UNIVERSIDAD SALESIANA A.C.

ESCUELA DE DERECHO

Incorporado a la Universidad Nacional Autónoma de México
Clave 3156-09

"LA IMPORTANCIA DE LA REGULACION JURIDICA A LA PROTECCION DE DATOS PERSONALES EN INTERNET"

T E S I S

QUE PARA OBTENER EL TITULO DE :

LICENCIADO EN DERECHO

P R E S E N T A:

MARIANA SANCHEZ VALDEZ

ASESOR DE TESIS:
LIC. MARIO ALBERTO MARTELL GOMEZ

Mexico, D.F., 2007

A MI MAMÁ

Por su eterno apoyo y comprensión
aún en los momentos más difíciles,
por sus palabras de aliento y
por ser mi mayor impulso para la
terminación de mis estudios.
A ti, mamá por ser un gran
ejemplo de mujer a seguir.
Por todo, por ser tú,
GRACIAS MAMÁ.

A MI HERMANO

Quien me alentó a seguir a pesar
de muchos desalientos,
correspondiendo al esfuerzo y
apoyo recibido, que ha hecho
que sea lo que soy, razón por
lo que lo admiro profundamente.

A MI PADRE

Por la confianza depositada
y por el apoyo brindado para
la culminación de mi carrera,
como un testimonio de gratitud,
con amor y respeto.

A MIS ASESORES

Por el apoyo brindado,
por sus invaluables enseñanzas
en este proyecto que tuvo
a bien realizarse.

A MIS AMIGOS Y FAMILIARES

Por sus palabras de ánimo y
hasta regaños que fueron el motor
y el empuje para este trabajo.

A ti, vida por estar ahí, justamente
en el momento preciso,
por tu apoyo y por mostrarme un
mundo totalmente diferente
del que conocía.

Gracias a mis Jefes por su estima
y los conocimientos que me
brindaron, por su apoyo.

A todos aquellos que,
aún sin quererlo me impulsaron
y me brindaron el coraje
para éste momento.
Gracias.

Contenido.

1. INTRODUCCIÓN.

Este trabajo toma como base el creciente desarrollo tecnológico de nuestros días, esto es el uso cada vez más frecuente de las computadoras y por consiguiente de la “navegación por Internet” para la obtención de datos, información, entretenimiento, noticias y hasta incluso para la búsqueda de personas con tan solo proporcionar su nombre.

Esto es así ya que el Internet, palabra de uso anglosajón, ha pasado a nuestro vocablo para expresar una forma de comunicación rápida, eficiente, que nos permite acercarnos con otras personas, a través de la cual se tiene la libertad de expresar lo que se desea, dentro de una comunidad muy variada de modos de pensamiento, culturas, idiomas, ideales, en la cual se pueden encontrar comentarios estudiantiles hasta conferencias de grandes profesionales.

Por otro lado, cabe hacer mención que si bien es cierto resulta de enorme utilidad este medio de comunicación, también lo es que nos enfrentamos a los riesgos de que sean violentados los Derechos Fundamentales necesarios para una sana vida social por la falta de un marco legal que rija la a los seres que conviven e interactúan por éste medio, al no existir un debido respeto de la privacidad de éstas personas.

La privacidad de las personas resulta ser un tema de importancia tomando en consideración que el poder oír las conversaciones o incluso entrar en la vida

personal de alguien sin que ésta lo sepa o incluso lo autorice, resulta de la curiosidad o por la necesidad de información privilegiada que se pudiera lograr con ello, esta interferencia de la privacidad se agudiza con la aparición del teléfono e incluso aún más desde la comunicación escrita, dejándose entrever así los peligros que podríamos afrontar.

Como ejemplo de lo anterior es de hacer notar la venta de datos del Instituto Federal Electoral de las personas registradas a una empresa de supuesta publicidad estadounidense, misma que a la fecha no se ha podido saber la utilidad que tendría para dicha empresa los datos de miles de personas mexicanas, noticia que al ser revelada creó total descontento entre la ciudadanía, ahora es de preguntarse ¿qué pasaría si dicha información tuviera un inadecuado manejo y como fue posible la obtención de dichos datos de un Instituto gubernamental?

Si a una institución de ésta índole les es robada dicha información, qué nos esperamos nosotros de los datos que confiadamente proporcionamos a través de el Internet para poder acceder a ella o más aún, con la nueva modalidad de los bancos denominada “BANCA NET” la cual es publicitada por dichas instituciones de crédito como una alternativa a ir personalmente a una banca y abstenerse de las largas filas, sin mencionar en ningún momento que su información es totalmente “*CONFIDENCIAL*” asegurando dicha situación y garantizando que la misma no será utilizada con otros fines, al respecto cabe mencionar que ha habido personas que se han hecho millonarias al poder entrar a la base de datos de instituciones bancarias, transfiriendo fondos ya sea por millones de dólares, en su

caso e inclusive se ha sabido de aquel que transfiriendo los centavos de las cuentas bancarias de los clientes de un banco se hizo multimillonario, sin que en ningún momento se hubieran despertado sospechas por parte del personal del banco que estaban siendo alteradas las cuentas de sus clientes transfiriéndose los fondos a una nueva cuenta, como lo fue el caso de Vladimir Levin, un graduado en matemáticas de la Universidad Tecnológica de San Petersburgo, Rusia, quien logró sustraer más de diez millones de dólares de cuentas corporativas del CITIBANK.

Esta conducta no es exclusiva a extranjeros, basta con conectarse al Internet para que en poco tiempo nos llegue hasta nuestro domicilio diversa publicidad dirigida a nuestro nombre, así como se llene nuestra página de correo de tantas ofertas publicitarias que en ningún momento solicitamos.

De ahí la necesidad de saber que nuestros datos que proporcionamos como confidenciales sean resguardados por alguna ley que prohíba y sancione la obtención y utilización de dicha información sin nuestro consentimiento, máxime que es un Derecho protegido por nuestra Constitución en su artículo 16 al establecer que "***LAS COMUNICACIONES PRIVADAS SON INVIOLABLES...***" de lo que se advierte una protección a nuestra ***privacidad***.

Así pues, tenemos que la Constitución Política de los Estados Unidos Mexicanos determina como una garantía de seguridad jurídica la protección a las **COMUNICACIONES PRIVADAS** toda vez que el derecho del hombre en lo que

atañe a su privacidad no es tan sólo en sus posesiones, domicilio, papeles o en su familia, sino también en su intimidad, trascendiendo así a sus papeles íntimos que es lo que constituye su correspondencia, así como todo tipo de medios de comunicación a excepción de la correspondencia que circule por el correo ordinario, cuyas prescripciones se regulan de forma independiente. Esto es, se refiere a todo tipo de comunicaciones tomando en cuenta los nuevos avances tecnológicos que facilitan grandemente el acceso a la vida privada.

Sin embargo, nuestra legislación penal vigente es relativamente "*nueva"* con respecto a los delitos que pudieran surgir a través de los equipos de informática por medio del Internet, no le proporciona la suficiente importancia al uso indiscriminado de los datos confidenciales que los usuarios de tal medio le proporcionan, tomando en consideración que al entrar a una página de Internet cualesquiera primeramente piden nuestros datos personales como lo son: nombre completo, domicilio, edad, estado civil, ocupación, entre otras.

Y no obstante que dicha información es necesaria para las instituciones que tienen páginas de Internet a disposición de la gente, para tener estadísticas del tipo de persona que frecuentan sus páginas y quien utiliza dichos medios; el problema surge cuando otras empresas o instituciones utilizan dicha base de datos para fines comerciales o ilícitos, más aún que en ningún momento se pidió la autorización de alguna persona para poder utilizar los datos que se cree son confidenciales para otros propósitos; se vulnera así la privacidad que ponemos en manos de quien suponemos utiliza nuestros datos únicamente para registro.

Dichos datos pueden ser obtenidos a través del uso de programas espía enviados a través del propio Internet o bien porque las empresas mismas a quienes les confiamos la información correspondiente se atribuye facultades que en ningún momento les delegamos como son inscribirnos en las denominadas "listas comerciales".

Por otra parte cabe señalar que las Instituciones Bancarias han adoptado un sistema denominado "***PROMESA DE PRIVACIDAD***" refiriendo que los datos proporcionados no les serán entregados a empresas diversas sin la previa autorización del cliente, sin embargo también hace referencia a que dado que el Banco puede actuar como facilitador en ofertas de compañías de "aprobada reputación" por lo que les proporcionan cierta información misma que no puede ser retenida, sin embargo al tener dicha información ya se hizo del conocimiento de diversas empresas lo cual no es informado previamente al cliente; asimismo, refieren que informan anualmente a sus clientes de la manera en que pueden excluir sus nombres de sus listas comerciales.

Sin embargo, yo considero que debería ser al contrario, esto es, que el cliente que se encuentre interesado en las listas comerciales de la Institución Bancaria se incluya en ellas bajo un procedimiento y no que el banco por sí apunte a todos sus clientes y después sean ellos quienes se excluyan dado que en ningún momento se solicitó dicho servicio ni mucho menos se autorizó la utilización de sus datos para fines distintos a la administración de un crédito, esto

trae aparejado que cuando se solicita la autorización de una tarjeta de crédito en cualquier institución bancaria, de un momento a otro, diversas instituciones similares localizan al solicitante informándole que le ha sido aprobada su solicitud aunque en ningún momento la haya realizado personalmente ante dicho Banco, generando así la desconfianza e incredulidad del solicitante que considera que sus datos estaban seguros.

Asimismo es necesario la creación de algún instituto que controle la base de datos que requieren las empresas asociadas al Internet, para evitar el mal uso que le pudieran dar a los mismos, así como su obtención a través de programas espías o facultades arbitrarias de las empresas a las que les confiamos nuestros datos, que atentan contra nuestra ***PRIVACIDAD***.

Ante lo cual y para el desarrollo del presente tema, nos basaremos principalmente en la investigación documental que al caso se genere, bajo una perspectiva jurídica, sin pasar por alto los antecedentes históricos de las comunicaciones, así como su inclusión en la Constitución Mexicana, utilizando además el método inductivo, determinando en principio las legislaciones existentes en la mayor parte del mundo para continuar con las actuales en México, se hará asimismo una descripción de aquellos conceptos que la misma materia informática requiere para su mayor comprensión.

Sin dejar de tomar en consideración que el objetivo principal del presente lo es el establecer la importancia que genera la garantía a la protección de la

privacidad en las personas, y la escasa normatividad con que se cuenta actualmente en el país para tal efecto, ante lo cual resulta indispensable la creación de un tipo penal específico que sancione las conductas tendientes a la violación de dicha garantía Constitucional.

Así pues, se propone un apartado específico en el Código Penal Federal para que, cuando no autoricemos explícitamente el uso de datos personales confidenciales, se sancione a quien tenga acceso a la misma así como a la empresa o institución que lo permitió.

CAPÍTULO 1.
ANTECEDENTES HISTÓRICOS – CRONOLÓGICOS DE LA GARANTÍA DE CORRESPONDENCIA E INVIOLABILIDAD DE CORRESPONDENCIA EN MÉXICO.

1.1 ANTECEDENTES PREVIOS A LA CONSTITUCIÓN DE 1912.

A efecto de entender el origen de la garantía de correspondencia e inviolabilidad de correspondencia en México, se tendrá que hacer un recorrido por las principales épocas históricas que vivió nuestro país y la importancia que la correspondencia y su inviolabilidad tenía, denotándose que, en la época precolombina, el castigo del mensajero en caso de incumplimiento, dependía del mensaje que se pretendía hacer llegar, en tanto que en la época colonial, no se le daba tanta importancia al sujeto, sino atendiendo al mensaje para evitar rebeliones, no obstante lo anterior, las comunicaciones fueron un factor importante para lograr la independencia de México para que en un momento dado se pudiera establecer como garantía Constitucional la inviolabilidad de la correspondencia y el derecho de toda persona a comunicarse.

1.1.1 ÉPOCA PRECOLOMBINA.

La cultura maya comenzó a desvanecerse hacia el año 800 de nuestra era por razones históricas complejas. Los españoles que invadieron México a principios del siglo XVI no encontraron ya sino vestigios de los mayas, centrando su lucha en los aztecas. Entre los objetos preciosos que reunieron en el primer botín en Veracruz, en 1519, había una especie de libros que el secretario privado de Hernán Cortés, López de Gómara, describió como que contenían “figuras, que

los mexicanos usan como letras". Se sabe ya con certeza que los únicos que podrían haber confeccionado aquellos libros no eran otros que los mayas. Desde prácticamente el momento en que esos preciosos testimonios fueron conocidos se iniciaron las especulaciones y la historia del desciframiento de aquellos signos que resultaron ser una escritura, mezcla de logogramas y de signos silábicos.[1]

Las estelas mayas y otros monumentos conmemorativos mayas y nahuas, los códices históricos, "libros de años" del mundo náhuatl prehispánico, redactados a base de una escritura principalmente ideográfica e incipientemente fonética, dan testimonio del gran interés que ponían, entre otros, nahuas y mayas por preservar el recuerdo de los hechos pasados de alguna importancia. Complemento de lo anterior eran los textos fielmente memorizados en sus centros prehispánicos de educación, donde se enseñaban a los estudiantes, además de otras cosas, las viejas historias acerca de cuanto había sucedido, año por año, tal como se consignaba en sus códices.[2]

Lo poco que ha llegado a la actualidad y que ha podido ser descifrado nos habla, desde las inscripciones monumentales, de hazañas, de guerras, de las familias reales. Y los viejos libros, los llamados Códices no son otra cosa que textos religioso – astronómicos. Los aztecas, y los pueblos que hallaron los españoles más al norte, concedían mayor valor a la elocuencia, a la palabra, promoviendo la transmisión oral. Se expresaban sin embargo de formas que aún hoy se conocen como dibujos en corteza de árboles ("amates") y en pieles de

[1] LOPEZ DE GÓMARA, Francisco, *Historia de la conquista de México, 2v., México, Editorial Robredo, 1943, p. 25.*
[2] Ibíd. p. 25

venado (“agave”).[3]

Aquellos signos eran “leídos” por expertos, una minoría. La pictografía y el discurso eran mucho más que la expresión de una clase o el instrumento de un poder. Como las leyes del discurso y del canto, los cánones de la pintura eran sólo el reflejo de un mundo superior y de un orden invisible. Esos cánones participaban de manera sistemática en el ordenamiento de una realidad que vinculaba íntimamente la experiencia humana y el mundo de los dioses. De estos tomaban los rasgos más sobresalientes, y señalaban los elementos más significativos, a expensas de lo accidental, lo arbitrario y lo individual. En ese sentido favorecían la representación, la manifestación antes que la comunicación.[4]

Bernal Díaz del Castillo[5] dejó registradas las formas de comunicación de los aztecas en varios de sus relatos. En los tramos finales de su gigantesca crónica cuenta algo de la vida cotidiana de los mexicanos:

> *“(tenían) librillos de un papel de cortezas de árbol que llaman amate...”* [6]

La persecución religiosa, como se dijo antes, fue en gran parte responsable de la desaparición de lo que podríamos llamar “lectores” o expertos en el reconocimiento de aquellos dibujos que hablaban. Muchos años más tarde los

[3] Ibíd. p. 28
[4] LEÓN PORTILLA, Miguel, *La Filosofía náhuatl, estudiada en sus fuentes,* México, Instituto Indigenista Interamericano, 1956, p. 87-89.
[5] DIAZ DEL CASTILLO, Bernal, *Historia verdadera de la conquista de la Nueva España*, 3 v., México, Robredo, 1939. Véase además la edición preparada por J. Ramírez Cabañas, 2 v., México, Porrúa, 1955. Hay otras ediciones. P. 36
[6] Ibíd. P. 39

librillos de que hablaba el cronista conquistador han sido descifrados.[7]

En el libro denominado “LA VISIÓN DE LOS VENCIDOS”[8] se relata la forma en que eran mandados los mensajeros por Moctezuma hacia las costas del Golfo por donde habían aparecido los forasteros al pensar que los recién llegados eran Quetzalcóatl de donde se advierte que dicho emperador a efecto de hacer cumplir sus órdenes determinaba que el que no las cumpliese los haría matar junto con su esposa, padres e hijos así como destruir sus casas, por lo que se denota el miedo que inspiraba a los mensajeros para hacer llegar los encargos o mensajes y así cumplir con las órdenes encomendadas.

1.1.2 ÉPOCA COLONIAL.

En la época colonial se vivió un sistema jurídico estamentario, el cual consistía en la impartición de justicia de acuerdo a la condición social, económica, religiosa o militar del individuo, por lo que se reconocían derechos mínimos a la clase baja y a la clase alta se le otorgaban mayores derechos en proporción a su posición social.[9]

La influencia del pensamiento enciclopedista de Europa, se hizo presente en nuestro país, mediante la obra de Fray Bartolomé de las Casas (El Memorial 1562/1563), en la que se condenan la conquista, la guerra, la violencia, la opresión y se justifica la rebelión de los indígenas, defendiendo su dignidad, libertad e igualdad.[10]

---

[7] Ibíd. p. 41
[8] LEON-PORTILLA, Miguel, *La Visión de los Vencidos,* 26ª reimpresión, UNAM, México, 2005.
[9] LOZANO, José Maria, *Estudio Del Derecho Constitucional Patrio*, Porrúa, México, 1987. p.374
[10] CASAS, Fray Bartolomé de las, *El Memorial,* México, FCE. 1563.

Paralelamente en Europa, se desarrollaron las estructuras sociales y políticas así como las económicas. Las ideas de Hobbes, Locke, Rousseau y Montesquieu, fundamentan el nacionalismo del siglo XIX, que posteriormente se introducen en nuestro país por medio de Alejandro de Humboldt.[11]

En la época colonial fue común la violación de la correspondencia. La suspicacia hizo ver peligros en todas partes y una carta dirigida a persona de quien se sospecha, fue ser un motivo terriblemente tentador para retenerla y abrirla. Con frecuencia sucedió que después de cometido ese abuso nada justificó las sospechas y temores que lo determinaron. Ordinariamente los conspiradores y los que con ellos simpatizaron no se sirvieron del correo público para comunicarse, pero la administración suspicaz y medrosa ve en todas partes enemigos y en todas partes buscó pruebas. Durante el gobierno de los generales Zuloaga y Miramón, se dio la orden a la Dirección General de Correos para que no se entregara carta alguna, sino después de abierta y leída por el Director en presencia del interesado. “Este abuso que no tuvo calificativo se consumió en los mismos términos que fue ordenado, y no hay noticia de que hubiera aprovechado a sus autores para contener los avances de una revolución que tenía en su favor la ley y la opinión pública”.[12]

1.1.3 ÉPOCA DE LA INDEPENDENCIA.

México ha tenido diversas constituciones a lo largo de su historia. Algunas han sido centralistas, es decir, que establecen el poder en un solo órgano que

[11] LOZANO, José Maria, Op. Cit. p. 376
[12] Idem.

controla todas las decisiones políticas del país y otras federalistas, como la actual, que reconocen la soberanía de los estados pero cuentan con mecanismos de coordinación para asuntos de la República como un todo. [13]

Las leyes fundamentales emanadas de un Congreso Constituyente en México son:[14]

- Acta constitutiva de la Federación y la Constitución Federal de los Estados Unidos Mexicanos, de 1824.
- Las Siete Leyes Constitucionales, de 1835-1836.
- Bases orgánicas de la República Mexicana de 1843.
- Acta constitutiva y de Reformas, de 1847.
- Constitución Federal de los Estados Unidos Mexicanos, de 1857, y
- Constitución Política de los Estados Unidos Mexicanos, de 1917.

Otros factores importantes en la Independencia de México fueron la Declaración de Independencia de los Estados Unidos (1776) y la Declaración de los Derechos del Hombre y del Ciudadano en Francia (1789). Así, mientras que a nivel internacional se inicia la normatividad de los Derechos Humanos sobre el individuo y la sociedad haciéndolas ley, en México se avanza hacia la independencia.[15]

Haremos ahora un breve recorrido para ver qué aspectos de la privacidad

[13] TENA RAMÍREZ, Felipe, *Leyes fundamentales de México*, *1808-1991*, 16a. ed., Porrúa, México, 1991, p. 38-43
[14] Ibíd. p. 43
[15] Ibíd. p. 44

han sido recogidos para su protección en nuestra historia constitucional, comenzando con textos a los que podríamos llamar preconstitucionales, como los Elementos Constitucionales de Ignacio López Rayón de 1811, que simplemente protegieron el desarrollo de la vida privada en el domicilio, al considerar a este "como un asilo sagrado" (punto 31). Poco después Don José María Morelos y Pavón consignó una fórmula similar en sus famosos Sentimientos de la Nación en 1813, al establecer en el punto 17: "Que a cada uno se le guarden las propiedades y respete en su casa como en un asilo sagrado, señalando penas para los infractores". Es claro que esta tutela del domicilio se refiere a varios aspectos, como la propiedad privada y la seguridad, pero también se está tutelando la vida privada, la intimidad y la vida familiar.[16]

Texto similar a los anteriores se recogió también en 1814 en el artículo 32 del Decreto Constitucional para la Libertad de la América Mexicana, conocido como Constitución de Apatzingán. Sin embargo, en esta Constitución se inicia ya también la tutela de otro aspecto, expresión de la privacidad, que es el correspondiente al honor, ya que el artículo 40 establecía una amplia libertad de pensamiento, expresión e imprenta, teniendo como únicos límites el no atacar al dogma, turbar la tranquilidad pública u ofender al honor. [17]

1.1.3.1 CONSTITUCIÓN DE 1824.

La primera constitución propiamente mexicana es la promulgada el 03 de octubre de 1824, denominada “Constitución Federal de los Estados Unidos

[16] Ibíd. p. 49
[17] Ibíd. p. 52

Mexicanos” ya que en ella se descarta todo tipo de legislación extranjera y se proclama el ejercicio absoluto de la soberanía y la autodeterminación.[18]

En la Constitución de 1824, la protección de la privacidad, vinculada con el domicilio, es ahora más extensa, ya que abarca los papeles y efectos personales de los individuos, en los términos del artículo 152, que literalmente establecía: "Ninguna autoridad podrá librar orden para el registro de las casas, papeles y otros efectos de los habitantes de la República, sino en los casos expresamente dispuestos por la ley, y en la forma en que ésta determine." En cambio, la tutela del honor en relación con las libertades de expresión e imprenta, que se había consignado en Apatzingán, aquí desaparece al dejarse a que sea la ley la que regule el ejercicio de dichas libertades, limitándose, como principio general, a proscribir la práctica de la previa censura.[19]

En las Siete Leyes Constitucionales de 1836, en la primera de ellas, dedicada a los "Derechos y obligaciones de los mexicanos y habitantes de la República", entre los derechos del mexicano consagrados en el artículo 2, se establece, en la fracción IV: "No poderse catear sus casas y sus papeles, si no es en los casos y con los requisitos literalmente prevenidos en las leyes." Y respecto a las libertades de imprenta, de nuevo se deja a la ley la reglamentación de su ejercicio.[20]

1.1.3.2 CONSTITUCIÓN DE 1857.

En el año de 1857 el orden jurídico se enaltece con la expedición de una

[18] Ibíd. p. 54
[19] Idem.
[20] Ibíd. p. 58

nueva Constitución, el 5 de febrero del mismo año.

Como es sabido la Constitución de 1857, en lo que se refiere a los derechos humanos, bajo su consagración como garantías individuales, contiene una amplia gama de derechos que es casi literalmente el texto que después es recogido por el Constituyente en 1916-1917, y que en gran parte de su contenido se mantiene en nuestra Constitución vigente hasta la fecha. Así pues, el texto constitucional de 1857, en su artículo 16 estableció como garantía el que: "Nadie puede ser molestado en su persona, familia, domicilio, papeles y posesiones, sino en virtud de mandamiento escrito de la autoridad competente que funde y motive la causa legal del procedimiento." Este texto pasó literalmente al mismo artículo 16 en la Constitución de 1917, y hasta la fecha es el párrafo inicial de este artículo que ha sido enriquecido con otros derechos, ya sea de nueva creación o reubicados dentro del texto constitucional. Además de los requisitos expresos para poder realizar cateos, actualmente en el párrafo noveno, en 1917 se añadió también la protección del domicilio respecto de la realización de visitas domiciliarias de la autoridad administrativa, las que se limitan y someten a las formalidades de los cateos.[21]

Podemos ver que aquí se tutela ya con mayor amplitud la vida privada del individuo, incluyendo la vida familiar, el domicilio y todas las posesiones, como un límite ya no sólo frente a otro derecho, sino también frente a la autoridad, es decir, frente al poder; constituyendo dichos aspectos de la privacidad valores fundamentales a respetar en la relación gobierno-gobernado, y derechos fundamentales del individuo garantizados por el Estado.

[21] Ibíd. p. 67

Otro aspecto de la privacidad tutelado desde la Constitución de 1857 es el relativo a la comunicación, ya que en el artículo 25 se garantizó la inviolabilidad de la correspondencia.[22]

El texto se recogió también en 1917 en el mismo numeral, y en 1983, por reforma constitucional, pasó al artículo 16, actualmente como párrafo once. Debemos entender aquí que lo que el legislador pretendió tutelar desde 1857 no fue la correspondencia misma, que es simplemente un medio; lo que se tutela es la confidencialidad de la comunicación, la privacidad de ésta, y como tal este artículo debiera adaptarse de manera que su protección alcance a los modernos medios de comunicación, por cierto algunos inimaginables en 1857, como el teléfono, el telégrafo, el fax, la comunicación por radio e incluso las novedosas redes de telecomunicación computarizada, las cuales, sin embargo, a falta de la reforma, también podrían ser tuteladas por la vía jurisdiccional.[23]

Por desgracia, en México nuestro máximo tribunal no se ha caracterizado sino por aplicar las normas de manera literal, y porque nunca su interpretación en relación con los derechos humanos ha resultado extensiva, por lo que seguramente será necesario esperar a la correspondiente reforma constitucional, ello es así en virtud de que a la fecha existe protección constitucional a las comunicaciones que son privadas, sin embargo no existe garantía alguna que se refiera a la vulnerabilidad para la intercepción de contenidos en las nuevas formas de comunicación y especialmente hablando de las computadoras, telefonía celular, Internet y demás medios que conforme a los avances tecnológicos existen

[22] Ibíd. p. 69
[23] Ibíd. p. 75

actualmente puesto que la mayoría de las autoridades al seguir un lineamiento de juzgar conforme a la letra de la ley no toman en cuenta que, al referirse a las comunicaciones estas pueden ser diversa índole y no limitarse a las conocidas popularmente encontrándose así en cierta forma impedidas para aplicar la ley conforme a sus propios criterios.

1.2. GARANTÍAS PREVISTAS EN LA CONSTITUCIÓN DE 1917.

A finales de **1916**, los revolucionarios se reunieron en Querétaro para reformar la Constitución de 1857. Finalmente decidieron redactar una nueva, pues las circunstancias de México en ese momento eran muy diferentes a las que había en tiempos de Juárez, cuando se hizo la de 1857. [24]

La nueva Constitución se promulgó el 5 de febrero de 1917. En ella se incorporaron ideas de todos los grupos revolucionarios. Retomó las libertades y los derechos de los ciudadanos, así como los ideales democráticos y federales de la de 1857. También reconoció los derechos sociales, como el de huelga y el de organización de los trabajadores, el derecho a la educación y el derecho de la nación a regular la propiedad privada de acuerdo con el interés de la comunidad.[25]

Cabe destacar que en el objeto directo del presente estudio referente al DERECHO A LA PRIVACIDAD se crea un paralelismo entre el derecho a la inviolabilidad del domicilio y el derecho a la inviolabilidad de la correspondencia, ya que en ambos puede hablarse y con idéntico contenido, de una doble perspectiva, directa e indirecta del objeto.

