiten un acercamiento al tema de protección de los datos personales, pero falta una adecuada legislación de desarrollo constitucional en los diversos países, que clarifique el modo y empleo y los noveles de protección sobre los datos personales utilizando este instrumento constitucional.[41]

Gregorio Guamaduz, nos dice que la mayor influencia en la legislación de nuestra región en estos temas proviene de Europa, en concreto de las normativas y políticas europeas sobre la Protección de Datos Personales, debemos señalar que la existencia de la Red Iberoamericana de Protección de Datos es parte de la política de incidencia en un desarrollo armónico de legislación en temas de protección de datos siguiendo la línea de europea.

---

[40] Piñar Mañas, José Luis “Protección de datos personales”, [en línea]: http://74.125.93.132/search?q=cache:rgPkBQAZoaEJ:www.agpd.es/upload/FOLLETO.PDF+derecho+a+la+proteccion+de+datos+personales&cd=37&hl=es&ct=clnk&gl=bo, [consulta: 26/01/09]

[41] Iriarte Ahon “Estado Situacional y perspectivas del derecho informatico en America Latina y el Caribe”CEPAL 2005

Un hito de suma importancia fue la Declaración en el II Encuentro Iberoamericano de protección de Datos de Cartagena de Indias y la Declaración de Santa cruz de la Sierra, Bolivia en la XII Cumbre Iberoamericana de Jefes de Estado y Gobierno que dice:

"45.- Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la declaración de La Antigua por lo que se crea la Red Iberoamericana de protección de Datos, abierta a los países de nuestra Comunidad."

La Red Iberoamericana de Protección de Datos (RIPD), surge con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos (EIPD) celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003, con la asistencia de representantes de 14 países iberoamericanos.

LA RIPD se constituye como una respuesta a la necesidad de fomentar, mantener y fortalecer un estrecho y constante intercambio de información, experiencias y conocimientos entre los Países Iberoamericanos, a través del diálogo y colaboración en materia de protección de datos de carácter personal. La RIPD se encuentra abierta a todos los países iberoamericanos que deseen promover y ejecutar iniciativas y proyectos relacionados con esta materia; este organismo pretende crear un foro integrador que permita involucrar a diversos actores sociales, tanto del sector público como privado. [42]

La Declaración Final de la XIII Cumbre de Jefes de Estado y de Gobierno de los países iberoamericanos celebrada en la ciudad de Santa Cruz de la Sierra, Bolivia, 14 y 15 de noviembre de 2003, reconocieron el carácter de la protección de datos personales como Derecho Fundamental, así como de la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos.

En la actualidad la RIPD, busca el impulso e implantación del Derecho Fundamental a la Protección de Datos de Carácter Personal a través de las entidades con capacidad y competencias para instar a los gobiernos nacionales a que elaboren

[42] Fernando Argüello Téllez, , [en línea]: La protección de datos personales en un mundo global http://74.125.45.104/search?q=cache:HPp2ED5sbNAJ:www.apdcat.net/media/315.pdf+red+iberoamericana+de+protección+de+datos+personales&hl=es&ct=clnk&cd=18&gl=bo, [consulta: 26/01/09]

una regulación normativa en esta materia a efectos de lograr la obtención de la Declaración de Adecuación por parte de la Comisión Europea.

OBJETIVOS DE LA RIPD

Los objetivos de la red Iberoamericana de protección de datos son:[43]

a)Promover la cooperación interinstitucional y el diálogo entre actores claves para el desarrollo de iniciativas y políticas de protección de datos.

b)Promover políticas, tecnologías y metodologías que permitan garantizar el derecho fundamental a la protección de datos personales.

c)Brindar asistencia técnica y transferencia de conocimientos a los países iberoamericanos que así lo soliciten. Promover convenios con instituciones públicas o privadas que permitan el desarrollo y ejecución de proyectos de su interés.

d)Promover programas de capacitación, orientación e información a los ciudadanos de cada país, acerca de las políticas de uso y destino de sus datos personales, así como de los derechos que puede ejercer frente al manejo que se haga de sus datos personales.

Argentina

En el caso de Argentina, se trata del segundo país en aprobar una Ley de protección de datos personales en la Ley 25.326, luego de la ley chilena del año 1999. Desde el año 1994 la Constitución Federal contempla el habeas data (art. 43) y el Código Civil ampara la privacidad en sus diversas formas desde la reforma por ley 21.173 (art. 1.071 bis Código Civil). Además Argentina es signataria de numerosos tratados internacionales que tienen jerarquía constitucional en el ordenamiento interno y que amparan la privacidad e intimidad.

[43] Fernando Argüello Téllez, , [en línea]: La protección de datos personales en un mundo global http://74.125.45.104/search?q=cache:HPp2ED5sbNAJ:www.apdcat.net/media/315.pdf+red+iberoamericana+de+protec cion+de+datos+personales&hl=es&ct=clnk&cd=18&gl=bo, [consulta: 26/01/09]

Argentina es un país muy activo en materia de datos personales, con mucha discusión judicial y académica del tema; asimismo Argentina fue el único país latinoamericano aprobado por la UE.

Chile

La ley Chilena sobre protección de datos personales, N°19.628 del año 1999, fue redactada con la asesoría directa de grupos, gremios y empresas interesadas en asegurar el negocio que constituye el procesamiento de datos personales, lo que se sumó al desconocimiento de los parlamentarios que la impulsaron.

La ley Chilena adolece de aspectos orgánicos esenciales, como la existencia de un registro de bases de datos particulares, de un ente fiscalizador, de un procedimiento de reclamo administrativo y de sanciones eficaces. La norma ha transformado al hábeas data en una mera declaración de intenciones, ya que por la vía de las excepciones y por establecer como regla general una enorme libertad en materia de procesamiento de datos personales, se permite su "tratamiento" sin autorización de los titulares.

Se eliminó la obligación de que se informara una vez al año a los titulares de los datos sobre su procesamiento, con lo cual se permitió el anonimato que hoy cubre el tráfico indiscriminado de información nominativa.

Uruguay

El modelo uruguayo, esta constituido por los artículos 72 y 332 de la Constitución de la República (1967), que consagran los principios generales como fuente de derecho sus datos personales tienen medios de protección consagrados en su Carta Magna.

Además, en este país, existe expresa consagración normativa de la protección de datos personales en normas de alcance sectorial, que vienen a regular distintos aspectos que conciernen a la protección de datos personales y al derecho de acceso. Así podemos mencionar la consagración del secreto tributario y previsional, el secreto bancario, el secreto estadístico, el derecho de acceso a la información, el acceso por la autoridad impositiva a los datos que se encuentren en poder de órganos u organismos públicos estatales o no estatales para el control de los

tributos, la acción de amparo, la protección de los datos de identificación civil, la prohibición de cesión, venta, reproducción o entrega a terceros de información relativa al estado civil de las personas del Registro de Estado Civil; el registro de las personas que tienen la condición de deudor alimentario moroso, el carácter reservado de los datos personales de los menores y adolescentes, los datos médicos, la consagración de la libertad de pensamiento e información, el sector comercial, la acción de habeas data, la creación de un Registro de Empresas Infractoras a la normativa laboral en la órbita del Ministerio de Trabajo y Seguridad Social. El sistema uruguayo de protección de datos, aún sin contener una ley que ampare con carácter general la protección de los datos personales, pero posee varias leyes que protegen a los datos personales.

2.7. DELITOS INFORMÁTICOS Y DATOS PERSONALES

Junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, ha surgido una serie de comportamientos ilícitos denominados, de manera genérica, delitos informáticos.

El autor mexicano Julio Tellez Valdez señala que los delitos informáticos "*son actitudes ilícitas en que tienen a las computadoras como instrumento o fin, son conductas antijurídicas y culpables* "[44].

Rafael Fernández Calvo define al delito Informático como *"cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito Informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin*"[45]

Por lo que podemos definir que, los delitos informáticos, son cualquier comportamiento criminal en que la computadora está involucrada como material u objeto; es toda acción u omisión culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima.

[44] Tellez Valdes Julio, Derecho Informático, Ed. Mc. Graw Hill, México, D.F. 1996
[45] Fernandez Calvo Rafael, "El Tratamiento del llamado delito Informático, Revista Iberoamericana de Derecho Informático, 155n1136, Nro 12, 1996

La informática esta hoy presente en casi todos los campos de la vida moderna; con mayor o menor rapidez todas las ramas del saber humano se generan ante los progresos tecnológicos, y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos realizaban manualmente. El progreso cada día más importante y sostenido de los sistemas de computación, permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de usuarios.

José Luis Castillo nos dice que *"las perspectivas de la informática no tienen limites previsibles y aumentan en forma vertiginosa. Las facilidades que pone a los usuarios, con rapidez y ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícito e ilícito, en donde es necesario que nuestra legislación regule los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social"*[46].

Esta marcha de las aplicaciones de la informática no sólo tiene un lado ventajoso sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración y la intimidad. La informatización se ha implantado en casi todos los países; tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente.

La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que no lleguen a descubrirse, se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

---

[46] Castillo Marcano, José Luis, "El Derecho a la Intimidad y la Protección de datos Personales en el Derecho Español": Boletín de la Academia de Ciencias Políticas y Sociales, Nº 134. Año Lxiv. Caracas, 1997

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos, la informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial estafas, apropiaciones indebidas, etc.

Proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

El delito Informático implica actividades criminales que un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, etc., sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho.

2.7.1. TIPOS DE DELITOS INFORMÁTICOS

Una de las clasificaciones de delitos informáticos es la siguiente:[47]

a) **Como instrumento o medio,** se tienen a las conductas criminales, que se valen de las computadoras como método, medio, o símbolo en la comisión del ilícito.

b) **Como fin u objetivo**, en ésta categoría se enmarcan las conductas criminales van dirigidas en contra de la computadora, accesorios o programas como entidad física.

2.7.2 REGULACIÓN DE OTROS PAÍSES

Los delitos informáticos son regulados en las diferentes legislaciones como veremos a continuación[48]:

España

En España, los delitos informáticos son un hecho sancionable insertas dentro su Código Penal en el que el delincuente utiliza, para su comisión, cualquier medio

[47] Alicia Chiaravalloti, [en línea]: http://www.chiaravalloti_asociados.dtj.com.ar/links_1.htm , [consulta: 26/01/09]
[48] Alicia Chiaravalloti, [en línea]: http://www.chiaravalloti_asociados.dtj.com.ar/links_1.htm , [consulta: 26/01/09]

informático, estos tienen la misma sanción que sus homólogos no informáticos, por ejemplo, se aplica la misma sanción para una intromisión en el correo electrónico que para una intromisión en el correo postal.

México

En México los delitos de revelación de secretos y acceso ilícito a sistemas y equipos de informática ya sea que estén protegidos por algún mecanismo de seguridad, se consideren propiedad del Estado o de las instituciones que integran el sistema financiero son hechos sancionables por el Código Penal federal en el titulo noveno capítulo I y II. El artículo 167 del Código Penal Federal sanciona con prisión y multa al que dolosamente o con fines de lucro, interrumpa o interfiera comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónicas o satelitales, por medio de las cuales se transmitan señales de audio,

de video o de datos.

Venezuela

Concibe como bien jurídico la protección de los sistemas informáticos que

contienen, procesan, resguardan y transmiten la información. Están contemplados en la Ley Especial contra los Delitos Informáticos, de 30 de octubre de 2001.

La ley tipifica los siguientes delitos:

- Contra los sistemas que utilizan tecnologías de información: acceso indebido (Art.6); sabotaje o daño a sistemas (Art.7); acceso indebido o sabotaje a sistemas protegidos (Art. 9); espionaje informático (Art. 11); falsificación de documentos (Art. 12).
- Contra la propiedad: hurto (Art. 13); fraude (Art. 14); obtención indebida de bienes o servicios (Art. 15); manejo fraudulento de tarjetas inteligentes o instrumentos análogos (Art. 16); apropiación de tarjetas inteligentes o instrumentos análogos (Art. 17); provisión indebida de bienes o servicios (Art. 18); posesión de equipo para falsificaciones (Art. 19);

- Contra la privacidad de las personas y de las comunicaciones: violación de la privacidad de la data o información de carácter personal (Art. 20); violación de la privacidad de las comunicaciones (Art. 21); revelación indebida de data o información de carácter personal (Art. 22);

Estados Unidos

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus informático, un gusano informático, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas, la nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona

que defraude a otro mediante la utilización de una computadora o red informática.

2.8. DELINCUENTE INFORMÁTICO

Para Julio Téllez es "*delincuente informático es la persona o grupo de personas que en forma asociada realizan actividades ilegales haciendo uso de las computadoras y en agravio de terceros, en forma local o a través de Internet*"[49].

Una de las prácticas más conocidas es la de interceptar compras "en línea" a través de Internet, para que haciendo uso del nombre, número de tarjeta de crédito y fecha de expiración, realizan compras de cualquier bien, mayormente software, o hasta

[49] Tellez Valdes Julio, "Derecho Informático", Edición Graw Hill, México, D.F. 1996

hardware y para lo cual proporcionan una dirección de envío, diferente a la del titular del número de la tarjeta de crédito que usan en forma ilegal.

Es un delincuente informático el "pirata" que distribuye software sin contar con las licencias de uso proporcionadas por su autor o representantes, pues no solo atenta contra la propiedad intelectual, provocando la fuga de talentos informáticos, si no que se enriquece ilícitamente y es un evasor de impuestos.

2.8.1 HACKER

Hacker es la persona con talento, conocimiento, inteligencia e ingenuidad, especialmente relacionadas con las operaciones de computadora, redes, seguridad, etc. Que disfruta aprendiendo detalles de los sistemas de programación y cómo tender sus capacidades, tan intensamente como, al contrario, muchos usuarios prefieren aprender sólo el mínimo necesario[50].

Si hacemos una analogía, un hacker sería como un intruso que sabe como abrir el candado de una caja fuerte, la abre, revisa que hay adentro y deja una nota diciendo que estuvo ahí y cuando sale deja todo como estaba.[51]

El cracker, por el contrario del hacker, no se contenta con dejar la nota de que estuvo ahí, también se roba todo lo que encuentra en la caja fuerte y además la deja abierta; o conforme con esto, además hace pública la forma en que abrió la caja fuerte.

Es indudable que muchas veces el hacker persona que comete el delito de hacking

jaqueo es la técnica de ejecutar una aplicación para robar contraseñas y romper la seguridad de un sistema, debe estar tipificado para que sea considerado como delito este utiliza el acceso indebido a un sistema de tratamiento de la información con el fin de cometer un fraude informático, un espionaje de datos, piratería o sabotaje.

En estos casos el ánimo del delincuente será cometer estos delitos y la violación a la prohibición de acceso no será más que un medio de consumación, ante esta

[50] Eric Raymond, [en línea]: http://murrow.journalism.wisc.edu/jargon/jargon.html[consulta: 26/01/09]
[51] Rich Crash Lewis, [en línea]:
http://www2.vo.lu/homepages/phahn/humor/hacker30.txt [consulta: 26/02/09]

primera situación motivacional, es necesario que para que exista hacking, éste debe estar tipificado de alguna forma en nuestra legislación.

Por ello, pueden presentarse algunas situaciones de lagunas jurídicas como podremos apreciar: en primer término, es posible que el delincuente, al acceder indebidamente a un sistema para cometer, por ejemplo, sabotaje informático, se enfrente a un tipo penal que sanciona el sabotaje y que incluye como elemento del delito el acceso indebido, en este caso, no será posible hablar de delito de hacking ya que el acceso contra derecho era parte integrante del tipo sabotaje.

Puede también suceder que la disposición que tipifica el sabotaje informático no considere el acceso indebido como uno de sus elementos objetivos, situación muy probable por que muchas veces los delitos se cometen por operadores que cuentan con una autorización que les permite el ingreso a los sistemas, y en tal caso podría considerarse la posibilidad de aplicar un concurso de delitos de sabotaje y hacking en el evento que otra disposición legal regulara separadamente el acceso indebido como delito; si tal norma no existe, se deberá sancionar exclusivamente el sabotaje.