[24] MÁRQUEZ RÁBAGO Sergio R. *EVOLUCIÓN CONSTITUCIONAL MEXICANA*, Porrúa, México, 2002, Pág. 389.
[25] Ibíd. p. 390

Ello es así ya que en ambos derechos es de una forma inmediata la intimidad, entendida como ámbito de datos de la persona que se pretende no sean conocidos. El objeto, de ambos derechos, considerados desde una perspectiva indirecta, puede servir además de garante de la seguridad personal y del honor, entre otros bienes de la personalidad.

La inviolabilidad de la correspondencia constituye no sólo un derecho que es especificación y concreción del derecho a la intimidad, sino además constituye una garantía procesal de primera magnitud, en cuanto que los datos o información obtenida de la correspondencia requisada deben haber sido obtenidos legalmente para que puedan ser utilizados como instrumentos de prueba.[26]

Por otra parte, constituye también una garantía en relación a posibles actuaciones arbitrarias por parte de fuerzas de seguridad del Estado a la par que garantiza la protección de las comunicaciones privadas.

Proteger los datos personales a través de la protección de la inviolabilidad de la correspondencia y de las comunicaciones privadas, es proteger indirectamente la seguridad personal, lo cual es especialmente importante en sistemas totalitarios, en los que el poder de la minoría dominante se sustenta, al menos en parte, en virtud del control que se realiza sobre la conductas de los ciudadanos.[27]

Concluyendo así que la necesidad de salvaguardar la intimidad personal frente a las intromisiones de una información malévola, indiscreta o meramente indeseada es inherente a la condición humana cualquiera que sea el medio con

[26] Como se puede denotar del contenido de los artículos 111, 121, 760, 770 Fracción III, 791, 800, 818 del Código de Procedimientos Civiles en el Distrito Federal.
[27] MÁRQUEZ RÁBAGO Sergio Op. Cit. p. 391

que tal inmisión se realice, resultando con ello una mayor sensibilidad de la gente respecto de su intimidad, como derecho humano intangible, con la consiguiente voluntad de hacerlo valer y defenderlo resueltamente.[28]

Es por todo lo anterior, que para la fundamentación de la presente, se tomará únicamente en consideración el apartado concerniente a la inviolabilidad de la correspondencia y de las comunicaciones privadas que se establece en el artículo 16 párrafo noveno de nuestra Constitución, contenido en el Título Primero, Capítulo I denominado "DE LAS GARANTÍAS INDIVIDUALES".

Es de resaltarse que la inviolabilidad de la correspondencia se encontraba establecida en el artículo 25 Constitucional (de la Constitución de 1857) y por efectos de la reforma publicada el día tres de febrero de 1983, su contenido pasó a formar parte del artículo 16 Constitucional adicionando dos párrafos como tercero y cuarto, vigente al día siguiente de su publicación estableciendo al respecto únicamente:[29]

"*La correspondencia que bajo cubierta circule por las estafetas estará libre de todo registro, y su violación será penada por la ley..." (párrafo tercero).*

Así la correspondencia por estafeta es una expresión que se refiere a los documentos que circulan por el correo ordinario, dicha reforma se basó principalmente en que el derecho del hombre en lo que atañe a su privacidad no es tan sólo en sus posesiones, domicilio, papeles o en su familia, sino también en

[28] Ibíd. p. 391
[29] Ibíd. P. 393

su intimidad, trascendiendo así a sus papeles íntimos, que es lo que constituye su correspondencia. [30]

El objetivo de ésta garantía es que la autoridad no actúe ni permita que otros lo hagan, violando el límite o ámbito de privacidad que el precepto tutela. Es una garantía que se ha dado como consecuencia de la inviolabilidad de la privacidad del hombre, ya que tiene todo el derecho de que no se le censure y no se abra su correspondencia como un medio de comunicación que tiene con sus semejantes.

Esta libertad tiene como limitaciones las órdenes de cateo y las contenidas en la Ley del Servicio Postal Mexicano en sus artículos 9 y 10 que se refieren a que no se viola el sigilo de la correspondencia:[31]

I. Cuando los informes se rindan en acatamiento a una orden judicial, o del Ministerio Público dictada por escrito,

II. Al rendir los datos estadísticos que deban proporcionar de acuerdo con las leyes,

III. En los casos permitidos expresamente en las leyes..."

Asimismo la violación al derecho a la privacía contenido en el precepto en análisis es sancionado por la Ley de Vías Generales de Comunicación en sus artículos 576, 577 y 578 al sancionar "al que indebidamente abra, destruya o substraiga alguna pieza de correspondencia cerrada, confiada al Correo".[32]

[30] Ibíd. Pág. 407
[31] Ley del Servicio Postal Mexicano.
[32] Ley de Vías Generales de Comunicación.

Y en el Código Penal Federal en sus artículos 173 a 175 al sancionar al:[33]

> "Que abra indebidamente una comunicación escrita que no esté dirigida a él y al que indebidamente intercepte una comunicación escrita que no esté dirigida a él, aunque la conserve cerrada y no se imponga de su contenido".

Asimismo se establece que no se considera que obren delictuosamente los padres "que abran o intercepten las comunicaciones escritas a sus hijos menores de edad, y los tutores respecto de las personas que se hallen bajo su dependencia y los cónyuges entre sí."[34]

Cabe señalar que el articulo 16 Constitucional sufrió diversas modificaciones siendo la **primera reforma** en la que se adicionan dos párrafos como tercero y cuarto vigentes al día siguiente de su publicación en el Diario Oficial de la Federación del 3 de febrero de 1983, erratas día 6 siguiente, mismos párrafos que se refieren a que la correspondencia que circule por las estafetas estará libre de todo registro, así como el alojamiento que podrán tener los militares en tiempo de guerra; posteriormente con fecha 03 de septiembre de 1993, se publica en el Diario Oficial de la Federación una **segunda reforma** en la que se modifican los dos primeros párrafos y se adicionan cinco más referentes principalmente a la fundamentación y motivación de todo acto de autoridad, sobre la querella, denuncia o acusación necesaria para el libramiento de una orden de aprehensión, la puesta a disposición inmediata ante la autoridad judicial del cumplimiento de una orden de aprehensión, respecto de los casos de delito flagrante, de la detención ordenada por el Ministerio Público y los plazos que tiene

[33] Código Penal Federal, artículo 173
[34] Ibíd. Artículo 174

dicha autoridad para poner a disposición a alguna persona ante un juez en caso de una retención.[35]

1.3 RELATORÍA DE LA EXPOSICIÓN DE MOTIVOS Y JURISPRUDENCIA QUE DERIVA EN LA REFORMA DEL ARTÍCULO 16 CONSTITUCIONAL RESPECTO DE LA GARANTÍA DE LA INVIOLABILIDAD DE CORRESPONDENCIA.

Posterior a la reforma antes señalada, con fecha 03 de julio de 1996 se publicó en el Diario Oficial de la Federación la adición de dos párrafos como noveno y décimo del artículo 16 Constitucional[36] para quedar en lo conducente, como sigue:

> *"Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente, por escrito deberá fundar y motivar las causas legales de la solicitud, expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor.*
>
> *Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes. Los resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio…."*

En la exposición de motivos de dicha reforma se sostiene:[37]

---

[35] MÁRQUEZ RÁBAGO Sergio Op. Cit. p. 415
[36] Ibíd. p. 420
[37] Ibíd. pp. 421 a 425

"I. INTRODUCCIÓN Y JUSTIFICACIÓN.

1. La delincuencia organizada es, sin duda, uno de los problemas más graves por los que atraviesa México y toda la comunidad mundial, que en sus diversas manifestaciones, entre las que destaca el narcotráfico, afecta a las vidas de miles de seres humanos y atenta contra los principios básicos de la vida comunitaria y de la esencia del Estado, generando descomposición social e inestabilidad política. Se trata, además de un fenómeno de carácter trasnacional, que plantea incluso una amenaza directa para la estabilidad de las naciones y constituye un ataque frontal contra las autoridades políticas de los Estados.

Los métodos y técnicas que utilizan en las formas modernas de delincuencia, así como su realización cada vez más violenta y su internacionalización, hacen que la delincuencia organizada observe actualmente una mayor eficacia frente a los medios tradicionales de control estatal, por lo que éstos también deben modernizarse para combatirla eficazmente. Si ello no ocurre, se debilita la capacidad efectiva del Estado para proteger los derechos fundamentales del ser humano.

II. REFORMAS CONSTITUCIONALES PROPUESTAS.

1. Reforma al artículo 16 Constitucional.

Una de las estrategias que se consideran indispensables para mejorar la capacidad del Estado en la lucha contra la delincuencia, particularmente la organizada, es organizada (sic) es la relativa a la intervención de comunicaciones telefónicas y de otros medios de comunicación similares por parte de la autoridad competente, ya que permite buscar pruebas judiciales al interceptar, mediante grabación magnetofónica, las comunicaciones telefónicas, radiotelefónicas ***y similares****, que se pertenecen o colaboran con una organización criminal.*

Este tema, sin embargo, no es nada sencillo y el debate público en torno a él ha provocado un creciente interés, dadas las consecuencias que puede implicar prohibirlo o regularlo. Así, por ejemplo, prohibirlo implicaría obstaculizar el diseño y establecimiento de medios eficaces del Estado tendientes a mejorar sus tareas de investigación policial; y regularlo, sin el debido cuidado, podría provocar que se vulneraran derechos fundamentales de la persona. Además de la desventaja que la prohibición trae para las Instituciones del Estado, se ampliarían las ventajas para las organizaciones criminales, que actualmente, dado su poderío económico, hacen uso de los métodos y técnicas más modernas, entre ellas las de intercepción de medios de comunicación y aprovechan los adelantos científicos y tecnológicos para colaborar a través de las fronteras nacionales e idear estrategias que ningún estado puede contrarrestar por sí solo, sobre todo si éstos no utilizan tales mecanismos.

En efecto, por lo que hace a la intervención de comunicaciones telefónicas y otros medios similares, cuya incorporación se considera

indispensable en la legislación penal como estrategia político criminal, ha provocado ciertas inquietudes respecto de su constitucionalidad, observándose diversidad de opiniones sobre el particular, desde las que consideran que su autorización tiene sustento constitucional hasta las que piensan que vulnera derechos fundamentales y, por ello, se contrapone a la Constitución. Ciertamente se han exteriorizado opiniones en el sentido de que permitir la intervención de medios de comunicación vulneraría garantías constitucionales, como lo es la ***"intimidad", o "vida privada"*** *de las personas, sobre todo si no se limita dicha intervención. Pero, igualmente existen opiniones que sostienen que, como todo acto de molestia, puede fundarse y motivarse por mandamiento de autoridad competente, como lo prevé el párrafo primero del artículo 16 Constitucional; por lo que regular la autorización de las intervenciones telefónicas y de otros medios de comunicación no contravendría la Constitución.*

Lo anterior indica que hay diversidad de criterios respecto de los alcances de ciertas previsiones constitucionales. Por lo que, atendiendo incluso a sugerencias en este sentido, para mayor seguridad, proponemos adicionar un párrafo noveno al artículo 16 de la Constitución, para regular precisamente lo que se conoce como ***intervenciones de medios de comunicación privada,*** *como la telefonía telegráfica o Radiotelefonía, o a través de la colocación secreta de aparatos de registro ambiental.*

Al analizar la posibilidad de regular la autorización de las intervenciones telefónicas y de otros medios de comunicación privada, se plantearon diversas alternativas: reformar el párrafo octavo del artículo 16 Constitucional, que se refiere a los cateos, o reformas al párrafo décimo de dicho artículo, que establece ***la inviolabilidad de la correspondencia****. Esta última alternativa implicaba, por una parte, ampliar esa garantía a otros medios de comunicación privada y, por otra, prever los casos en que dichos medios de comunicación podrían ser interferidos así como los requisitos para ello.*

Se consideró, en cambio, que si hacemos alguna breve referencia histórica observamos que el contenido del actual párrafo décimo del artículo 16 Constitucional se ha mantenido inalterado desde la Constitución de 1857, en 1983 sólo cambió de ubicación, pasando a formar parte del artículo 16, pero sin referirse a los modernos medios de comunicación que a la fecha se han alcanzado a raíz de los extraordinarios avances tecnológicos en esta materia. Puede admitirse que, si bien la "intimidad" o la "vida privada" o "privacidad" es el bien jurídico que está de por medio y por cuya razón se protege, por ejemplo, la correspondencia y se sancionan ciertas conductas que la afectan, el Constituyente Permanente no tuvo la intención de preverla a nivel Constitucional, porque no le proporcionó protección adecuada a la intimidad o vida privada frente a los nuevos medios de comunicación, pudiéndose pensar que, para los actos de molestia que, implicaría su aplicación, se haya considerado aplicable el párrafo primero del propio

artículo 16 Constitucional.

Es incuestionable que el desarrollo industrial y tecnológico introduce descubrimientos que facilitan grandemente el acceso a la vida privada, como es el caso de los medios de vigilancia electrónica, frente a los cuales resulta inútil todo intento de salvaguardar la esfera privada de la persona mediante fórmulas jurídicas tradicionales.

Por tal razón, hemos considerado conveniente proponer la adición de un párrafo noveno al artículo 16 de la Constitución, para regular expresamente las intervenciones de medios de comunicación privada, como la telefónica y telegráfica, entre otros, para que desde el plano constitucional se prevea posibilidad de su uso para ciertos fines relacionados sobre todo con la justicia penal.

Se precisa en la propuesta de reforma, ***que la intervención de cualquier medio de comunicación privada, o bien la colocación secreta de aparatos tecnológicos, podrán ser utilizados sólo por la autoridad judicial federal, con lo cual su práctica se limita****. Pero además se establece que dichas intervenciones se ajustarán a los requisitos y límites que las leyes respetivas prevean. Dada la naturaleza del acto de molestia, se precisa, por una parte, que la autoridad competente para expedir el mandamiento únicamente sea la judicial y, por otra, que dicha autoridad judicial sea la federal, para restringir el uso de esta diligencia. Y, para mayor garantía de que su uso no se haga arbitraria y descontroladamente, se precisa que quienes las realicen sin los requisitos que la ley prevé, serán sancionados penalmente, aparte de que los resultados de tales diligencias carecerán de todo valor probatorio.*

Finalmente, debe entenderse que la mencionada intervención o interferencia adquiere sentido si se trata de comunicaciones privadas; por esa razón es que se precisa en la propuesta, que las comunicaciones que pueden ser objeto de alguna intervención, registro o interferencia, son las privadas."

De lo anteriormente reproducido se desprende que el ámbito de protección de esta garantía se limita en principio a las comunicaciones telefónicas; sin embargo, la redacción del precepto y una interpretación pro gobernado, "permite establecer que se refiere a todo tipo de comunicaciones, con excepción de la correspondencia que circule por el correo ordinario, cuyas prescripciones se regulan de forma independiente". [38]

[38] Ibid, p. 411.

Se establece la garantía individual de la inviolabilidad de las comunicaciones que no circulen por el correo ordinario, así como la posibilidad que la autoridad judicial federal ordene la intervención a petición de la autoridad federal competente o del Ministerio Público de las entidades federativas. La solicitud de intervención deberá ser por escrito, fundando y motivando las razones por las que se pide la intervención, señalando además el tipo de ésta, los sujetos y su duración. El resultado de estas intervenciones que no se ajuste a estos requisitos no tendrá valor probatorio alguno. [39]

La Constitución es firme en prohibir las intervenciones de comunicaciones en materia electoral, fiscal, mercantil, civil, laboral o administrativo, donde la inviolabilidad de las comunicaciones es absoluta, de lo que se desprende que el resultado de la intervención sólo podrá utilizarse en materia penal.

Al respecto ya existen pronunciamientos de la Segunda Sala de la Suprema Corte de Justicia de la Nación a saber:

Novena Época
Instancia: Segunda Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
Tomo: XII, Diciembre de 2000
Tesis: 2a. CLX/2000
Página: 428

COMUNICACIONES PRIVADAS. EL DERECHO A SU INVIOLABILIDAD, CONSAGRADO EN EL ARTÍCULO 16, PÁRRAFO NOVENO, DE LA CONSTITUCIÓN FEDERAL, ES OPONIBLE TANTO A LAS AUTORIDADES COMO A LOS GOBERNADOS, QUIENES AL TRANSGREDIR ESTA PRERROGATIVA INCURREN EN LA COMISIÓN DE UN ILÍCITO CONSTITUCIONAL. Del análisis de lo

[39] ROJAS CABALLERO, Ariel Alberto, *LAS GARANTÍAS INDIVIDUALES EN MÉXICO*, Porrúa, México, 2002, p. 364

dispuesto en diversos preceptos de la Constitución Política de los Estados Unidos Mexicanos, se advierte que la misma contiene mandatos cuyos destinatarios no son las autoridades, sino que establece deberes a cargo de los gobernados, como sucede, entre otros casos, de lo dispuesto en sus artículos 2o., 4o. y 27, en los que la prohibición de la esclavitud, el deber de los padres de preservar el derecho de los menores a la satisfacción de sus necesidades y a la salud física y mental, así como los límites a la propiedad privada, constituyen actos u omisiones que deben observar aquellos, con independencia de que el mandato constitucional constituya una garantía exigible a las autoridades y que, por ende, dentro de su marco competencial éstas se encuentren vinculadas a su acatamiento. En tal virtud, al establecer el Poder Revisor de la Constitución, en el párrafo noveno del artículo 16 de la Constitución General de la República, que las "comunicaciones privadas son inviolables", resulta inconcuso que con ello estableció como derecho fundamental el que ni la autoridad ni los gobernados pueden intervenir una comunicación, salvo en los casos y con las condiciones que respecto a las autoridades establece el propio numeral y, por tanto, la infracción de los gobernados a tal deber conlleva la comisión de un ilícito constitucional, con independencia de los efectos que provoque o del medio de defensa que se prevea para su resarcimiento, en términos de la legislación ordinaria correspondiente.
Amparo en revisión 2/2000. Norma Angélica Medrano Saavedra. 11 de octubre del año 2000. Unanimidad de cuatro votos. Ausente: José Vicente Aguinaco Alemán. Ponente: Guillermo I. Ortiz Mayagoitia. Secretaria: María Elena Rosas López.

Novena Época
Instancia: CUARTO TRIBUNAL COLEGIADO EN MATERIA PENAL DEL PRIMER CIRCUITO.
Fuente: Semanario Judicial de la Federación y su Gaceta
Tomo: XVIII, Julio de 2003
Tesis: I.4o.P.21
Página: 1146

INTERVENCIÓN DE COMUNICACIONES PRIVADAS. SUJETO PASIVO DEL DELITO. El respeto a las comunicaciones privadas es acogido por el artículo 16 constitucional, específicamente en el párrafo noveno, erigiéndose así en un derecho público subjetivo, el cual, como toda garantía, se halla sujeto a limitaciones o excepciones que se sustentan, fundamentalmente, en la protección de intereses de la sociedad y derechos de los gobernados, limitaciones que, incluso, han dado origen a la figura de intervención de comunicaciones privadas previa autorización judicial. En estas condiciones, al encontrarse obligado el Estado, como sujeto pasivo de la citada garantía, a velar por dichos intereses, con apego a las normas constitucionales y legales, se

constituye en garante del interés social y establece normas que tienden a protegerlo, tal es el caso de la infracción penal por intervención de comunicaciones privadas cometida por servidores públicos. Por ello, en casos como el analizado, **el bien jurídico recae en el interés común, pues la finalidad perseguida con la incursión de la figura de la intervención de comunicaciones privadas previa autorización judicial, fue precisamente la de proteger a la colectividad contra el constante incremento del crimen organizado**, de ahí que la lesión por el ilícito estudiado recaiga en la sociedad, convirtiéndose así en sujeto pasivo de la infracción punitiva, puesto que la salvaguarda de la seguridad y privacidad de las comunicaciones, como se dijo, encuentra su limitante en la satisfacción del interés común de la sociedad, quien es la interesada en que el derecho a la privacía no sea violado sino sólo en los casos permitidos por la ley.
CUARTO TRIBUNAL COLEGIADO EN MATERIA PENAL DEL PRIMER CIRCUITO.
Amparo en revisión 744/2002. 3 de diciembre de 2002. Unanimidad de votos. Ponente: José Rafael Vásquez Hernández. Secretario: Joel Reyes Martínez.

Novena Época
Instancia: Segunda Sala
Fuente: Semanario Judicial de la Federación y su Gaceta
Tomo: XII, Diciembre de 2000
Tesis: 2a. CLXI/2000
Página: 428

COMUNICACIONES PRIVADAS. LAS PRUEBAS OFRECIDAS DENTRO DE UN JUICIO CIVIL, OBTENIDAS POR UN GOBERNADO SIN RESPETAR LA INVIOLABILIDAD DE AQUÉLLAS, CONSTITUYEN UN ILÍCITO CONSTITUCIONAL, POR LO QUE RESULTAN CONTRARIAS A DERECHO Y NO DEBEN ADMITIRSE POR EL JUZGADOR CORRESPONDIENTE. El artículo 16, párrafo noveno, de la Constitución Política de los Estados Unidos Mexicanos establece que las comunicaciones privadas son inviolables; que exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada; que dicha petición deberá ser por escrito, en la que se funden y motiven las causas legales de la solicitud, expresando el tipo de intervención, los sujetos de la misma y su duración; y que no se podrán otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor. El párrafo décimo de dicho numeral señala que las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes, y que los

> resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio. Ante ello, debe estimarse que fue voluntad del Poder Revisor de la Constitución establecer como derecho fundamental la inviolabilidad de las comunicaciones privadas y, en contrapartida, la obligación exigible tanto a las autoridades como a los gobernados de respetar dicha prerrogativa, lo que da lugar a que si un gobernado realiza la intervención de alguna comunicación privada sin el consentimiento expreso e irrefutable de los que la entablan, incurrirá en un ilícito constitucional; por ende, si dentro de un juicio civil, en cualquiera de sus especies, una de las partes ofrece como prueba la grabación de una comunicación privada que no fue obtenida legalmente, tal probanza debe estimarse contraria a derecho y, por tanto, no debe admitirse por el juzgador correspondiente, pues ello implicaría convalidar un hecho que en sí mismo es ilícito.
>
> Amparo en revisión 2/2000. Norma Angélica Medrano Saavedra. 11 de octubre del año 2000. Unanimidad de cuatro votos. Ausente: José Vicente Aguinaco Alemán. Ponente: Guillermo I. Ortiz Mayagoitia. Secretaria: María Elena Rosas López.

Posterior a lo antes referido, se presentó una **cuarta reforma** publicada en el Diario Oficial de la Federación el día 8 de marzo de 1999 el cual modifica el párrafo segundo del artículo en estudio mismo que se refiere a la comprobación del *cuerpo del delito* para poder librar una orden de aprehensión.[40]

De todo lo cual se puede observar que el *DERECHO A LA PRIVACIDAD* se encuentra consagrada como una Garantía Constitucional por lo tanto resulta obligatorio velar por su protección, no solo en la aplicabilidad a las comunicaciones privadas, sino en el sentido más amplio que pudiera tenerse de la propia privacidad, y tomando en cuenta al tema específico de este trabajo, en lo que se refiere a la privacidad de nuestros datos personales y el uso moderado de los mismos previo consentimiento de nosotros sea cual sea nuestra posición económica y aún y cuando el conocimiento de estos sea para nuestro beneficio

[40] MÁRQUEZ RÁBAGO Sergio Op. Cit. p. 420

considero que debe tenerse un especial cuidado de ellos ya que su uso indiscriminado puede traernos varios problemas tanto económicos, personales y hasta pueden servir para la comisión de delitos en nuestro agravio o de nuestros familiares.

CAPÍTULO 2.
GENERALIDADES DE LA GARANTÍA DE CORRESPONDENCIA E INVIOLABILIDAD DE LAS COMUNICACIONES Y SU RELACIÓN CON LOS DATOS PERSONALES EN LA INFORMÁTICA.

Como se estableció en el capítulo anterior, la Constitución Política de los Estados Unidos Mexicanos determina como una garantía de seguridad jurídica la protección a las Comunicaciones Privadas toda vez que el derecho del hombre en lo que atañe a su privacidad no es tan sólo en sus posesiones, domicilio, papeles o en su familia, sino también en su intimidad, trascendiendo así a sus papeles íntimos que es lo que constituye su correspondencia, así como todo tipo de medios de comunicación a excepción de la correspondencia que circule por el correo ordinario, cuyas prescripciones se regulan de forma independiente. Esto es, se refiere a todo tipo de comunicaciones tomando en cuenta los nuevos avances tecnológicos que facilitan grandemente el acceso a la vida privada.

Ahora bien, en éste capítulo se establecerán para mayor comprensión, los conceptos de garantías individuales, de inviolabilidad, de comunicación, de la privacidad, de la intimidad y sus generalidades, su importancia a nivel civil y penal, se delimitará el concepto de derecho informático y de la libertad informática, así como una breve historia de la red Internet al constituir un medio utilizado para la adquisición de los datos personales, la seguridad utilizada para su manejo y en contrario, el surgimiento de los programas espías y su uso por algunas empresas, asimismo se determinan algunas consecuencias jurídicas y sociales de no evitar la proliferación de dichos programas espías, así como la obtención de los datos

personales por otros medios que no sean precisamente por Internet, pero que se pueden obtener por este medio.

2.1 CONCEPTO DE GARANTÍAS INDIVIDUALES.

Las Garantías individuales se pueden determinar como aquellos derechos fundamentales o libertades individuales que conforman la dignidad de la persona, que se recogen y expresan en la Constitución de un Estado como reconocimiento a los gobernados. Estos derechos fundamentales constituyen el estatuto personal de los individuos, por lo que son inalienables y están salvaguardados en las propias constituciones frente al Estado y sus órganos de gobierno.[1]

De acuerdo con Alfonso Noriega, las garantías individuales "son derechos naturales, inherentes a la persona humana, en virtud de su propia naturaleza y de la naturaleza de las cosas que el estado debe reconocer, respetar y proteger mediante la creación de un orden jurídico y social que permita el libre desenvolvimiento de las personas, de acuerdo con su propia y natural vocación, individual y social."[2]

En nuestro sistema constitucional, las garantías individuales y más bien los derechos fundamentales garantizados por la Constitución, aluden no sólo a la persona física, sino que involucran a todo gobernado, por lo que también son merecedoras de aquellas las personas morales de derecho privado al ser constituidas por personas físicas.

[1] ROJAS CABALLERO, Ariel Alberto, Op. Cit. p. 372
[2] NORIEGA CANTU, Alfonso, *LECCIONES DE AMPARO.* Porrúa, México, 1980, p. 54

Al respecto existen criterios jurisprudenciales que delimitan el alcance y contenido de las garantías individuales, como se puede observar en la siguiente jurisprudencia:

Época: Novena.
Instancia: Pleno.
Fuente: Semanario Judicial de la Federación y su Gaceta.
Parte : III, Junio de 1996.
Tesis: P. LXXXVI/96.
Página: 459.

GARANTÍAS INDIVIDUALES. CONCEPTO DE VIOLACIÓN GRAVE DE ELLAS PARA LOS EFECTOS DEL SEGUNDO PÁRRAFO DEL ARTÍCULO 97 CONSTITUCIONAL.