Un segundo supuesto motivacional del hacker estará determinado por un ánimo que podríamos llamar "no dañoso" es posible, y así ha ocurrido muchas veces, que el delincuente busque la violación de la negativa al acceso, entiéndase códigos, passwords de nuestros correos electrónicos, etc., como una forma de autoratificación de sus capacidades técnicas e intelectuales; el hacker perseguirá la satisfacción de lograr vencer un obstáculo y de demostrar que los programadores que dispusieron las medidas de seguridad no pudieron contra su inteligencia.

Asimismo, dentro de esta motivación "no dañosa", se encuentran los hackers que buscan burlar los códigos de acceso con la finalidad del simple divertimiento o por razones de curiosidad; estas conductas, a pesar de no causar un daño directo y tangible, son delitos en si mismos y deben, necesariamente, estar reguladas y sancionadas por nuestro ordenamiento jurídico.

Podemos concluir que el hacker que no causa daños o fraudes, si viola la privacidad de los datos, ingresando a nuestros correos electrónicos, afectando la intimidad del usuario entrando, de manera no autorizada, en la propiedad ajena. A modo de corolario, citaremos las palabras del experto Sneyers: la sociedad debe tomar conciencia de que el hacker es una persona que comete un acto ilegal con pleno

conocimiento de causa sólo por el mero hecho de introducirse, sin autorización, en un sistema informático ajeno, exista o no intención de causar un daño o ánimo de lucro.

2.8.2 CRACKER

El término cracker viene del termino en ingles crack, que en español significa romper, en conclusión son las personas que se roban información, es como el ladrón en un robo, es aquella persona que haciendo gala de grandes conocimientos sobre computación y con un obcecado propósito de luchar en contra de lo que le está prohibido, empieza a investigar la forma de bloquear protecciones hasta lograr su objetivo, es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño, se considera que la actividad de esta clase de cracker es dañina e ilegal, por que busca un beneficio ya sea económico o de otra índole.

La actividad del cracker consiste en interceptar en forma dolosa un sistema informático para apoderarse, interferir, dañar, destruir, conocer, difundir o hacer uso de la información que se encuentra almacenada en los ordenadores pertenecientes a instituciones públicas y privadas, de seguridad, entidades financieras y usuarios particulares que utilicen la Internet o una de sus funciones como el correo electrónico, deben estar tipificados para que sean considerados como un delincuentes; también se llama cracker a quien descifra los esquemas de protección anti-copia de los programas comerciales para así poder utilizar o vender copias ilegales. Los crackers modernos usan programas propios o muchos de los que se distribuyen gratuitamente en cientos de páginas web en Internet, tales como rutinas desbloqueadoras de claves de acceso o generadores de números para que en forma aleatoria y ejecutados automáticamente pueden lograr vulnerar claves de accesos de los sistemas, obviamente que antes que llegar a ser un cracker se debe ser un buen hacker. La practica el cracking que es la acción de modificar el código fuente a un programa, esta actividad está prohibida a menos que el programa al que se le aplica sea de Software libre y debe estar tipificada para que sea considerada ilegal.

Por ello, los crackers son temidos y criticados por la mayoría de hackers, por el desprestigio que les supone ante la opinión pública y las empresas, son aquellos que utilizan sus conocimientos técnicos para perturbar procesos informáticos, pueden considerarse un subgrupo marginal de la comunidad de hackers.
En muchos países existen crackers "mercenarios" que se ofrecen para romper la seguridad de cualquier programa informático que se le solicite y que contenga alguna protección para su instalación o ejecución. Las formas de daño más comunes del cracker son de introducir un virus al sistema. Los virus *"son elementos informáticos que tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son, eventualmente, susceptibles de destrucción mediante un antivirus adecuados frente a los cuales pueden incluso desarrollar resistencias"*[52]

2.9 PIRATERÍA INFORMÁTICA

Aunque la palabra pirata es evocativamente romántica, este apelativo es atribuido a las personas que hacen uso del software creado por terceros, a través de copias

obtenidas ilegalmente[53]. Es decir, sin permiso o licencia del autor utilizan el software, al software no original se la denomina como “copia pirata”, pero en términos reales y crudos debe llamarse un software robado.

La palabra pirata, asociada al uso ilegal del software, fue nombrada por primera vez por William Gates en 1976, en su "Carta abierta a los Hobistas"[54], por este medio quiso expresar su protesta debido a que muchos usuarios de computadoras estaban haciendo uso de un software desarrollado por él, sin su autorización; al contrario de lo que ocurre con otras cosas que adquirimos, las fuentes y las aplicaciones de software que compramos no nos pertenecen. Nos convertimos en usuarios con licencia; adquirimos el derecho a utilizar el software en un único equipo, no podemos instalar copias en otros equipos, ni pasárselo a nuestros amigos.

Por lo que podríamos definir, a la piratería informática como la distribución o reproducción ilegal de las fuentes o aplicaciones de software de Adobe para su utilización comercial o particular; sea deliberada o no, la piratería informática es ilegal y está castigada por la ley. Muchos de los virus y gusanos actuales han sido

[52] Alicia Chiaravalloti, [en línea]: http://www.chiaravalloti_asociados.dtj.com.ar/links_1.htm , [consulta: 26/01/09]
[53] http://www.delitosinformaticos.com.ar/blog/
[54] Eric Raymond, [en línea]: http://murrow.journalism.wisc.edu/jargon/jargon.html[consulta: 26/01/09]

diseñados por piratas informáticos con el propósito de infectar rápidamente millones de ordenadores en el mundo a través de la Internet y usando como medio el “correo electrónico y entornos de colaboración”.

El coste a nivel mundial de los virus y gusanos en 2005 fue estimado en 19.000 millones de dólares, al mismo tiempo, las compañías están siendo agobiadas con correo electrónico no solicitado mas conocido como spam. Los analistas estiman que el spam alcanza un rango entre el 50% a 70% de todo el correo electrónico transmitido por Internet; además el spam no es sólo una amenaza a la productividad corporativa, se ha convertido en el “Transporte Oficial” del código peligroso que llega o intenta llegar a nuestros PCs.

CAPITULO III

DERECHO A LA INTIMIDAD

3.1 DERECHO A LA INTIMIDAD

El derecho a la intimidad es uno de los derechos fundamentales que garantiza la integridad y dignidad de los individuos, se considera inherente a toda persona e inviolables, y explicitan y concretan los valores de la libertad y la dignidad humana.

Ana Herran nos dice que el derecho a la intimidad constituye una respuesta jurídica a las aspiraciones de cada persona por alcanzar un ámbito de desarrollo interior, ajeno a la intromisión de terceros.[55]

Por tanto el derecho a la intimidad, asegura una calidad mínima de vida en las relaciones con los terceros, para que únicamente se conozca aquello que cada persona desea compartir y revelar a los demás.

El alcance de la protección del derecho a la intimidad esta en:

1.- La vida privada: esta comprende el derecho de establecer y desarrollar relaciones con otros seres humanos en la sociedad. La diversidad de situaciones calificadas como relaciones de vida privada podrían sistematizarse en las siguientes áreas: i) relaciones interpersonales. En el que la personalidad individual encuentra su pleno desarrollo; ii) integridad física y moral, donde la vida privada cubre la integridad física y moral de la persona y comprende la vida sexual ; y iii) la libre disposición del propio cuerpo constituye el soporte natural de la vida humana.

2.- Vida Familiar: en esta esfera se ha de referir al estrecho vínculo que puede existir entre la vida propia y personal de un individuo con determinados aspectos de la vida de otras personas, que por la relación existente entre ellas inciden en la personalidad del individuo. La vida privada y la vida familiar se superponen necesariamente en la zona común de la vida privada de los individuos que la integran y del domicilio en que se realiza.

3.- Domicilio: donde no podrá ser intervenido el domicilio de una persona a menos que medie una resolución judicial que lo justifique; el allanamiento del domicilio aun justificada, se constituye en la intromisión en ese reducto físico que constituye la morada o la vivienda de una persona, generalmente con su familia, el recinto donde su vida se desenvuelve cerrada ala observación de los extraños.

[55] Herran Ortiz Ana Isabel “El derecho a la protección de datos en la sociedad de información, cuadernos Deusto de derechos Humanos Nro 26 Universidad Deusto, Bilbao, España, 2005

4.- Correspondencia: se refiere a la prohibición de intervenir las comunicaciones realizadas entre personas en su vida privada, independientemente del medio por el que se haya efectuado la comunicación.

El concepto de intimidad nace del deseo de proteger el conjunto de facetas de la personalidad del individuo que carecen de significación consideradas aisladamente pero que, coherentemente enlazadas, pueden arrojar un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado en tanto afecte a su honor, nombre o imagen.

La privacidad o privacy tiene un sentido activo que tiende a concretar la protección de los particulares impidiendo que terceros se ocupen de la vida privada de otros; al mismo tiempo, implica que si el banco de datos es legal y permitido sea también "privado", en el sentido de lograr confidencialidad y secreto, seguridad y privacidad en la transmisión que se efectúa.

Toda persona tiene derecho a vivir su propia vida, a desarrollarse conforme pueda y pretenda, a generar relaciones con otros o a mantenerse ajeno y en soledad; su comportamiento será externo cuando se proyecten hacia otros dando publicidad a esos actos, o serán internos e intransferibles cuando permanezcan en el espacio interior de la persona.

El derecho a la intimidad, es un derecho constitucionalmente reconocido, en nuestro país, que constituyen el ámbito de la vida privada de la persona que no puede ser vulnerado. El Tribunal Constitucional de Bolivia, en lo que respecta a la intimidad ha sostenido que: *"El derecho a la intimidad o la privacidad es la potestad o facultad que tiene toda persona para mantener en reserva determinadas facetas de su personalidad."*[56]

Como podemos apreciar el derecho a la intimidad, es un derecho que se inscribe en el marco del valor supremo de la libertad en su dimensión referida al "status" de la persona que implica la libertad de autonomía, lo que esta íntimamente relacionado con el derecho al libre desarrollo de la personalidad; la consagración de este derecho se encamina a proteger la vida privada del individuo y la de su familia, de todas aquellas perturbaciones ajenas que de manera indebida, buscan penetrar o develar los eventos personales o familiares.

El derecho a la intimidad, al ser inherente a otros derechos fundamentales como son el libre desarrollo de la personalidad y el derecho a la dignidad humana, goza de mecanismos de protección constitucional y legal; se entiende que la persona debe ser protegida de las molestias o angustias que le puedan ocasionar el que otros no respeten su intimidad, o busquen inmiscuirse en ella.

La intimidad se concibe como una libertad positiva para ejercer un derecho de control sobre los datos referidos a la propia persona que, si bien han emergido al exterior, fuera de la esfera íntima de la persona, y se han incorporado a un archivo electrónico, nada impide que puedan continuar bajo control y salvaguarda de su titular; en definitiva se identificaría con el mismo derecho a la autodeterminación informativa.

[56] Duran Ribera Willman "Los Derechos Fundamentales como contenido esencial del estado de derecho", [en línea]: http://www.tribunalconstitucional.gov.bo/search_res.html, [consulta: 06/11/08]

3.1.1 FUNDAMENTOS DE LA INTIMIDAD

Nuestra cultura actual reconoce que existe un ámbito de la intimidad de cada persona que solamente concierne a esta y queda reservado para los demás; este ámbito es la consecuencia de la individualidad, de la autonomía y de la libertad que se admiten como propias de cada individuo. El derecho de todo hombre de mantener secretas e inviolables ciertas manifestaciones de su vida; sin su expreso consentimiento nadie puede inmiscuirse dentro de este ámbito.

Según Wagner su esencia consiste en la protección de la tranquilidad moral de los ciudadanos, concepto que en cierta forma corresponde al que dio un tribunal francés al manifestar que: *"El derecho a la intimidad pertenece al patrimonio moral de toda persona física y constituye como su imagen, la prolongación de su personalidad "*[57]

Las principales razones de inquietud provienen de:

a) La expansión sin precedentes de los medios masivos de comunicación de prensa como la radio, cine, televisión y el aumento de información de índole sensacionalista.
b) Nuevos descubrimientos e inventos como las computadoras e internet facilitan grandemente al acceso a la intimidad sin que el afectado se de cuenta de ello.
c) La intensificación de las relaciones y contactos social especialmente dentro de las grandes conglomeraciones humanas.

3.1.2 OBJETO DE LA INTIMIDAD

El trabajo mas importante realizado hasta ahora es el de la Conferencia Nórdica, en Estocolmo, en mayo de 1967[58] la cual reúne el mayor numero de aspectos prácticos que asume a la privacidad en la realidad social; por eso se dice que este significa el derecho del individuo a vivir su propia vida protegido de:

a) Ingerencias en su integridad mental o física o su libertad moral o intelectual;
b) Ataques en su honra o a su reputación;
c) Verse colocado en situaciones equívocas;
d) La revelación fuera de propósito, de hechos penosos dela vida privada;
e) El uso del nombre, identidad o semejanza;
f) Ser copiado, atisbado, observado y acosado;
g) Violaciones a su correspondencia;
h) Abuso de sus medios de comunicación;
i) Revelación de información dada o recibida en virtud del secreto profesional.

La lista de actividades que viola a la intimidad confeccionada por la Conferencia Nórdica las que utilizan otros organismos, como la Asamblea Consultiva del

[57] W. Wagner, Cit, P. 370 Sentencia Referida Es Citada Por Lindon Corresponde A Los Fallos Del 23y 25 de Junio de 1966

[58] Conferencia que se celebra donde Participan Juristas de diferentes partes del Mundo. Sus Conclusiones Están Publicadas en la Obra Imperio del Derecho Derechos Humanos, Principios y Definiciones, Comisión Internacional de Juristas, Ginebra ,1967

Consejo de Europa, tiene gran éxito y es seguida por muchas legislaciones.

La vida intima de una persona esta constituida por :

a) Hechos de la vida intima, como costumbres, modo de vivir, desgracias personales, supersticiones, situación económica, divergencias conyugales, educación de los hijos, amistades, enemistades, estados mentales, infidelidad conyugal, valor personal o cobardía, modos de vestir, comportamiento, comportamiento en las relaciones sociales, y otros aspectos similares.
b) Publicaciones, fotografías, personales o de familiares.
c) Orígenes familiares, y cuestiones relaciones a la filiación.

Por una parte se aprecia en esas referencias un particularismo muy acentuado, capaz de demostrar que es la experiencia de cada cual, incluyendo en ella la que aportan los conocimientos prácticos que dan la vida y las actividades profesionales y de estudio.

3.1.3 CARACTERÍSTICAS DE LA INTIMIDAD

Para German Bidart las características de la intimidad que son:[59]

a) Son manifestaciones o fenómenos que normalmente quedan sustraídos al conocimiento de personas extrañas o cuando menos ajenas al circulo familiar del sujeto, o de sucesos que no se desarrollan normalmente a la vida de las personas.
b) Los hechos referidos son de aquellos cuyo conocimiento por otros provoca normalmente al sujeto una turbación moral en razón de ver afectado su sentido de pudor o del recato.
c) El sujeto no quiere que otros tomen conocimiento de esos hechos.

Todas estas características tienen, una clara proyección al campo del derecho, por que sin ellas no podría reclamarse por el interesado el respeto a lo que por su virtud se considera dentro la intimidad de una persona, por que requieren de puntualizaciones que tocan aspectos jurídicos. Estas características de la intimidad se convierten en auténticos requisitos, que nos permiten determinar si algo debe o no considerarse como invasión a nuestra intimidad.

La intimidad esta constituida por aquellos fenómenos, comportamientos, datos y situaciones de una persona que normalmente están sustraídos al conocimiento de extraños y cuyo conocimiento por estos puede turbarla moralmente por afectar su pudor o su recato, a menos que esa misma persona asiente a ese conocimiento.