Las violaciones graves de garantías a que se refiere dicho artículo, son hechos generalizados consecuentes a un «estado de cosas», acaecidos en una entidad o región determinados, y su averiguación tiene lugar cuando ocurren acontecimientos que debiendo ser afrontados y resueltos por las autoridades constituidas con estricto apego al principio de legalidad, esos acontecimientos no se logran controlar por la actitud de la propia autoridad, produciéndose, en consecuencia, violaciones a los derechos fundamentales de los individuos. Por ende, la grave violación de garantías individuales se actualiza cuando la sociedad no se encuentra en seguridad material, social, política o jurídica, a consecuencia de que: a) Las propias autoridades que deben proteger a la población que gobiernan, son las que producen o propician los actos violentos, pretendiendo en tal forma obtener una respuesta disciplinada, aunque aquellos sean violatorios de los derechos de las personas y de las instituciones. b) Que frente a un desorden generalizado las autoridades sean omisas, negligentes o impotentes para encauzar las relaciones pacíficas de la comunidad, o bien que sean totalmente indiferentes en obtener el respeto a las garantías individuales.

Solicitud 3/96. Petición del Presidente de los Estados Unidos Mexicanos para que la Suprema Corte de Justicia de la Nación ejerza la facultad prevista en el párrafo segundo del artículo 97 de la Constitución Federal. 23 de abril de 1996. Unanimidad de once votos. El Tribunal Pleno, en su sesión privada celebrada el tres de junio en curso, aprobó, con el número LXXXVI/1996, la tesis que antecede; y determinó que la votación es idónea para integrar tesis de jurisprudencia. México, Distrito Federal, a tres de junio de mil novecientos noventa y seis.

2.1.1 GARANTÍA DE CORRESPONDENCIA E INVIOLABILIDAD DE LAS COMUNICACIONES.

Como se desprende de la evolución histórica de las leyes Constitucionales en México, se le reconocen a las personas diversas garantías como lo son las de libertad, de igualdad, de equidad, de seguridad, como el derecho de tránsito, de elegir el trabajo que más le acomode, de asociación con todo fin lícito, de un salario digno y remunerador, el derecho a la tierra, el derecho a un proceso justo, entre otras.

Estas prerrogativas descansan en los principios de autonomía, inviolabilidad y dignidad de la persona que se traducen en una esfera de derecho, en la legitimación para buscar la felicidad en el modo particular que se entienda, privilegiando el interés general, pero sin demérito de la persona en lo particular, quien además puede, en cierta medida y en ciertos casos limitar sus derechos.

Sobre estos principios, naturalmente, descansa el derecho a la integridad física y moral de la persona, el derecho a que se proteja su intimidad personal y familiar así como su honor.

Así entonces, al protegerse la intimidad de las personas se engloba lo referente a las comunicaciones entre éstas, pues todos tenemos derecho a tener privacidad en nuestra vida, por lo que el legislador al establecer como garantía la inviolabilidad de las comunicaciones tutela la intimidad personal con la única excepción de que la intervención de las comunicaciones se puede utilizar como prueba en materia penal previo procedimiento establecido por la ley como se especificó en el capítulo que antecede.

2.1.2 CONCEPTO DE INVIOLABILIDAD

De acuerdo al Gran Diccionario Jurídico de los Grandes Juristas, inviolabilidad "es la cualidad de un derecho que no puede ser violado; incolumidad, intangibilidad, santidad, prohibición rigurosa de tocar, violar o profanar una cosa, de infringir un precepto o de atentar contra alguien o contra algo".[3]

Igualmente puede definirse como aquella "prerrogativa otorgada a los jefes del Estado, miembros del Parlamento y a algunos funcionarios con el fin de asegurar el ejercicio de su misión, poniéndolos a cubierto de persecuciones infundadas"[4]

Ahora bien, conforme al tema de la presente tesis podemos determinar que la inviolabilidad de la correspondencia es una exigencia de la libertad de comunicación, por la cual no se puede tener acceso a cualquier forma de comunicación sin previa autorización del interesado, encontrándonos así ante la inviolabilidad de la privacidad.

2.1.3 CONCEPTO DE COMUNICACIÓN.

La comunicación es el proceso de transmisión y recepción de ideas, información y mensajes. En los últimos 150 años, y en especial en las dos últimas décadas, la reducción de los tiempos de transmisión de la información a distancia y de acceso a la información ha supuesto uno de los retos esenciales de nuestra sociedad.

La comunicación actual entre dos personas es el resultado de múltiples

[3] Inviolabilidad (voz), CANALES MENDEZ, G. Javier, *Gran Diccionario Jurídico De Los Grandes Juristas,* 1ª Ed. México, p. 805.
[4] Ibíd. P. 806

métodos de expresión desarrollados durante siglos. Los gestos, el desarrollo del lenguaje y la necesidad de realizar acciones conjuntas tienen aquí un papel importante.[5]

Los pueblos antiguos buscaban un medio para registrar el lenguaje. Pintaban en las paredes de las cuevas para enviar mensajes y utilizaban signos y símbolos para designar una tribu o pertenencia. A medida que fue desarrollándose el conocimiento humano, se hizo necesaria la escritura para transmitir información. La primera escritura fue pictográfica, posteriormente se desarrollaron elementos ideográficos, en donde el símbolo no sólo representaba el objeto, sino también ideas y cualidades asociadas a él. Más tarde, la escritura cuneiforme incorporó elementos fonéticos, es decir, signos que representaban determinados sonidos. El alfabeto se originó en Oriente Próximo y lo introdujeron los fenicios en Grecia, donde le añadieron los sonidos de las vocales.[6]

Con el desarrollo de la civilización y de las lenguas escritas surgió también la necesidad de comunicarse a distancia de forma regular, con el fin de facilitar el comercio entre las diferentes naciones e imperios, así tenemos el desarrollo del papel y la impresión, los servicios postales los cuales siguieron creciendo con la aparición del ferrocarril, los vehículos de motor, los aviones y otros medios de transporte, surgió también el telégrafo, el teléfono hasta llegar a las computadoras u ordenadores que fue uno de los avances más espectaculares dentro de las comunicaciones —comunicación de datos—se ha producido en el campo de la

[5] BERLO, David K. *El proceso de la comunicación;* Biblioteca Nuevas Orientaciones de la Educación, Buenos Aires, Argentina, 1973, p. 34
[6] Ibíd. p. 42

tecnología de los ordenadores.[7]

Desde la aparición de las computadoras digitales en la década de 1940, éstas se han introducido en los países desarrollados en prácticamente todas las áreas de la sociedad (industrias, negocios, hospitales, escuelas, transportes, hogares o comercios). Mediante la utilización de las redes informáticas y los dispositivos auxiliares, el usuario de un ordenador puede transmitir datos con gran rapidez. Estos sistemas pueden acceder a multitud de bases de datos. A través de la línea telefónica se puede acceder a toda esta información y visualizarla en pantalla o en un televisor convenientemente adaptado, con estos ordenadores ha surgido el correo electrónico.[8]

También ha surgido la tecnología láser; donde los haces de luz coherente producidos por láser presentan una capacidad de transmisión de mensajes simultáneos muy superior a la de los sistemas telefónicos convencionales. Los prototipos de redes de comunicación por láser ya son operativos y puede que en el futuro sustituyan en gran medida a las ondas de radio en telefonía. Los rayos láser también se utilizan en el espacio en los sistemas de comunicación por satélite.[9]

2.1.4 CONCEPTO DE PRIVACIDAD.

Corresponde ahora preguntarnos, desde una perspectiva jurídica, qué debemos entender por privacidad, por vida privada y por intimidad, porque sin

[7] Ibíd. p. 43
[8] Cfr. GODED, Jaime, *Antología sobre la comunicación humana;* Lecturas universitarias, México, Núm. 25. P. 32
[9] Ibíd. p. 48

tener claro a qué nos referimos seguirá siendo imposible construir normas que nos permitan defender ese "ámbito privado" del individuo, que en la normativa actual parece limitarse al honor y a la reputación o buena fama.

En este campo aparecen dos términos que cuentan con gran similitud, pero que en Derecho son diferentes. Por un lado tenemos la intimidad, que se refiere al espacio donde se desenvuelven las características más reservadas de la vida de un ciudadano (singularmente su domicilio- entendido como cualquier lugar donde viva, no solamente su piso o casa, sino también una habitación de hotel o una caravana- y sus comunicaciones). Por otro lado, aparece el vocablo privacidad, mucho más amplio que el anterior, que agrupa a aspectos segmentados de la vida de un individuo sin significación especial, pero que agrupados, contrastados y analizados en su conjunto nos permiten obtener con detalle un perfil muy concreto de su personalidad que también ha de permanecer protegido. Este “perfil” o conjunto de rasgos personales pueden tener una gran importancia, sobre todo cuando incluyan datos sobre ideología, estado de salud, nivel de gasto, preferencias comerciales, o identidad sexual, muy importantes a la hora de suscribir una póliza de seguros o solicitar un empleo.[10]

Así tenemos que la privacidad abarca todos aquellos aspectos y facetas de la vida del individuo cuyo conocimiento carece de un interés para la sociedad y por lo tanto debe quedar reservado, como sería su vida personal.

En tanto que en términos generales, debemos entender por “vida privada la actividad realizada por cada individuo en su esfera personal y familiar, que no está

[10] MEJAN, C. Manuel, *El Derecho a la intimidad*, Ed. Porrúa, México, 1996 p. 24 – 56.

destinada a trascender o a impactar a la sociedad de manera directa". [11]

Ahí encontraremos campos como las propias relaciones personales y familiares, tanto afectivas como de filiación, las creencias y filiación religiosa, las convicciones personales y políticas, las condiciones personales de salud, la propia identidad, las preferencias sexuales, e incluso la situación financiera personal y familiar, así como las comunicaciones personales por cualquier medio.[12]

Por supuesto queda que la tutela de la privacidad no puede ser absoluta en sí misma, ya que aunque inicialmente sea una información que corresponde a una actividad reservada, al ámbito personal y familiar, la misma puede en ocasiones llegar a trascender y a impactar a la sociedad, e incluso afectar los derechos de los demás, específicamente el derecho a la información, o a la misma paz y orden sociales. Así, se plantea la necesidad evidente de establecer niveles de control y acceso a esa información personal, vinculados a la necesidad de su conocimiento y al uso que pueda hacerse de esa información personal, de manera acorde con nuestros principios constitucionales.

Ahora bien, de acuerdo a Manuel C. Mejan,[13] habrá así un primer nivel de información personal que podríamos denominar como de público acceso, como es el nombre, la edad, fecha y lugar de nacimiento, domicilio, ocupación, estado civil; lo que se denomina en términos morales los "generales" de la persona, que no son más que un conjunto de datos que nos permiten identificar con precisión a un individuo, información elemental y suficiente para la interacción social, y que

[11] MARTINEZ BULLE GOYRI Víctor M. *Genética Humana y Derecho a la Vida Privada, UNAM,* México, 2004 p. 36
[12] Ibíd. p. 37
[13] MEJAN, C. Manuel, Op. Cit. p. 57

satisface en términos generales la necesidad de registros públicos de control de población; así como posibilita el desarrollo de trabajo estadístico básico, necesario para la planeación. Esta información debe considerarse como de público acceso hasta el nivel individual.

Existe otro nivel de información necesario para controles y trabajos estadísticos más especializados o sofisticados, como pueden ser los relativos a condiciones de salud, nivel de ingreso económico, etcétera; donde se aportan datos personales pero con el fin de sumarlos a un universo que será manejado de manera global, y nunca para fines de control o fiscalización individual. Aquí el acceso a la información estadística global es público, pero debe estar absolutamente vedado el acceso y manejo de información individual, sobre la que debe garantizarse la confidencialidad.[14]

Habrá un nivel más de información, ésta sí individualizada y específica, necesaria para determinadas actividades e incluso en beneficio del propio individuo, como son las historias clínicas personales, los registros fiscales, la información crediticia y comercial personal, los registros policíacos necesarios para la seguridad pública colectiva, etcétera. Se trata de información que se integra en archivos personales individualizados, pero destinados a un fin específico y a un uso reservado en atención a dicho fin. El acceso a este tipo de archivos ha de ser restringido y sujeto a controles suficientes que garanticen su no uso o acceso indiscriminado.[15]

Con referencia a este tipo de archivos es que se ha construido doctrinal y

[14] Ibíd. p. 59
[15] Idem.

normativamente lo que autores como Antonio E. Pérez Luño denominan "el derecho a la autodeterminación informativa", como un nuevo derecho fundamental que implica en sí mismo un conjunto de derechos, como son: en primer lugar, el de conocer la existencia de bancos de información donde existan archivos personales propios; el derecho de acceso a esa información; el derecho al control de la veracidad y la calidad de la información personal que se encuentre en los mencionados archivos, que implica en sí mismo un derecho a corregir o a enmendar la información errónea, inexacta o incompleta, e incluso poder exigir la desaparición del archivo personal, y finalmente, el derecho a disponer o autorizar el traspaso o transmisión de esa información a otras bases de información con fines diferentes a aquellos para los que fueron recolectados o cedidos originalmente.[16]

Finalmente, sin duda es necesario un espacio privado intocable, un espacio íntimo que constituiría lo que podríamos denominar como el "ámbito de la intimidad"; un ámbito sobre el cual no es posible injerencia externa alguna, tanto porque se trata de una información que no afecta ni impacta a la sociedad ni a los derechos de los demás, por referirse a aspectos estrictamente personales o familiares, como porque el uso o conocimiento de esa información, sin aportar ningún beneficio o utilidad a la sociedad, puede ser origen o causa de acciones discriminatorias frente a las cuales el individuo quedaría en absoluto estado de indefensión.[17]

Nos referimos aquí a lo que algunos autores denominan como "información

[16] PÉREZ Luño, Antonio E. *Informática y protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1993 (Cuadernos y Debates, núm. 43). P. 79.
[17] Cfr. MEJAN, C. Manuel, *El Derecho a la intimidad*, op. Cit. P. 60-72

susceptible o sensible". Aquí agruparíamos la información sobre el origen familiar, social y racial, las convicciones o preferencias políticas, las creencias y filiaciones religiosas, las preferencias y prácticas sexuales. Información toda ella que corresponde a la propia concepción del individuo sobre sí mismo, que no afecta ni interesa más que al propio individuo y a quienes él libremente se la quiera compartir. Éste sería lo que podríamos denominar el núcleo duro de la intimidad, a cuya información "sólo sería posible el acceso en casos gravemente justificados por su posible impacto social, y mediante estrictos controles, de preferencia judiciales, y vedándose de manera absoluta su inclusión en bancos de datos de uso público". [18]

Los derechos de la personalidad son considerados como derechos esenciales o fundamentales y son, a su vez innatos, porque nacen con la persona titular sin requerir acto jurídico alguno que motive su adquisición, esto es nace y se extingue con el hombre, por que, jurídicamente hablando es una condición o cualidad connatural al ser humano, así pues, los derechos de la personalidad son lo que permiten al hombre el goce de si mismo, tomando en cuenta bienes inmateriales, ideales, carentes de valoración económica.[19]

Así pues, "los derechos a la personalidad son verdaderos derechos objetivos en cuanto que el interés subjetivo es digno de protección y que son derechos, no sobre la propia persona, sino sobre los atributos o manifestaciones esenciales de la personalidad."[20]

[18] MARTINEZ BULLE GOYRI, Víctor M. Op. Cit. P. 41.
[19] Ibíd. P. 42
[20] ROMERO COLOMA, Aurelia Ma. *DERECHO A LA INFORMACIÓN Y LA LIBERTAD DE EXPRESIÓN*. Ed. Bosh, Madrid, 1984, p. 9

De ahí que se distinguen las siguientes características de estos Derechos:

a) Son derechos *innatos* esenciales e independientes del sistema seguido por cada ordenamiento para su configuración y de los medios que establezcan para asegurar su desarrollo.

b) Son *inherentes a la persona* distintos de los derechos de crédito, la violación de ellos representa un ataque a la persona, a su propio ser, así son derechos individuales, privados y absolutos.

c) Son *extra patrimoniales* al ser bienes ideales fuera del comercio de los hombres, aunque, la forma normal de reparación de un daño a estos derechos se lleva a cabo mediante indemnización.

d) Son *inexpropiables e inembargables*

e) Son *imprescriptibles* no se pueden perder ni adquirir por prescripción.

Es conveniente destacar, que de acuerdo a la línea de algunos doctrinarios se establece que:

> *"cuando los datos personales son conocidos por un número cuantioso de personas, sin que su titular pueda saber o impedir que una vez conocido sean libremente difundidos dentro de unos límites de respeto y de convivencia cívicos, se les denomina como datos públicos, en contraposición a los datos privados en los cuales hay una conciencia social favorable a impedir su difusión y respetar la voluntad de secreto de su titular, siendo regulada las situaciones o circunstancias en las cuales el individuo debe suministrarlos".* [21]

[21] DAVARA RODRÍGUEZ, Miguel Ángel, *MANUAL DE DERECHO INFORMÁTICO.* Ed. Arazandi, Pamplona España, 1993, p. 47

2.2 EL DERECHO A LA INTIMIDAD.

Entre los derechos que tiene el hombre, el que sufre más riesgo de pérdida o disminución es el derecho a la intimidad, el cual hace mucho tiempo se tenía la duda de que existiera, hoy podemos afirmar que efectivamente existe y más aún se encuentra reconocida en la Declaración de Universal de los Derechos del Hombre hecha por la Organización Naciones Unidas en diciembre de 1948 así como en la Convención Europea de los derechos del Hombre firmada en Roma el 4 de noviembre de 1950 donde se ha apreciado la existencia de este derecho y la necesidad de su protección, misma que en diversos países se ha llevado a las leyes constitucionales, Código Civil, Penal o bien en leyes especiales, de ahí la gran importancia de establecer primeramente en que consiste el Derecho a la Intimidad.[22]

Con este derecho nos referimos al derecho que compete a toda persona a tener una esfera reservada en la cual desenvolver su vida sin que la indiscreción ajena tenga acceso a ella, "*es el derecho que concierne a toda persona de ser ella la que determine cuándo y hasta donde quiere entrar en contacto con la sociedad.*"[23]

La intimidad está ligada no sólo con la personalidad, sino con la libertad. Existen medios mecanizados cuya utilización puede entrañar una lesión a la intimidad de las personas; la alianza hombre – máquina puede volverse contra el hombre y este perjuicio está lesionando su derecho a la intimidad.

De acuerdo al jurista Stefano Rodotá se establece que *"la gravedad de la*

[22] ROMERO COLOMA Aurelia María, Op. Cit. P. 5
[23] Ibíd. P. 7

invasión a la vida privada del ciudadano se acentúa por la coincidencia de tres elementos: la posibilidad casi ilimitada de recolección de informaciones personales por parte de instituciones públicas y privadas, por el rapidísimo acceso al total complejo de informaciones obtenidas por su tratamiento por procedimientos electrónicos de elaboración y la elevada circulación de la información."[24]

Ahora bien, resulta indispensable distinguir el derecho a la intimidad y el derecho a la protección de datos personales. En consecuencia y tomando en consideración los conceptos antes planteados, se puede resumir que el derecho a la intimidad es, el derecho que se refiere a una esfera privada de la persona, mientras que el derecho a la protección de los datos personales en parte, presume el tratamiento de la información sobre personas, hace que esa información no sea secreta, sino todo lo contrario, que sea objeto de un tratamiento, inclusive de un tratamiento masivo, pero exige una conducta activa por parte de los que realizan ese tratamiento, y esa conducta activa se insiste, debe ser básicamente garantista y en lo que concierne al presente trabajo, en el tratamiento de datos automatizados en las computadoras, ante los crecientes fenómenos tecnológicos.

2.2.1 GENERALIDADES DEL DERECHO A LA INTIMIDAD.

Para efectos de establecer los antecedentes del derecho a la intimidad es indispensable que me baso principalmente en lo señalado por la Aurelia M. Romero Coloma [25] quien señala que éstos datan del siglo XVIII con el jurisconsulto Donello, quien resaltó que en el derecho romano no se tomaron en cuenta los

[24] STEFANO, Rodotá, *Democracia y protección de datos,* Italia, 2004, Traducción revisada por José Luis Piñar Mañas. P. 125
[25] ROMERO COLOMA Aurelia María, Op. Cit. p. 10 – 11.

derechos de la persona, puesto que la protección de la persona sólo funcionaba a través de la “actio iniurarium”.

Asimismo señala, que fue hasta que la Escuela de Derecho Natural exaltó los “derechos naturales o innatos”, considerándolos como aquellos derechos connaturales al hombre que nacen con él, corresponden a su naturaleza, están unidos a su persona y son preexistentes a su reconocimiento por el Estado.[26]

En la época del Estado absoluto, los derechos otorgados por el Rey a ciertas clases (burguesía) como contrapartida de sus servicios estaban a merced del soberano. Posteriormente, con la Revolución Francesa se proclamó la igualdad de todos los individuos, no solo frente al Estado sino también en relación con los demás individuos, el problema surge cuando estos derechos sólo fueron reconocidos para los ciudadanos franceses.[27]

Señala la misma autora, que con el fenómeno de la codificación surgió la idea de organizar la protección privativa de la personalidad. El “code Napoleón” de 1804 trató de derogar el sistema feudal hasta entonces vigente sustituyéndolo por uno inspirado en las ideas de igualdad y libertad influenciando en toda Europa, así, Austria aprueba su código en 1812, Italia en 1865, España en 1889, Alemania en 1900, Suiza en 1910, Italia en 1942, Grecia en 1947, Egipto en 1948 y Portugal en 1966. Sin embargo la protección del individuo sólo era contenida dentro de los Códigos Civiles siendo así meramente privatista, adquiriendo con posterioridad un carácter público hasta a partir de la Segunda Guerra Mundial fue cuando adquiere

[26] Ibíd. p. 11
[27] Idem.

un contenido naturalmente publicista.[28]

La reglamentación más completa y detallada de los códigos señalados fue la portuguesa quien dedica a los derechos de la personalidad toda la Sección segunda del Título II del Libro I, comprendiendo los artículos 70 a 81, ambos inclusive, protegiendo los siguientes derechos: el nombre, el seudónimo, la reserva sobre cartas confidenciales y las no confidenciales con aplicación a las memorias familiares, el derecho a la imagen y reserva sobre la intimidad de la vida privada.[29]

Sin restar importancia a la promulgación de la Constitución Política de los Estados Unidos Mexicanos, que sentó las bases para que en el plano internacional se incorporaran los Derechos Humanos, caracterizándose su evolución después de la Segunda Guerra Mundial, con el nacimiento de diversos tratados y convenios multinacionales entre los que destacan los siguientes:[30]

a) La Declaración Americana de Derechos y Deberes del Hombre de la Organización de los Estados Americanos (1948).

b) La Declaración Universal de Derechos Humanos, adoptada en el marco de la Organización de las Naciones Unidas (10 Dic. 1948).

c) Los Pactos de Derechos Civiles y Políticos, Derechos Económicos, Sociales y Culturales, ambos de la Organización de las Naciones Unidas (1966).

d) La Convención Europea para la Protección de los Derechos

[28] Ibíd. P. 12
[29] Idem.
[30] Ibíd. p. 13

Humanos y Libertades Fundamentales (1950).

e) La Convención Americana de los Derechos Humanos: Pacto de San José de la Organización de los Estados Americanos (1969).

Durante esa época, se desarrolla un sistema de protección de los Derechos Humanos a nivel internacional, con procedimientos y órganos especiales encargados de velar por el fiel cumplimiento de las obligaciones contraídas internacionalmente por los países al observarse como garantía de seguridad jurídica en amplio sentido, protegiendo a sus gobernados, pero la abstracción que surge al interpretarlo en cuanto al derecho a la intimidad es, con respecto al proteger los bienes y privacidad de las mismas personas.[31]

Ahora bien, el derecho a la intimidad de las personas, es un derecho que se viene reconociendo por las principales declaraciones internacionales de Derechos Humanos mediante el reconocimiento implícito del derecho a través del reconocimiento genérico del derecho a la libertad[32]; así pues, de conformidad con el artículo 1º de la Declaración Americana de Derechos del Hombre[33] que establece: "*Todo ser humano, tiene derecho a... la libertad...*"

En tanto que el artículo 3º de la Declaración Universal de Derechos Humanos[34] que afirma: "*Todo individuo tiene derecho a la... libertad...*".

Igualmente de una forma también implícita a través del reconocimiento del genérico derecho a la seguridad personal:

Artículo 1º de la Declaración Americana de Derechos del Hombre que

[31] Ibíd. p. 12
[32] Idem.
[33] Declaración Americana de Derechos del Hombre
[34] Declaración Universal de Derechos Humanos.

señala: "*Todo ser humano tiene derecho a... la seguridad de su persona"* y el artículo 3º de la Declaración Universal de Derechos Humanos al establecer "*Todo individuo tiene derecho a... la seguridad personal".*

Así también se reconoce el derecho a la intimidad y la inviolabilidad de la correspondencia en el artículo 12 de la Declaración Universal de Derechos Humanos: "*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia... Toda persona tiene derecho a la protección de la Ley contra tales inmisiones o daños"*

Es por lo anterior que el *derecho a la inviolabilidad de la correspondencia* se conceptualiza como "aquel derecho, derivación y concreción del derecho a la intimidad, por virtud del cual se prohíbe a los poderes del Estado la detención y la apertura ilegal de la correspondencia".[35]

Así pues, quien se ostenta como el sujeto titular del derecho a la intimidad es toda persona, sin distinción alguna por razón de nacionalidad, sexo, edad y que obviamente tenga la capacidad de goce y ejercicio necesarios para poder ejercerlo. A este último respecto resulta importante destacar que también los niños son poseedores de este derecho, puesto que si bien es cierto no tienen la capacidad de ejercicio también lo es que en la Convención Internacional sobre los Derechos del Niño[36], adoptada por la Asamblea General de las Naciones Unidas el 20 de Noviembre de 1989, en su artículo 16 establece:

"Los Estados partes reconocen el derecho del niño a no ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su

[35] TENA RAMÍREZ Felipe, op.cit. p. 77.
[36] Convención Internacional sobre los Derechos del Niño.

correspondencia..."

De forma similar la regulación que establece el artículo 17.1 del Pacto Internacional de Derechos Civiles y Políticos[37] señala:

"*Ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada... o su correspondencia."*

2.2.2 EL POR QUE DE LA TUTELA CIVIL Y PENAL A LA PRIVACIDAD.

Hasta aquí por lo que se refiere a la tutela de la privacidad e intimidad por normas constitucionales, pero es necesario acudir a otras normas secundarias que también tutelan distintos aspectos de la vida privada. Comenzando por el Código Civil del Distrito Federal, que en su artículo 1916 establece la figura del daño moral, entendiendo por tal: *"la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada y aspectos físicos, o bien en la consideración que de sí misma tienen los demás.".*[38]

Pareciera por esta conceptuación que la privacidad, imagen y honor quedan ampliamente tutelados por la figura del daño moral; sin embargo, el segundo párrafo del artículo citado, nos señala que sólo es causa de responsabilidad cuando el acto u omisión que lo produzcan sean ilícitos, lo que frente a la pobre regulación de la privacidad en general que existe en nuestro país, hace punto menos que imposible caer en la ilicitud.[39]

Para mayor abundamiento, el artículo 1916 BIS del mismo Código establece que: "No estará obligado a la reparación del daño moral quien ejerza

[37] Pacto Internacional de Derechos Civiles y Políticos
[38] Código Civil del Distrito Federal.
[39] Artículo 1916 párrafo segundo del Código Civil del Distrito Federal

sus derechos de opinión crítica, expresión e información en los términos y con las limitaciones de los artículos 6º y 7º de la Constitución general de la República."[40]

Si relacionamos esta disposición con la del artículo 5 de la Ley de Imprenta, que señala como lícita la publicación de datos, privados o no, siempre que sean ciertos[41], de nuevo encontramos que la protección jurídica de la privacidad e intimidad resulta sumamente pobre, si no es que nula.

Por otra parte, también en lo que corresponde al campo del Derecho Penal, se tutelan algunos aspectos de la privacidad, con figuras delictivas específicas establecidas en el Código Penal Federal[42], como son la intervención de comunicaciones telefónicas (artículo 167, fracción IX), la violación e interceptación de comunicaciones escritas (artículo 173), la revelación de secretos (artículo 210), el acceso a información en equipos de informática (artículo 211 bis al 211 bis 7); así como en el Código Penal para el Distrito Federal en lo concerniente a la violación de correspondencia (artículo 333) y violación a las comunicaciones privadas (artículo 334).[43]

2.3 EL DERECHO INFORMÁTICO Y SU APLICACIÓN EN LA CONFIDENCIALIDAD DE LOS DATOS PERSONALES.

El Derecho Informático, como nueva rama del conocimiento jurídico es una disciplina en continuo desarrollo, teniendo en su haber antecedentes a nivel histórico, sin embargo a partir del año 1949 fue Norbert Wiener en su obra[44] quien

[40] Artículo 1916 Bis del Código Civil del Distrito Federal
[41] Ley de Imprenta
[42] Código Penal Federal.
[43] Código Penal para el Distrito Federal.
[44] WIENER, Norbert, *CIBERNÉTICA Y SOCIEDAD*, FCE, México 1980, p. 97.

señaló en su capítulo IV, consagrado al derecho y las comunicaciones, la influencia que ejerce le cibernética respecto a uno de los fenómenos sociales más significativos: el jurídico. Dicha interrelación se da a través de las comunicaciones, a lo que habría que mencionar que si bien estos postulados tienen cerca de cuarenta años, en la actualidad han adquirido matices inimaginables para la época en que se plantearon.

El cambio tecnológico que se ha vivido desde a mediados del siglo XX ha producido efectos en todas las áreas del quehacer humano. Cuando se habla de tecnología, no puede dejarse de hacer alusión a la informática y a las telecomunicaciones, estos dos fenómenos han producido la entrada de la sociedad en la llamada era de la información. Atrás han quedado la etapa agrícola y la etapa industrial. El advenimiento de las telecomunicaciones y su fusión con la informática ha llevado a algunos autores a afirmar que estamos en la denominada era digital.[45]

Cabe señalar que en la reiterada interrelación Derecho – Informática, en los términos de un Derecho Informático se contemplan una serie de implicaciones tanto de orden social, económico, técnico, práctico y evidentemente jurídico, suscitadas por el uso de la informática.[46]

De reciente aparición en la historia del hombre, el surgimiento de tal rama del derecho la podemos considerar a partir del momento en que las personas comenzaron a relacionarse a través de la computadora, compartiendo e intercambiando información, trayendo como consecuencia la aparición de actos

[45] TÉLLEZ Valdez Julio, *Derecho Informático*, Mc. Graw Hill, México 2003, p. 19
[46] Idem.

jurídicos, muchos de los cuales no se encuentran regulados en la actualidad.

Esta rama jurídica se puede definir como el sector normativo de los sistemas, dirigido a la regulación de las nuevas tecnologías de la información y la comunicación, es decir, la informática y la telemática. Tomando en cuenta que el concepto de Informática es muy general, es preciso tener en consideración el concepto de informática que refiere el Maestro Julio Téllez Valdez "como un proceso físico – mecánico de datos, teniendo como dato al elemento referencial de un hecho", mientras que la telemática o la teleinformática es "el modo de transmitir mediante las telecomunicaciones y permite asimilar más atingentemente al planeta como un verdadero mercado único de productos y servicios".[47]

Así pues, podemos decir que "el Derecho Informático es una rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática)."[48]

Integran al Derecho Informático las preposiciones normativas, es decir, los razonamientos de los teóricos del Derecho que tienen por objeto analizar, interpretar, exponer, sistematizar o criticar el sector normativo que disciplina la informática y la telemática. Las fuentes y estructura temática del Derecho Informático afectan las ramas del Derecho tradicionales.[49]

Así entonces se inscriben en el ámbito del Derecho Público el problema de la regulación del flujo internacional de datos informatizados, que interesa al Derecho Internacional Público, la libertad informática o defensa de las libertades frente a eventuales agresiones perpetradas por las tecnologías de la información y

[47] Ibíd. p. 15
[48] Ibíd. P. 22
[49] Idem.

la comunicación, objeto de especial atención por parte del Derecho Constitucional y Administrativo; o los delitos informáticos, que tienen a configurar un ámbito propio en el Derecho Penal actual. En tanto que, en el ámbito del Derecho Privado se incide en los contratos informáticos, que pueden afectar tanto al hardware como al software, dando lugar a una rica tipología en los negocios en la que pueden distinguirse contratos de compraventa, alquiler, copropiedad, multi contratos de compraventa, mantenimiento y servicios; como los distintos sistemas para la protección jurídica de los objetos tradicionales de los Derechos Civiles y Mercantiles.[50]

Es ese mismo carácter interdisciplinario que distingue al Derecho Informático lo que ha suscitado debates teóricos al tratar de distinguir si es un sector de normas dispersas pertenecientes a diferentes disciplinas jurídicas o constituye un conjunto unitario de normas (fuentes), dirigidas a regular un objeto bien delimitado, que se enfoca desde una metodología propia, en cuyo supuesto se estaría ante una disciplina jurídica autónoma. [51]

2.3.1 INFORMÁTICA JURÍDICA.

En amplio sentido se puede establecer que la informática jurídica es el "*conjunto de aplicaciones de la informática (ciencia del tratamiento lógico y automático de la información) en el ámbito del Derecho.*"[52]

[50] Ibíd. p. 23
[51] Ibíd. p. *24*
[52] Ibíd. p. 25

Orígenes.

Surge en el año de 1959 en los Estados Unidos sufriendo innumerables cambios conforme la evolución de la misma informática.

De acuerdo al autor Julio Téllez Valdéz[53], las primeras investigaciones en materia de recuperación de documentos jurídicos en forma automatizada se remontan a los años cincuenta, en que se comienza a utilizar las computadoras no sólo con fines matemáticos sino también lingüísticos. Lo anterior fue realizado en el Health Law Center (Centro de la Ley de Salud, HLC por sus siglas en inglés) de la Universidad de Pittsburg en donde el entonces director del Centro, John Horty estaba convencido de la necesidad de encontrar medios satisfactorios para tener acceso a la información legal. Para 1959, el Centro colocó los ordenamientos legales de Pennsylvania en cintas magnéticas. El sistema fue demostrado en 1960 ante la Barra de la Asociación Americana de Abogados en la Reunión Anual en Washington, D.C. Esta fue la primera demostración de un sistema legal automatizado de búsqueda de información.

Este sistema fue rediseñado y destinado a integrarse a la Corporación de Sistemas Aspen que lo explotó comercialmente. A principios de 1966, doce estados de la Unión Americana se propusieron desarrollar un sistema interno de recuperación de documentos legales.[54]

Para 1968, esta compañía había computarizado los ordenamientos de cincuenta estados de aquel país, en cerca de un billón de caracteres, trabajo conocido como el Sistema 50. este sistema, originalmente destinado para

[53] Ibíd. p. 27
[54] Idem.

abogados y corporaciones, encontró mucho éxito en las legislaturas locales.[55]

El segundo logro por parte del HLC fue el sistema LITE, hoy llamado ELITE (Información Legal Federal a través de computadoras), que fue desarrollado por la Universidad de Pittsburg bajo contrato con la Fuerza Aérea Norteamericana en 1969.

De lo anterior podemos concluir que la informática jurídica se refiere al uso de las computadoras en el ámbito jurídico.

O bien como lo refiere nuevamente el Maestro Téllez Valdez "*por informática jurídica entendemos la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación".*[56]

En sus inicios la informática jurídica se presentó en forma de una informática documentaria de carácter jurídico, es decir de creación y recuperación de información de datos principalmente jurídicos, sin embargo poco a poco se empezó a vislumbrar la idea de que de estos bancos de datos jurídicos se podían obtener no sólo informaciones, sino también, mediante programas estudiados expresamente, verdaderos actos jurídicos como certificaciones, contratos, promociones, mandatos judiciales, etcétera, así nació a fines de los años sesenta la llamada informática jurídica de gestión.[57]

Lo que pareció en un momento un método práctico para un control estricto

[55] Idem.
[56] Ibid. p. 28
[57] Idem.

de datos e información de distinta índole, con posterioridad llegó a ser un peligro para la protección de la confidencialidad, por los novedosos métodos para la violación de la seguridad con que se contaba. [58]

Ello fue así que en enero de 1992, los medios de comunicación social dan la noticia de que ha sido descubierta la existencia de una red ilegal de venta de datos informatizados, cuyos bancos de datos contenían información de datos íntimos de muy variada índole, de veintiún millones de ciudadanos españoles. Los datos habían sido obtenidos ilegalmente de los Ministerios de la Presidencia Interior, Trabajo y Hacienda.[59]

En esa época debido al acelerado avance tecnológico en materia informática y del derecho a la libertad informática, no existía ningún texto internacional de Derechos Humanos que hiciera referencia explícita de dicho derecho fundamental, en cambio pudiera pensarse que se tenía reconocido el mismo en los artículos de las declaraciones internacionales que hacían referencia al derecho a la libertad, a la seguridad personal y a la intimidad, y no así a la protección jurídica de los datos personales.[60]

En nuestro país aconteció un evento similar se detectó la venta de datos de las personas registradas ante el Instituto Federal Electoral a una empresa de supuesta publicidad estadounidense, sin que a la fecha se haya podido establecer la utilidad que tendría para dicha empresa la información de miles de personas mexicanas, noticia que al ser revelada creó total descontento entre la ciudadanía, que creía segura su información ante una institución de tal índole, sin que existiera

[58] Idem.
[59] Idem.
[60] Idem.

por parte de la Secretaría de Gobernación alguna exigencia a la empresa extranjera para que explicara los motivos y medios con los que contó para realizar dicha transacción de información, lo que denotó la facilidad con que cualquier persona física o moral puede tener acceso a los bancos de datos de la ciudadanía mexicana sin que pueda ser sancionada por tal acción y que decir si se trata de extranjeros, creando con ello una vulnerabilidad política y social puesto que no existen leyes ni siquiera reglamentos que impidan dicha situación y si en cambio demuestra que teniendo el dinero suficiente, sea quien sea, puede tener acceso ilimitado a una gran infinidad de datos sin tener que hacerse responsable por el mal uso que pudiera darles.

Este ejemplo es solo una muestra de cierta información que se dio a conocer ante la ciudadanía y de lo que son capaces de hacer algunas personas para obtener esas investigaciones, faltaría por reseñar todas y cada una de las obtenciones de datos que aún siguen sin descubrirse o aún sabiéndolo no son del conocimiento popular por diversos intereses políticos.

2.4 EL DERECHO A LA LIBERTAD INFORMÁTICA

Denominado también como derecho a la autodeterminación informática es un derecho fundamental de muy reciente aparición y poco tratado en nuestra legislación penal mexicana. Está vinculado a la fuerte evolución tecnológica que ha experimentado la informática en los últimos veinte años, lo cual ha permitido el almacenamiento, tratamiento y transmisión automatizada de una enorme cantidad

de información personal.[61]

La posibilidad de poder cruzar información procedente de distintas bases de datos ha multiplicado las posibilidades de lesión de los derechos de los ciudadanos a través de la informática.

Así pues, podemos conceptuar el **Derecho a la libertad Informática** como aquel "*derecho fundamental de naturaleza autónoma, aunque derivado del genérico derecho a la intimidad, que asegura la identidad de las personas ante el riesgo de que sea invadida o expropiada a través del uso ilícito de las nuevas tecnologías, bien por parte del Estado o por parte de particulares, mediante la aplicación del Derecho de la informática a través de leyes, normas y principios aplicables a los hechos y actos derivados de la informática."*[62]

Así tenemos que son sujetos activos de este derecho:

a) La persona individual
b) La familia
c) Los grupos sociales de todo tipo religiosos, profesionales, culturales, minorías raciales, etc.

El sujeto activo lo es el Estado y aquellos grupos sociales (como los económicos) que pueden tener interés en conculcar el derecho a la libertad informática en beneficio propio, bien de una forma lucrativa, bien a través de la obtención de los datos que les permiten aumentar su poder de dominación o de

[61] Ibíd. p. 29
[62] DÁVARA RODRÍGUEZ, Miguel Ángel. Op. Cit. P. 53

influencia.

Los bienes de la personalidad sobre los que recae la protección de la libertad informática son:[63]

- La intimidad, entendida conforme al Informe Younger sobre la intimidad, publicado en Inglaterra en Julio de 1972, en un doble sentido:[64]
  - La intimidad física que supone "libertad frente a toda intromisión sobre uno mismo, su casa, su familia o relaciones" y,
  - La intimidad informativa, que es el "derecho a determinar por uno mismo cómo y en qué medida se puede comunicar a otros información sobre uno mismo". Es pues, la autodeterminación informativa de la propia intimidad.
- La seguridad personal,
- La libertad personal,
- En general, todos los bienes de la personalidad que, en su caso, puedan verse afectados por la violación de este derecho.

Así entonces tenemos que el derecho a la libertad informática supone o implica el derecho a acceder y controlar, a través de las adecuadas vías procesales, las informaciones que les conciernen, procesadas en bancos de datos informatizados, el derecho a exigir de los bancos de datos públicos y privados la corrección de datos inexactos, el derecho a exigir de los bancos de datos públicos y privados el cancelar aquellos datos que resulten anticuados, inapropiados o

[63] Ibíd. p. 56
[64] Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca, Revista Jurídica Ius Et Praxis *"DERECHO A LA AUTODETERMINACIÓN INFORMATIVA Y LA ACCIÓN DE HABEAS DATA EN IBERO AMÉRICA",* Chile 1997, año 3, No. 1 pág. 37

irrelevantes, a exigir de los bancos de datos públicos y privados el cancelar aquellos datos personales que hayan sido obtenidos por procedimientos ilegales, a exigir que se tomen las medidas necesarias y suficientes para garantizar la intimidad en relación a los datos estadísticos y a exigir que se tomen las medidas suficientes para evitar la transmisión de datos a personas o entidades no autorizadas.

La libertad informática o autodeterminación informativa es la necesaria respuesta al fenómeno de la contaminación de las libertades en los sistemas jurídicos democráticos, debido al desajuste existente entre la lenta expedición de normas jurídicas y el desarrollo de las garantías de los derechos fundamentales contra el vertiginoso avance tecnológico.[65]

En los sistemas democráticos se hace preciso un estricto control sobre los bancos de datos que obran en poder de los órganos del Estado. Y ello como garantía tanto frente a la actuación por parte del Estado, como frente a la actuación de los particulares.[66]

Es preciso tomar en cuenta que esos datos confidenciales, sin un control adecuado, pueden ser utilizados peligrosamente en el mercado de trabajo (aplicación de criterios discriminatorios por razones de raza, creencias, etc.) o en otros aspectos de la vida social que pueden llegar a ser extremadamente perversos y atentatorios contra los Derechos Humanos.

Este control pudiera ser llevado a cabo mediante la implantación de una verdadera Legislación Informática que se encuentra denominado como “un

[65] DÁVARA Rodríguez Miguel Ángel. Op. Cit. p. 65
[66] Ibíd. p. 65

conjunto de reglas jurídicas de carácter preventivo, correctivo y punitivo derivadas del uso (inadecuado) de la informática"[67].

Determinándose así que se hace necesaria una reglamentación de puntos específicos que debe tomar en cuenta algunas consideraciones como lo serían el establecer si se recurre a un cuestionamiento de las reglas existentes para acordar si es posible su aplicación análoga frente al problema o si resulta necesaria una ampliación en cuanto a su ámbito de cobertura; esperar la evolución de la jurisprudencia dada la creciente presentación de casos ante los órganos jurisdiccionales en los que se fijen pautas resolutorias o conciliatorias en su caso; o bien, crear un cuerpo de nuevas reglas integrándolas a ordenamientos ya existentes o mejor aún, dar lugar a una nueva ley de carácter específico.

Esta legislación informática debe tener como principal problemática: la regulación de los bienes informacionales ya que la información como producto informático requiere de un tratamiento jurídico en función de su innegable carácter económico y la "*protección de datos personales esto es, el atentado a los derechos fundamentales de las personas provocado por el manejo inapropiado de informaciones nominativas.".*[68]

2.5 LOS DATOS PERSONALES EN LA INFORMÁTICA.

Al permitir las computadoras un manejo rápido y eficiente de grandes volúmenes de información, facilitan la concentración automática de datos referidos a las personas, constituyéndose así en un verdadero factor de poder.

[67] TELLEZ VALDEZ Julio, op. Cit. p. 59
[68] Idem.

En la época de los años setenta comenzaron a surgir numerosos archivos con informaciones de tipo personal, con un conjunto mínimo de datos como filiación, fecha y lugar de nacimiento, domicilio, estado civil, etc., hasta otro tipo de datos con caracteres más distintivos como raza, religión, inclinaciones políticas, ingresos, cuentas bancarias, historia clínica, preferencias sexuales, etc. Estos datos al ser recopilados en diferentes centros de acopio como lo son los registros censales, civiles, parroquiales, médicos, académicos, deportivos, culturales, administrativos, fiscales, bancarios, laborales, hospitales públicos o privados, negocios, etc., ya no por medios exclusivamente manuales, sino con el apoyo de medios automatizados, provocan una gran concentración, sistematización y disponibilidad instantánea de ese tipo de información para diferentes fines.[69]

Este tipo de datos no son vulnerables por sí mismos, sino según el destino del que pudieran ser objeto el cual es variado ya que pueden ser empleadas para fines publicitarios, comerciales, fiscales, policíacos, etc., convirtiéndose de esta manera en un instrumento de opresión y mercantilismo.[70]

Así por ejemplo un expediente médico puede ser visto por una aseguradora provocando con ello desventajas ante esa compañía o bien que la información delicada sobre funcionarios públicos como lo son ingresos, domicilio, familia, fotografías, pueda ser utilizada para intentar un secuestro. La variedad de los supuestos posibles de indefensión frente al problema provoca que los individuos estén a merced de un sinnúmero de situaciones que alteren sus derechos fundamentales en sociedad, provocados por discriminaciones, manipulaciones,

[69] Ibíd. p. 74
[70] Idem.

persecuciones, presiones, asedios, entre otros, todo ello al margen de un control jurídico adecuado, así pues en el caso de las instituciones financieras es latente el riesgo de que un banco entregue datos personales a una empresa publicitaria o de cobranzas.

Ya desde 1968, en el seno de la Asamblea de los Derechos Humanos auspiciada por la Organización de las Naciones Unidas, se mostraba una gran preocupación por la manera en que la ciencia y la tecnología podrían alterar los derechos del individuo, empezando a denotar la necesaria emanación de un régimen jurídico que pudiera afrontar de manera cabal este género de situaciones.[71]

Esta problemática abarca diversas figuras de índole jurídico como lo son los Derechos Humanos, derechos personales, derechos patrimoniales, libertades públicas y privadas, derecho de la privacidad en el caso de los países anglosajones, derecho a la intimidad y al honor de las personas como en España, o aún las garantías individuales y sociales como pudiera ser el caso de nuestro país, todas ellas como protección eventual, han tendido hacia una sujeción apropiada en cuanto a la concentración y destinación de los datos de carácter personal.[72]

Estos datos se encuentran recopilados en archivos los cuales pueden ser, dependiendo de su contenido archivos públicos (aquellos manejados por el Estado), archivos privados (manejados por empresas privadas), manuales (si son procesados en forma manual), automáticos (si son procesados en forma

[71] Ibíd. p. 70
[72] Idem

automática), sobre personas físicas (sean residentes o no de un determinado país) o personas morales, resaltando que no todos estos archivos se encuentran sujetos a una regulación jurídica.[73]

Así pues, si hablamos de una regulación jurídica entonces existen determinados derechos y excepciones como son: [74]

a) **Derecho de acceso**. Es aquel que permite a los interesados conocer las instituciones y el tipo de información que disponen sobre su persona.

b) **Derecho de rectificación**. Complementario al anterior, dicho derecho permite solicitar al interesado una modificación en los términos de alteración o ampliación, o una supresión o cancelación de aquellos datos que, referidos a su persona, considere como inexactos o irrelevantes.

c) **Derecho de uso conforme al fin**. Este consiste en que el interesado pueda exigir que su información nominativa sea destinada para los objetivos por los cuales se proveyó, es decir, si era de índole administrativo, que no trasciende a niveles más allá de los planteados en un principio.

d) **Derecho para la prohibición de interconexión de archivos.** Consistente en que una base de datos administrativos no podrá ser objeto de consulta por otra instancia (fiscal, policial) que no sea aquella a la cual se le administraron los datos o información.

[73] Ibíd. pp.. 69-74
[74] Ibíd. p. 71

Resaltando que el incumplimiento a estos derechos puede generar diferentes sanciones de índole civil, administrativa o incluso penal, dependiendo de las circunstancias. Por cuanto hace a las excepciones a dichos derechos fundamentales en el equilibrio del Estado y su poder coercitivo y los integrantes de la sociedad, tenemos a aquellas derivadas con motivo de la seguridad del Estado, tanto en lo interno como en lo externo, así como las relativas a intereses monetarios, persecución de delitos, motivos de salud, etc.[75]

2.6 LA RED "INTERNET".

Para poder entender un poco más sobre la forma en que los datos personales pueden ser adquiridos a través de las bases informáticas que existen, debemos analizar de forma breve la historia de la red Internet, pues constituye el medio utilizado para éstos propósitos.

La Internet ha significado una revolución sin precedentes en el mundo de la informática y las comunicaciones transformando a la humanidad. Han contribuido a ello los inventos del teléfono, radio, satélites, computadoras, dispositivos de hardware, los protocolos o estándares de comunicaciones y software especializados tales como navegadores, correo electrónico, video conferencias, etc.[76]

Resulta ya obvio hacer referencia a la revolución que ha supuesto la informática y la tecnología, y las posibilidades de digitalización de la información

[75] Ibíd. p. 74
[76] BINI, Rafael, *El Internet*, Ed. Sagitario, España, 1997, p. 15

(ya sea en forma de textos, imágenes, animaciones o sonidos), para su posterior almacenamiento, manipulación o transmisión, de cara al tratamiento de datos de carácter personal.

Internet ha incrementado las posibilidades anteriores gracias a la interconexión de equipos informáticos y de bases de datos, la descentralización y crecimiento de redes, y, especialmente, por el hecho de reunir, en un instrumento interactivo y multi direccional, el mayor número de usuarios que puede englobar un medio. Los avances en Internet han obligado a aumentar la capacidad de los ordenadores, han permitido el desarrollo de nuevas vías de negocio así como de nuevas formas de Marketing, si bien a la vez se han puesto de manifiesto también vulnerabilidades y faltas de seguridad importantes.[77]

Junto a esto, el carácter transnacional de Internet (multitud de servidores desperdigados por el globo) y los problemas de jurisdicción y competencia judicial, dificultan el control y aplicación de gran parte de las garantías legales que pretenden, de algún modo, regular los contenidos o el flujo de datos a través de la red.[78]

Para entender con mayor claridad el avance tecnológico de la Red Internet, es necesario conocer sus orígenes, por lo que de acuerdo al autor Alejandro Piscitelli[79], tenemos que el 4 de octubre de 1957 la entonces denominada Unión Soviética de Repúblicas Socialistas puso en órbita el primer satélite artificial llamado SPUTNIK. Este importante hecho marca el inicio del uso de las

[77] Véase el artículo *La privacidad de los menores y el marketing a través de Internet*, disponible en noticias.jurídicas.com, @rea Digital –APTICE.
[78] BINI, Rafael, Op. Cit. p. 24
[79] PISCITELLI Alejandro, *Internet la imprenta del siglo 21*, Ed. Gedisa Mexicana, ed. 2005, Colección Cibercultura/Gedisa, p. 35

comunicaciones globales. Un año después el Presidente DWIGTH EISENHOWER ordenó la creación de la Advanced Research Projects Agency (ARPA por sus siglas en inglés, Agencia de Proyectos de investigación Avanzados, en español) creado por el Departamento de Defensa de los Estados Unidos de Norteamérica, así como la NASA.

Encargando su creación a J. C. R. LICKLIDER quien al exponer en 1962 su concepto de GALACTIC NETWORK (Red Galáctica) concibió una red interconectada globalmente a través de la que cada uno pudiera acceder desde cualquier lugar a la información y a los programas, este concepto era muy parecido a la Internet actual. Licklider fue el principal responsable del programa de investigación en computadores de la ARPA desde octubre de 1962.[80]

Mientras trabajó en ARPA convenció a sus sucesores Iván Sutherland Bob Taylor, y el investigador del MIT Lawrence G. Roberts de la importancia del concepto de trabajo en red. Entre 1962 y 1968 se trabajó el concepto de intercambio de paquetes, desarrollado por Leonard Kleintock y su origen y uso fue meramente militar. La idea consistía en que varios paquetes de información pudiesen tomar diferentes rutas para uno o más determinados destinos, consiguiendo con ello una mejor seguridad en el transporte de la información. Se siguieron conectando computadores rápidamente a la ARPANET durante los años siguientes y el trabajo continuó para completar un protocolo host a host funcionalmente completo, así como software adicional de red.[81]

En Octubre de 1972, un investigador de apellido Kant organizó una gran y

[80] Idem.
[81] Idem.

muy exitosa demostración de ARPANET en la International Computer Communication Conference (Conferencia de Comunicación por Computadora o ICCC por sus siglas en inglés). Esta fue la primera demostración pública de la nueva tecnología de red. Fue también en 1972 cuando se introdujo la primera aplicación: el correo electrónico.[82]

En el mes de julio de 1973 Lawrence G. Roberts investigador del Massachussets of Technology (MIT por sus siglas en inglés) escribió el primer programa de utilidad de correo electrónico para relacionar, leer selectivamente, almacenar, reenviar y responder a mensajes. Desde entonces, la aplicación de correo electrónico se convirtió en la mayor de la red durante más de una década. Fue precursora del tipo de actividad que observamos hoy en día en la World Wide Web, es decir, del enorme crecimiento de todas las formas de tráfico persona a persona.[83]

En 1976 el Dr. Robert M. Metcalfe desarrolla ETHERNET, cuyo sistema permite el uso de cables coaxiales que permiten transportar la información en forma más rápida. En 1979 IBM crea BITNET (Because it is Time Network) que sirve para mensajes de correo y listas de interés.[84]

En 1981 se crea una red de comunicaciones llamada CSNET que transmite a 56 kbps, sin necesidad de acceder a ARPANET y es en este año que se empieza a independizar el control científico civil del control miliar.[85]

En 1985-86 la Nacional Science Foundation (NSF) conectó seis centros de

[82] Idem.
[83] Ibíd. p. 36
[84] Idem.
[85] Idem.

súper computación a través de su país. Esta red es llamada la NSFNET, o sea la troncal (backbone) de la NSF. Para expandir el acceso a Internet, la NSF auspició el desarrollo de redes regionales, las cuales fueron conectadas al troncal de la NSFNET, sumándolo a esto la NSF apoyó a instituciones, tales como universidades y centros de investigación en sus esfuerzos para conectarse a las redes regionales.[86]

Para 1989 la troncal de la red es elevada a "T1", con ello la red queda habilitada para transmitir datos de hasta 1.5 millones de bits por segundo, o lo que es lo mismo hasta 50 páginas de texto por segundo.[87]

En 1990 la ARPANET es disuelta. En 1991 es creado el GOPHER por la Universidad de Minnesota, sistema que es capaz de localizar información en la Internet, facilitando enormemente su uso. En 1992 se funda la Internet Society.[88]

En 1993 el European Laboratory for Particle Physics in Switzerland (CERN) libera el Word Wide Web (www), desarrollado por Tim Berners-Lee. El WWW usa el protocolo de transferencia de hipertexto (HTTP) y encadenándolos muy fácilmente, cambiando así la ruta o camino de la información, la cual entonces puede ser organizada, presentada y accedida en la Internet.[89]

En 1993 la troncal de la red NSFNET es elevada a "T3" lo que lo habilita para transmitir datos a una velocidad de 45 millones de bits por segundo, o sea, cerca de 1400 páginas de texto por segundo.[90]

En 1993-1994 el visualizador (browsers) gráfico de Web Mosaic y Netscape

[86] Idem.
[87] Idem.
[88] Idem.
[89] Ibíd. P. 37
[90] Idem.