[59] Bidart Campos, Germán. 1994. La Interpretación de los Derechos Humanos, Buenos Aires, Ed. Ediar

3.2 EXIGENCIA DE QUE LOS HECHOS PUEDAN PRODUCIR TURBACIÓN MORAL AL SUJETO EN EL CASO DE SER CONOCIDOS POR EXTRAÑOS

Rosenn Keith nos dice que *"este requisito es una reacción medida que el hecho conocido por extraños puede originar que los seres humanos de un determinado grupo social, reacción que envuelve una perturbación moral que deriva en una lesión a los sentimientos de recato o de pudor del afectado, por lo que el bien jurídicamente protegido por las legislaciones que conceden una tutela legal a la intimidad."*[60]

El ser humano debe ser protegido de las molestia, pesadumbre o desazón que al común de los hombres ocasiona el que otros no respeten su intimidad o busquen inmiscuirse indebidamente en ella en cuanto tomen conocimiento de los hechos que el deseaba mantener ocultos a otros, en razón de que estima que tal conocimiento vulnera su sentido del decoro, del pudor natural, o de su propia dignidad.

3.3 VIOLACIÓN DE LA INTIMIDAD

Eduardo Novoa Monreal nos dice que: "el derecho a la intimidad se viola en el momento en que un extraño entendido por tal, para este afecto a cualquiera, salvo aquellos en razón de cierta clase de relaciones íntimas o de la aceptación de su titular sean partícipes de la información, toma conocimiento de cualquier parte del ámbito de la vida privada."[61]

Por lo que podemos deducir que, lo mas genuino del atentado contra la intimidad, en consecuencia, radica que un entraño obtiene información sobre nuestra intimidad, despreciando la exclusividad que corresponde a su titular; para este fin, ese extraño se inmiscuye en la intimidad ajena o busca información sobre lo que a ella le concierne.

Se trata de una injerencia en algo oculto que debe respetarse como tal la cual puede rechazarse de muchas maneras, su esencia es la intrusión indebida dentro de una esfera intima ajena que ha de ser respetada, a no ser que su titular lo autorice. Para el atentado contra la intimidad se consume no es necesario que quien la ha violado de esa manera divulgue además los hechos privados que ha llegado a conocer indebidamente. La comunicación de esos datos a otro o a muchos o el

[60] Rosenn, Keith, "Comparación de la Protección de los Derechos Individuales En las Nuevas Constituciones Latinoamericanas de Colombia y Brasil"
[61] Novoa Monreal Eduardo, "Derecho a la Vida Privada y La Libertad de Información", Siglo Veintiuno Editores, Quinta Edición, 1997

hecho de hacerlos públicos, puede aumentar la gravedad de la violación a la intimidad ofendida y en este sentido pasar a convertirse en una circunstancia agravante del atentado, como lo manifiesta el Articulo 300 de nuestro Código Penal que señala: *"se elevara la pena a 2 años cuando el autor de tales hechos divulgare el contenido de la correspondencia y despachos indicados".*

La profanación de la intimidad tuvo lugar en el momento mismo en que un extraño penetro en ella tomando conocimiento de lo reservado; por consiguiente para atentar contra la intimidad, basta la sola indiscreción, aun no seguida de la comunicación del secreto a otras personas; es así que la violación de la intimidad, empieza cuando un extraño se procura información acerca de ella, esto no niega que el daño que causa a la víctima es mucho mayor cuando al conocimiento por alguien al secreto se le añade la divulgación publica de el.

3.4 INTIMIDAD EN LA RED DE INTERNET

Carlos Delpiazzo nos dice que *"la Internet es una amenaza para la intimidad de los usuarios en la difusión de elementos relativos a la persona, por diferentes características que encontramos en ella, como las que mencionaremos a continuación:"*[62]

La Red de internet, es un medio de comunicación polifacético, debido a la existencia de múltiples medios para distribuir información. Ellos son: el correo electrónico, los boletines, los foros de discusión y también la información presente en la www.

Debemos tener en cuenta los siguientes elementos:[63]

a) la infraestructura de Internet está basada en datos personales (IP),

b) un segundo elemento se refiere a los instrumentos técnicos utilizados, los software de navegación, por ejemplo, que envían más información de la requerida para la realizar una conexión,

c) y en tercer lugar la cantidad de datos que nos solicitan para realizar actividades comerciales en línea.

Se nos plantea una dependencia entre la utilización de Internet y el dar datos personales; y esta relación está signada por la desigualdad entre el proveedor y el usuario. Otro elemento relevante es la desinformación del usuario, que la mayoría de las veces no sabe que sus datos se han recopilado.

Existen tres elementos de fundamental importancia con relación al manejo de datos, que son:

---

[62] Delpiazzo, Carlos, E "Protección de los Datos Personales en los Tiempos de Internet, El Nuevo Rostro de la Intimidad", Revista de Derecho de la Universidad Católica Del Uruguay, Nro III, Montevideo, 2002

[63] Delpiazzo, Carlos, E "Protección De Los Datos Personales En Los Tiempos de Internet, El Nuevo Rostro de la Intimidad", Revista De Derecho De La Universidad Católica Del Uruguay, Nro Iii, Montevideo, 2002

1)Las **Cookies:** podemos definirlas como fichas de información automatizada, las cuales se envían desde un servidor web al ordenador del usuario, con el objetivo de identificar en el futuro las visitas al mismo sitio. Las cookies son una potente herramienta para almacenar o recuperar información empleada por los servidores web debido al protocolo de transferencia de ficheros (http). Los riesgos ya los conocemos: recopilación de gustos, preferencias, hábitos, nombre y contraseña de correos electrónicos y además que algún experto podría manipular estos archivos.

2) Los **Navegadores**: que suelen enviar más información que la necesaria para conectarse, como por ejemplo el tipo y lengua del navegador, que otros programas se encuentran instalados, cual es el sistema operativo del usuario, cookies, etc

*3) **Contenidos Activos**: ejecución de programas con este tipo de contenidos, como por ejemplo Java y Activex.*

Por otra parte Alejandra Castro nos dice que el derecho a la privacidad en línea, es un concepto que abarca diferentes aspectos, como podemos ver a continuación:[64]

Privacidad de una persona. Existen ciertos derechos de privacidad que se adhieren a los rasgos de personalidad como: su nombre, su identidad, fotografía, voz, etc. Cualquier utilización indebida de esa información por otro individuo constituye una invasión de la privacidad del sujeto pasivo.

Privacidad de datos con respecto a una persona. El derecho de privacidad también existe en cuanto a la información sobre cada individuo pueda ser recolectada y utilizada por terceros. Esto incluye, por ejemplo, información sobre los hábitos de gastos; historia médica; afiliaciones políticas o religiosas; de empleo, o de seguros; antecedentes penales; etc.

Privacidad de las comunicaciones de una persona También existen derechos con respecto a las comunicaciones como la de línea, esto es, los mensajes que sean enviados o recibidos por una persona. Así, bajo ciertas circunstancias, el monitoreo o la revelación del contenido de una comunicación electrónica por cualquier persona distinta del emisor o receptor puede constituir una invasión a la privacidad.

3.5 REVELACIÓN DE DATOS SIN SABERLO

Cada vez que alguien utiliza el correo electrónico, navega por la web, interviene en foros de conversación on line, puede revelar datos sensibles acerca de su personalidad, economía, gustos, hábitos sociales, residencia, etc., datos estos que pueden ser maliciosamente

[64] Castro Bonilla, Alejandra, "Derechos Fundamentales", [en línea] http://www.hacienda.go.cr/centro/datos/Articulo/Los%20Derechos%20Fundamentales%20en%20Internet.doc, [consulta: 06/11/08]

recolectados y utilizados por terceros, en perjuicio del usuario. Por ejemplo, las acciones que realicemos pondrán en evidencia nuestra forma de ser, que compramos, que leemos, nuestros datos financieros y económicos, etc., y con ello ser víctimas de plagas de las comunicaciones electrónicas como el junk-mail o spam, que abarrotan nuestro buzón de correo, en el mejor de lo casos con promociones o marketing personalizado, y en el peor, utilizado para la suplantación del usuario, y poder enviar mensajes en nuestro nombre a terceros.

No sólo los datos que voluntariamente damos a cada página web conforman los datos personales, también son datos personales las opiniones, hábitos de navegación y compra, de viajes, y toda aquella información que, al ser rastreada, permita trazar un perfil de cualquier individuo.

Frossini nos dice que la proliferación de los bancos de datos personales no es de reciente data, como veremos en el siguiente ejemplo: "*Los bancos de datos personales con procesamiento electrónico tienen una organización privada puede administrar una documentación de tales dimensiones, como antes no se le habría permitido hacer sino a una entidad pública, considerando la relación entre los sujetos denunciados y los bancos de datos y la relación entre los bancos de datos y los ocultos por falta de denuncia, se puede calcular que ya en 1987 funcionaban en Italia cerca de medio millón de bancos de datos personales.*"[65]

Bajo este concepto, podemos ver que una persona es definida por los cheques que emite; al examinarlos, se puede conocer quiénes son sus médicos, sus aliados políticos, sus contactos sociales, sus afiliaciones religiosas, sus intereses educativos, los periódicos y revistas que lee, y así mucho mas de lo que podemos imaginar. Las transacciones bancarias de un individuo proveen un informe exacto de su religión, ideologías, opiniones e intereses.

Como vemos, la protección de los datos personales no se refiere solamente a los datos individuales de la persona física, sino también a los datos personalizados, es decir, a aquellos sobre los cuales una persona puede ejercer un derecho de propiedad reservada, por cuanto están dentro de su posesión personal, como el número de una tarjeta de crédito, o de una cuenta corriente bancaria, que permiten realizar operaciones de cálculo informático únicamente a su titular.

Todos estos datos conforman, según Frosini, una nueva figura jurídica llamada "*El bien informático debe ser reconocido, definido y protegido en el derecho interno (civil y penal), así como aparece ya identificado en el derecho de las relaciones internacionales, que regulan (por lo menos en parte) el flujo internacional de los datos informáticos personales.*"[66]

---

[65] Frosini, Vittorio. La Protección De La Intimidad: De La Libertad Informática Al Bien Jurídico Informático. Revista Derecho Y Tecnología Informática. Nº 3. Bogotá, Enero, 1990.

[66] Frosini, Vittorio. La Protección De La Intimidad: De La Libertad Informática Al Bien Jurídico Informático. Revista Derecho Y Tecnología Informática. Nº 3. Bogotá, Enero, 1990.

Un ejemplo interesante de demanda por invasión de privacidad fue la demanda intentada por miembros de la tarjeta de crédito American Express contra la American Express Company.

El caso se basó en la práctica reiterada de la empresa de categorizar y calificar a sus miembros según sus hábitos de gastos, para luego alquilar esta información a comerciantes como parte de un programa conjunto de mercadeo y ventas. Al parecer, American Express analizaba datos tales como los lugares donde compraban sus miembros y cuánto gastaban, considerando también características de conducta y sus records de gastos. Luego, la compañía ofrecía crear una lista de los tarjeta habientes que más propensos serían a comprar en ésta o aquella tienda, y alquilaban esa lista a los dueños de la tienda en cuestión.

Los tarjeta habientes alegaron que esta práctica constituía una invasión a su privacidad puesto que ellos no habían dado su autorización para que tal información fuera utilizada. La Corte declaró la demanda sin lugar, expresando que: "*…al utilizar la tarjeta American Express, un tarjeta habiente está, voluntaria y necesariamente, dando información a los demandados, la cual, si es analizada, revelará los hábitos de gastos y preferencias de los tarjeta habientes. No podemos sostener que el demandado ha cometido una intrusión para luego alquilar esta compilación.*"[67]

Como podemos ver la protección de los datos personales en el ámbito en línea no es menos complicada; la Internet ofrece muchos servicios en los que se pide a los usuarios que aporten sus datos personales, los cuales pueden ser utilizados por los administradores de red para conformar un perfil de cada individuo que puede posteriormente ser vendido o alquilado a empresas ".com", las cuales, a su vez, pueden utilizar dicha información para hacer estudios de mercado, enviar mensajes con material de mercadeo directo no solicitado a los usuarios.

Además, los administradores de red tienen la capacidad de conformar un

perfil década usuario con el simple registro de las páginas o categorías de páginas más visitadas por cada individuo, lo cual permite, al igual que en el mundo real, construir un esquema de comportamiento que revele los hábitos de navegación y compra, el tipo de productos o servicios que más le interesan a cada usuario.

La forma en que esto se hace posible es mediante el número Identificación Personal (IP) que los Proveedores de Servicios de Internet (PSI) asignan a cada usuario. Este número no es fijo, los servidores de red lo asignan a los usuarios cada vez que éstos se conectan, son los llamados cookies y clicktrails, los cuales recogen y depositan registros electrónicos de los intereses y hábitos de los usuarios de Internet. Los servidores tienen la capacidad de asociar este número IP con el usuario por vía de datos como el log-in name o nombre de usuario. Cada vez que nos conectamos en la Red, el servidor asocia el número IP asignado por el servidor con nuestro nombre de usuario, y va creando un registro de nuestro comportamiento en línea o definida como on-line.

Existen grandes empresas de contratación de publicidad en-línea que utilizan este registro de hábitos de cada usuario y tienen la capacidad de analizar los datos recibidos para crear un browsing profile o perfil de búsqueda, con el cual pueden

[67] Dwyer Vs. American Express Company, Corte De Apelaciones De Illinois, 1995. Traducción Libre.

determinar los gustos e intereses, por ejemplo, si un usuario tiene por costumbre visitar una página de noticias todos los días, pero se ha determinado por su browsing profile que le interesa el golf, que ha buscado información sobre Hawai en los últimos días, y que visitó la página de una gran aerolínea, alguna de estas empresas de publicidad on-line estarían en la capacidad de colocar un banner anunciando algún club de golf en Hawai en la página preferida de noticias de ese usuario la próxima vez que éste la visite. Al mismo tiempo, este usuario podría comenzar a recibir ofertas de productos de golf no solicitadas por e-mail.

3.6 DERECHO A LA INTIMIDAD A LA PROTECCIÓN DE DATOS PERSONALES

El derecho a la intimidad abarca aquello que se considera más propio y oculto del ser humano entendiéndose por propio y oculto la información que mantiene para sí mismo; pero el contacto permanente del ser humano con sus semejantes al interior de la sociedad a la que pertenece, así como todos aquellos avances tecnológicos que han venido desarrollándose en la sociedad, han comenzado a transgredir aquellos ámbitos que forman parte de la intimidad el ser humano.

La intimidad como una disciplina jurídica ha perdido su carácter exclusivo individual y privado, para asumir progresivamente una significación pública y colectiva, consecuencia del cauce tecnológico. Esto es, en palabras de Lusky, la privacy, más que un mero sentido estático de defensa de la vida privada del conocimiento ajeno, tiene la función dinámica de controlar la circulación de informaciones relevantes para cada sujeto. Por su parte, Fried se pronuncia en el mismo sentido, señalando que la privacy no implica sencillamente la falta de información sobre nosotros por parte de los demás, sino más bien el control que tenemos sobre las informaciones que nos conciernen.[68]

Consecuentemente, frente a una actual sociedad de la información, resulta insuficiente hoy concebir a la intimidad como una derecho garantista de defensa frente a cualquier invasión indebida de la esfera privada, sin contemplarla al mismo tiempo, como un derecho activo de control sobre el flujo de informaciones que afectan a cada sujeto.