Navigator aparecen y rápidamente son difundidos por al comunidad de la Internet, debido a su naturaleza intuitiva y a la interfaz gráfica, estos browsers hacen que los www y la Internet sean más atractivos al público en general.[91]

En 1995 la troncal de la red NSFNET es reemplazado por una nueva arquitectura de redes, llamada VBNS (very high speed backbone network system), esto significa sistemas de redes con troncal de alta velocidad, que utiliza los Network Service Providers (Proveedores de Servicios de Redes), redes regionales y Network Access Points (NAPs o Puntos de Acceso a la Red correspondiendo su traducción al español).[92]

Cuando se logra la conexión de varias computadoras entre sí compartiendo sus recursos e información y estando conscientes una de otra estamos hablando de las llamadas redes informáticas. Cuando las PC's comenzaron a entrar en el área de los negocios, el conectas dos PC's no traía ventajas, pero esto desapareció cuando se empezaron a crear los sistemas operativos y el Software multiusuario; las redes se clasifican en base al tamaño y espacio que ocupan así tenemos:[93]

a) LAN – Redes de área local. Es una red que se expande en un área relativamente pequeña, se encuentran dentro de una edificación o conjunto de edificaciones que estén contiguos, pueden ser desde dos computadoras hasta cientos de ellas, todas se conectan entre sí por varios medios y topología a la computadora (s) que se encarga de llevar el control de la red,

[91] Idem.
[92] Ibíd. p. 38
[93] BINI, Rafael, Op. Cit. p. 26

llamada “servidor” y las computadoras que dependen del servidor son llamadas “nodos” o “estaciones de trabajo”.[94]

b) WAN – Redes de área amplia. Es una red comúnmente compuesta por varias LANs interconectadas y se encuentran en una amplia área geográfica. Estas LANs que componen la WAN se encuentran interconectadas por medio de líneas de teléfono, fibra óptica o por enlaces aéreos como satélites. Entre las WAN más grandes se encuentran la ARPANET que fue creada por la Secretaria de Defensa de los Estados Unidos y se convirtió en lo que es actualmente la WAN mundial: INTERNET, a la cual se conectan actualmente miles de redes universitarias, de gobierno, corporativas y de investigación entre otras.[95]

Pero invariantemente, es necesario el uso de herramientas para armar y construir una red de forma física, llamados tales materiales como componentes de red y lo que compone una red en forma básica y tangible es:[96]

- Software. Podemos conceptuar en sentido amplio como “una secuencia de instrucciones o indicaciones destinadas a ser utilizadas directa o indirectamente en un sistema informático para realizar una función o tarea o para calcular un resultado cualquiera

[94] Ibíd. p. 24
[95] Ibíd. p. 26
[96] BRIGGS, Asa. *De Gutemberg a Internet*, Narrativa y ensayo. Ed. Taurus, El Colegio de México, 2007, p. 95

que sea la forma de su expresión o fijación"[97]

- Servidor (server). El servidor es la máquina principal de la red, la que se encarga de administrar los recursos de la red y el flujo de la información. Muchos de los servidores son "dedicados" es decir, están realizando tareas específicas, como lo sería un servidor de impresión que sirve solo para imprimir.[98]
- Estación de trabajo (workstation). Es una computadora que se encuentra conectada físicamente al servidor por medio de algún tipo de cable. Muchas de las veces esta computadora ejecuta su propio sistema operativo y ya dentro, se añade al ambiente de la red.[99]
- Sistema operativo de red. Es el sistema (software) que se encarga de administrar y controlar en forma general la red. Para esto tiene que se un sistema operativo multiusuario, conceptual izándose dicho sistema como aquel en que múltiples usuarios pueden hacer uso de una terminal sin variar o alterar el contenido de la misma.[100]
- Recursos a compartir. Estamos hablando de todos aquellos dispositivos de hardware que tienen un alto costo y que son de alta tecnología, como lo son las impresoras que pueden ser láser, de color, plotters y todos aquellos periféricos que se necesitan para el

[97] Ibíd. p. 95
[98] Ibíd. p. 96
[99] Idem.
[100] Ibíd. p. 97

desenvolvimiento de dicha red.[101]

- Hardware de red. Son aquellos dispositivos que se utilizan para interconectar a los componentes de la red, serían básicamente las tarjetas de red (NIC->Network Interface Cards) y el cableado entre servidores y estaciones de trabajo, así como los cables para conectar los periféricos como lo son los routers y bridges que son equipos especiales que permiten conectar varias LAN de un mismo tipo.[102]

2.6.1 SEGURIDAD EN INTERNET

Habiendo explicado en forma breve la historia del Internet y sus componentes cabe señalar que al entrar a éste sistema aparecen sujetos específicos tales como la operadora de telecomunicaciones, el operador de acceso a Internet o el Proveedor de Servicios de Internet, que para el desarrollo de su actividad y prestación de sus servicios requieren del tratamiento de los datos de los usuarios, y que por tanto quedan sometidos a la normatividad sobre protección de datos general y específica en el sector de las telecomunicaciones.[103]

La Red 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.[104]

Para enfrentar este desafío debemos tener en cuenta los siguientes

[101] Idem.
[102] Ibíd. P. 98.
[103] PALAZZI, Pablo Andrés, *El Derecho y la sociedad de la información, la importancia de Internet en el mundo actual,* Ed. Porrúa, México, 2007, p. 46
[104] Ibíd. p. 46

elementos: [105]

- a) En primer lugar que 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 realizar una conexión.
- c) En tercer lugar la cantidad de datos que nos solicitan para realizar actividades comerciales en línea.

Si queremos efectivamente realizar *e-commerce* vamos a tener indefectiblemente que estar brindado una serie de datos personales, que no necesariamente están acorde con los principios generales que rigen en materia de recolección. Un ejemplo de este último caso es que al realizar la compra de un e-book, transacción de comercio electrónico directo, en el cual la transacción completa se realiza a través de Internet, se suelen solicitar datos como profesión, dirección postal completa, números de teléfonos, en formularios electrónicos que en caso de no ser completados en su totalidad no habilitan realizar el próximo paso.[106]

Existe entonces una clara dependencia entre la utilización de Internet y el brindar datos personales. Y esta relación está signada por la desigualdad entre el proveedor y el usuario. Desigualdad que desde hace ya muchos años ha detectado la jurisprudencia francesa en materia de contratos informáticos, y que

[105] ARAGÓN REYES Manuel y Fernández Esteban María Luisa. *Incidencia de Internet en los Derechos Fundamentales*. Edita Banco Santander Central Hispano – Asesoría Jurídica del Negocio – C/ Alcalá 49 – 28014 Madrid. P. 12
[106] Ibíd. p. 13

no se refiere al aspecto económico sino a la formación e información tecnológica que posee el proveedor. Además, debemos tener presente que el usuario no es conciente de que sus datos se han recopilado, bastaría realizar una búsqueda con nuestro propio nombre en un buscador de la red solicitando la información que circula en Internet sobre nosotros, sin que jamás se nos haya notificado, mucho menos solicitado autorización.[107]

Podemos destacar de Internet tres elementos de fundamental importancia que manejan datos, recopilando y enviando información sin que los usuarios estemos al tanto como lo son:

1. **Cookies** son 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 y proporcionan información sobre los sitios Web visitados, las preferencias y enlaces seleccionados, pero también almacenan otros datos más importantes, si cabe, como el nombre de usuario y clave de acceso a un sitio Web o el número de la tarjeta de crédito, todo ello en relación con la dirección IP asignada a un equipo, generalmente para una sesión, por el proveedor de acceso a Internet. 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 y

[107] PALAZZI, Pablo Andrés, op. Cit. P. 57

además que algún experto podría manipular estos archivos.[108]

2. **Navegadores**: envían más información que la necesaria para establecer una comunicación, como por ejemplo el tipo y lengua del navegador, que otros programas se encuentran instalados, cual es el sistema operativo del usuario, cookies, etc.[109]
3. **Contenidos Activos**: ejecución de programas con este tipo de contenidos, como por ejemplo Java y ActiveX.[110]

Así pues, se puede concluir que en Internet la Privacidad y el anonimato NO existen ya que cuando navegamos por la red, se está revelando a cada sitio visitado:[111]

- El tipo de Browser que utiliza
- El sistema operativo de su computadora
- El idioma por defecto
- El último sitio visitado
- La dirección IP de su equipo en ese momento
- El dominio de su proveedor (Ej. Entelméxico.net)
- La resolución de su monitor y cantidad de colores

Luego, gracias a tecnologías como las Cookie's Web bugs, se revela: [112]

- Preferencias de navegación

[108] MENDOZA LUNA, Amílcar. *"Los cookies: ¿amenaza a la privacidad de información en la Internet? [En línea]. Disponible:* www.derecho.org/redi, 28 de enero de 2007
[109] Idem
[110] Idem.
[111] Idem.
[112] Idem.

- Datos personales que se suponen confidenciales por el usuario.

Finalmente, cuando solicita un producto o servicio, entrega su identidad, haciéndose totalmente identificable para la empresa, con sus gustos, preferencias, etc.

Factores de Riesgo para la privacidad en Internet: [113]

- **Interacción con la Web:** Entrega voluntaria de datos
  Cookie's
  Web bugs
- **Uso personal del e-mail**
- **E-mail marketing**
- **Mensajería instantánea:** Yahoo Messenger
  MSN Messenger
  Firetalk
- **Tecnologías de servicio al cliente** a través del Web. (tecnología de seguimiento del usuario de mi sitio, lo puedo seguir y conectarme on-line con él en tiempo real por chat).

La inseguridad del destino de los datos entregados se presenta tanto en lo sitios de empresas privadas como en organismos públicos.

El tema de la seguridad en Internet, como se puede apreciar, resulta ser bastante complejo y extenso; complejo porque la clasificación categórica exige una tarea de selección que incluye el análisis de varios componentes tales como la fuente del ataque, el objeto del ataque, las calidades de los atacantes y los atacados, y la diferenciación entre ataque a la seguridad y a la privacidad; es

[113] ROJAS Angélica, Protección de la Privacidad, Octubre 2001 (En línea). Disponible: www.utem.d/cyt/derecho/proteccion.html

extenso porque involucra la tarea de prever defensas dirigidas a los bienes jurídicos tradicionalmente dignos de protección, e implica diseñarlas para aquellos que por su sola condición de nuevos no carecen de importancia.[114] Es por lo anterior que se tratará de referir de los métodos para la violación de la "seguridad" del Internet.

2.7 EL SURGIMIENTO DE LOS PROGRAMAS ESPÍA O "SPYWARE" Y SU USO POR ALGUNAS EMPRESAS.

Existe una distribución de forma indiscriminada de la información que se puede acceder por el uso de programas, en primer grado por el tipo de material que se intercambia; con frecuencia archivos de sonido, multimedia la cual es el que mezcla audio y video o más tipo de medios y en segundo grado, la clase de material que se distribuye con estos programas, aunque sea protegido por los derechos de autor.

Estas observaciones son mínimas, si las comparamos con el hecho de que como individuos al hacer uso de estos programas, pagamos aparte de los costos para acceder a la Internet un precio más alto: la invasión a nuestra intimidad.

Para hacerlo, estos programas al instalarse, conllevan una carga que los ha denominado como *programas espía o spyware.* [115]

El término spyware o malware se refiere a los programas de software espía que tienen la capacidad de auto-instalarse en las computadoras personales de los usuarios, con objeto de conocer su identidad y monitorear su comportamiento al

[114] Idem.
[115] WALKER, Andy, *Seguridad, Spam spyware y virus,* Ed. Anaya, p. 97

usar sistemas de cómputo o navegar en Internet. El software espía —al igual que las famosas cookies — es capaz de crear bases de datos y proporcionar información y up dates sobre las preferencias y hábitos personales de los usuarios al sistema donde están instalados, mediante la utilización subrepticia de la conexión a la red, a un lugar exterior, el cual por lo general resulta ser una empresa de publicidad de Internet. Estas acciones son llevadas a cabo sin el conocimiento del usuario.[116]

El verdadero nombre de estos archivos espías es ADWARE (o software advertidor traduciéndolo) y procede de "Advertissing Supported Software".[117]

Hay que aclarar que aunque evidentemente tienen cierta similitud con los programas denominados "Troyanos", [118], los spyware no representan un peligro de manipulación ajena del sistema, ni de daños a nuestro ordenador por parte de terceros. Sus efectos son, simple y llanamente la violación de nuestros derechos de confidencialidad de nuestros datos, así como una navegación más lenta.[119]

El spyware puede ser utilizado por hackers y alguno que otro tech savy para llevar a cabo actividades ilícitas como el robo de identidad, o conocer información personal que incluye, por ejemplo, detalles de acceso a portales, números de cuenta bancarios y otras claves personales con los cuales los delincuentes usan la identidad de determinada persona para retirar dinero de cuentas bancarias, realizar compras o cometer otra serie de ilícitos.[120]

[116] Ibíd.. p. 97
[117] Ibíd. P. 99
[118] Aplicaciones que parecen inofensivas, pero que llevan instrucciones maliciosas o destructivas al ordenador que las ejecuta, a fin de dejar desprotegido el equipo para una manipulación externa y sin permiso del usuario. Para mayor información visítese: http://microasist.com.mx/noticias/.
[119] WALKER, Andy, Op. Cit. p. 99
[120] Ibíd. p. 100

Llegan a nuestro sistema de una manera muy sencilla:

Los introducimos nosotros mismos, aunque, por supuesto sin tener conocimiento de este hecho. Normalmente estos archivos vienen acompañados de programas de tipo “shareware”, gratuito y sobre todo que incorporen publicidad. Estos programas suelen ser una oferta tentadora para multitud de usuarios, ya que algunos de ellos son excelentes programas útiles y, en ocasiones, de los mejores de su categoría, por lo que resulta extraño que su difusión sea “gratuita”, pero en muchos casos la inclusión de un “banner”[121] publicitario que se mantendrá activo mientras dure la utilización del programa hace parecer una correspondencia justa por la utilización gratuita, por lo que no se levantan sospechas.[122]

Cuando instalamos uno de estos programas, al mismo tiempo introducimos en nuestro sistema los archivos que revelarán nuestros datos a empresas muy interesadas en ellos.

Actualmente, no se conoce una causa específica relacionada con el spyware que permita controlar su crecimiento, sin embargo, los principales síntomas pueden ser: (i) lentitud del sistema operativo, tanto al abrir programas como al guardar documentos en el disco duro; (ii) funcionamiento inadecuado del teclado y otras funciones primordiales de la computadora y en general, cambios sorpresivos en las barras de herramientas de la computadora que puedan llevarla hasta el famoso “crash”; (iii) desplegar una dirección en Internet o URL distinta a la que originalmente se tecleó, o incluir direcciones Web en la lista de sitios favoritos del navegador; (iv) el navegador baja e instala programas de manera automática o

[121] Cuadro publicitario regularmente animado, el cual promociona un producto o servicio. Tomado de un artículo de Jaime Olivera Díaz. http://microasist.com.mx/noticias/tp/jodtp2607.shtml.
[122] WALKER, Andy, Op. Cit. P. 146

cambia constantemente la página principal e inclusive; (v) registro de números telefónicos en el extranjero a través del uso del módem, lo que representa cargos importantes de llamadas de larga distancia para el usuario.[123]

Su funcionamiento se basa normalmente en que estos programas instalan un enlace dinámico de librerías, esto es, un archivo .dll (dinamic library lance por sus siglas en inglés, archivos necesarios para el funcionamiento de cualquier programa y que traducido es biblioteca Dinámica de Lanzamiento) que se instala automáticamente en la carpeta System de Windows, cuando instalamos los programas que lo incorporan. Este es el caso de los archivos espía tipo Aureate, difundidos por la empresa Radiate.[124]

Estos archivos denominados "Aureate" pueden realizar diferentes funciones, dependiendo del archivo concreto, esto es en el Archivo ADVERT.DLL se guardan las direcciones de las páginas visitadas en el disco duro, en una carpeta a la que el usuario no tiene acceso. Estos datos son enviados utilizando nuestra conexión a la red por encriptación, a los servidores de Aureate usando el puerto 1749 del sistema.[125]

Es interesante conocer que, algunos programas que incorporan este tipo de archivos espías, dejarán de funcionar si estos son eliminados, pero, por el contrario si desinstalamos[126] el programa anfitrión, en muchos casos no sucede a la inversa, es decir, el archivo espía permanece quedando totalmente funcional.

El uso que se puede dar a esos datos es en principio, el suponer que esos

[123] Ibíd. p. 154
[124] Ibíd. p. 155
[125] Ibíd. p. 168
[126] Desinstalar es retirar parte o la totalidad de un programa dentro de una computadora, sea de forma manual o automática, personalizadamente o bajo las características que ofrece el fabricante del programa.

datos capturados y emitidos son posteriormente comercializados por ésta y otras empresas similares, con motivos publicitarios.

Esos datos transmitidos pueden ser, desde poco relevantes (número de conexiones, duración de las mismas, sistema operativo), pasando por algunos importantes (páginas visitadas, tiempo de estancia en las mismas, banners sobre los que se pulsa, descargas de archivos efectuadas) llegando a ser personalmente relevantes e íntimos (dirección de correo electrónico, número de dirección IP, DNS de la dirección que efectúa la conexión, es decir ISP y área del país, número telefónico al que se realiza la conexión y contraseña de la misma, si está guardada, listado de todo el software instalado, extraído del registro).[127]

Tras entender esto, queda claro que con esa información se puede establecer un comercio muy lucrativo, cualquier empresa de publicidad estaría interesada en ellos.

Pero lo cierto es que no se sabe a ciencia cierta el destino de esa información, lo que resulta de por si mucho más preocupante. Algunas empresas denunciadas por emplear este tipo de programas han sido MATTEL, utilizando el archivo Broadcast, Real Networks, Netscape navigator entre otros.[128]

Los casos más conocidos de spyware, se han dado, por supuesto, en Estados Unidos de Norteamérica. Por ejemplo, en fechas recientes un periodista americano descubrió después de haber instalado un juego de la empresa de juguetes Mattel® en la computadora de su hija, una pieza de software conocida como “Broadcast” que sin saberlo conectaba directamente la computadora de su

[127] WALKER, Andy, Op. Cit. P. 179
[128] Ibíd. p. 179

hija hacia el servidor Web de Mattel, hecho que la compañía señala que se hacía únicamente con el propósito de proporcionar software updates a sus usuarios.[129]

Como consecuencia de este suceso, algunos grupos de lobbying, en defensa de las garantías individuales y los derechos de la privacidad alrededor del mundo, señalaron que el software de Mattel contenía capacidades técnicas adicionales que permitían invadir de manera flagrante los derechos de privacidad de los usuarios, al acceder a archivos personales del disco duro y monitorear de forma detallada la frecuencia con la que los usuarios empleaban los juegos de Mattel en sus sistemas de cómputo. Finalmente, después de una serie de negociaciones, Mattel acordó remover completamente el "Broadcast" de sus productos.[130]

Las empresas desarrolladoras de estos spywares alegan que la identidad del usuario se mantiene siempre a salvo, ya que ningún dato sobre esta es captado y que si bien recogen información, ésta se utiliza "únicamente" con fines de marketing y estadística. Una aseveración ridícula que podemos ejemplificar de manera burda, si se esgrime este argumento al que se sorprenda revisando nuestro buzón de correos sin abrir los sobres.[131]

Pero este tipo de empresas de publicidad disponen de otros recursos además de los archivos espías. Es relevante el caso de la Compañía Doubleclick y sus famosas Cookies. Esta empresa consigue que se descarguen desde páginas que alojen algún banner publicitario de su compañía y las utiliza para rastrear las actividades de los navegantes, en principio, pero el asunto ha suscitado una gran

[129] Inid. p. 187
[130] Idem.
[131] Ibíd. p. 188

polémica en Estado Unidos, cuando esta empresa decidió asociar la información obtenida de las cookies a una gran base de datos que contenía millones de domicilio americanos. Las autoridades tomaron conocimiento y la empresa tuvo que disponer de una dirección donde se podían dar de baja de esta utilización por parte de la empresa citada.[132]

Estas cookies, combinadas con técnicas de archivos espías y Web Bug, establecen una corriente de datos, en ocasiones bastante relevantes como para que nadie quiera facilitarlos indiscriminadamente, cuya utilización por parte de estas empresas supone por las mismas una actividad lucrativa difícil de eludir por el usuario, el cual se encuentra indefenso, principalmente por desconocimiento del proceso, el cual se realiza "subterráneamente".

WEB BUG. Un Web Bug es una imagen incrustada en un documento html, esto es, una página Web o un mensaje de correo en este formato. Esta imagen resulta invisible al visitante, ya que su tamaño es inapreciable, pudiendo ser este de un píxel y transparente. Si la página es descargada o el correo abierto, el Web Bug puede ser rastreado por la compañía emisora, lo que proporciona información sobre la actividad del usuario en la red. [133]

Las páginas Web y el formato del correo electrónico, que provoca la ejecución del navegador, pueden, asimismo introducir en nuestro sistema las conocidas cookies, estos cookies permitirán al remitente recoger cierta información, como la dirección IP que tenemos en ese momento, el tipo de navegador que usamos y los datos de las demás cookies almacenadas en nuestro

[132] Ibíd. p. 189
[133] Ibíd. p. 192

sistema, lo que devela con exactitud los sitios Web que visitamos.[134]

Al monitorizar mediante un Web Bug la recepción de un mensaje que lo porte, estamos develando que dicho mensaje ha llegado a una dirección real, la cual una vez confirmada será blanco seguro de multitud de mensajes no deseados.

Por ahora tan sólo pocas compañías (entre ellas Microsoft en conjunción con su afamado programa Windows Media Player) pueden desarrollar esta técnica, aunque esto no quiere decir que únicamente sea esta empresa la que la utilice. Monitorizar nuestros hábitos al navegar de momento no tiene otras connotaciones perjudiciales que no sean la captura de información no autorizada por el usuario, con la violación de la privacidad que ello supone.[135]

DIALERS O MARCADORES. Se pueden definir como aplicaciones que se auto instalan desde determinadas páginas de contenido llamado pornográfico o aquellas de acceso público, como los foros de consulta, cuya fuente de financiación es el acceso mediante tarificación especial a través de los prefijos 906.[136] Estos programas se introducen por un consentimiento viciado (regularmente se le solicita al usuario que vote por un sitio o dominio Web para su subsistencia o que lo catalogue). [137]

Al introducirse en la máquina, sobre todo en aquellas que su acceso es vía marcador o dial up, marcan un número con el prefijo 906, sin que el usuario lo conozca, y este puede estar navegando directamente en la Web (regularmente de

[134] Bini Rafael, Op. Cit. p. 96
[135] Ibíd. p. 97
[136] Ibíd. p. 98
[137] Informática y protección de datos personales, Madrid, Centro de Estudios Constitucionales, 1993 (Cuadernos y Debates, núm. 43).

forma más lenta) o con la inclusión de un sitio pornográfico (que aparece al principio de la sesión de navegación).[138]

Su problema radica en introducirle a la máquina un código malicioso, que aún después de desinstalarse del ordenador afectado, como con el software espía, manda datos sensibles a la compañía que lo diseñó, además de no retirarse en la totalidad del mismo.[139]

Si bien es cierto que existen recomendaciones amplias y sencillas para evitar la instalación de programas espías en nuestros equipos de cómputo también lo es que debe existir una sanción para aquellas personas o empresas que utilicen éstos programas para su conveniencia sin importarles la violación a nuestra privacidad máxime que no todos tenemos conciencia de que existan dichos programas ni menos aún que somos investigados por terceros.

Existen un par de herramientas que pueden instalarse en un equipo para protegerse contra el spyware:

- **Software antivirus.** Es necesario instalar, actualizar y ejecutar periódicamente algún tipo de software antivirus. Algunos de los software antivirus encontrarán y removerán spyware, pero no podrían ser capaces de encontrar spyware al estar monitoreando el equipo en tiempo real. Se debe establecer el software antivirus de tal forma, que se ejecute un escaneo completo del equipo de forma periódica. [140]

[138] Ibíd. p. 99
[139] Ibíd. p. 100
[140] Tomado de un artículo de Cristos Velasco San Martín y otro "Spyware, el software espía", marzo de 2005 (En línea). Disponible: www.enterate.unam.mx/Articulos/dos/enero/protecci:htm

Entre los distribuidores antivirus más importantes se encuentran:[141]

- Symantec Corporation (*http://www.symantec.com*)
- Trend Micro (*http://www.trendmicro.com*)
- Panda Software (*http://www.pandasoftware.com*)
- McAffee (*http://www.mcafee.com/mx/*)
- Sophos (*http://esp.sophos.com*)
- F-secure (*http://www.f-secure.com*)
- Computer Associates (*http://www.ca.com/offices/mexico/*)

- **Herramientas anti-spyware.** Muchos distribuidores ofrecen productos que escanearán el equipo en busca de spyware y lo removerán. Este tipo de software puede ser configurado de forma similar a un antivirus y, a menudo, es fácil de administrar.[142]

Entre los principales productos utilizados para remover spyware se encuentran: [143]

- Microsoft AntiSpyware (*http://www.microsoft.com*)
- Ad-Aware (*http://www.lavasoftusa.com*)
- SpySweeper (*http://www.spysweeper.com*)
- PestPatrol (*http://www.pestpatrol.com*)
- Spybot Search and Destroy (*http://www.safer-networking.org*)

2.8 CONSECUENCIAS JURÍDICAS Y SOCIALES A CORTO, MEDIANO Y LARGO PLAZO DE NO EVITAR LA PROLIFERACIÓN DE ESTOS PROGRAMAS ESPÍA.

De lo antes expresado, se advierte que la intimidad, como un derecho constitucional del individuo así como el anonimato de las personas, se ven amenazadas con el uso generalizado de los sistemas de comunicación

[141] Idem.
[142] Idem.
[143] WALKER, Andy, op. Cit. P. 234

electrónicos. Cada vez que alguien utiliza el correo electrónico, navega por la Web, interviene en foros de conversación, participa en los grupos de noticias, o hace uso de un servidor, está revelando datos sensibles acerca de su personalidad, economía, gustos, hábitos sociales, residencia, etc., que pueden ser maliciosamente recolectados y utilizados por terceros, en perjuicio del que los usa.