Este derecho, consecuencia del desarrollo tecnológico y el creciente almacenamiento de información relativa a la persona, así como la inmersión cada vez mayor de la misma y de la propia sociedad a tenido que ir ampliando sus

[68] Peréz Luño, A.,“Derechos humanos, Estado de derecho y Constitución”, Editorial Tecnos, Madrid 2005

directrices, ya no sólo dentro de su contexto de los sentimientos, emociones, del hogar, de los papeles, la correspondencia, las comunicaciones telefónicas, video vigilancia, etcétera, sino que además, hoy, es necesario su reconocimiento, y más aún, el establecimiento de mecanismos de protección que puedan hacer frente a su uso y manejo, ahora se contempla la posibilidad de conocer, acceder y controlar las informaciones concernientes a cada persona.

El derecho a la intimidad, como el más reciente derecho individual relativo a la libertad, ha variado profundamente, fruto de la revolución tecnológica. Por tanto ha sido necesario ampliar su ámbito de protección, así como el establecimiento de nuevos instrumentos de tutela jurídica.

Al tratarse de un derecho con un carácter abierto y dinámico que está frente a una sociedad donde la informática se ha convertido en el símbolo emblemático de la cultura actual, Frossini, señala que: el control electrónico de los documentos de identificación, el proceso informatizado de datos fiscales, el registro de crédito, así como de las reservas de viajes, representan muestras conocidas de la omnipresente vigilancia informática de la existencia habitual de la persona. Por lo que la vida individual y social corre el riesgo de hallarse sometida a un juicio universal permanente.[69]

Cada ciudadano fichado en un banco de datos se halla expuesto a una vigilancia continua e inadvertida que afecta potencialmente incluso a los aspectos más sensibles de su vida privada, aquellos que en épocas anteriores quedaban fuera de todo control, por su variedad y multiplicidad, y que hoy, además de tomar conciencia de ello, comienzan a exigir un reconocimiento sobre el uso y control de los datos personales.

La protección de la intimidad frente a la informática no significa impedir el proceso electrónico de informaciones, sino el aseguramiento de un uso democrático de la información tecnológica.

En consecuencia, si el derecho a la intimidad en la vida del ser humano, ha sido viable; un tratamiento y almacenamiento tecnológico de sus datos, también lo puede ser; por ende, un derecho a la protección de sus datos personales en pleno siglo XXI, también debe implicar el reconocimiento de este último derecho como fundamental; por lo que el fenómeno de la intimidad aparece en todas las sociedades humanas.

3.7 ANTECEDENTES INTERNACIONALES

[69] Frosini, Vittorio, "Cibernética, derecho y sociedad", Editorial Tecnos, Madrid 1982

En ese contexto el derecho a la intimidad o la privacidad está consagrado por los siguientes instrumentos internacionales:

Declaración Universal de los Derechos Humanos (DUDH)

En su artículo 12 dice: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o as u reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

Pacto Internacional de Derechos Civiles y Políticos (PIDCP)

En su artículo 17 define: "1. Nadie 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 reputación".

Este artículo ha merecido los "comentarios generales" del Comité de los Derechos Humanos que ha señalado lo siguiente:

En el artículo 17: "Se prevé el derecho de toda persona a ser protegida respecto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, así como de ataques ilegales a su honra y reputación.

A juicio del Comité, este derecho debe estar garantizado respecto de todas esas injerencias y ataques, provengan de las autoridades estatales o de personas físicas o jurídicas. Las obligaciones impuestas por este artículo exigen que el Estado adopte medidas legislativas y de otra índole para hacer efectivas la prohibición de esas injerencias y ataques y la protección de este derecho".

El término "ilegales" significa que no puede producirse injerencia alguna, salvo en El cumplimiento del artículo 17 exige que la integridad y el carácter confidencial de la correspondencia estén protegidos de jure y de facto. La correspondencia debe ser entregada al destinatario sin ser interceptada ni abierta o leída. Debe prohibirse la vigilancia, por medios electrónicos o de otra índole, la intervención de las comunicaciones telefónicas, telegráficas o de otro tipo, así como la intervención y grabación de conversaciones.

La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las

particulares o entidades privadas, deben estar reglamentados por la ley.

Los Estados deben adoptar medidas eficaces para velar por que la información relativa a la vida privada de una persona no caiga en manos de personas no autorizadas por ley para recibirla, elaborarla y emplearla y por que nunca se la utilice para fines incompatibles con el Pacto.

Para que la protección de la vida privada sea lo más eficaz posible, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado.

Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación".

Convención Americana sobre Derechos Humanos (CADH)

En su artículo 11 dice: “1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad; 2. 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”.

Estas normas, en términos generales, prevén 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.

CAPITULO V
PROTECCIÓN DE LOS DATOS PERSONALES

5.1 EL DESARROLLO DE LA TECNOLOGÍA Y LOS DATOS PERSONALES

La globalización es un fenómeno mediante el cual un país que pretenda desarrollarse debe estar económica y políticamente interconectado con otros, fenómeno que se traslada a los habitantes quines buscan mejorar su situación y por tanto buscan la mayor interacción posible con su comunidad y la de otros países en la cual el intercambio de datos juega un papel fundamental.

Una persona que busque ser aceptado socialmente no puede quedar aislada del resto de su comunidad, en este rubro el avance de la tecnología y la creación de enormes bancos de datos públicos y privados ha generado que un desconocido deje de serlo en cuestión de minutos, lo cual implica el beneficio de la interrelación económica política y social.

Actualmente la informática es indispensable para el desarrollo de la actividad social, hoy en día se facilita reiteradamente información personal a terceros la cual se procesa con la finalidad de utilizarla en forma más eficiente, lo cual representa un importante avance ya que mediante la utilización de las computadoras se puede procesar un enorme cúmulo de información con lo cual la atención del solicitante de algún servicio puede demorar solo minutos; sin embargo, este proceso debe realizarse con el consentimiento de la persona y solo en relación con el fin para el que le fueron requeridos los datos, es decir la solicitud de un crédito, una compra, una reservación, etc.

En la mayoría de los casos la persona no autoriza que los datos que se le solicitan sean relacionados con otras fuentes de información ya que por este medio se pueden obtener informes más fidedignos de su comportamiento crediticio o de otras características sociales, lo cual desde luego representa una información sumamente personal.[85]

[85] Castillo Marciano, José Luis, "El Derecho a la Intimidad y la Protección de Datos Personales en el Derecho Español": Boletín de la Academia de Ciencias Políticas y Sociales, N° 134. Año LXIV. Caracas, 1997.

No obstante de no contar con autorización para correlacionar bases de datos en nuestro país es una práctica recurrente, de esta forma se invade a la intimidad, mediante nuevas estrategias comerciales que empieza a proliferarse considerablemente.

5.2 DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

El concepto de protección de datos nació como una mera contraposición a la interferencia en la intimidad de las personas facilitada por el avance tecnológico. Sin embargo, con el transcurso del tiempo, esa concepción fue evolucionando hasta llegar al momento actual en el que la doctrina internacional lo entiende como la protección jurídica de las personas en lo concerniente al tratamiento de sus datos personales, tanto en forma manual como automatizada; por otro lado, como nos dice Carlos Correa, también ha evolucionado la concepción del derecho a la intimidad, pues ha dejado de concebirse como la libertad negativa de rechazar u oponerse al uso de la información personal para convertirse en la libertad positiva de supervisar su uso.[86]

Por lo que podemos definir como protección de datos al amparo de los ciudadanos contra la posible utilización de sus datos personales por terceros, en forma no autorizada, para confeccionar una información que, identificable con él, afecte su entorno personal, social o profesional, en los límites de su intimidad, o como la protección de los derechos fundamentales y libertades de los ciudadanos contra el almacenamiento de datos personales y su posterior cesión.

Es indudable que la posibilidad de disponer información sobre las personas ha ido paulatinamente en aumento; si a ello se le suma el importante papel que las bases de datos desempeñan en el mundo tecnificado y globalizado de hoy, surge con pocos cuestionamientos el derecho de las personas a protegerse frente a la intromisión de los demás.

Como explica Pablo Murillo de la Cueva, el bien jurídico subyacente es la autodeterminación informativa que consiste en el derecho que toda persona tiene a controlar la información que le concierne, sea íntima o no, para preservar de este modo y en último extremo, la propia identidad, su dignidad y libertad.[87]

---

[86] Correa, Carlos María, "Derecho Informático", Editorial Depalma, Buenos Aires, 1994

[87] Murillo de la Cueva, Pablo Lucas, "El derecho a la autodeterminación informativa". Editorial Tecnos. Madrid, España, 1990.

Es el derecho a la personalidad, es la facultad de decidir por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida, además que esta facultad requiere de especiales medidas de protección ya que la interconexión de varias colecciones de datos puede converger en la elaboración de un perfil de la personalidad y puede influir en la autodeterminación del individuo y en su libertad de decisión.

Basado en la exigencia de consentimiento para que la recogida y el tratamiento de datos sean lícitos, el derecho a la autodeterminación informativa sobre el que se apoya el concepto de protección de datos personales, no sólo entraña un específico instrumento de protección de los derechos del ciudadano, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona y decidir sobre la difusión y la utilización de sus datos personales.

El Tribunal Constitucional Español, en la Sentencia del 30/11/2000, Fundamento 6, manifiesta que el derecho fundamental a la protección de datos persigue garantizar a las personas el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado.

Por lo que, podemos definir que la protección de datos personales es un derecho concedido a todo titular de datos de carácter personal, a fin de controlar la información referente a su persona, frente a cualquier tratamiento de sus datos efectuado por terceros que surge como consecuencia del avance de la tecnología informática ampliando el campo de protección del derecho a la intimidad.

Tres de cada cuatro países no disponen de ningún tipo de legislación sobre privacidad “online” y las normas del 25% restante son tan dispares que resultan insuficientes para hacer frente al carácter global de la Internet.

La Ley Orgánica de Protección de Datos de carácter personal (LOPD) define una serie de conceptos que valorados conjuntamente permiten determinar si algo tiene la consideración de dato personal o no. Por ejemplo, se define: 1) qué debe entenderse por el concepto dato de carácter personal; 2) cuándo se entenderá que un dato personal puede identificar a alguien; 3) y qué tratamiento deben tener esos datos personales para ser considerados objeto de protección.[88]

---

[88] De Wikipedia, la enciclopedia libre, “Ley Orgánica de Protección de Datos de Carácter Personal de España” [en línea] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML [consulta:30/02/2009]

5.2.1 OBJETIVO DEL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES

El objetivo del derecho a la protección de datos personales es mas amplio que el relativo al derecho a la intimidad, ya que no se reduce a los datos íntimos de la persona, sino a cualquier dato personal; de esta manera y como respuesta al avance de la tecnología, surge el derecho a la protección de datos como un derecho personal de tercera generación que garantiza el pleno desarrollo de la personalidad individual y el libre ejercicio de los derechos de un individuo, al momento de otorgar a este la facultad de determinar por si mismo el tratamiento de sus datos por terceras personas.

El objetivo del derecho a la protección de datos personales son los datos de carácter personal cuando estos sean objeto de tratamiento; por un lado datos personales refiere a toda información sobre una persona física identificada o identificable; considerando identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un numero de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social; en definitiva lo que se busca proteger son aquellos datos personales que puestos de forma organizada, permitan identificar a la persona y confeccionar un perfil de cualquier naturaleza

que pueda llegar a constituir una amenaza para el desarrollo del individuo. Tanto en la sociedad como en su vida privada, en contraposición los datos aislados en anónimo o disociados de su titular y que no puedan ser atribuidos o identificar con posterioridad a su titular, escapan del objeto de protección de derecho a la protección de datos personales.

5.2.2 NATURALEZA DEL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES

La naturaleza del derecho a la protección de datos personales esta basada en el principio constitucional de la dignidad e integridad de la persona; la función del derecho a la protección de datos personales es garantizar a toda persona el poder de control sobre sus datos personales, tanto su uso como su destino, con el propósito de impedir su trafico ilícito y la potencial vulneración de la dignidad del afectado.

El concepto tomado por la Directiva 95/46/CE, de 24 de octubre de 1995 del Parlamento y el Consejo Europeo de tratamiento de los datos es "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite al acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión, o destrucción.[89]

5.2.3. PRINCIPIOS DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

Los principios generales de la protección de datos son los que definen las pautas encaminadas a garantizar tanto la veracidad de la información contenida en los datos almacenados en los archivos, registros, bancos o bases de datos, cuanto la congruencia y la racionalidad de la utilización de los mismos.[90]

1.- Principio de legalidad; también conocido como principio de limitación de la recolección, establece que el procedimiento de recogida de datos no debe ser realizado en forma ilícita o desleal, la recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la ley.
Como por ejemplo, pueden mencionarse como métodos fraudulentos, ilegales o desleales de recolección de datos, a las investigaciones privadas realizadas por detectives, el uso de instrumentos de grabación o escucha de conversaciones privadas, la violación de correspondencia o papeles privados, o cualquier otro en el que se oculte la verdadera finalidad de la recogida de datos y posterior tratamiento. Lo que pretende este principio es evitar actuaciones delictivas por intermedio de las cuales pueda vulnerarse el bien jurídico protegido.

2.- Principio de calidad de los datos: el objeto de este principio es procurar que la información que revele los datos personales sean lo mas fiable posible, para evitar perjuicios a los titulares de los datos personales, en este sentido, los datos personales deberán ser correctos exactos y en la medida posible actualizados, necesarios, pertinentes y adecuados con la finalidad para la que fueron recopilados; además deberán conservarse los datos de forma tal que se procure su seguridad y

---

[89] De Wikipedia, la enciclopedia libre, "Ley Orgánica de Protección de Datos de Carácter Personal de España" [en línea] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML [consulta:30/02/2009]

[90] Correa, Carlos María, "Derecho Informático", Editorial Depalma, Buenos Aires, 1994

que esa conservación no durara mas tiempo de lo necesario para cumplir con la finalidad del tratamiento.

3.- Principio de pertinencia: también conocido como principio de proporcionalidad, este principio exige que los datos que se recaben y almacenen en una base de datos sean pertinentes y adecuados, es decir, que estén relacionados con el fin perseguido en el momento de creación de la base de datos.

Javier Salom señala que, este principio supone que no obstante la posible autorización del titular de los datos o la habilitación legal para someter la información a tratamiento, no se permite que puedan incluirse más datos que aquellos que sirvan o puedan servir para la consecución de la finalidad que justifica dicho tratamiento, que debió determinarse en el momento de la obtención del consentimiento, o que sirve para presumir la concurrencia de éste en los supuestos en que se establecen presunciones legales de su otorgamiento.[91]

El principio de pertinencia, delimita las circunstancias personales sobre las que pueden indagar y recabar información quienes mantengan bases de datos que incluyan información personal.

4.- Principio de seguridad: donde se obliga al responsable del tratamiento que adopte las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales tratados, por los riesgos que podrían padecer por su perdida parcial, total, modificación o acceso no autorizado, las medidas de seguridad deberán ser apropiadas y acordes al tratamiento que se vaya a efectuar y a la categoría de datos que se trate.

5.- Principio de finalidad: este principio, para Emilio Del Peso Navarro engloba a los de pertinencia y utilización no abusiva, implica que los datos de carácter personal que sean recabados para incorporarse a una base de datos deben tratarse con un objetivo específico que debe conocerse antes de la creación de la base misma e informar en el momento en el que la información personal es recolectada.[92]

El principio de finalidad exige que los datos se obtengan y traten de manera leal y lícita, y que su almacenamiento se realice para unos fines concretos y legítimos.

6.- Principio de utilización no abusiva: el objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquéllas que motivaron su obtención.

---

[91] Salom Aparicio, Javier, "Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal", Editorial Aranzadi. Pamplona, España, 2000

[92] Del Peso Navarro, Emilio, "Ley de Protección de Datos, La Nueva LORTAD", Editorial Diaz de Santos. Madrid, España, 2000

7.- Principio de exactitud: los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario y que los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate.

Al exigir que los datos personales recogidos a los efectos de su tratamiento sean exactos y estén actualizados, con la correlativa obligación para el responsable del archivo, registro, banco o base de datos de suprimir, sustituir o completar aquellos datos total o parcialmente inexactos o incompletos, cabe entender también que será necesario proceder a su actualización.