La amenaza más evidente de la que todo el mundo es conciente, consiste en los ataques a la confidencialidad, autenticidad e integridad del correo electrónico. Hoy en día resulta sencillo hacer frente a estos ataques mediante los protocolos de comunicaciones basados en procedimientos criptográficos, es decir tener que mandar comunicaciones mediante códigos únicamente descifrables por nuestro receptor y viceversa.[144]

A pesar de ello, la mayoría de los usuarios no es conciente de la cantidad de la información privada que, de forma inadvertida e involuntaria está revelando a terceros al hacer uso de la Internet. Cada vez que se visita un sitio Web, se suministra de forma rutinaria una información que puede ser archivada por el administrador del sitio. A éste no le resulta difícil averiguar la dirección de Internet, de la máquina desde la que se está operando, la dirección de correo electrónico del usuario, qué paginas lee y cuales no, que figuras mira, cuántas páginas ha visitado, cuál fue el sitio recientemente visitado y también que sistema operativo y que navegador usa.

Con ello se expone a ser víctima de las últimas plagas que han entrado en la escena de las comunicaciones electrónicas: el correo basura (junk-mail o spam) que puede llenar nuestro buzón de correo, empleado por marcas comerciales sin

[144] Ibíd. p. 236

escrúpulos o por aficionados para promocionar indiscriminadamente sus productos por toda la red, la suplantación del usuario para enviar mensajes ofensivos en su nombre a terceros, que le pueden poner en una situación incómoda; el marketing personalizado, que explota información que los usuarios van revelando inadvertidamente a medida que navega por la red sobre sus gustos y preferencias, etc.[145]

Pero estos efectos son menores, sin comparamos con el riesgo al ser monitoreados de nuestras actividades y ver nuestros datos, sean privados, íntimos o sensibles, del uso inmediato que se les de, a ejemplo de lo anterior caben señalar algunos acontecimientos que se han suscitado últimamente:

En México, no existe una legislación específica para regular el software espía y es poco probable que se defina una a corto plazo puesto que por un lado, todavía existe un gran desconocimiento del "usuario promedio" acerca de los sistemas de cómputo y programas de software, y por el otro, el tema no es prioritario en la agenda de nuestros legisladores, puesto que desde el año de 2001 no se ha logrado la aprobación de una Ley Federal de Protección de Datos Personales ni se ha presentado un nuevo proyecto de Ley al respecto.

La cultura de la seguridad informática en nuestro país se encuentra aún en una etapa intermedia de desarrollo y, actualmente, su papel es de carácter preventivo, debido a que se limita a proporcionar herramientas educativas y tratar de crear conciencia en los empleados de empresas y usuarios del Internet con el objeto de que se incremente la seguridad en sus sistemas de cómputo y redes, para evitar daños, perjuicios y pérdidas económicas. Sin embargo, es conveniente

[145] Ibíd. p. 237

que los usuarios mexicanos profundicemos en este problema, para salvaguardar la seguridad de los equipos de cómputo y software en que hemos invertido.

Al respecto se ha encaminado el llamado E-gobierno mexicano, que es una manera simple de poder realizar trámites de manera rápida, "segura y fiable en la fuente" además de ser "una innovación continua en la entrega de servicios, la participación de los ciudadanos y la forma de gobernar mediante la transformación de las relaciones externas e internas a través de la tecnología, Internet y los medios de comunicación." Con ello algunas Secretarias y Organismos dependientes del Ejecutivo han empezado su adherencia a tal plan, empezando por el IMSS, ISSSTE, INFONAVIT y actualmente la Secretaria de Hacienda y Crédito Público, al implementar el pago de impuestos vía Internet, el sello digital "infalsificable" y el uso de la firma electrónica como de validez legal en las transacciones realizadas por Internet.[146]

Todo esto enmarca un futuro prometedor en el desarrollo de la tecnología, la inclusión de nuestro Estado Mexicano con la modernidad tecnológica mundial, pero solo en una mínima parte ya que si bien es cierto que el esquema que se nos presenta es de eficiencia y rapidez, además de un ahorro de recursos humanos que conlleva la realización de dichos trámites, no existe lamentablemente la confianza en nuestro Gobierno de que tenga la infraestructura necesaria para realizarlo, esto es no se cuenta con el equipo para sostenerlo.

Como ejemplo de lo anterior se tiene el caso del registro de examen al Instituto Politécnico Nacional, que ha sido desde 1999 vía Internet y aunque dicha

[146] Ello se denota con las múltiples páginas de Internet de las Secretarías y dependencias de Gobierno enfocadas a la información de sus actividades a la ciudadanía, solo basta buscar las páginas con terminación gob.mx

institución ha hecho lo posible de conllevar la realización de tal trámite, por la cantidad de aspirantes a ingresar, se bloquea el servidor o peor aún se quedan los datos enviados, dejándolos a la vista de quien quiera realizar el mismo trámite.

Reafirmando lo anterior, el Ejecutivo, por conducto de la Presidencia para la innovación Gubernamental, ha implementado el uso del llamado e-gobierno en las dependencias del INFONAVIT[147], si concatenamos lo anterior de una manera amplia, podemos dilucidad que junto a los datos requeridos en ésta página (número de seguro, RFC, dirección, número telefónico, lugar de labor, etc.) la amplitud de los datos que se pueden obtener son altamente sensibles sin que se tenga la suficiente confianza que de quedarán a manera de confidenciales.

Tal pudiera parecer un tanto exagerado lo anterior, pero tiene su fundamento: se han visto ejemplos claros de invasión a nuestra intimidad y nuestros datos como lo fue el hecho de que se haya recabado el total del padrón electoral mexicano y se haya vendido a un gobierno extranjero, sin saber que uso se les dará a los mismos.

La red Internet es una herramienta de gran utilidad, una fuente poderosa de difusión de recursos, información, datos, y que agiliza la funcionalidad de una empresa y su administración, pero como toda novedad, también debe concientizarse sobre los peligros que existen y la necesidad de regular un marco jurídico concreto, justo y eficaz que permita salvaguardar la confianza que tenemos al proporcionar nuestros datos.

[147] Visítese y obsérvese www.micasa.gob.mx

2.9 OBTENCIÓN DE DATOS PERSONALES POR OTROS MEDIOS.

No solo es en la red Internet donde son recabados y utilizados nuestros datos personales para beneficios de otros; tal es el caso de las Bancas de crédito, las cuales en principio para la obtención de cualquier servicio principalmente la obtención de una tarjeta de crédito o apertura de cuentas requieren de los datos personales del cuenta habiente los cuales son proporcionados de buena fe, sin embargo es con posterioridad cuando el cliente se da cuenta que los datos proporcionados fueron utilizados no solo para el manejo de sus cuentas bancarias, sino que fueron distribuidos a empresas de diferente índole como es el caso de agencias de viajes, tiendas departamentales, telefónicas entre otras, para posteriormente sólo informar la banca que si el cliente no está de acuerdo en que sus datos se publiquen, puede darse de baja de las listas comerciales, situación que debería ser contraria, esto es, que sea el cliente quien decida si quiere estar en la lista comercial o no y no ser él quien tenga que darse de baja de una lista en la cual en ningún momento solicitó su afiliación.

Al respecto cabe señalar que las instituciones de banca de crédito refieren que sólo intercambian información con “fuentes confiables de información y agencias especiales de clasificación de información” de conformidad con la legislación aplicable, si esto realmente fuera cierto, entonces porqué en algún momento hemos recibido una llamada ofreciendo un servicio que en ningún momento requirió informando que el nombre, domicilio, edad y ocupación fueron proporcionados por un Banco o a través de una tarjeta de crédito o débito.

Asimismo en la actualidad se ha comprobado que hasta internos de

prisiones de “alta seguridad” principalmente en el estado de Jalisco tienen una base de datos de personas que utilizan para tratar de defraudarlos, ello es así ya que se ha difundido que hay internos que llaman por teléfono a determinadas personas haciéndose pasar por policías que tratan de “ayudar” a un familiar de a quien le hacen la llamada solicitando un depósito en una cuenta bancaria para su liberación; hasta aquí solo sonaría a broma, la preocupación surge cuando se toma conciencia de que unas personas que ni siquiera viven en nuestro mismo estado, tienen conocimiento de nuestro nombre, dirección, teléfono y sobre todo del nombre de familiares cercanos y más aún que no se sabe cómo es que obtuvieron esa información que se presume es confidencial, por lo que la inseguridad crece hasta en nuestro propio domicilio pues ya no resulta fácil tener la confianza de asentar nuestros datos correctos cuando nos son requeridos puesto que en realidad no se sabe que finalidad tendrán.

CAPITULO 3.
PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES.

Hasta ahora se han determinado los antecedentes históricos cronológicos de la garantía de correspondencia e inviolabilidad de las comunicaciones privadas, así como una conceptualización para su mayor entendimiento, sin dejar de pasar por alto una breve reseña de la red Internet de los inicios hasta el día de hoy, su avances y los riesgos de seguridad implementados para efecto de obtener información confidencial de los usuarios.

Así pues, en éste capítulo se realizará una visión desde la perspectiva jurídica para determinar los daños causados a la ciudadanía, así como la protección y sanciones que en diversos países se establecen para limitar el uso de los datos personales sin el consentimiento del afectado.

3.1 BIENES JURÍDICOS AFECTADOS POR LA OBTENCIÓN ILÍCITA DE DATOS PERSONALES.

Tomando en consideración el surgimiento del Internet es fácil advertir que esta nueva forma de comunicación trae aparejada una nueva categoría de derechos a proteger, así pues, al existir nuevos bienes jurídicos a tutelar, se deduce que éstos presentan nueva o especial vulnerabilidad. Por lo cual estos bienes y los conocidos tradicionalmente, pueden ser objeto de nuevos ataques, en virtud de lo cual aparece una categoría distinta de ejecutores (en este caso no se puede hablar siquiera de delincuentes, ya que para ello hace falta previamente establecer el delito).

Nuestra legislación todavía no ha captado figuras nuevas, de entre las que se pueden originar por el uso de Internet, ni ha ignorado las ya existentes. A modo de comparación observamos que la legislación española ya ha avanzado sobre este tema, incluyendo y adecuando en su Código Penal, la tutela de los siguientes tópicos:

- Difusión y exhibición de material pornográfico a menores (Art. 186);
- Pornografía infantil (Art. 189);
- Interceptación de correo electrónico (Art. 197);
- Cesión de datos reservados de carácter personal (Art. 197.2);
- Difusión de mensajes injuriosos o calumniosos (Art. 211);
- Estafas electrónicas (Art. 248)
- Uso de terminales de comunicación sin autorización (Art. 256);
- Daños informáticos (Art. 264.2);
- Delitos contra la propiedad intelectual (Art. 270)
- Relevación de secretos (Art. 278);
- Publicidad engañosa (Art. 282);
- Falsedad documental (Art. 390)

Llegándose a hablar de ciberdelitos[1], que aunque con poco tecnicismo, para hacer referencia a un nuevo grupo de ataques contra bienes jurídicos nuevos, pone de manifiesto que la sociedad busca su defensa.

[1] PARDINI Aníbal A., *DERECHO DE INTERNET.,* Ed. *La Rocca*, Argentina, *2002,* P. 78

Respecto de los ciberdelitos cabe señalar cuatro características a saber: [2]

- Falta una debida tipificación, la cual no solo dificulta encuadrarlos, sino que implica un esfuerzo para luchar en desigual posición contra la *ciberdelincuencia.*
- No se requiere la presencia física para su comisión;
- Aprender a delinquir en la red es relativamente fácil;
- Se requiere poca inversión, en comparación con el daño que causan.

Dentro de la taxonomía de delitos, éstos pueden ser agrupados[3] según se ataquen: [4]

- Datos (robo, interceptación, modificación);
- Redes (sabotaje, interferencia, *hacking,* distribución de virus);
- Mediante computadoras en red (fraude)

Entre los delitos que son captados por algunas legislaciones[5] se encuentran:

- Intercepción de datos (en su transmisión)
- Modificación de datos (borrado, destrucción o alteración)
- Robo de datos (como figura penal, captada en forma

[2] Ibíd. p. 81
[3] Ibíd. p. 82
[4] Idem.
[5] Al respecto cabe señalar que esta es la única materia acerca de la cual ha avanzado nuestra legislación mediante la sanción a la intervención a las comunicaciones privadas en el Código Penal para el Distrito Federal en el artículo 334 así como en los numerales 211 bis 1 al 211 bis 8 séptimo párrafo del Código Penal Federal, realizando la aclaración que la protección está brindada para el dato, esté o no en Internet.

independiente de las leyes de propiedad intelectual)

- Interferencia de redes (impidiendo el acceso a usuarios o la provisión del servicio a ISP,
- Sabotaje de redes (modificación o destrucción de sistemas o configuraciones de redes),
- Acceso no autorizado (a bases o programas, mediante hacking o cracking),
- Diseminación de virus (en distintos ámbitos, redes o sistemas),
- Apología (facilitando a invitando a cometer ciberdelitos),
- Fraude informático (alteración de datos para lograr beneficios económicos)
- Falsificación (alteración de datos con el objeto de simular la autenticidad de certificados o firmas digitales).

En cuanto a los efectos se propicia uno en particular: el alcance del delito en Internet, es tan vasto como la red misma, por lo cual, en principio, aún existiendo legislación que reprima este tipo de delitos sólo en un país o en varios países dispersos, no hay un accionar contundente. Por ello, es necesario un acuerdo de tipo internacional, a través de los tratados con que se cuenten al respecto, para penalizar los estándares mínimos delictuales en la red, que permita sancionar, en cualquier lugar este tipo de actividades y más aún formar una cultura en nuestro país que en un principio prevenga la comisión de éstos delitos haciendo saber su alcance así como el daño que pueden generar, más aún cuando se pone en riesgo nuestra privacidad, puesto que no se tiene un verdadero

conocimiento de la magnitud de este problema. Así pues, el inconveniente de la territorialidad de las legislaciones penales y la globalidad que Internet requiere, tiene como solución, que la comunidad internacional y en consecuencia la mexicana, reconozca una conducta como delictiva, para lograr homogeneidad en su accionar.

Amenazas a la privacidad en las relaciones profesionales y laborales.

Las amenazas a la privacidad son más sutiles y se han planteado generalmente en el uso de los denominados e-mails, al respecto pueden ser establecidos algunos límites, cuya elección tendría como parte del análisis a quienes intervengan relacionándose mediante esta forma de comunicación. De esta manera, las comunicaciones establecidas entre un alumno y su profesor no requerirán el mismo nivel de seguridad que las efectuadas entre un abogado y su cliente, en relación con el caso que los vincula.

En este caso, el estándar de protección requiere mayor diligencia por parte del profesional, o la autorización escrita de su cliente para utilizar este vulnerable medio de comunicación; para lograr un cierto estado de confidencialidad se han establecido códigos para enviar los mensajes, por ejemplo, un e-mail se puede hacer seguro usando un programa de encriptado: el software de encriptación traduce el mensaje a un código confidencial, para que sólo pueda ser leído por la persona que tiene el código descriptador correcto, es decir, aquel a quien se lo está enviando. Este método es seriamente cuestionado y existen tanto opiniones a favor como en contra basándose principalmente en la confidencialidad de los

asuntos y el riesgo de ser interceptadas las comunicaciones. [6]

Por otro lado por cuanto se refiere a las relaciones laborales es de señalar que en determinadas empresas o bien dentro del mismo gobierno, es más frecuente la instalación de Internet para facilitar la comunicación entre sucursales dentro de las cuales se lleva a cabo el monitoreo de e-mails esto deriva en dos intereses fundamentales: las del empleador que prohíbe el uso de los medios de comunicación para lo cual realiza monitoreo de sus mensajes y el de los empleados que con frecuencia hacen uso de estos medios para usos personales, con lo que tomando en cuenta por asimilación del e-mail al concepto de domicilio o correspondencia, la garantía de inviolabilidad se ve afectada en el punto de vista del trabajador trayendo consigo una lucha de intereses por ambas partes.[7]

3.2 DELITOS INFORMÁTICOS.

Conforme al autor PABLO A. PALAZZI[8] la clasificación de los delitos informáticos se realizar tomando en consideración el bien jurídico protegido, y dentro de estas categorías, se distinguen las acciones típicas que la vida cotidiana o experiencia local o comparada nos dan noticia, para así centrar las bases para fijar una adecuada política de reforma al Código Penal en materia de delitos informáticos que contemple las verdaderas necesidades que requiere una verdadera legislación criminal.

Distinguiendo de esa manera:

[6] Ibíd. p. 67
[7] Idem.
[8] PALAZZI, Pablo A. *Delitos Informáticos*, Ad-Hoc, Buenos Aires, 2000, p. 39.

- *Delitos contra el patrimonio.*

Los cuales son perpetuados a través de máquinas o en cajeros automáticos a efecto de defraudar a la gente por la transformación del dinero tradicional a nuevas formas dinerarias como ser el dinero plástico y más recientemente el dinero electrónico, dentro de esta misma clasificación cabe citar a aquellos delitos cometidos por la falsificación de bandas magnéticas en las tarjetas de crédito.[9]

- *Delitos contra la intimidad.*

Como ha quedado asentado en los capítulos anteriores, la información ha adquirido un valor muy especial pues se le trata como mercancía, lo que conlleva a la comercialización de datos de carácter personal, invadiendo la intimidad de las personas que desconocen que sus datos son objeto de dicho intercambio. [10]

Esta afectación directa al bien jurídico denominado *intimidad* no se encuentra contemplada como tal en el Código Penal para el Distrito Federal ni en el Código Penal Federal y si bien es cierto que en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en su Capítulo IV denominado "Protección de Datos Personales" establece los lineamientos que deben tomar en cuenta las personas que cuenten con bancos de datos personales, únicamente establece que el inadecuado uso de dichos datos será objeto de responsabilidad administrativa por los servidores públicos o en su caso lo más que puede hacer es presentar *recomendaciones* a las dependencias y entidades para el buen manejo de los datos que están bajo su resguardo.

[9] Ibíd. p. 43
[10] Ibíd p. 44

Sin embargo en ningún momento se establece que pudiera ser objeto de algún delito el uso indebido de tal información, ello a pesar de que actualmente hay nuevos medios tecnológicos que permiten acceder en lugares de la privacidad del individuo antes inaccesibles pues como lo refiere el mismo autor:

> "…con una simple conexión a Internet cualquiera puede saber si su vecino fue inhabilitado por el Banco Central para operar en cuenta corriente bancaria[11] o mediante satélite es posible fotografiar cualquier superficie de la tierra, o por medio de un scanner térmico podemos detectar que sucede dentro de un hogar... así en lo referente a la informática, se habla de protección de datos y de un nuevo espacio que se debe proteger: el *ciberspacio."*[12]

- *Delitos contra la seguridad pública y las comunicaciones.*

En esta clasificación se refiere a la dependencia que se está viviendo hacia el acceso y buen funcionamiento de un ordenador para realizar cualquier tarea cotidiana, por lo que los ataques que se haga en contra de las mismas no sólo puede afectar a un bien individual sino a uno colectivo. [13] Por ejemplo la paralización de un ordenador o una red de computadores podría ocasionar catástrofes nacionales e incluso mundiales, como pueden serlo por ejemplo los ataques de los denominados hackers.[14]

- *Falsificaciones informáticas.*

Las falsedades cometidas por medios informáticos constituyen el antecedente de la comisión de un delito contra el patrimonio, ya que por lo general

[11] Véase para su entendimiento la base de datos del B. C. R. A. que está en línea disponible en: http://www.bcra.bov.ar.)
[12] PALAZZI, Pablo A. Op. Cit. P. 45
[13] Idem.
[14] Para mayor abundamiento leer el anexo sobre Vladimir Lenin, autor del más grande fraude electrónico.

los documentos electrónicos no tienen un valor jurídico en sí mismos considerados por la carencia de un régimen legal que los contemple. Así para evitar la alteración en la información para la toma de decisiones se están desarrollando nuevos medios para la identificación de personas mediante un código único o una clave determinada, para lo cual resulta necesario un método electrónico de firma (criptográfico o biométrico), así como la protección de la fe pública cuando esta se instrumenta mediante ordenadores.[15]

- *Contenidos ilegales en Internet.*

El paso de un ámbito académico a un medio comercial de Internet, hizo que la red fuera invadida por una gran cantidad de material ilícito, como ser propaganda discriminatoria o antisemita, contenidos pornográficos y pedófilos inconvenientes para menores los cuales son los que navegan más por Internet. En Europa y Estados Unidos aún se está debatiendo como regular este nuevo ámbito y si es necesario extender al ámbito penal la protección existente de antaño.[16]

De lo anterior se advierte que los delitos que se pueden cometer a través de las computadoras son vastos y afectan tanto a las personas en lo particular como a la sociedad en general, sin embargo debido a la gran ignorancia que respecto a este tema existe en México, no se tiene conocimiento de ello, pues existe gente que aún no sabe siquiera para que pudieran ser utilizados sus datos personales o que al momento de pagar con su tarjeta de crédito pudieran ser “robados” sus

[15] PALAZZI, Pablo A. op. Cit. P. 46
[16] Ibíd.. P.47

datos confidenciales al ser clonada su tarjeta ni menos aún que los bancos no tienen medios suficientes para la protección de sus propias cuentas bancarias, sin embargo aún y con la extensa clasificación que se pudieran hacer de los delitos informáticos, en este trabajo de investigación se determina tomar únicamente en consideración lo concerniente a la protección de los datos personales los cuales considero más importantes que el patrimonio mismo, pues atenta contra un bien mayor que lo es la PRIVACIDAD, ante lo cual resulta indispensable un sistema de protección de datos.

Se trata así de garantizar al titular de los datos que los terceros, bien se trate del sector público o del sector privado, utilizarán sus datos personales con el respeto debido al mismo, de forma que aquél pueda tener un control sobre los mismos, y en todo momento sepa que va a hacer quien trata sus datos, para qué los recoge, cómo los trata y para qué los utiliza o a quién se los cede o comunica.

Es necesario señalar que la protección de datos es un derecho fundamental, si bien no referidos como tales en la Constitución mexicana, si se hace referencia a la protección de la privacidad de las personas, y como tal, ha de ser respetado por todos, comenzando por la concienciación del propio sujeto titular de los datos. Además, una formación adecuada sobre los derechos que se atribuyen al ciudadano permitiría a éste un mejor control sobre sus datos y evitaría acciones innecesarias, que en el caso de denuncias pueden conllevar la apertura de un procedimiento sancionador al responsable del fichero.

3.3 TRATAMIENTO, VENTA Y PROCESAMIENTO ILEGITIMO DE LA INFORMACIÓN PERSONAL.

Como ya se ha manifestado con anterioridad, las computadoras permiten almacenar y manejar una gran cantidad de información personal en forma automatizada. Cabe aclarar que siempre se recopiló información personal, pero lo que se hace hoy mediante la ayuda de ordenadores no es sólo almacenarla, sino relacionarla con otros bancos de datos, logrando así la posibilidad de crear perfiles de individuos para conocer sus hábitos, costumbres de consumo, y en general sus inclinaciones personales.

En la vida diaria damos mucha información a terceros, por ejemplo al realizar un trámite en una oficina pública, al solicitar la expedición de documentación, al comprar un auto, una casa o cualquier otro bien o servicio, al irnos de vacaciones y hospedarnos en algún hotel, etc. Esta información no se pierde, por el contrario es cuidadosamente guardada en ordenadores, y ya sea voluntaria y legalmente o a través de empleados infieles o hechos ilícitos, o por descuidos, llega a bancos de datos que se encargan de procesarla para proveer información por suscripción a terceros. Pero a veces la adquisición de estos datos puede ser hecha en forma ilegal.

Por ejemplo, en enero de 1993 en Madrid fueron arrestadas tres personas que se dedicaban a la venta de datos personales que habían sido almacenados en el Centro de Informática del Departamento del Trabajo de la Seguridad Social. Se trataba de los datos personales (sexo, estado civil, nombre y dirección, número, edad y sexo de los hijos, nivel de ingresos, información sobre su vivienda), correspondientes a más de dos millones de ciudadanos españoles. Igualmente en

Alemania en 1995 se produjo otro escándalo con relación al tratamiento de datos personales de millones de ciudadanos de la entonces República Federal, se trataban de datos muy sensibles como la situación económica de las personas afectadas, su historial laboral e incluso penal. El número de afectados superó los diez millones.[17]

A comienzos de 1998[18] se conoció en Argentina el caso de un disco óptico conteniendo una base de datos de la ANSeS, la D. G. I., y otros registros estatales, con todo el padrón de autónomos, y que había sido sustraída ilícitamente y se intentó vender, entre otras, a varias administradoras de fondos de jubilaciones y pensiones. Lo interesante del caso es que esa información había sido sustraída del Estado nacional y no existían leyes que reprimieran su venta desleal por parte de quienes habían realizado tal accionar. Este caso llegó a la justicia a través de una denuncia realizada por uno de los afectados. El juez federal a cargo de la investigación, siguiendo el dictamen del fiscal de primera instancia sobreseyó en la causa, concluyó que esta conducta no quedaba amparada por el Código Penal Argentino.

El derecho comparado, en especial en Europa como veremos en su momento oportuno, ha prestado gran atención a este tipo de delitos. Así la ley Federal de protección de datos de Alemania[19], establece un marco para la regulación del manejo de información personal almacenada en bancos de datos. El artículo 43 de dicha ley establece las ofensas criminales referidas a la violación

[17] WALKER, Andy, op. Cit. P. 235

[18] Cfr. CANTOR, Damián: "Investigan la venta de bases de datos de la ANSeS y la D. G. I." Y PALAZZI, Pablo: "Las leyes no dan cuenta de los cambios de los delitos", ambos publicados en el diario *Buenos Aires Económico,* del 12/I/98.