El cumplimiento de la exigencia de que los datos sean exactos y actualizados recae sobre los responsables de los archivos o bancos de datos, lo que pretende este principio es que los datos respondan con veracidad a la situación real de su titular.

8.- Principio de derecho al olvido; este principio se encuentra íntimamente relacionado con el principio de exactitud, también conocido como principio de limitación en el tiempo, que implica que los datos deben desaparecer del archivo o base de datos una vez que se haya cumplido el fin para el que fueron recabados.[93] Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

9.- Principio de publicidad: la conveniencia de la creación y mantenimiento de un registro público en el que figuren los archivos o bases de datos que poseen datos de carácter personal, radica en que a través de su consulta los ciudadanos pueden tomar conocimiento de los archivos en los cuales pueden existir datos referidos a su persona y de la identidad de los responsables de su tratamiento, para poder ejercer una defensa adecuada de sus derechos.

10.- Principio de consentimiento: como regla general, el tratamiento de datos de carácter personal requiere el consentimiento libre, expreso e informado del titular de los datos; el propósito del consentimiento requerido es el de proporcionar a la persona el derecho a elegir qué datos referidos a su persona pueden ser sujetos a tratamiento, una vez prestado el consentimiento, el titular de los datos puede revocarlo en cualquier momento, sin que se le puedan atribuir efectos retroactivos.

5.3 DERECHOS DE LOS TITULARES DE DATOS PERSONALES.

[93] Correa, Carlos María,"Derecho Informático", Editorial Depalma, Buenos Aires, 1994

Como enseña Emilio Suñe, multiplicadas son las facultades de la persona para reaccionar frente al manejo y apropiación del derecho a los datos personales. Por la importancia y la trascendencia que tienen como instrumentos para proteger la intimidad de las personas las mas importantes son las siguientes:[94]

a) Derecho de acceso e información: se le reconoce al titular del dato personal el derecho a obtener del responsable del tratamiento de los daros de forma libre, sin restricción, con una periodicidad razonable y sin retrasos ni gastos excesivos, el poder conocer; si existe o no algún tratamiento de sus datos personales, la finalidad del tratamiento. La categoría de los datos, los destinatarios de los datos tratados si hay cesión, el origen de captura de los datos, los medios que tiene para hacer valer sus derechos de rectificación y cancelación de los datos.

El derecho de acceso se complementa con la obligación que le impone a los responsables de las bases de datos de almacenar los datos de modo que permitan el ejercicio del derecho de acceso de su titular y permite que cualquier persona pueda conocer no sólo si sus datos personales figuran en una base de datos, sino también cuáles son; sólo si los datos se almacenan de tal forma, el titular de los datos personales registrados en un archivo o base de datos podrá ejercer el derecho de acceso.

El derecho de acceso no es más que el derecho que tienen los ciudadanos a obtener en intervalos razonables y sin demoras o gastos excesivos la confirmación de la existencia o inexistencia de información relativa a su persona en una base de datos, así como la comunicación de tales datos en forma inteligible.

Siempre que se garantice la identificación del titular o, en caso de personas fallecidas, el vínculo correspondiente con la presentación de la declaratoria de herederos, la solicitud de información no requiere de fórmulas específicas y puede efectuarse de manera directa, presentándose el interesado ante el responsable o usuario del archivo, registro, base o banco de datos, o de manera indirecta, a través de una intimación fehaciente por medio escrito que deje constancia de su recepción.

El acceso podrá consistir en la mera consulta de los archivos por medio de la visualización, o en la indicación de los datos objeto de tratamiento por escrito, por medios electrónicos, telefónicos, de imagen u otro idóneo a tal fin permite que el titular de los datos:

---

[94] Suñé Llinás, Emilio,"Marco Jurídico del tratamiento de datos personales en la Unión Europea y España", en "XI Encuentros sobre Informática y Derecho", Editorial Aranzadi, Pamplona, España 1998

1) Conozca si se encuentra o no en el archivo, registro, base o banco de datos.

2) Conozca todos los datos relativos a su persona que consten en el archivo.

3) Solicite información sobre las fuentes y los medios a través de los cuales se obtuvieron sus datos.

4) Solicite las finalidades para las que sus datos fueron recabados.

5) Conozca el destino previsto para sus datos.

b) Derecho a rectificación y cancelación de los datos: se reconoce el derecho al titular de los datos personales el solicitar y obtener de manera efectiva la rectificación, bloqueo, cancelación y borrado de los datos tratados por el responsable del tratamiento, cuando esos datos personales sean inexactos, incorrectos o incompletos.

c) Derecho a oposición: este derecho reconoce al individuo para oponerse en cualquier momento, por razones legitimas propias de si situación particular, al tratamiento de sus datos personales cuando sea necesario para el cumplimiento de una misión de interés publico o inherente al ejercicio del poder publico conferido al responsable del tratamiento. Este derecho permite al titular de los datos personales negarse a facilitar un dato de carácter personal en el caso de que no sea obligatorio hacerlo, ninguna persona puede ser obligada a proporcionar datos sensibles.

d) Derecho de información: este derecho, presupuesto de los restantes, se convierte en el derecho básico del afectado para poder ejercitar, con ciertas garantías, los controles que la ley articula en los diversos momentos del tratamiento de datos.

Las personas a las que se le soliciten datos de carácter personal tienen el derecho de ser previamente informadas de modo expreso, preciso e inequívoco de las siguientes circunstancias:

1) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios;

2) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable;

3) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente;

4) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos;
5) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos.
Esta información deberá aparecer en los todos los formularios que se utilicen para recoger datos de carácter personal.

e) Derecho de rectificación, cancelación o supresión: como correlato lógico a los principios de finalidad, pertinencia y exactitud que en forma de deberes la ley impone a los responsables de los archivos o bases de datos que contengan datos de carácter personal, para exigir que cuando los mismos sean inexactos o incompletos, sean rectificados o actualizados, y cuando corresponda, suprimidos o sometidos a confidencialidad.
El derecho de cancelación permite eliminar del archivo o base de datos a aquellos datos personales que, por diversas circunstancias, no deben figurar en el mismo, es importante poner de manifiesto que el término "cancelación" debe ser entendido en forma amplia como la acción tendiente a hacer irreconocibles los datos archivados, ya sea anulando, destruyendo, borrando, tornando ilegibles o declarando su nulidad; la metodología empleada diferirá de acuerdo a las circunstancias, demás está decir que existen casos en los que, por cuestiones de interés público, será imposible eliminar completamente una información.

5.4 DEBERES Y OBLIGACIONES DE LOS RESPONSABLES DE BASES DE DATOS.

Además de los derechos de defensa a los titulares de los datos de carácter personal, también se prevé una serie de garantías específicas tendientes a asegurar su respeto, deberes que pesan sobre la persona del responsable del archivo o base de datos, entre los que se destacan los siguientes: [95]

1.- Deber de Secreto

O también llamado "deber de confidencialidad", obliga al responsable y a las personas que intervengan en cualquier fase del tratamiento de datos personales a respetar el secreto profesional respecto de los mismos, exigencia que deberá subsistir aun después de finalizada la relación con el titular del archivo de datos.

[95] Juan Carlos Cervantes Gómez, "Protección de datos personales". {en línea] http://www3.diputados.gob.mx/camara/content/download/193820/464897/file/datos%20personales.pdf. [consulta: 12/2/09]

El deber de secreto profesional responde a la finalidad de evitar que la información salga del círculo de personas a quienes está destinada, habida cuenta que sobre los archivos o bases de datos pesa una presunción de secreto.

2.- Deber de Inscripción

Los responsables de los archivos, registros, bases o bancos de datos público, y privados destinado a proporcionar informes, tienen el deber de inscribirlos en un Registro que al efecto se habilite para la Protección de Datos Personales.

La inscripción de archivos, registros, bases o bancos de datos deberá comprender como mínimo la siguiente información:

1) Nombre y domicilio del responsable;

2) Características y finalidad del archivo;

3) Naturaleza de los datos personales contenidos en cada archivo;

4) Forma de recolección y actualización de datos;

5) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos;

6) Modo de interrelacionar la información registrada;

7) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información;

8) Tiempo de conservación de los datos;

9) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

3.- Deber de Información

Cuando se recolecten datos de carácter personal que requieran el consentimiento de sus titulares, el responsable del tratamiento ponga a disposición de los mismos una serie de informaciones que le permitan decidir en forma libre la conveniencia de proporcionar datos referidos a su persona. Dicha información deberá indicar qué se va a hacer con los datos, quienes serán los destinatarios de la información y la identidad y dirección del responsable del archivo o base de datos.

4.- Deber de Seguridad

El responsable del tratamiento deberá adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento; el responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales,

de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

5.- Deber de velar por la calidad de los datos.

Este deber consiste en el necesario respeto por parte del responsable y los usuarios de los archivos o bases de datos, de las reglas establecidas para la recogida, tratamiento, uso, conservación, almacenamiento y cesión de datos. De esta forma, la calidad estará medida de acuerdo a los parámetros de la pertinencia, proporcionalidad, lealtad, congruencia, exactitud y accesibilidad por parte del titular de los datos.

6.- Deber de dar acceso a los datos.

El deber de dar acceso a los datos que la ley coloca en cabeza del responsable de la base de datos, exige que los responsables de las bases de datos almacenen la información de forma tal que el ejercicio del derecho de acceso de su titular esté garantizado.

El responsable de la base de datos debe suministrar información amplia sobre la totalidad del registro perteneciente al titular de los datos personales. Además, el deber se complementa con la obligación de que el informe sea claro, exento de codificaciones y, en caso de ser necesario, que se entregue acompañado de una explicación escrita en lenguaje accesible al conocimiento medio de la población, podrán ofrecerse los siguientes medios alternativos de información:

1) Visualización en pantalla.

2) Informe escrito entregado en el domicilio del requerido.

3) Informe escrito remitido al domicilio denunciado por el requirente.

4) Transmisión electrónica de la respuesta, siempre que esté garantizada la identidad del interesado y la confidencialidad, integridad y recepción de la información.

5) Cualquier otro procedimiento que sea adecuado a la configuración e implantación material del archivo, registro, base o banco de datos, ofrecido por el responsable o usuario al mismo.

Los responsables o usuarios de bancos de datos públicos puedan denegar, mediante resolución fundada, la información solicitada por los titulares de datos de carácter personal, cuando por intermedio de ello se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre

el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas.

7.- Deber de rectificación, cancelación y supresión.

Al advertir el error o falsedad en una información, el responsable o usuario del mismo debe proceder a la rectificación, supresión o actualización de la información registrada, Como señala Javier Salom, este deber es la consecuencia lógica del principio de pertinencia, pues si sólo pueden tratarse los datos que sean adecuados a la finalidad que lo justifica, aquellos que hayan dejado de serlo, por los motivos que fuere, no pueden seguir siendo objeto de tratamiento.[96]

8.- Deber de bloqueo.

El derecho de rectificación, actualización o supresión, exige que durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos proceda a bloquear el archivo, o consignar, al proveer información relativa al mismo, la circunstancia de que se encuentra sometida a revisión.

9.- Deber de controlar la cesión de datos a terceros.

El deber de controlar la cesión a terceros de los datos, constituye el requisito último y fundamental de la pretensión legal de preservar la intimidad de los datos incorporados en archivos o bases de datos.

La regla general parte de la imposibilidad de ceder tales datos, las excepciones, requieren la concurrencia de un triple requisito:

1) El consentimiento del afectado,

2) Que la cesión constituya un requisito para el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario.

3) Que la cesión le sea informada al titular de los datos, indicándose además la finalidad de la cesión, la identidad del cesionario y los elementos que permitan hacerlo.

5.5 DERECHO A LA AUTODETERMINACIÓN INFORMÁTICA

El caudal de información nominativa susceptible de ser tratada por medios informáticos y aún transmitida a distancia gracias al desarrollo de las

[96] Salom Aparicio, Jaiver, "Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal", Editorial Aranzadi. Pamplona, España, 2000

telecomunicaciones, ha despertado gran preocupación en diferentes legislaciones; por que puede existir un serio riesgo para los derechos fundamentales, desde que permite a quien dispone de la información acceder a parcelas de nuestra vida que legítimamente debían tenerse en resguardo y aun servirse de ella para condicionar el ejercicio de nuestras libertades.

La información personal denota valores personales, la prevención frente a su tratamiento no suscita tan solo problemas individuales, sino conflictos que importan a la sociedad en su conjunto, ya que el uso de la información permite coartar y controlar el comportamiento del usuario.[97]

Emilio Suñé Llinás, nos dice que, "el derecho a la autodeterminación informativa se construye a partir del derecho a la intimidad, tanto como éste lo hizo sobre la base del derecho de propiedad; y, en que, a diferencia de cuanto ocurre con el derecho a la intimidad, la autodeterminación informativa se circunscribe a amparar todo dato que se predica de determinada persona".[98]

El Tribunal Constitucional de España resguarda el derecho a la intimidad y propugna que este constituye un derecho fundamental autónomo, mediante la cual se preservan los derechos fundamentales frente a los ataques de que puedan ser objeto mediante la tecnología informática.

Constitucionalmente, el derecho a la autodeterminación informativa ha merecido reconocimiento, con mayor o menor precisión y extensión, en diversas cartas fundamentales; así lo es en los artículos 18 de la Constitución de España de 1978, 10 de la Constitución de los Países Bajos de 1983, 5 de la Constitución de la República Federativa de Brasil de 1988, la Constitución Política de Colombia de 1991, 2 de la Constitución Política del Perú de 1993, 43 de Constitución de la Nación Argentina de 1994, entre otras.

Por su parte, las Naciones Unidas han emitido directrices aplicables al tratamiento de datos personales, que los define como "Principios rectores para la reglamentación de los ficheros computarizados de datos personales", adoptados por la Asamblea General de la Naciones Unidas en su resolución 45/95, de 14 de diciembre de 1990; que en su articulo 7 dice que el derecho a la vida privada, consagra, como categoría autónoma, la libertad informativa en los siguientes términos:

---

[97] Pérez Luño, Antonio Enrique, "Informática y Derecho", Cuadernos elaborados por la UNED, Centro Regional de Extremadura, Editorial Aranzadi, número 1, 1995.

[98] Suñé Llinás Emilio, "Tratado de Derecho Informático. Volumen I: Introducción y Protección de Datos Personales", Universidad Complutense Madrid, España. 2000.

Artículo 8. Protección de los bienes de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

Puede apreciarse claramente que la construcción del derecho a la autodeterminación informativa, sigue los derroteros propios de los derechos fundamentales de nueva generación: surgen a raíz de la "liberties pollution".

5.6 FICHEROS SOBRE CUMPLIMIENTO O INCUMPLIMIENTO DE OBLIGACIONES DINERARIAS

La inclusión de los datos de carácter personal en los ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias, sólo podrá efectuarse cuando exista una deuda cierta, vencida y exigible, que haya resultado impagada, y después de que se haya requerido al ciudadano afectado el pago de la deuda por el acreedor.

No podrán ser incluidos en ficheros de esta naturaleza los datos personales de un ciudadano cuando exista un principio de prueba documental que contradiga la existencia de la propia deuda; del mismo modo, tal circunstancia determinará la cancelación cautelar del dato personal desfavorable en los supuestos en que ya se hubiera efectuado la inclusión en el fichero.

Los responsables de estos ficheros sólo podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los ciudadanos y que no se refieran, cuando sean adversos, a más de seis años, y siempre que respondan con veracidad y exactitud a la situación actual de éstos; en el caso de que el ciudadano incluido en este tipo de fichero haya procedido al pago de la deuda deberá procederse a la cancelación del dato referido al mismo.

Para ello, el acreedor tendrá que comunicar al responsable del fichero común de información de solvencia patrimonial y crédito, en el plazo de una semana, la inexactitud o inexistencia de la deuda, por lo tanto, si la deuda ya se ha pagado, el acreedor tiene la obligación de informar al responsable del fichero común para que proceda a la rectificación del dato del ciudadano que no responde a su situación actual.

El responsable de un fichero o tratamiento común de morosidad tiene la obligación de notificar al ciudadano que ha procedido a incluirlo en el mismo haciendo referencia de los datos incluidos, así como al derecho que le asiste para recabar información de la totalidad de ellos en los términos establecidos en la LOPD.[99]

Se efectuará una notificación por cada deuda concreta y determinada, con independencia de que ésta se tenga con el mismo o con distintos acreedores.

5.7 FICHEROS DE MARKETING Y PUBLICIDAD

Las entidades que se dedican a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial, etc., pueden utilizar los nombres y direcciones, así como otros datos personales que figuren en fuentes accesibles al público.

Las guías telefónicas y las listas de personas pertenecientes a un Colegio profesional, que contengan los datos de nombre, título, profesión, actividad, grado académico, y la dirección son fuentes de acceso público, también lo son los diarios y boletines oficiales y los medios de comunicación.

Los interesados pueden ejercer el derecho de acceso para conocer sus datos personales y el origen de los mismos, cuando una entidad toma datos personales de una fuente accesible al público para realizar un tratamiento de publicidad o marketing debe informar al interesado del origen de los datos y de la identidad del responsable del tratamiento, diarios y boletines oficiales y medios de comunicación.[100]

[99] Piñar Mañas, José Luis, Protección de datos personales, [en línea]: http://74.125.93.132/search?q=cache:rgPkBQAZoaEJ:www.agpd.es/upload/FOLLETO.PDF+derecho+a+la+proteccion+de+datos+personales&cd=37&hl=es&ct=clnk&gl=bo, [consulta: 26/01/09]

[100] Piñar Mañas, José Luis, Protección de datos personales, [en línea]: http://74.125.93.132/search?q=cache:rgPkBQAZoaEJ:www.agpd.es/upload/FOLLETO.PDF+derecho+a+la+proteccion+de+datos+personales&cd=37&hl=es&ct=clnk&gl=bo, [consulta: 26/01/09]

CAPITULO VI

LEGISLACIÓN COMPARADA

Tanto en Estados Unidos como en la Unión Europea protegen jurídicamente los datos personales; asimismo, en algunos países de América Latina, como Argentina, Uruguay y México, se ha empezado su protección jurídica introduciendo en sus legislaciones como veremos a continuación:

6.1 PROTECCIÓN DE DATOS EN ESTADOS UNIDOS

Estados Unidos, si bien cuentan con un marco jurídico bastante amplio en materia de intimidad, también ha adoptado una política de autorregulación que ha estado a cargo en gran medida del sector privado, respondiendo satisfactoriamente a las demandas y necesidades de sus grandes corporaciones y protegiendo en la medida de lo posible los derechos básicos de los consumidores y de los ciudadanos con base en la primera enmienda de su Constitución

Por otro lado, la política de regulación de los Estados Unidos ha evolucionado de tal forma que hoy en día se ha ocupado más de legislar aquellos sectores que se consideran más sensibles y vulnerables para la sociedad, como son el sector salud y la protección y confidencialidad de la información que proporcionen niños menores de edad a sitios en Internet.

Las empresas de Estados Unidos por motivos meramente económicos sigue siendo en Internet muy superior, en general, a las europeas, es habitual encontrarnos con situaciones en las cuales una empresa española oferta servicios de hosting a otras empresas, generalmente también españolas, pero los servidores que realmente usan están en Estados Unidos, o por lo menos los datos de sus clientes van desviados hacia allá. En tal caso, estamos ante una transferencia internacional de datos; con la entrada en vigor de la Directiva europea sobre protección de datos, el 25 de octubre de 1.998, el Departamento de Comercio de los EE. UU. Publicó el 21 de julio de 2000 un grupo de principios denominados Safe Harbor (o de puerto seguro). La finalidad de tal texto fue que las empresas americanas que aplicasen dichos principios tendrían el visto bueno de la Unión Europea, y por tanto, en política de protección de datos evitarían todo este control en la Comunidad. No obstante, en la práctica, si se transfieren datos a una empresa USA, y la misma no está en dicho listado, cabe una solución a ello, que es simplemente elaborar un documento en el cual, entre otras cosas, se garantice que dicha empresa extranjera se somete a la

jurisdicción española y a la Agencia de Protección de Datos, en todas aquellas cuestiones relacionadas con dicho tránsito de datos, comprometiéndose también a facilitar al titular de los datos, el ejercicio de los derechos que en España hubiese podido tener.[101]

La política de los Estados Unidos, a pesar de haber dictado normas sectoriales que protegen la privacidad, es no interferir el normal desenvolvimiento del mercado mediante el dictado de leyes que pueden llegar a entorpecer el desarrollo del comercio y dejar que las mismas las fuerzas intrínsecas del mercado se encarguen de obligar a las empresas a cumplir ciertas pautas mínimas de comportamiento. Aquellas empresas que no cumplan, por ejemplo, con los códigos de conducta de su sector no sólo perderán clientes, pudiéndose, en un mundo digital, divulgarse rápidamente tal hecho, condenando al responsable al ostracismo, sino también ser pasibles de sanciones.[102]

6.2 PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA

Algunos estados miembros de la Unión Europea han considerado los temas de intimidad y protección de datos personales como asuntos prioritarios en su agenda legislativa, con el propósito de hacer no sólo un frente comercial común a fuertes bloques comerciales regionales como por ejemplo el MERCOSUR entre otros en Latinoamérica, sino sobre todo como una medida proteccionista para salvaguardar y proteger los derechos y libertades de las personas físicas, en particular del derecho a la intimidad y la libre circulación de datos personales, derechos consagrados en las constituciones y leyes de los estados miembros y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, buscando con base en estos ordenamientos jurídicos, proteger a los ciudadanos europeos al momento en que proporcionen información personal a empresas, filiales, sitios y organismos gubernamentales y no gubernamentales en línea que se encuentren físicamente localizados dentro del continente europeo o que tengan sus servidores fuera de países miembros de la Unión Europea.

La Directiva 95/46 del Parlamento Europeo y del Consejo del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, mejor conocida como la Directiva sobre Privacidad y Protección de Datos, entró en vigor el 25 de octubre de

[101] http://www.helpdesk-software.ws/es/it/31102005.htm
[102] Dr. Fernando Maresca, http://www.portaldeabogados.com.ar/colaboraciones/0824.htm

1998 y su objeto es proporcionar un marco general de referencia para los países miembros. Esta Directiva establece reglas muy estrictas para la protección de los derechos y garantías de libertad de los ciudadanos europeos y en particular la protección del derecho a la intimidad con relación a la obtención y procesamiento de datos personales.

6.3. LEY ORGÁNICA DE DATOS DE CARÁCTER PERSONAL ESPAÑA (LOPD)[103]

La Ley Orgánica 15/1999, de 13 de diciembre, de Datos de carácter Personal, se estructura de la siguiente manera:

TITULO I, Disposiciones generales: que esta conformado por el Objeto, ámbito de aplicación y definiciones, donde se puede encontrar el glosario de términos que utiliza esta Ley ;

TITULO II, Principios de la protección de datos: la calidad de datos, derechos de información en la recogida de datos, consentimiento del afectado, datos especialmente protegidos, datos relativos a la salud, seguridad de los datos, deber de secreto, comunicación de datos, acceso a los datos por cuenta de terceros, en este capitulo podemos encontrar la protección de datos;

TITULO III, Derechos de las personas: impugnación de valores, derecho de consulta al registro General de protección de datos, derecho de acceso, derecho de rectificación y cancelación, procedimiento de oposición, acceso, rectificación o cancelación, Tutela de los derechos, derecho a indemnización, en este titulo podemos encontrar, los derechos que tiene el titular de los datos personales;

TITULO IV, este titulo se divide en dos capítulos que son:

CAPITULO I Ficheros de titularidad publica: creación, modificación o supresión, comunicación de datos entre Administraciones Publicas, ficheros de las Fuerzas y cuerpos de seguridad, excepciones a los derechos de acceso, rectificación y

[103] http://civil.udg.es/normacivil/estatal/persona/PF/lo15-99.htm

cancelación, otras excepciones a los derechos de los afectados, en este titulo encontramos los datos personales de las instituciones publicas;

CAPITULO II Ficheros de titularidad privada: creación, notificación e inscripción registral, comunicación de la cesión de datos, datos incluidos en las fuentes de acceso publico, prestación de servicios de información sobre solvencia patrimonial y de crédito, tratamientos con fines de publicidad y de prospección comercial, censo promocional, códigos tipo, en este capitulo encontramos los datos personales de entidades privadas y cual su normamiento;

TITULO V Movimiento internacional de datos: norma general, excepciones, en este titulo se encuentra cual es la regulación en cuanto a los datos personales y el movimiento internacional;

TITULO VI Agencia de protección de datos: naturaleza y régimen jurídico, el director, funciones, consejo consultivo, el registro general de protección de datos, potestad de inspección, órganos correspondientes de las comunidades autónomas, ficheros de las comunidades autónomas en materia de su exclusiva competencia, en este titulo encontramos la Agencia de protección de Datos personales, cuales son sus funciones, su competencia;

TITULO VII Infracciones y sanciones: responsables, tipos de infracciones, tipo de sanciones, infracciones de las administraciones publicas, prescripción, procedimiento sancionador, potestad de inmovilización de ficheros, en este titulo encontramos las infracciones y sanciones que impone esta ley.

OBJETO

La Ley Orgánica de Protección de Datos de Carácter Personal de España No. 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (LOPD), tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar.

Su objetivo principal es regular el tratamiento de los datos y ficheros, de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de

los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan. Así lo determina en el Art 1. (*Objeto)*

ÁMBITO DE APLICACIÓN

El ámbito de aplicación de esta ley abarca el sector público y privado, protege los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores (articulo 2).

SEGURIDAD DE DATOS

La Ley Orgánica de Protección de Datos de Carácter Personal, en su Artículo 9 señala que, el encargado de la seguridad de los datos personales es el responsable de los ficheros: *"El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida 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"*.

INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y DE CRÉDITO

Esta Ley determina en su Artículo 29 que: Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento. De la misma manera señala que: Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. Finalmente señala que sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia

económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquellos.

DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES

Los ciudadanos tienen derecho a:

Impugnación de valoraciones, es decir a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad. (Artículo 13).

Derecho de consulta al Registro General de Protección de Datos, cualquier persona podrá conocer, información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. Este Registro General será de consulta pública y gratuita. (Artículo 14).

Derecho de acceso, el interesado tendrá derecho a solicitar y obtener información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. (Artículo 15)

Derecho de rectificación y cancelación, serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos. el responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días. (Artículo 16)

ÓRGANO DE CONTROL

El órgano de control del cumplimiento de la normativa de protección de datos dentro del territorio español, con carácter general es la Agencia Española de Protección de Datos (AEPD), existiendo otras Agencias de Protección de Datos de carácter autonómico, en las Comunidades Autónomas de Madrid Cataluña y en el País Vasco. Así lo determina en el Art. 35: La Agencia de Protección de Datos es un ente

de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones.

SANCIONES

Las sanciones tienen una elevada cuantía, siendo España el país de la Unión Europea que tiene las sanciones más altas en materia de protección de datos. Dichas sanciones dependen de la infracción cometida.

En el Articulo 45 se divide en:

Sanciones leves van desde 601,01 a 60.101,21 euros.

Sanciones graves van desde 60.101,21 a 300.506,05 euros

Sanciones muy graves van desde 300.506,05 a 601.012,10 euros

En el sector público, la citada Ley regula igualmente el uso y manejo de la información y los ficheros con datos de carácter personal utilizados por todas las administraciones públicas.

MOVIMIENTO INTERNACIONAL DE DATOS

En su Artículo 33 manifiesta que no podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de

datos, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Se considera que el incremento en la utilización de las bases de datos personales incide en el derecho a la intimidad de los ciudadanos, esta preocupación fue recogida por las instancias europeas que incluso dispuso que el 28 de enero se celebrara anualmente el "Día Europeo de la Protección de Datos". Los datos personales se clasifican en función de su mayor o menor protección debiendo permanecer en un soporte seguro y siendo obligatoria su comunicación al organismo protector de los datos.

Existen internacionalmente diversos sistemas legales que permiten la regulación de esos datos; en algunos de ellos son las personas las que deben autorizar que sus datos sean recogidos, en otros sistemas, como el español, las empresas pueden recabar esos datos de diversas formas, siendo potestad del posible perjudicado el reclamar su cancelación o modificación ante un organismo fuera de su lugar de residencia, de tal forma que, por ejemplo, las imágenes de una persona pueden ser grabadas siendo el interesado el que debe ejercitar sus derechos para que las mismas sean destruidas.

La ley Orgánica 15/1999 de Protección de Datos de Carácter Personal de España, cuenta con 49 artículos, es una de las mas completas, es la pionera en cuanto a la protección de datos personales, y se la utiliza como base para otras legislaciones. Es muy rigurosa y una de las mas severas en cuanto a sus sanciones.

6.4. LEY DE PROTECCIÓN DE DATOS ARGENTINA LEY NRO. 25326 [104]

[104] http://www.red.org.ar/ley.htm

En el caso de Argentina, las normas de Derecho relativas a la protección de datos personales están reguladas mediante leyes generales y sectoriales, todas ellas de efecto jurídico obligatorio.

Las normas generales están contempladas en su Constitución, la Ley 25 326 sobre protección de datos personales y el Decreto Reglamentario No 1558/2001. Asimismo la Constitución Argentina prevé un recurso judicial especial, denominado "habeas data", para proteger los datos personales. Se trata de una subcategoría del procedimiento contemplado en la Constitución para proteger los derechos constitucionales para la protección de datos personales a la categoría de derecho fundamental; el tercer párrafo del artículo 43 de su Constitución, para tomar conocimiento de los datos que se refieren a ella y de su finalidad que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, exigir la supresión, rectificación, confidencialidad o actualización de aquellos.

La Ley 25 326 sobre protección de datos personales, de 4 de octubre de 2000 se estructura de la siguiente manera:

CAPITULO I, Disposiciones generales: objeto y definiciones, en esta capitulo encontramos el objeto y las definiciones que utiliza esta ley;

CAPITULO II, Principios generales relativos a la protección de datos: calidad de datos, consentimiento, información, categoría de datos, datos relativos a la salud, seguridad de los datos, deber de confidencialidad, cesión, transferencia internacional, en este capitulo encontramos los principios de protección en los cuales esta basada esta ley;

CAPITULO III, Derechos de los titulares de datos: derecho de información, derecho de acceso, contenido de la información, derecho de rectificación, actualización o supresión, excepciones comisiones legislativas, gratuidad, impugnación de valoraciones personales, este capitulo esta basado en los derechos que tiene el titular de los datos personales;

CAPITULO IV, Usuarios y responsables de archivos, registros y bancos de datos: registro de archivos de datos, inscripción: archivos, registro o banco de datos públicos, supuestos especiales, archivos, registros o bancos de datos privados, prestación de servicios informatizados de datos personales, prestación de servicios de información crediticia, archivos, registros o bancos de datos con fines de

publicidad, archivos, registros o bancos de datos relativos a encuestas, en este capitulo encontramos los responsables de los datos personales y sus obligaciones;
CAPITULO V Control: órgano de control, códigos de conducta, en este capitulo encontramos el órgano de control encargado de proteger los datos personales;
CAPITULO VI Sanciones: sanciones administrativas, sanciones penales, este capitulo se fundamenta en las sanciones que aplica la presente ley;
CAPITULO VII Acciones de protección de datos personales: procedencia, legitimación activa, legitimación pasiva, competencia, procedimiento aplicable, requisitos de la demanda, tramite, confidencialidad de la información, contestación del informe, ampliación de la demanda, sentencia, ámbito de aplicación, en este capitulo encontramos las acciones a los que tiene derecho el titular de los datos personales.