[19] Cfr. Ley Federal de Protección de Datos del 20 de diciembre de 1990 –BGBI.I 1990 S.2954-, reformada por la ley del 14 de septiembre de 1994 (BGBI.1 S.2325)

de la privacidad por medios informáticos; se tipifica la acción de cualquiera que sin autorización almacena, modifique, comunique, permita acceder a terceros o recupere u obtenga para sí o para terceros archivos o datos protegidos por la ley estableciendo una pena de prisión hasta de un año.[20]

Aunque vivimos en la llamada "era del acceso a la información" y de las nuevas tecnologías, las normas jurídicas suelen prestar poca atención a estas cambiantes realidades. El marco jurídico del comercio electrónico en México es relativamente reciente, sin embargo la protección de datos personales en el área de negocios y consumidores ya se encuentra regulado en la Ley Federal de Protección al Consumidor y actualmente dicha legislación contempla la posibilidad de que los proveedores y consumidores puedan celebrar transacciones a través de medios electrónicos.[21]

La fracción I del artículo 76 bis de la Ley Federal de Protección al Consumidor le impone la obligación a los proveedores de mantener la confidencialidad de la información y la prohibición de difundirla o transmitirla a otros proveedores, a menos que el consumidor lo haya autorizado por escrito (*opt in*) o que exista un requerimiento de alguna autoridad, asimismo, la fracción II de este mismo artículo impone al proveedor la obligación de mantener segura y confidencial la información e informar al consumidor sobre las características generales de los elementos técnicos disponibles antes de la celebración de una transacción.[22]

Sin que en ningún momento ésta ley, se refiera a los datos presentados en

[20] PALAZZI, Pablo Andrés, op. Cit. P. 87
[21] Ley Federal de Protección al Consumidor
[22] Idem.

las empresas por los mismos trabajadores o en las escuelas por los alumnos ni menos aún se protege la información almacenada en bancos de datos estatales (salvo que el Estado actúe como empresario) ni aquella referida a la intimidad o a datos privados de los ciudadanos, pues este es un ámbito distinto al derecho de los secretos comerciales o de la confidencialidad, conocido como "protección de datos" o *habeas data.*

En el Derecho comparado, son varias las legislaciones que prohíben la cesión de datos de entidades públicas, tales como España, Alemania, Francia, el Reino Unido, etc. El derecho de la protección de datos en la Unión Europea se vio reforzado por una Directiva del año 1995, que entró en vigor en el año 1998, por la cual todos los Estados miembros de ese bloque económico deben uniformar sus legislaciones conforme a lo instrumentado en ese documento.[23]

3.4 PANORAMA INTERNACIONAL GENERAL.

En función del innegable carácter económico inherente a este problema, es necesario presentar la situación internacional de hecho y de derecho en torno al mismo, estructurada en tres grupos de países bien definidos de acuerdo con el régimen económico prevaleciente, a saber países desarrollados, y los que se encuentran en desarrollo, para posteriormente señalar una semblanza del acuerdo existente en materia de protección de datos personales: el Convenio de Estrasburgo.[24]

[23] Palazzi Pablo A. Op. Cit. p. 53
[24] Cfr. TÉLLEZ Valdez, Julio, *Derecho informático*. Op. Cit. p. 72-77

3.4.1 PAÍSES CON ALTO DESARROLLO ECONÓMICO.

Encontrándose en este rubro aquellos países en los que existe una consigna a nivel constitucional, como es el caso de Portugal, España, Austria, Holanda, Suiza y Alemania, a través de una sentencia del tribunal constitucional, siendo así Portugal el primer país en contemplar a partir de 1976 esta situación a nivel internacional; por otra parte España en su Constitución del 29 de diciembre de 1978 en su artículo 18 fracción IV complementado por la ley del 5 de mayo de 1982 y la de 1992, dispone las limitaciones de que será objeto la informática en función del honor y la intimidad personal y familiar de los ciudadanos. Desarrollado bajo las consideraciones de una regulación civil contractual sin desconocer la protección penal, Holanda hizo lo propio en 1985 en la sección 10 párrafos segundo y tercero.[25]

Por otra parte se encuentran aquellos países que cuentan con una ley de carácter general, que contiene un conjunto de disposiciones relativas al problema, como es el caso de Estados Unidos con su *Privacy Act* o Ley de la Privacidad del 31 de diciembre de 1974, bajo las consideraciones de una protección a la vida privada, siendo los tribunales federales el órgano jurisdiccional competente con sanciones de tipo penal, complementándose esta ley con otras disposiciones.[26]

Asimismo, con un ordenamiento general con disposiciones particulares tenemos a Canadá con su *Human Rights Act* o Ley de Derechos Humanos del 14 de julio de 1977, inspirada en la ley norteamericana, y cuyo capítulo IV aborda específicamente los problemas derivados de la informatización respecto a los

[25] Ibíd. p. 73
[26] Idem.

derechos humanos, existiendo una autoridad encargada de velar el cumplimiento de dicha ley, como es el caso del comisario para la protección de la vida privada nombrado por el ministro de justicia.[27]

Por otro lado, tenemos a aquellos países que dentro de este grupo disponen de una ley que en forma expresa regula el fenómeno de la protección de datos personales; tal es el caso de Suecia con su *Datalag* o Ley de Datos del 11 de mayo de 1973 (primera regulación a nivel nacional) con un organismo supervisor como es la *Data Inspektion Board (DIB – Tabla de Registro de Datos)*, y complementada por la ley de Información sobre Solvencia de 1973 y la Ley de Trabajos y Cobros de Créditos por cuenta ajena de 1974.[28]

Asimismo tenemos a Alemania con su *Bundesdatenshutzegesetz* o Ley Federal de Protección de Datos del 27 de enero de 1977, con un comisario federal de datos encargado de velar su cumplimiento y complementada por diversos ordenamientos en materia de recaudación tributaria, identificación personal, registros de población, seguridad social, manejo de archivos policíacos, confesión religiosa, etc.[29]

Francia, con su Ley relativa a la Informática, Archivos y Libertades del 6 de enero de 1978, con su Comisión Nacional de Informática y Libertades como órgano especial y autónomo con funciones de control por medio de reglamentos, con derecho a informarse y obligación de informar.[30]

Otros países con disposiciones específicas son Dinamarca con sus leyes

[27] Idem
[28] Idem
[29] Idem
[30] Ibíd. p. 74

sobre Archivos Públicos y Privados del 8 de junio de 1978; Noruega con su Ley sobre Datos de Carácter Personal del 9 de junio de 1978; Austria y su Ley de Protección de Datos del 18 de octubre de 1978; Luxemburgo y su Ley reglamentaria de la Utilización de Datos Nominativos en los Tratamientos Informáticos del 11 de abril de 1979, así como las de Islandia del 1 de enero de 1982, de la Gran Bretaña del 1 de julio de 1984, de Irlanda de 1988, Holanda y su ley de enero de 1989, Portugal y su ley del 29 de abril de 1991 y Bélgica y su ley del 8 de diciembre de 1992. Encontrándose también dentro de este grupo otros países como son: Japón, Italia, Finlandia, Australia, Nueva Zelanda y Grecia. [31]

3.4.2 PAÍSES DE ECONOMÍA EMERGENTE.

En este grupo, si bien el grado de informatización no llega a ser considerable aún así el problema de la protección jurídica de los datos personales no deja de estar latente. Dentro de este grupo se encuentra México en donde a pesar de existir consignas a nivel constitucional que garantizan el derecho a la información, derecho de petición o algunos privilegios personales (familia, papeles, posesiones etc.), o disposiciones penales sobre violación de correspondencia y a las comunicaciones privadas, revelación de secretos y hasta hace poco a nivel Federal sobre la obtención de información contenida en sistemas o equipos de informática, daño moral en materia civil e incluso una Ley de Información Estadística y Geográfica del 30 de diciembre de 1980 y su reglamento con fecha 3 de noviembre de 1982 y algunos otros ordenamientos, lo cierto es que el problema se manifiesta cada vez con mayor intensidad, al no disponer realmente de una

[31] Idem.

reglamentación sobre una protección jurídica eficaz.[32]

3.4.3 CONVENIO DE ESTRASBURGO.

Este acuerdo internacional con fecha 28 de enero de 1981 denominado Convención para la protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal y más conocido con el nombre de Convenio 108 de Estrasburgo, suscrito por países tales como Austria, Alemania, Bélgica, Dinamarca, España, Francia, Grecia, Holanda, Irlanda, Italia, Luxemburgo, Portugal, Reino Unido, Suecia y Turquía, ratificado por varios de éstos países y abierto a la firma de todos los países interesados, contiene una serie de disposiciones (27 artículos integrados en 7 capítulos) relativas a objetivos, definiciones, ámbitos de aplicación, obligaciones de las partes, derechos, excepciones, sanciones, autoridades, consignas generales y específicas no solo en materia de protección de datos personales, sino también a nivel del flujo de datos transfronterizos.[33]

3.5 PROTECCIÓN DE LA PRIVACIDAD EN EL DERECHO COMPARADO.

Los trabajos de la Organización para la Cooperación y el Desarrollo Económico.

De acuerdo a Pablo A. Palazzi[34] la Organización para la Cooperación y el Desarrollo Económico (OCDE) fue el primer organismo internacional que se abocó al estudio de los problemas relativos a la privacidad y las nuevas

[32] Ibíd. p. 77
[33] Idem
[34] Ibíd. p. 180

tecnologías, mediante el desarrollo de una guía de principios, sin embargo no hace referencia a cuáles fueron éstos principios, señala que dicho estudio comenzó en 1977 y en 1980 las Recomendaciones fueron adoptadas por el Consejo de la OCDE, como una recomendación a sus Estados miembros. Si bien estas pautas no son vinculantes para los 29 Estados miembros que las han aceptado, se recomendó el cumplimiento de ocho principios sobre el tratamiento de información personal que se hallan presentes en muchas de las legislaciones existentes, sin embargo nuevamente el autor no señala los principios que cita.[35]

En términos generales, podemos señalar que el contenido de estas guías sobre privacidad y protección de datos, proporcionan principios y reglas específicas a seguir para que los gobiernos adopten políticas de regulación efectivas sobre privacidad y protección de datos y sobre todo sirven como fundamento para uniformar legislaciones en materia privacidad que permitan, simultáneamente, evitar distorsiones al libre flujo transfronterizo de la información y los datos personales a nivel internacional.

El Consejo de Europa

Paralelamente, a lo antes expuesto, el Consejo de Europa promovió y logró la suscripción de un acuerdo sobre la materia que sí resultó vinculante. En 1981 se adoptó la Convención para la protección de los individuos en relación al procesamiento automatizado de datos personales,[36] que entró en vigencia el 1º de octubre de 1985.

[35] Cfr. PALAZZI Pablo A. *Delitos Informáticos, op. Cit. p.185-189*

[36] El texto en español de la Convención puede consultarse en *Informática y Derecho,* vol. 6, Depalma, Buenos Aires, 1998, pp. 203 y ss.

La convención incluye diez principios básicos en materia de protección de datos que representan en estándar mínimo que se requiere a los países que la cumplan. Entre estos principios se encuentran la justificación social, la limitación a la recolección de datos, la calidad de la información, la finalidad específica, la limitación a la comunicación, medidas de seguridad a la que deben someterse los bancos de datos, limitación temporal, e identificación. Basado en el principio de protección equivalente, la principal regla de la Convención es que la transparencia de datos a un país que otorgue un nivel de protección equivalente no puede ser limitada, salvo las excepciones previstas en el convenio.[37]

La Convención no hace alusión expresa a normas penales, sino que deja librado a cada uno de los países miembros la necesidad de sancionar los ilícitos relacionados con la privacidad y la informática.[38]

Así el artículo 10 dice: *"Sanciones y recursos.* Cada parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de Derecho interno que hagan efectivos los principios básicos para la protección de datos enunciados en el presente capítulo."[39]

En la práctica, varios países han establecido sanciones penales en sus leyes de protección de datos. Un comité de expertos que trabajó en el Consejo de Europa, preparó una lista mínima de acciones que deberán ser consideradas como delito por las legislaciones de sus países miembros. Entre otras situaciones

[37] Ibíd. p. 187
[38] Ibíd. p. 188
[39] Convención para la protección de los individuos en relación al procesamiento automatizado de datos personales.

se señaló penalizar:[40]

- La revelación de secretos personales cometidos por funcionarios públicos, empleados del correo o los tenedores de secretos específicos (personal médico, abogados, empleados de banco) que los hayan obtenido en el curso de una tarea profesional;
- La revelación ilegal u obtención de datos personales almacenados en ordenadores, si estos actos ponen en peligro de alguna manera la privacidad de los registrados o violan el requisito formal de notificación al interesado. [41]

La Unión Europea.

Aunque la Unión Europea ha incursionado desde 1976 en temas relativos a la protección de la privacidad, el gran avance se produjo en 1995 con la sanción de la Directiva Europea en materia de protección de datos[42] y un año después con la sanción de una directiva similar relativa a la protección de datos en redes digitales.

Desde su aparición en el Código noruego, que tipifica la utilización clandestina de medios técnicos con el fin de escuchar conversaciones de terceros en lugares cerrados, conversaciones telefónicas, grabaciones en cintas magnéticas y la instalación de dispositivos para tales fines (artículo 145.a) la legislación penal europea ha receptado estos tipos penales.

Así la Ley de Reforma del Código Penal de Austria de 1965 (párr. 310.d) y

[40] Palazzi Pablo A. Op. Cit. p. 186
[41] Ibíd.. p. 186
[42] Publicado en *Derecho y Nuevas Tecnologías*, Año 1, No. 0, Ad-Hoc, Buenos Aires, 1998.

el Código Penal de 1974; el párrafo 298 ley 22/12/67 *StGB* de la República Federal de Alemania, y el artículo 201 del Código de 1975; el artículo 179 quáter de la ley Suiza 20/12/68 Cp; los artículos 263 y 264 del Código Penal de Dinamarca, texto según ley 24/3/72; la reforma introducida en 1974 al Código Penal Italiano, así como también en los modernos Códigos de Portugal (1982), Francia (1994) y España (1995). [43]

En Francia se contempla el montaje de palabras e imágenes como delito (artículo 370 del Código Penal). Consiste en publicar conscientemente, por cualquier medio, el montaje realizado de palabras o figuras de otro, sin su consentimiento, siempre que no se evidencia la manipulación ni se haga expresa mención de la misma. Se trata de una forma especial de atentado a la privacidad. Consistente en el montaje – fotográfico o auditivo -, y su posterior reproducción dolosa, en un documento que contiene una falsa interpretación del sujeto, con apariencia de verosimilitud.[44]

La privacidad y la protección de datos personales en Internet son temas que la comunidad internacional se ha enfocado a estudiar y analizar con más detenimiento, a raíz de los atentados terroristas del 11 de Septiembre del 2001.

Muchos países, como por ejemplo algunos estados miembros de la Unión Europea, han considerado los temas de privacidad y protección de datos personales como asuntos prioritarios en su agenda legislativa[45], con el propósito

[43] SÁEZ, CAPEL José, *El derecho a la intimidad y las intervenciones telefónicas,* en JA, 22/7/98. p. 23
[44] Ibid, p.34
[45] Ver 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, disponible en la siguiente dirección:

de hacer no sólo un frente comercial común a fuertes bloques comerciales regionales como son el Tratado de Libre Comercio de América del Norte y el MERCOSUR, 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.[46]

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 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 privacidad en relación a la

http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=es&numdoc=31995L0046&model=guichett

[46] Palazzi Pablo A. Op cit. p. 187

obtención y procesamiento de datos personales. [47]

Una de las disposiciones más controvertidas que contiene esta Directiva, es el artículo 25 que establece la prohibición a sus estados miembros de transferir datos personales e información a terceros países que no proporcionen una suficiente y adecuada protección a la privacidad. Aún y cuando algunos países puedan proporcionar o satisfacer un adecuado nivel de seguridad y protección de los datos personales, dicha Directiva impone obligaciones adicionales bastante restrictivas para llevar a cabo la transferencia de datos a terceros países.[48]

Esta Directiva, si bien ha sido adoptada por la mayoría de los países miembros, también ha encontrado algunas dificultades de implementación por parte de algunos otros estados miembros, al no contar con una legislación que contemple la protección a los datos personales. Cabe señalar que en enero de 2000, la Comisión Europea decidió llevar a cabo procedimientos administrativos de sanción en contra de Francia, Alemania, Holanda, Irlanda y Luxemburgo por no haber comunicado a tiempo las medidas que tomaron para implementar esta Directiva en cada una de sus legislaciones internas.[49]

En mayo del 2002, la Comisión Europea elaboró un cuestionario dirigido a los estados miembros con el objeto de poder implementar efectivamente la Directiva. La mayoría de los gobiernos enviaron la primera parte de sus respuestas a la Comisión Europea en junio de 2002. [50]

Recientemente, el Gobierno del Reino Unido envió parte de sus respuestas

[47] SÁEZ, CAPEL José, Op. Cit.. p. 35
[48] Idem.
[49] Idem.
[50] Ibíd. p. 36

a este cuestionario a la Comisión Europea y entre otros puntos propone revisar no sólo algunas reglas para poder implementar esta Directiva en su país debido a la rapidez y cambios que ha habido en los desarrollos tecnológicos, sino sobre todo con el propósito de darle mayor flexibilidad y efectividad a sus organismos de vigilancia, al mismo tiempo que le permita salvaguardar la protección de los datos personales de los ciudadanos ingleses. Entre las propuestas del gobierno inglés se encuentran: (i) revisar las definiciones de "datos personales", "sistema de aplicación de datos personales" y "datos sensibles" con el objeto de mejorarlas y hacerlas más consistentes al momento de ponerlas en práctica; (ii) mejorar las reglas sobre procesamiento de datos personales; (iii) establecer reglas especiales de algunas definiciones como "datos sensibles" para que tengan una aplicación más práctica; (iv) revisar los arreglos de acceso en la materia para encontrar un balance entre los intereses de los sujetos que proporcionan datos personales y los intereses de los organismos controladores de datos, sin reducir la efectiva protección de los datos personales; (v) revisar las reglas relacionadas con la transferencia de datos personales a terceros países y establecer criterios más simples y flexibles.[51]

Recientemente, Finlandia, Suecia y Austria solicitaron cambios a la Directiva con el objeto de remover obstáculos burocráticos costosos e innecesarios.[52]

El artículo 25 de la Directiva sobre Privacidad y Protección de Datos contiene una clara restricción comercial que ha tenido un grave impacto a nivel

[51] Idem.
[52] Ibíd. p. 37

mundial, sin embargo a pesar de ello, muchos países, como es el caso de países latinoamericanos como Argentina, Chile y Paraguay han introducido legislación sobre protección de datos consistente con esta Directiva con el objeto de estrechar sus lazos comerciales y diplomáticos con el continente europeo, sin tomar en cuenta que la prohibición del libre flujo transfronterizo de datos e información podría ocasionarles graves distorsiones comerciales con terceros países, como los Estados Unidos y Canadá, que eventualmente los podrían llevar a tener que substanciar una controversia en el ámbito de la Organización Mundial del Comercio (OMC).[53]

Es por estas razones, que nuestros legisladores tendrán que ser muy cautelosos al tratar de adoptar un esquema de regulación europeo que pudiera inhibir no solamente el comercio transfronterizo de bienes y la prestación de servicios con terceros países, sino particularmente las actividades de comercio electrónico, el flujo transfronterizo de datos personales y las inversiones que se están realizando en México en el sector de las tecnologías de la información y los empleos que estas generan.

España.

El artículo 18.4 de la Constitución Española establece “la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”. Con este objetivo, la Ley Orgánica de Protección de Datos (LOPD) establece el derecho de los ciudadanos a conocer qué datos personales están contenidos en las bases de datos de las

[53] Ibíd. p. 38

empresas y entidades públicas y quienes son los responsables de éstas. Así mismo, establece una serie de obligaciones a los responsables de los tratamientos y una serie de sanciones para el caso de incumplimiento de aquéllas.[54]

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, vigente desde el mes de enero del año 2000, adecuó la legislación española a la normativa establecida por la Unión Europea en este ámbito. Dicha Ley Orgánica aumentó el grado de protección de los datos personales e ideó mecanismos para garantizar a los afectados el ejercicio de sus derechos, principalmente el derecho de acceso y rectificación de los datos facilitados.[55]

Por otro lado se endurecieron las multas por incumplimiento de la legislación, así las sanciones que puede imponer la Agencia a las empresas que incumplan los aspectos de la dicha normativa, pueden llegar hasta 601.012,10 €, en el caso de las infracciones muy graves.[56]

Con la nueva regulación, cualquier fichero automatizado que contenga datos de carácter personal, deberá ser comunicado a la Agencia de Protección de Datos para que esta proceda a su control y posterior registro. Las medidas de seguridad que deberá implantar el titular del fichero, dependerán del tipo de datos que este contenga.

El Real Decreto 994/1999, que desarrolla la Ley Orgánica 15/1999, clasifica los datos de carácter personal en datos de nivel básico, medio o alto, dependiendo de hasta que punto éstos pueden afectar a la intimidad de sus titulares y a la

[54] Palazi Pablo A. Op. Cit. p. 188
[55] Idem.
[56] Ibíd. p. 189

mayor o menor necesidad de garantizar la confidencialidad y la integridad de dichos datos. Así se contempla:[57]

- Nivel básico: Se prevé cuando los ficheros contienen datos personales tales como nombres, apellidos, dirección o teléfonos.
- Nivel medio: se contempla para aquellos casos en que los datos a tratar consisten en datos de servicios financieros, infracciones administrativas, infracciones penales, datos de la Hacienda Pública, o datos de ficheros de solvencia patrimonial o de crédito.
- Nivel alto: se prevé cuando se trata de ficheros que contienen datos de carácter personal referentes a ideología, religión, creencias, afiliación sindical, origen racial o étnico, vida sexual o relativos a la salud.

Portugal

Por lo que a éste país se refiere se cuenta con la Ley número 67/98 del 26 de Octubre de 1998. Esta Ley de protección de datos personales se encuentra dirigida a la Orden Jurídica Portuguesa la Directiva 95/46/CE, del Parlamento Europeo en Consejo, del 24 de octubre, relativa a la protección de las personas y el respecto al tratamiento de datos personales y libre circulación de esos datos.[58]

Estados Unidos.

Estados Unidos cuenta con un marco jurídico bastante amplio en materia de

[57] Agencia de Protección de Datos. "Recomendaciones para la protección de datos personales en Internet", 13 al 15 de abril de 2005. [En línea], Disponible: http://www.agenciaprotecciondatos.org
[58] Palazi Pablo A. Op. Cit. p. 189

privacidad (como ejemplo de ello, podemos citar la Ley de Privacidad de 1974 (Privacy Act of 1974) cuyo objeto es regular la obtención y el uso de la información personal dentro del sector público), 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. [59]

Por otro lado, cabe destacar que la política de regulación de los Estados Unidos ha evolucionado de tal forma que ahora 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 (como por ejemplo el "Health Insurance Portability and Accountability Act de 1996 (HIPPA)" – Ley de Responsabilidad y Movilidad del Seguro de Salud – que es una ley de carácter federal que protege la confidencialidad de los antecedentes y datos médicos de las personas) y la protección y confidencialidad de la información que proporcionen niños menores de edad a sitios en Internet (como lo es el "Children's Online Privacy Protection Act de 1998" – Ley para la Protección de Niños en Línea - cuyo propósito es limitar la obtención, utilización y divulgación de información personal de niños menores

[59] La primera enmienda de la Constitución de los Estados Unidos de América textualmente señala: Amendment I Religious and Political Freedom. Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peacebly to assemble, and to petition the Government for a redress of grievances". (Enmienda I. Libertad política y religiosa. El Congreso no creará ley respectiva de una permanente religión o prohibición del ejercicio libre de la misma; o la privación de la libertad de expresión o de la opresión o la correcta reunión pacífica de las personas y la petición al Gobierno de la reparación de injusticias o agravios).

de 12 años de edad por parte de los operadores de portales y sitios Web que vayan dirigidos a la población infantil).[60]

En este orden de ideas, podemos decir que los Estados Unidos ha adoptado una política mucho más flexible sobre privacidad y protección de datos que la Unión Europea cuyo objetivo es proteger y tutelar los derechos de consumidores, la población vulnerable y más aún que se caracteriza por la adopción de un esquema más liberal para el sector empresarial. Los Estados Unidos han confiado sus políticas de regulación y privacidad a sus empresas por que saben que el gobierno esta consciente de que estas acciones y mecanismos fomentan y reactivan el comercio electrónico no sólo a nivel interno sino también a nivel mundial, promueven las inversiones del sector de las tecnologías de información y sobre todo permite que las pequeñas y medianas empresas puedan realizar actividades de comercio electrónico en todos los niveles.[61]

En el estado de California, en 1992 se adoptó la *Ley de Privacidad* en la que se contemplan los delitos informáticos, pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta ley.[62]

Canadá

Ha seguido políticas de regulación sobre privacidad y protección de datos que se han caracterizado por la adopción de la llamada "Tercera Vía" (The Third Way), es decir, ha tratado de adoptar un marco regulatorio que no sea ni excesivamente sobre regulado por el gobierno ni tampoco que se sea libremente

[60] PALAZZI, Pablo A. op. Cit. p. 188
[61] Ibid p. 188
[62] Ibíd. p. 188

autorregulado por las empresas, sino que combine legislación y políticas de autorregulación eficientes que respondan específicamente a las necesidades individuales de sus nacionales, buscando con ello proteger los derechos de los ciudadanos y consumidores, sin menoscabar los intereses patrimoniales de las medianas y grandes empresas, estableciendo reglas claras y organismos gubernamentales ad-hoc eficientes para su debida vigilancia.[63]

El 13 de Mayo del 2002 el gobierno de la provincia de la Columbia Británica, convocó una consulta pública a fin de crear una Iniciativa de Ley sobre Protección de la Privacidad para el Sector Privado como respuesta a los requerimientos de la Ley Federal denominada "The Personal Information Protection and Electronic Documents Act (PIPED Act – Ley a la protección de la información personal y documentos electrónicos); misma que para el sector privado de la provincia de la Columbia Británica se encuentra vigente y fue el resultado de un consenso con todos los partícipes interesados de esta provincia (empresas, grupos de consumidores, ONG's, órganos de gobierno, académicos y ciudadanos)[64].

IBEROAMÉRICA: ORDENAMIENTOS JURÍDICOS

Por lo que hace a los países de Ibero América, únicamente se señalarán aquéllos que cuenten con legislación respectiva a la protección de datos personales y la ley que la contempla, ello para no extender más lo relativo al punto

[63] Ibíd. p. 189

[64] The Freedom of Information and Protection of Privacy Act de la Provincia de British Columbia (La libertad de información y Protección de la privacidad. Ley de la provincia de la Columbia Británica) se encuentra disponible en la siguiente dirección: http://www.legis.gov.bc.ca/37th3rd/3rd_read/gov07-3.htm

que se trata. Así tenemos:[65]

Argentina.

* Ley 25.326. Ley de Protección de Datos Personales. (Publicada en el Boletín Oficial del 2/11/2000, Núm. 29517).

* Decreto 995/2000. Habeas Data. (Publicado en el Boletín Oficial del 2/11/2000, Núm. 29517.

* Decreto 1558/2001. Protección de Datos Personales (Publicado en el Boletín Oficial del 3/12/2001, Núm. 29787).

Colombia

* Constitución Federal de la República (artículo 15).[66]

Costa Rica

* Proyecto de Ley de Habeas Data. Expediente Núm. 12.827.[67]

Chile

* Ley Núm. 19.628 sobre Protección de la vida privada en lo concerniente a datos personales.- Dicha norma, legalizó el SPAM o envío de Correo Comercial no solicitado, al señalar en su artículo 4o: "No requiere autorización el tratamiento de datos personales que provengan o que se recolecten de fuentes accesibles al

[65] DAVARA RODRÍGUEZ, Miguel Ángel, "Privacidad y Protección de datos personales en Internet" Octubre, 2003, [En Línea] Disponible: http://www.davara.com/, Febrero 2005.

[66] Idem.
[67] Idem

público, cuando... sean necesarios para comunicaciones comerciales de respuesta directa o comercialización o venta directa de bienes o servicios".[68]

En dicha ley se establece el derecho a las personas a la información, modificación, cancelación o bloqueo de sus datos personales, sin embargo no ha considerado un órgano fiscalizador, ha establecido que la información es pública y no privada, y no ha exigido autorización previa para actividades relacionadas con los datos personales y el marketing directo, ni tampoco se prevé lo peligroso del envío indiscriminado de correos electrónicos. Esta ley establece la posibilidad de bloqueo de datos personales, pero el proceso es muy complejo para llevarlo a cabo.[69]

* Decreto Núm. 779/2000. Prueba el Reglamento del Registro de Bancos de Datos Personales a Cargo de Organismos Públicos.[70]

Tratados Internacionales de Chile: [71]

- Pacto de Santo José de Costa Rica, Art. 11 No 2.
- Pacto Internacional de Derechos Civiles y Políticos, adoptado por la Asamblea General de la O. N. U. (1966). Artículo 17.
- Convención Americana de Derechos Humanos (1969). Artículo 11.