OBJETO

La legislación Argentina cubre la protección de los datos personales contenidos en archivos, registros, bancos de datos u otros medios técnicos públicos y la protección de datos personales contenidos en archivos, registros, bancos de datos u otros medios técnicos privados “destinados a dar informes”, incluidos aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito.
Esta Ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional. (Art. 1)

ÁMBITO DE APLICACIÓN

La Ley 25 326 sobre protección de datos personales se aplica en el ámbito publico y privado.

SEGURIDAD DE DATOS

El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, para evitar su adulteración, pérdida,

consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales, de información, ya sea que los riesgos provengan de la acción humana o de algún medio técnico. (Articulo 9)

INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y DE CRÉDITO

En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial, relativos a la solvencia económica y de crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con el consentimiento del titular de los datos personales. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor. (Art. 26)

DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES

Los derechos que reconoce esta ley a los titulares de los datos personales son los siguientes:

Derecho de Información, toda persona puede solicitar información al organismo de control relativa a la existencia de archivos, registros, bases o bancos de datos personales, la finalidad con la que se la utiliza y la identidad de sus responsables. El registro que se lleve al efecto será de consulta pública y gratuita. (articulo 13)

Derecho de acceso, el derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto. El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes. (articulo 14)

Asimismo el contenido de la información, la información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen. (articulo 15)

Derecho de rectificación, actualización o supresión, toda persona tiene derecho a que sean rectificados, actualizados y cuando corresponda, suprimidos o sometidos a confidencialidad los datos personales de los que sea titular, que estén incluidos en un banco de datos. (articulo 16)

ÓRGANO DE CONTROL

Se creó la Dirección Nacional de Protección de Datos Personales como órgano de control, gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación. Así lo determina en su articulo 29

SANCIONES

La legislación Argentina prevé sanciones efectivas y disuasorias, tanto de naturaleza administrativa como penal. Además, en caso de que el tratamiento ilícito haya causado perjuicios, se aplican las normas de la legislación Argentina relativas a la responsabilidad civil. (Articulo 31)

Las Sanciones administrativas, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos.

Sanciones penales, con la pena de prisión de un mes a dos años al que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales. Con la pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales. (Articulo 32)

TRANSFERENCIA INTERNACIONAL

En cuanto a la Transferencia internacional, se prohíbe la transferencia de datos personales de cualquier tipo, con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados. (articulo 12)

La Ley de protección de los datos personales de Argentina, Ley Nro. 25 326 cuenta con 48 artículos, es el único país latinoamericano que cuenta con la aprobación de la Agencia de protección de Datos de España y es considerado como puerto seguro por este país.

Sus sanciones son bastante severas ya que incluso penaliza estas con prisión de 2 hasta 3 años; actualmente no se han aprobado 2 artículos en cuanto a la autonomía del órgano de control, como hemos podido apreciar es muy similar con la Ley Orgánica de Protección de datos de Carácter Personal de España.

6.5 LEY DE PROTECCIÓN DE DATOS PERSONALES PARA EL ESTADO Y LOS MUNICIPIOS DE GUANAJUATO

En México existen leyes sectoriales, como es el caso del Decreto número 266. Ley de Protección de Datos Personales Para el Estado y los Municipios De Guanajuato[105], se encuentra estructurado de la siguiente manera:

TITULO PRIMERO Disposiciones generales: objeto, sujetos obligados, definiciones, excepciones, seguridad, en este titulo encontramos el objeto y las definiciones que esta ley utiliza;

TITULO SEGUNDO, se divide en:

CAPITULO PRIMERO Tratamiento de datos personales: sujetos obligados, consentimiento del titular, confidencialidad, en este capitulo se encontramos los sujetos obligados al cumplimiento de esta ley;

CAPITULO SEGUNDO Derechos de los titulares, este capitulo determina los derechos que los titulares de los datos personales tiene;

CAPITULO TERCERO Solicitudes, en este capitulo se refiere a que tipo de solicitudes y como hacerlas efectivas;

CAPITULO CUARTO Sesión de datos personales: sujetos obligados, sección de datos, en este capitulo encontramos la sección de datos personales y quienes están obligados a cumplirlas;

TITULO TERCERO Autoridades, este titulo se divide en 2 capítulos que son:

CAPITULO PRIMERO Instituto y sus atribuciones, este titulo determina la Institución encargada de hacer efectiva la presente ley;

CAPITULO SEGUNDO Director general del instituto y sus atribuciones;

TITULO CUARTO Registro estatal de protección de datos personales;

CAPITULO ÚNICO Registro estatal de protección de datos personales;

TITULO QUINTO Medios de impugnación;

CAPITULO ÚNICO Registro de queja: procedencia, interposición, medida preventiva, substanciación;

TITULO SEXTO Infracciones y sanciones;

CAPITULO ÚNICO Infracciones: servidores públicos, responsabilidad administrativa.

[105] htt://www.ordenjuridico.gob.mx/Estatal/GUANAJUATO/Leyes/GTOLEY35.pdf.

OBJETO

En su articulo 1 establece que la Ley de Protección de Datos Personales para el Estado y los Municipios De Guanajuato tiene por objeto garantizar la protección de los datos personales.

ÁMBITO DE APLICACIÓN

En su articulo 2 preceptúa que esta ley es de orden público e interés general, los sujetos obligados para la aplicación de esta ley son:

I. El Poder Legislativo;

II. El Poder Ejecutivo;

III. El Poder Judicial;

IV. Los Ayuntamientos;

V. Los organismos autónomos, y

VI. Cualquier otra dependencia o entidad estatal o municipal.

SEGURIDAD DE DATOS

Esta ley manifiesta que los servidores públicos que por razón de sus actividades tengan acceso a algún archivo o banco de datos, están obligados a mantener la confidencialidad de los mismos, serán relevados de dicha obligación cuando medie resolución jurisdiccional o existan circunstancias que pudieran alterar o poner en riesgo la seguridad o la salud pública. (Articulo 8)

INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y DE CRÉDITO

La Ley de Protección de datos personales para el Estado y Municipios de Guanajuato no prevé la información sobre solvencia patrimonial y de crédito.

DERECHOS DE LOS TITULARES DE DATOS PERSONALES

En México los titulares de los datos personales tienen el derecho a solicitar y obtener gratuitamente informes de sus datos personales, así como la corrección y cancelación de los mismos contenida en archivos o bancos de datos de los sujetos obligados;

Obtener la corrección, o en su caso, la cancelación de los datos personales, cuando sea procedente. Revocar el consentimiento otorgado a los sujetos obligados para la cesión de datos. Conocer la identidad de los terceros a quienes se hayan cedido sus datos, así como las razones que motivaron el pedimento de la misma.

Conocer del carácter obligatorio u optativo de su respuesta para la obtención de datos personales, así como de las consecuencias de la negativa a proporcionarlos.

ÓRGANO DE CONTROL

En México se creo como organismo de control al Instituto de Acceso a la Información Pública

SANCIONES

El articulo 33 define como infracciones por parte de los servidores públicos, las siguientes:

I. Impedir u obstaculizar injustificadamente el ejercicio de los derechos del titular;

II. Incumplir con la entrega de informes dentro del plazo establecido en esta ley;

III. Notificar fuera del plazo que establece la presente ley, el acto mediante el cual se efectúe, en su caso, la corrección o cancelación de los datos personales;

IV. Negar sin causa justificada, la corrección o cancelación de datos personales;

V. Realizar la cesión de datos en contravención a lo dispuesto por esta ley;

VI. Violentar el principio de confidencialidad que deben guardar por disposición de esta ley;

VII. Realizar el tratamiento de datos contraviniendo las disposiciones que señala este ordenamiento, y

VIII. No atender el sentido de una resolución favorable para el recurrente, emitida con motivo de la interposición del recurso de queja.

Los servidores públicos que incurran en las infracciones, se les impondrán las siguientes sanciones:

Amonestación, para los casos de las fracciones II y III;

Multa para los casos de las fracciones I, IV y VII, y

Destitución para los casos de las fracciones V, VI y VIII.

MOVIMIENTO INTERNACIONAL DE DATOS

La Ley de Protección de datos personales para el Estado y Municipios de Guanajuato no prevé el movimiento internacional de datos.

En el caso de la Ley de protección de datos personales en el Estado y los municipios de Guanajuato Decreto Nro. 266, cuenta con muchas deficiencias, el ámbito de aplicación solo se refiere al sector publico y no al sector privado causando vacíos jurídicos para su aplicación.

Como ley sectorial no se aplica a todo el territorio Mexicano, causando un caos en cuanto las sanciones que pudiesen haber, de uno y otro estado.

Sus sanciones son muy leves, la mayor es la destitución provocando que no sea tomada con seriedad.

6.6 URUGUAY LEY DE PROTECCIÓN DE DATOS PERSONALES PARA SER UTILIZADOS EN INFORMES COMERCIALES Y ACCIÓN DE HABEAS DATA [106]

En el caso de Uruguay, las normas de Derecho relativas a la protección de datos personales están reguladas mediante la Ley de Protección De Datos Personales Para ser utilizados en Informes Comerciales y Acción de Habeas Data Ley Nº 17.838, Publicada el primero de octubre de 20004 - Nº 26599, se encuentra estructurada de la siguiente manera:

TITULO I

CAPITULO I. Protección de datos personales de informes comerciales: objeto excepciones;

CAPITULO II. Principios generales: obtención, consentimiento, protección, obligación;

CAPITULO III. Del tratamiento de datos personales relativos a obligaciones de carácter comercial: autorización, duración de registro de datos personales, responsables, cancelación;

TITULO II.

CAPITULO I. Habeas Data: acción, requerimiento, acceso a información, personas jurídicas, rectificación, actualización, eliminación o supresión de datos personales;

CAPITULO II. Acción de protección de los datos personales: acción de protección de datos personales, acción de habeas data;

CAPITULO III. Órgano de control: órganos de control, medidas sancionatorias;

TITULO III. Disposiciones finales: responsables, acreedores por obligaciones incumplidas;

OBJETO

El objeto de esta ley es de regular el registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración, y en general, el tratamiento de datos personales asentados en archivos, registros, bases de datos, u otros medios

[106] http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=17838&Anchor=

similares autorizados, sean éstos públicos o privados, destinados a brindar informes objetivos de carácter comercial. (Articulo 1) El tratamiento regulado involucra toda forma de registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración y toda otra forma del mismo o similar alcance.

ÁMBITO DE APLICACIÓN

El ámbito de aplicación de la Ley de Protección de datos personales para ser utilizados en informes comerciales y acción de Habeas Data es de orden privado. (articulo 22)

SEGURIDAD DE DATOS

Aquellas personas físicas o jurídicas que obtengan legítimamente información proveniente de una base de datos que brinde tratamiento a los mismos, están obligadas a utilizarla en forma reservada y exclusivamente para las operaciones habituales de su giro o actividad, estando prohibida toda difusión de la misma a terceros. (Articulo 6)

INFORMACIÓN SOBRE SOLVENCIA PATRIMONIAL Y CREDITICIA

El tratamiento de datos personales relativos al cumplimiento o incumplimiento de obligaciones de carácter comercial o crediticia, que permitan evaluar la concertación de negocios en general, la conducta comercial o la capacidad de pago del titular de los datos, están autorizados, en aquellos casos en que los mismos sean obtenidos de fuentes de acceso público o procedentes de informaciones facilitadas por el acreedor (Articulo 8)

Podrán estar registrados por un plazo de cinco años contados desde su incorporación, en caso que al vencimiento de dicho plazo la obligación permanezca incumplida, el acreedor podrá solicitar al titular de la base de datos, por única vez, su nuevo registro por otros cinco años.

Las obligaciones canceladas o extinguidas por cualquier medio, permanecerán registradas, con expresa mención de este hecho, por un plazo máximo de cinco años, no renovable, a contar de la fecha de la cancelación o extinción.(Articulo 9)

DERECHOS DE LOS TITULARES DE LOS DATOS PERSONALES

Tienen derecho a:

Tomar conocimiento de los datos referidos a su persona y de su finalidad y uso, que consten en registros o bancos de datos públicos o privados y, en caso de error,

falsedad o discriminación, a exigir su rectificación, supresión o lo que entienda corresponder. Cuando se trate de datos personales cuyo registro esté amparado por una norma legal que consagre el secreto a su respecto, el Juez apreciará el levantamiento del mismo en atención a las circunstancias del caso. (Artículo 12).

Derecho de acceso sólo podrá ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se hubiere suscitado nuevamente un interés legítimo de acuerdo con el ordenamiento jurídico.

Solicitar la rectificación, actualización y la eliminación o supresión de los datos personales que le corresponda que estén incluidos en una base de datos o similares.(Articulo 15)

ÓRGANO DE CONTROL

El Ministerio de Economía y Finanzas actúa como órgano de control en el tratamiento de datos personales comprendidos en esta ley y tendrá como cometido implementar, vigilar y asesorar en todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley.(Articulo 20)

SANCIONES

El Ministerio de Economía y Finanzas podrá, en su función de órgano de control, aplicar las siguientes medidas sancionatorias (Artículo 21)

1) Apercibimiento;
2) Multa de hasta doscientas unidades reajustables;
3) Clausura del archivo, registro o base de datos respectivo. A tal efecto se faculta al Ministerio de Economía y Finanzas a promover ante los órganos jurisdiccionales competentes, la clausura, hasta por un lapso de seis días hábiles, de las personas o empresas que dispongan de archivos, registros o bases de datos respecto de los cuales se comprobare que infringen o transgreden la presente ley.

MOVIMIENTOS INTERNACIONALES

La Ley de Protección de datos personales para ser utilizados en informes comerciales y acción de habeas data de Uruguay no prevé el movimiento internacional de datos.

La Ley de Protección De Datos Personales de Uruguay para ser utilizados en Informes Comerciales y Acción de Habeas Data Ley Nº 17.838, da un aporte interesante, ya que incluye el recurso de habeas data en la misma, establecido en la misma el recurso lo cual no contradice a su Constitución.

Otro aporte importante de esta ley establece como periodo máximo de registro crediticio con un máximo de cinco años.

Como hemos podido apreciar, actualmente tanto los países desarrollados como EE.UU. y la Unión Europea como países de Latinoamérica como Argentina, vienen adoptando medidas jurídicas sobre la protección de los datos personales, asegurando así la protección de la intimidad y el desarrollo del comercio internacional, es muy importante que en nuestro país se adopten medidas efectivas de seguridad para la protección de los datos personales.

6.7 ANTEPROYECTOS

Actualmente, se ha incrementado la preocupación de los estados para la protección jurídica de los datos personales existen anteproyectos como en el caso de Venezuela Ecuador y Costa Rica para este propósito.

CONCLUSIONES

La presente investigación, nos permitió arribar a las siguientes conclusiones:

1. El hombre nace con la plena facultad de decidir con quien compartir sus ideas, sentimientos o hechos de su vida personal o simplemente reservarlos para si mismo, ya que el derecho de disponer de los datos es del titular, si tal garantía es violada se convierte en una transgresión a las libertades individuales. El atentado contra la intimidad radica, cuando un entraño obtiene información sobre nuestra intimidad, despreciando la exclusividad que corresponde a su titular; para este fin, ese extraño se inmiscuye en la intimidad ajena o busca información sobre lo que a ella le concierne.

2. El ser humano a lo largo de su vida va dejando una enorme estela de datos que se encuentran dispersos, actualmente con la utilización de nuevos medios tecnológicos, resulta posible agrupar e interpretar dichos datos, lo que lleva a crear un perfil determinado del individuo que puede interferir en su intimidad.

La simple selección de temas de información preferidos, puede brindar información de sumo interés; las consultas médicas, los tipos de estudios realizados, permiten elaborar un perfil ideológico, sanitario o intelectual de cada persona, el desafío es mejorar la seguridad de la intimidad; también son datos personales las opiniones, hábitos de navegación y compra, de viajes, y toda aquella información que, al ser rastreada, permita trazar un perfil de cualquier individuo. Una persona puede ser definida por los cheques que emite; al examinarlos, se puede conocer quiénes son sus médicos, sus aliados políticos, sus contactos sociales, sus afiliaciones religiosas, sus intereses educativos, los periódicos y revistas que lee, y así mucho mas de lo que podemos imaginar.

3. Existen grandes empresas de contratación de publicidad que utilizan este registro de hábitos de cada usuario y tienen la capacidad de analizar los datos recibidos para crear un perfil de búsqueda.

Posiblemente en nuestra vida haya alguien que siga nuestros pasos por algún interés particular; sin embargo sí es posible que determinadas empresas estén muy interesadas en saber, cuáles son nuestros gustos a la hora de comprar, si practicamos o no algún deporte, etc., para elaborar sus propios estudios de mercado y ofrecernos casualmente justo el producto que encaja como un guante en nuestras necesidades y/o aficiones.

La información equivale al poder, todos tienen un acceso casi ilimitado a los medios de movilización y donde cada vez se hace más fácil manipular información ajena, que pueden constituir armas para causar daños patrimoniales o morales.

4. Por otra parte el interesado posee la autodeterminación informativa como una facultad para el resguardo del derecho a la intimidad, haciendo especial hincapié en la necesidad de evitar la elaboración de un perfil de la persona a partir de la interacción de archivos que resguardan distintos datos personales del individuo; por tanto, el concepto de derecho a la intimidad ha sufrido una importante variante, pues evoluciona de ser un simple derecho de exclusión en el que el individuo reafirmaba su derecho a la intimidad o "derecho a estar solo" para adquirir una nueva dimensión como derecho facultativo que le permite ejercer acciones en defensa del derecho a la intimidad. Con lo que se ha comprobado la aprobación de la hipótesis "La ausencia de una normativa que proteja los datos personales en nuestro país trae como consecuencia la vulneración del derecho a la intimidad";

Es derecho del titular a preservar el control sobre sus datos personales y la aplicación de las nuevas tecnologías de la información, deben ser el contexto en el cual se debe consagrar el derecho fundamental a la protección de datos de carácter personal.

5. La regulación de la privacidad y protección de datos personales ha sido abordada a nivel mundial en forma muy particular por cada país, ello se debe, en gran medida, a los intereses económicos, políticos y sobre todo responde a las estrategias comerciales de cada país. Asimismo, la transferencia internacional de datos personales de un Estado a otro se ven seriamente amenazados, si no se establece un control que marque límites de garantía y seguridad en la transmisión telemática o en la transferencia de los datos personales cruzando fronteras; por ello, la regulación de los límites a la transferencia de datos se encuentra, en el origen de las normas nacionales e internacionales reguladoras de la protección de datos.

Actualmente, el continente Europeo es el pionero y que resguarda con mayor efectividad la protección personal de datos y el flujo transfronterizo de los mismos, inhibiendo en forma considerable sus relaciones comerciales con otros países como Estados Unidos, Canadá.

6. Nuestra legislación no ofrece condiciones adecuadas de seguridad jurídica a los datos personales provocando un vació jurídico, que trae como consecuencia que estos puedan ser utilizados con un fin distinto al que se los recopilo, es necesario

un agravamiento y ampliación de las figuras protectoras y mayores exigencias de seguridad para quienes almacenan datos de las personas.

Se debe garantizar al titular el poder de control sobre sus datos personales, sobre su uso y su destino con el propósito de impedir su trafico ilícito y lesivo para resguardar la dignidad y el derecho del afectado.

Nuestra Constitución Política, en su Articulo 130 protege a la privacidad, otorga tutela jurídica a la intimidad de las personas, la legislación Civil protege la dignidad de las persona y la intimidad; por que constituyen dentro de los derechos personalísimos, motivo por el cual son inviolables; asimismo nombre y la imagen, pero nuestra normativa vigente no es clara ni específica en cuanto a la protección de los datos personales.

7. Con la propuesta de "Ley de Protección de Datos Personales" se busca garantizar la protección íntegra de los datos personales de las personas naturales o jurídicas asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, tanto públicos como privados destinados a dar informes, para garantizar el derecho al honor, imagen y a la intimidad de las personas ante la potencial agresividad de la informática.

Se debe poner barreras limitativas a las personas encargadas de suministrar los datos personales. Una norma especifica que resguarde el derecho a la protección de datos personales, con limitación de tiempo, ente fiscalizador, conocer los destinatarios, otorgar normas sobre los ficheros de cumplimiento o incumplimiento de obligaciones dinerarias, recopilación, transmisión, publicación de los datos personales, y buscar puertos seguros de Transferencia internacional de datos personales.

BIBLIOGRAFÍA

1. ALEGRE MARTÍNEZ, MIGUEL ÁNGEL,
"El Derecho a la Propia Imagen". Ed. Tecnos,
Madrid, España. 1997

2. ALCALA, GILBERTO,
"Proyecto de Ley Sobre la Vida Privada y su Incidencia en el Derecho a la Información"
Revista del Consejo de la Judicatura. Nº 32. Año 9. Caracas, 1984.

3. ARTEAGA SANCHEZ, ALBERTO,
"La Intercepción, interrupción, impedimento o Revelación de comunicaciones privadas ajenas"
Revista de la Facultad de Ciencias Jurídicas y Políticas. Año XL. Nº 97. Caracas, 1995.

4. BIDART CAMPOS, GERMÁN,
La Interpretación de los Derechos Humanos,
Editorial Ediar, Buenos Aires,1994.

5. CABANELLAS, GUILLERMO,
Diccionario Enciclopédico de Derecho Usual,
Editorial Heliasta, Buenos Aires, Argentina, 1996,

6. CASTILLO MARCANO, JOSÉ LUIS,
"El Derecho a la Intimidad y la Protección de datos Personales en el Derecho Español",
Boletín de la Academia de Ciencias Políticas y Sociales, Nº 134. Año Lxiv.
Caracas, 1997

7. CONFERENCIA INTERNACIONAL AMERICANA,
Ix,"Declaración Americana de los Derechos y Deberes del Hombre",
Bogotá, Mayo de 1948

8. CÓDIGO CIVIL,
Decreto Ley Nro. 12760,
Editorial el Original
9. CÓDIGO PENAL,
Porfirio Franklin Pérez Aquino,
Editorial Megalito, Bolivia 2001

10. CONSTITUCIÓN POLÍTICA DEL ESTADO,
Asamblea Constituyente,
Honorable Congreso Nacional, Bolivia 2008

11. CORREA, CARLOS MARÍA,
"Derecho Informático",
Editorial Depalma, Buenos Aires, 1994

12. DE ESTEBAN, JORGE Y PEDRO GONZÁLEZ-TREVIJANO,
Curso de Derecho Constitucional Español I. Primera edición, Servicio de publicaciones de la Facultad de Derecho, Universidad Complutense de Madrid, Madrid, 1992

13. DE CASTRO, FERNANDO,
"Derecho Civil en España"
Vol. I. Madrid, 1955.

14. DELPIAZZO, CARLOS,
"Protección de los Datos Personales en los Tiempos de Internet, El Nuevo Rostro de la Intimidad", Revista de Derecho de la Universidad Católica Del Uruguay, Nro III, Montevideo, 2002

15. DEL PESO NAVARRO, EMILIO,
"Ley de Protección de Datos, La Nueva LORTAD",
Editorial Diaz de Santos. Madrid, España, 2000

16. DWYER VS. AMERICAN EXPRESS COMPANY,
Corte de Apelaciones de Illinois,
Traducción Libre, 1995.

17. ESCOBAR DE LA SERNA, LUIS,
"Sociedad, Información y Constitución",
Editorial Universitas S. A., Madrid, 1999

18. ESPINOZA ESPINOZA JUAN,
"Derecho de las Personas",
4ª Edición, Palestra, Lima, 2004

19. FERNANDEZ CALVO RAFAEL,
"El Tratamiento del llamado delito Informático",
Revista Iberoamericana de Derecho Informático", 155n1136, Nro 12, 1996

20. FLORES DAPKEVICIUS, RUBEN,

“Amparo, Hábeas Corpus, Hábeas Data”,
Editorial B De F, Buenos Aires 2004

21. FROSINI, VITTORIO,
“Cibernética, derecho y sociedad”,
Editorial Tecnos, Madrid 1982

“La Protección de la Intimidad de la libertad Informática al bien Jurídico informático. Revista Derecho Y Tecnología Informática. Nº 3. Bogotá, Enero, 1990.

22. FUNDACIÓN DE DERECHOS HUMANOS,
“Declaración Americana de los Derechos y Deberes del Hombre”,
Serie Cuadernos Divulgativos, Fundación Sánchez Editores, Caracas, 1993.

23. GARCÍA MAYNEZ EDUARDO,
Filosofía Del Derecho,
Editorial Porrúa, 1999

24. HERRAN ORTIZ ANA ISABEL,
“El derecho a la protección de datos en la sociedad de información cuadernos Deusto de derechos Humanos”
Nro 26 Universidad Deusto, Bilbao, España, 2005

25. IRIARTE AHON,
“Estado Situacional y perspectivas del derecho informatico en America Latina y el Caribe”
CEPAL, 2005

26. KOFI ANNA,
Mensaje en el Cincuentenario de La Declaración Universal de los Derechos

Comisión Internacional de Juristas,
Edición Especial, 1968

27. LYNCH, HORACIO MARÍA,
Notas sobre el derecho en la Era Digital, En La Ley,
Año Lx, Nro 93, 15 de mayo de19996

28. MURILLO DE LA CUEVA, PABLO LUCAS,
"El derecho a la autodeterminación informativa",
Editorial Tecnos. Madrid, España, 1990.

29. NOVOA MONREAL EDUARDO,
“Derecho a la Vida Privada y la Libertad de Información”,

5ta Edición Siglo Veintiuno Argentina Editores, 1997

30. PEÑARANDA QUINTERO HÉCTOR RAMON,
Derecho Civil I: Personas Y Familia,
Maracaibo, 12 De Junio De 2001

31. PERÉZ LUÑO, ANTONIO ENRIQUE,
“Informática y Derecho”,
Cuadernos elaborados por la UNED, Centro Regional de Extremadura, Editorial Aranzadi, número 1, 1995.

“Derechos humanos, Estado de derecho y Constitución”,
Editorial Tecnos, Madrid 2005

32. PRIETO SANCHIS, LUIS.
Estudios de Derechos Fundamentales,
Editorial Debate, Madrid, 1990.

33. REBOLLO DELGADO, LUCRECIO,
“El Derecho Fundamental a la Intimidad”,
Segunda Edición Actualizada, Ed. Dykinson, S.L. Madrid, 2005

34. SALOM APARICIO, JAVIER,
"Estudio sobre la Ley Orgánica de Protección de Datos de Carácter Personal",
Editorial Aranzadi Pamplona, España, 2000

35. SAGUES, NESTOR,
Subtipos De Hábeas Data,
Nota A Fallo, "Ja", 1995.Iv

36. SESIN, DOMINGO,
“Remedio Contra El Abuso Del Poder Informático: El Habeas Data”,
Editores Abeledo-Perrot, Argentina, 1998.

37 SUÑÉ LLINÁS, EMILIO,
"Marco Jurídico del tratamiento de datos personales en la Unión Europea y España", en "XI Encuentros sobre Informática y Derecho",
Editorial Aranzadi, Pamplona, España 1998

"Tratado de Derecho Informático. Volumen I: Introducción y Protección de Datos Personales", Universidad Complutense Madrid, España. 2000.

38. TELLEZ VALDES JULIO,
“Derecho Informatico”,

Edición Mc. Graw Hill, México, D.F. 1996

CONSULTAS ELECTRÓNICAS

39. ARGÜELLO TÉLLEZ, FERNANDO,
La protección de datos personales en un mundo global, [en línea]:
http://74.125.45.104/search?q=cache:HPp2ED5sbNAJ:www.apdcat.net/media/315.pdf+red+iberoamericana+de+proteccion+de+datos+personales&hl=es&ct=clnk&cd=18&gl=bo, [consulta: 26/01/09]

40. BARZALLO, JOSÉ LUIS,
“El Comercio Electrónico en el Ecuador. Desafío frente al nuevo siglo”,
Revista Electrónica de Derecho Informático, [en línea]:
http://www.alfa-redi.org/rdi-articulo.shtml, [consulta: 06/10/08]

41. CHIARAVALLOTI, ALICIA,
Revista de Derecho informatico, [en línea]:
http://www.chiaravalloti_asociados.dtj.com.ar/links_1.htm , [consulta: 26/01/09]

42. CRASH LEWIS, RICH,
Hacker [en línea]:
http://www2.vo.lu/homepages/phahn/humor/hacker30.txt [consulta: 26/02/09]

43. CASTRO BONILLA, ALEJANDRA,
Derechos Fundamentales, [en línea]:
http://www.hacienda.go.cr/centro/datos/Articulo/Los%20Derechos%20Fundamentales%20en%20Internet.doc, [consulta: 06/11/08]

44. CERVANTES GÓMEZ, JUAN CARLOS
“Protección de datos personales”. [en línea]
http://www3.diputados.gob.mx/camara/content/download/193820/464897/file/datos%20personales.pdf. [consulta: 12/2/09]

45. DE WIKIPEDIA, LA ENCICLOPEDIA LIBRE,
“Ley Orgánica de Protección de Datos de Carácter Personal de España” [en línea]
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML
[consulta:30/02/2009]

46. DURAN RIBERA WILLMAN

Los Derechos Fundamentales como contenido esencial del estado de derecho, [en línea]: http://www.tribunalconstitucional.gov.bo/search_res.html, [consulta: 06/11/08]

47. GUADAMUZ, A.
Habeas Data: The Latin-American Response to Data Protection. The Journal Of Information, Law And Technology (Jilt) [en línea]:
Wwwwarwick.Ac.Uk [consulta: 06/11/08]

48. GELMAN, ROBERT.
La Declaración Universal de Derechos Humanos del Ciberespacio, [en línea]:
http://www.arnal.es/free/info/declaracion/html [consulta: 26/02/09]

49. HOFFMAN, LANCE J.
Civilizing Cyberspace: Priority Policy Issues in a National Information Infrastructure[en línea]: (Marzo,1994) Traducción Libre.
Www.Seas.Gwu.Edu/Seas/Instctp/Docs/Paper [consulta: 26/02/09]

50. Ley Orgánica de Protección de Datos de Carácter Personal. [en línea]

http://civil.udg.es/normacivil/estatal/persona/PF/lo15-99.htm, [consulta: 19/11/08]

51. OTERO CARVAJAL, LUIS ENRIQUE,
Derechos Humanos y sociedad de la información. Nuevas formas de acción social. [en línea]
http://www.ucm.es.../la%20sociedad%20informacional%20y%20los%20derechos%20humanos.html [consulta: 19/11/08]

52. PIÑAR MAÑAS, JOSÉ LUIS,
Protección de datos personales, [en línea]:
http://74.125.93.132/search?q=cache:rgPkBQAZoaEJ:www.agpd.es/upload/FOLLETO.PDF+derecho+a+la+proteccion+de+datos+personales&cd=37&hl=es&ct=clnk&gl=bo, [consulta: 26/01/09]

53. RAYMOND, ERIC,
Protección de los datos personales, [en línea]:
http://murrow.journalism.wisc.edu/jargon/jargon.html[consulta: 26/01/09]

54. Red Iberoamericana de Protección de Datos, [en línea]

https://www.agpd.es/portalweb/internacional/red_iberoamericana/index-ides-idphp.php, [consulta: 10/09/08]