Estos tratados se encuentran firmados por Chile y vigentes como Ley de la República.

[68] Idem
[69] Idem
[70] Idem
[71] Idem

Perú

* Ley Núm. 27489. Ley que regula las centrales privadas de información de riesgos y de protección al titular de la información (Promulgada el 27/6/2001, publicada el 28/6/2001).[72]

Uruguay

* Proyecto de Ley - Derecho a la información y acción de habeas data.[73]

3.6 EL DERECHO PROCESAL PENAL Y SUS ALCANCES EN LAS NUEVAS TECNOLOGÍAS.

Las nuevas tecnologías no sólo generan nuevas formas delictivas, sino que también permiten el uso de nuevas formas de combatir el crimen organizado, nuevas herramientas tecnológicas para descubrir la comisión de delitos y tecnologías que ayudan a la prevención o comisión de hechos ilícitos; el uso de estas tecnologías, si bien beneficia a toda la sociedad al facilitar la persecución de crimen, puede en algunos casos plantear problemas relacionados con las garantías constitucionales.

Hablar de nuevas tecnologías de la información es hablar en un término muy genérico, que puede incluir a muy diversos conceptos. Por tecnologías de información se entienden a: “los modernos desarrollos que tienen por objeto el tratamiento de información en forma automatizada, tanto en su recolección, como

[72] Idem
[73] Idem

en su acceso, uso, consulta o difusión"[74].

Enseguida y conforme a lo señalado por Pablo A, Palazzi[75], se reseñarán en forma breve una serie de nuevas herramientas tecnológicas que facilitan la investigación del delito pero que pueden atentar al mismo tiempo en contra de algunos derechos constitucionales (como el derecho a la privacidad) y que llevarán a una reformulación de los mismos:

- Controladores automáticos de peaje, cámaras ocultas o de seguridad, registros de entrada o salida de personas, dispositivos para la recuperación de vehículos robados, métodos de identificación biométrica, y en general cientos de ordenadores que se usan para registrar trámites, pedidos, formularios, fichas y toda clase de datos personales. Las tecnologías encargadas de colectar información personal cada vez están mas difundidas y afincadas en la sociedad. Se calcula que en los Estados Unidos, un ciudadano deja diariamente en registros o bancos de datos un rastro de entre diez y veinte datos con sus actividades normales, la posible reunión de todos estos datos en una sola ficha permite reconstruir la actividad diaria de una persona hasta en sus más mínimos detalles.
- Satélites comerciales privados cuyos servicios pueden colocarse para fotografiar con precisión métrica cualquier sector del planeta. La existencia de estos medios nos da una idea de cuán amenazada se halla la privacidad por esta tecnologías, estos servicios se pueden contratar hasta por Internet y pagar

[74] PALAZZI, Pablo A. op. Cit. P.233
[75] Cfr. PALAZZI, Pablo A. op. Cit. P. 233-240.

con una tarjeta de crédito, estando al alcance de cualquier persona.

- Sistemas de reconocimiento de imágenes para detectar a personas en multitudes como aeropuertos, o en protestas en lugares públicos.
- En el caso de los test genéticos y de ADN, la posibilidad de obtener información a partir de muestras del propio cuerpo y su análisis inmediato presenta una potencialidad discriminatoria y de violación a la privacidad muy alta.
- El control y monitoreo de las estaciones de trabajo, de las comunicaciones (el correo electrónico por ejemplo) es cada vez más común en el ámbito laboral, existiendo incluso un software comercial dedicado a realizar este tipo de vigilancia.
- Comunicaciones telefónicas y móviles, videoconferencias, correo electrónico y chat, casillas de mensajes electrónicos, etc. Cada vez hay más formas de comunicación digitales que facilitan el acceso a estos mensajes por quien conozca la tecnología y sus debilidades.
- El uso de sensores remotos para detectar delitos nos lleva a preguntarnos cuales son los límites de esta tecnología. El increíble desarrollo que en los últimos años han tenido las cámaras y sensores que abundan instalados en infinidad de lugares, desde satélites comerciales hasta estacionamientos, comercios facilitará enormemente la persecución del delito. La sensibilidad de estas tecnologías sugiere que son capaces de captar imágenes fotográficas de cualquier objeto que se encuentre en la tierra, incluyendo con precisión calles, edificios, automóviles. Los nuevos satélites tienen la capacidad de proveer increíbles detalles de cualquier lugar de la tierra

una vez cada tres días, y a un precio tan accesible como cien dólares por milla cuadrada en una determinada área.

Estos son sólo algunos ejemplos de lo que se puede llegar a realizar con el uso de las nuevas tecnologías, toda la información que vamos dejando por la vida puede ser integrada en un perfil de la persona, de sus gustos, de sus comportamientos e intereses. Estas situaciones se presentan así como atentados a ciertos derechos de rango constitucional, sobre todo la privacidad, pero también constituyen beneficios para la sociedad. Para los organismos de investigación del delito, una cantidad importante de información puede recolectarse a través de estas tecnologías y usarse como prueba.

Para los usuarios, la seguridad de no llevar efectivo, la comodidad de los pagos y de los débitos automáticos y de servicios que adivinan nuestros gustos ofreciéndonos catálogos o informaciones en forma automatizada e instantánea son algunas de las ventajas que nos da formar parte de la sociedad de la información.

El precio que hay que pagar en consecuencia, es *perder un poco de privacidad*. En algunos bancos estos sistemas están tan estandarizados que para obtener la privacidad del usuario hay que realizar determinadas acciones para salir del “sistema” que conecta a empresas comerciales lo que deja ver que no estamos tan lejos de perder completamente nuestra privacidad sin que estemos enterados de ello.

CAPITULO 4.

PROPUESTA DEL DELITO CONTRA LA PRIVACIDAD DE LOS DATOS PERSONALES EN INTERNET.

Ahora bien, una vez que se han determinado los conceptos inherentes al presente trabajo de investigación, resulta indispensable hacer un recorrido por la situación actual en que se encuentra México respecto de la protección de los datos personales en la red Internet, que es principalmente el objetivo principal de éste proyecto.

Así pues, se denotará que nuestra legislación penal vigente es relativamente "*nueva"* con respecto a los delitos que pudieran surgir a través de los equipos de informática por medio del Internet, ya que no le proporciona la suficiente importancia al uso indiscriminado de los datos confidenciales que los usuarios de tal medio le proporcionan, tomando en consideración que al entrar a una página de Internet cualesquiera primeramente piden nuestros datos personales como lo son: nombre completo, domicilio, edad, estado civil, ocupación, entre otras.

Lo anterior se realiza sin tomar en cuenta que existen empresas o instituciones que utilizan dicha base de datos para fines comerciales o ilícitos, más aún que en ningún momento se pidió la autorización de alguna persona para poder utilizar los datos que se cree son confidenciales para otros propósitos; se vulnera así la privacidad que ponemos en manos de quien suponemos utiliza nuestros datos únicamente para registro.

Dichos datos pueden ser obtenidos a través del uso de programas espía

enviados a través del propio Internet o bien porque las empresas mismas a quienes les confiamos la información correspondiente se atribuye facultades que en ningún momento les delegamos como son inscribirnos en las denominadas "listas comerciales".

De ahí que afirmo mi propuesta de contemplar un apartado específico para que, en el caso de que al no existir la autorización expresa del uso de datos personales confidenciales, se sancione a quien tenga acceso a la misma así como a la empresa o institución que lo permitió.

4.1 SITUACIÓN JURÍDICA EN MÉXICO RESPECTO A LA PROTECCIÓN DE LOS DATOS PERSONALES.

En México actualmente no existe ninguna ley cibernética que proteja los derechos de los ciudadanos en el campo de la informática y digitalización, por lo que es indispensable impulsar una legislación idónea por la creciente demanda y utilización del Internet y los procesos digitales de información de datos personales.

Esta situación ha sido expuesta por la Diputada Federal, Eloísa Tavera Hernández, en el Primer Congreso Nacional denominado "Cultura de la Legalidad e Informática Jurídica" realizado en la Ciudad de México, organizado por la Secretaria de Gobernación el 29 de octubre del año 2003.[1]

En ese Congreso, la Diputada Tavera estableció que el obligar a las empresas e instituciones a integrar bases de datos compartibles, distribuibles y accesibles resulta ser un elemento central para la competitividad empresarial, sin

[1] Distribuido mediante Boletín 15/03 enviado por Comunicación Social del Partido de Acción Nacional bajo el título "*Legislarán el uso de datos personales en Internet y sistemas informáticos"*, Sección de Política Científica.

embargo se deben de tomar en cuenta tres aspectos centrales a saber:

- La capacidad de los ciudadanos de hacer valer su derecho a la privacidad, a la integridad, veracidad y el manejo de su información personal, siendo una capacidad establecida jurídicamente, lo que hasta la fecha no acontece.
- Los ciudadanos deben de contar con medios reales y efectivos para hacer valer estos derechos, por el hecho de que hay quienes cuentan con acceso informático y otros que por su condición económica carecen de este derecho.
- La responsabilidad jurídica de las empresas y del estado en su función de salvaguardar la información. Cuestión que tiene que ver con el uso responsable de los datos e información.

Lo anterior denota que si bien existe una disposición por parte de Diputados y Senadores para una legislación para la protección de datos personales, en la actualidad se carece de ella, a pesar de que un aproximado de 17 millones de mexicanos son usuarios de Internet y el país carece de mecanismos para proteger la privacidad de los ciudadanos.

En México no tenemos protección para la defensa del tráfico con datos personales, porque las leyes no permiten a los propietarios de esos datos tener control sobre quienes los almacenan por distintos motivos, ya sean instituciones financieras, hospitales públicos o privados, negocios y otros; por lo que debido a que esa información circula de manera profusa en Internet, los riesgos pueden ser

varios, desde que un expediente médico sea visto por una aseguradora y provoque desventajas ante esa compañía, hasta que información delicada sobre funcionarios públicos como sus ingresos, domicilios, familia y fotografías, puedan ser usada para intentar un secuestro.

Si bien en la actualidad existen leyes que sancionan a las personas que obtienen de forma engañosa la información, como en el caso de los correos electrónicos que presuntamente llegan de un banco y piden nuevamente los datos personales, cuando en realidad se trata de defraudadores, también lo es que no existe ley alguna que explícitamente ofrezca alguna protección a la circulación de los datos de todos y cada uno de los usuarios por Internet, por parte de los bancos y empresas comerciales sin el consentimiento del ciudadano.

4.2 LEGISLACIÓN MEXICANA.

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos representa el marco jurídico de la privacidad en nuestro país, no obstante lo anterior, falta precisar cabalmente el texto, en el que específicamente, se establezca y consagre la protección jurídica de los datos personales.

Es de hacer notar que para la realización de los apartados correspondientes a la Ley de Protección de datos personales de algunos estados, así como de la Ley Federal atiendo a lo señalado en las conferencias realizadas en el "IV Encuentro Iberoamericano de Protección de Datos Personales", organizado por el Instituto Federal de Acceso a la Información Pública, celebrado del 4 de noviembre del año 2005, en la mesa denominada *"La protección de los datos personales en los Estados de la República Mexicana"* con sede en la Universidad Anáhuac,

Campus Norte, Auditorio de Rectoría, a cargo de la Doctora María Marván Laborde, Comisionada Presidenta del Insittuto Federal de Acceso a la Información Pública, IFAI México, Licenciada Ramona Carvajal Cárdenas, Comisionada Presidenta de la Comisión Estatal para el Acceso a la Información Pública del Estado de Colima, Maestro Alfonso Villarreal Barrea, Consejero del Instituto Coahuilense de Acceso a la Información Pública, Maestra María Pérez Cepeda, Comisionada Presidenta de la Comisión Estatal de Información Gubernamental de Querétaro, Doctor Carlos Paniagua Bocanegra, Consejero del Instituto de Transparencia y Acceso a la Información Pública del Estado de México y del Maestro Vicente Hernández Delgado, Comisionado de la Comisión Estatal para el Acceso a la Información Pública del Estado de Sinaloa.

Dentro de las normas federales en las cuales existe algún derecho o principio de *Habeas Data*, encontramos:

- Ley Federal de Acceso a la Información Pública.

Publicada el 11 de junio del año 2002, en esta ley se contempla el derecho de los ciudadanos para la protección de sus datos personales, evitar que se difundan, se transmitan o se comercialicen sin su consentimiento, pero únicamente de aquellos datos personales que obran en poder del Estado, sin que dicha protección trascienda al sector privado.

En este sentido, el Instituto Federal de Acceso a la Información Pública (IFAI), se encarga de la protección de los datos personales en posesión de la Administración Pública Federal, existiendo en el sitio de Internet del propio Instituto, un listado de los sistemas de datos personales que están en el gobierno,

como en caso de la Secretaria de Hacienda que posee una gran base de los datos de todos los contribuyentes de México, información que se encuentra a disposición del público para el efecto de que ejerza el derecho de acceso y corrección.[2]

La Ley Federal de Acceso a la información Pública en su artículo 37, obliga a todos los sujetos obligados de la ley, no sólo al Poder Ejecutivo Federal, sino también por ejemplo al Congreso, a expedir lineamientos en materia de mantenimiento, seguridad en bases de datos y protección de ellos en general; detalla los principios de protección, que son la calidad de los datos, que deben ser actualizados, exactos, no excesivos a los propósitos a los cuales se recabaron, las medidas de seguridad con que debe contar el sistema; se regula con respecto a la parte técnica, quiénes tienen acceso a la base de datos, quién es el responsable, el encargado, los usuarios que tienen que acceder a éstos para el ejercicio de sus funciones, cuáles son las bitácoras, llaves de acceso, lo cual lo convierte en un documento más técnico, estableciendo las bases y los transitorios para que las dependencias cumplan con todo lo que la Ley Federal de Acceso a la información Pública en su capítulo de protección de datos establece; por otra parte obligan a las dependencias y entidades de la administración pública federal, a informarle a las personas, desde el momento en que recaban su información, para que fines se van a utilizar y se les da un plazo para que cambien su formato.

Se hace referencia también a lo que se denomina Autodeterminación Informativa, que implica que una persona tiene el derecho a saber quién, cuándo y bajo que circunstancias está utilizando sus datos.[3]

[2] Para mayor información visítese www.ifai.gob.mx
[3] Ley Federal de Acceso a la información Pública

La Ley Federal de Acceso a la información Pública tiene un capítulo de protección de datos personales, pero es, en general, muy abstracto, ante lo cual se detallan ciertos lineamientos para establecer los responsables del manejo de sistemas de datos personales, a los encargados y al usuario; define lo que es la transmisión de los datos, en que casos se pueden transmitir, esto en el ámbito del Gobierno Federal y define los principios de protección de datos, ya al final existe un capítulo de medidas de seguridad de informática y unos transitorios amplios para que las dependencias puedan cumplir.

Hay 23 estados de la República que ya tienen su propia Ley de Acceso a la Información en donde cuentan con un capítulo sobre protección de datos personales en posesión de los gobiernos, estatales o municipales, como lo son por ejemplo, el estado de Colima, Coahuila, Distrito Federal, Estado de México, Sinaloa, Jalisco, entre otros.

- Ley de Protección de datos personales del Estado de Colima.

Vigente a partir del 22 de junio de 2003, esta ley contiene objetivos similares a los que se determinan para el “habeas data” como son que el ciudadano tiene derecho a conocer de su inclusión en los bancos de datos o registros; tener acceso a la información que sobre él conste en los bancos de datos o registros, actualizar o corregir en su caso, la información que obre en dichos bancos, y lo más importante es que tiene derecho a conocer los fines para los que se va a utilizar esa información.

Garantiza la confidencialidad de determinada información obtenida legalmente, para evitar el conocimiento de terceras personas, así como se

garantiza la supresión de la información que se encuentre en poder de terceros y que se refiera a cuestiones personales. Estos derechos tienden a proteger el derecho a la privacidad del individuo, derivado del mandato consignado en la fracción VI del artículo 1º de la Constitución del Estado de Colima, el cual establece que las autoridades del estado velarán por la defensa de los derechos humanos e instituirán los medios adecuados para su salvaguarda.[4]

La ley consta de 23 artículos en seis capítulos. El primer capítulo trata del tema de las disposiciones generales; el segundo habla de los datos personales; el tercero trata de la creación y protección de dichos datos, el cuarto se dedica al tema de los archivos, el quinto capítulo, de la Comisión de Acceso a la Información Pública que es la encargada de tutelar la Ley de Protección de Datos Personales; en tanto que el sexto capítulo se refiere a las infracciones y a las sanciones. En un primer plano se precisa que la ley será aplicable dentro del estado de Colima a los datos de carácter personal, que serán registrados en los sectores tanto **público como privado** en cualquier soporte físico que nos permita el tratamiento de los datos.

El artículo 4º de la propia Ley establece los principios bajo los cuales deberán manejarse los datos personales, entre los que se destacan:

- Sólo podrán obtenerse y ser sujetos de tratamiento cuando sean adecuados, pertinentes y no excesivos;
- Que deben usarse esos datos expresamente para los fines que fueron obtenidos y que deben ser correctos y actualizados,
- Deberán obtenerse por medios lícitos siendo necesario el consentimiento

[4] Ley de Protección de datos personales del Estado de Colima

del interesado, quien debe estar informado de su existencia y fin del archivo

- No podrán proporcionarse datos personales a terceros.

De ahí que hasta ahora solamente el Estado de Colima cuenta con la legislación específica para proteger a las personas del uso indebido de sus datos personales, tanto en el sector público como privado.

- El **Estado de Guanajuato** es el único que cuenta con una ley de protección de datos personales independiente a la Ley de Transparencia y Acceso a la información, la cual fue publicada en el Periódico Oficial el 19 de mayo de 2006 denominada “Ley de Protección de Datos Personales para el Estado y los Municipios de Guanajuato”, se compone de 23 artículos y entró en vigor el 23 de mayo del mismo año, esta ley es aplicable para el sector público y considera como sujetos obligados al Poder Legislativo, al Poder Ejecutivo, al Poder Judicial, los ayuntamientos, los organismos autónomos y cualquier otra dependencia o entidades estatal o municipal.

- En el **Estado de Coahuila** desde octubre de 2003 se envió a su Congreso un paquete de cuatro anteproyectos de ley en relación a la transparencia. El primero fue de acceso a la información, el segundo de archivos públicos, el tercero fue la creación al Instituto Coahuilense de Acceso a la Información Pública y finalmente, el proyecto de ley de la Iniciativa de “Ley a la Protección a la Intimidad de las Personas”. Las tres primeras fueron aprobadas en el pleno del Congreso, quedando pendiente de aprobación la ultima señalada.

Este proyecto de ley contempla garantizar el derecho a la intimidad de las personas y el derecho de la protección de los datos personales, a partir de los principios de la calidad de los datos, la transparencia o la publicidad del tratamiento, el consentimiento informado, la seguridad de los datos, la interpretación constitucional más favorable, la libre circulación de los datos con fines lícitos y considera el galantismo de los datos en poder de las entidades públicas y de los particulares; se consideró como poder autónomo de las personas, con la posibilidad de que estas personas definieran libremente que actividades o que aspectos formaban parte de su círculo íntimo, personal o familiar. Asimismo se determina los derechos de ciertos grupos en torno a una relación jurídica con el estado u otros particulares pretendiendo establecer como un interés público y social la protección a la intimidad de éstos grupos como lo son los niños, las mujeres, la juventud, los adultos mayores, las personas con preferencias sexuales diferentes y las personas con capacidades diferentes, a estos grupos se les reconoce como grupos vulnerables y en ese sentido gozan de una tutela preferente en la medida que su derecho a la intimidad resultara restringido o afectado por la discriminación. En este aspecto, establece las bases para la prohibición de afectar la esencia al derecho a la intimidad, esto es, ninguna persona podría ser obligada a declarar sobre ideología, religión, cuestiones de honor, creencias o preferencias o algunos otros datos personales que afectaran sensiblemente su dignidad. [5]

De forma relevante, destaca lo relacionado a que los inculpados no podrán ser sometidos a ninguna prueba que pudiera afectar su intimidad y en caso de

[5] Ley de Acceso a la información del Estado de Coahuila

hacerlo tendrá que existir el consentimiento expreso. Se considera que la comunicación entre el inculpado y su defensor es algo privado e inviolable y que los centros penitenciarios deberán tener un lugar para asegurar este derecho. Ante la violación de los datos personales y la intimidad de las personas toda diligencia o prueba carecerá de valor probatorio.

De esta manera establece que la vida privada y la vida familiar son inviolables en los términos de la ley. Se establece que la protección de los datos personales son una garantía individual de interés legítimo, que genera información que es irrenunciable, intransferible, no negociable e indelegable.

Establece el sistema garantista de la acción con dos herramientas jurídicas que son la acción para exigir proteger el dato personal y la otra que era el juicio para la protección del derecho a la intimidad.

Por disposición constitucional, el Instituto Coahuilense de Acceso a la Información es el garante de la protección de los datos personales, sin embargo al carecer del marco jurídico para poder tener las funciones que la iniciativa propone representa inseguridad jurídica para las entidades públicas y privadas en el manejo de los datos, así como para las personas físicas que se pudieran ver afectadas en su vida privada, familiar, integridad física, genética, moral, entre otras.

- En la Constitución del **Estado de México** y específicamente en el artículo 5º párrafos segundo y tercero establece que el Estado garantizará el derecho a la información, garantizará la protección de los datos personales y la transparencia de la función pública.

Esta modificación de la constitución estatal se dio el 30 de abril del año 2004 y entró en vigor el 1º de agosto del mismo año, dando origen a la Ley de Transparencia y Acceso a la Información Pública del Estado de México, misma que crea el Instituto de Transparencia de Acceso a la Información Pública como organismo público descentralizado, no sectorizado en reforma publicada en diciembre de 2004.

Esta ley en su artículo 1º establece que es reglamentaria de los párrafos segundo y tercero del citado artículo 5 Constitucional, garantizando el derecho de acceso a la información y protege los datos personales, estableciendo en su artículo 2º fracción II como dato personal la información concerniente a una persona física identificada o identificable, como lo establece la Ley Federal. Los artículos 25 fracción I y 55 fracción I de la ley estatal establecen que: El dato personal es una información confidencial; no puede divulgarse si afecta a la privacidad de las personas.

- En el **Estado de Sinaloa** también se tiene su respectiva Ley de Acceso a la Información Pública, asimismo existe un proyecto de "Ley de protección de datos personales" que se presentó al Congreso en junio de 2003, sin que haya sido aprobada en la actualidad. Contempla la figura del "habeas data" en la legislación federal de acceso a la información donde se establece un capítulo referente a la protección de datos personales y además contempla un reglamento que regula el tema.

- En el **Estado de Jalisco** se aprobaron una serie de reformas que

específicamente consistieron en insertar dentro del Código Civil, una Ley de Protección de Datos Personales que consta de 39 artículos, en los cuales se tratan diferentes materias, inclusive, el manejo de la información crediticia.

Asimismo, para respaldo de la información siguiente, atiendo a lo señalado en las conferencias realizadas en el "IV Encuentro Iberoamericano de Protección de Datos Personales", organizado por el Instituto Federal de Acceso a la Información Pública, celebrado del 3 de noviembre del año 2005, en la mesa denominada *"Protección de datos personales por los Gobiernos"* con sede en el Salón "Don Alberto", del hotel Sheraton Alameda del Distirto Federal, a cargo del Licenciado Carlos Arce Macías, entonces Procurador Federal del Consumidor, Doctora Guillermina González Durán, entonces Directora de Estándares y Nomenclaturas en la Dirección General de Coordinación de los Sistemas Nacionales, Estadísticos y de Información Geográfica del INEGI, Doctor Andrés Albo Márquez, entonces Consejero electoral del Instituto Federal Electoral, Licenciado Andrés Calero Aguilar, entonces Tercer Visitador General de la Comisión Nacional de Derechos Humanos, Doctor Fernando Martínez Coss, entonces responsable del proyecto de Firma Electrónica Avanzada y Factura Electrónica Administrador Central de la Operación para la Asistencia al Contribuyente al Servicio de la Administración Tributaria de la Secretaria de Hacienda y Crédito Público, así se tiene que:

- Ley Federal de Protección al Consumidor, reformada y adicionada por decreto publicado el 29 de mayo de 2001, en su artículo 76 BIS fracciones I y II

establece que el proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o trasmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente; y que el proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos, asimismo protege al consumidor ya que establece disposiciones específicas sobre comercio electrónico en temas como la confidencialidad y seguridad de la información del consumidor, así como los datos que el vendedor debe proporcionar antes de celebrar cualquier transacción, no obstante lo anterior, no establece alguna sanción en caso de incumplimiento a lo anterior aunado al hecho de que esta ley solo es aplicable en las operaciones realizadas en territorio mexicano.

PROFECO es un organismo descentralizado de servicio social, tiene personalidad y patrimonios propios, desarrolla funciones de autoridad administrativa relativas a proteger y promover los derechos de los consumidores, procurar la equidad y la seguridad jurídica en la relación entre proveedores y consumidores, tramitan anualmente cerca de 150 mil quejas de este tipo.

Al ser las compras por Internet una práctica cada vez más común entre los mexicanos, debido al comercio electrónico al representar una alternativa de compra sin necesidad de desplazarse físicamente a una tienda para adquirir bienes como ropa, libros, enseres domésticos, programas de cómputo o servicios de entretenimiento. Por ello, la Procuraduría Federal del Consumidor (PROFECO)

publicó un artículo en la Revista del Consumidor de Junio de 2004, donde ofrece recomendaciones para que los cibernautas no corran riesgos al momento de realizar alguna compra en línea.[6]

La página de PROFECO,[7] contiene una sección de consumo informado, con énfasis en el comercio electrónico y en el spam, áreas en las que los datos personales de los consumidores pueden ser fácilmente vulnerados, son explicados precisamente ahí; las alertas que expone continuamente PROFECO son otro mecanismo que busca ayudar a la población para cuidar entre otras cosas, sus datos personales.

El artículo 76 bis se incluyó dentro del Capítulo VIII BIS de la Ley Federal de Protección al Consumidor, tomando en cuenta los Lineamientos para la Protección al Consumidor en el Contexto del Comercio Electrónico de la Organización para la Cooperación y el Desarrollo Económico (OCDE).[8]

- **Ley de Información Estadística y Geografía,** (norma rectora del Instituto Nacional de Estadística, Geografía e Informática), publicada en el Diario Oficial de la Federación el 30 de diciembre de 1980, en cuyo articulado establece que son considerados como informantes las personas físicas y morales cuando les sean solicitados sus datos estadísticos y geográficos por las autoridades competentes; que los datos que se proporcionen con fines estadísticos serán manejados, para efectos de esta ley, bajo la observancia de los principios de confidencialidad y

[6] Esta información es visible en la página de PROFECO: ucs@profeco.gob.mx
[7] www.profeco.gob.mx
[8] Estos lineamientos se encuentran disponibles en su versión en español en la página de la OCDE en la siguiente dirección: **http://www.oecd.org/EN/document/0,,EN-document-44-1-no-24-320-44,00.html**

reserva y no podrán comunicarse, en ningún caso, en forma nominativa o individualizada, ni harán prueba ante autoridad administrativa o fiscal, ni en juicio o fuera de él; que la información estadística, sólo podrá proporcionarse a particulares, organismos o gobiernos extranjeros por conducto de la desaparecida Secretaria de Programación y Presupuesto (cuyas funciones fueron atraídas por la actual Secretaria de Hacienda y Crédito Público) o de las unidades que formen parte de los servicios nacionales, que hubieran sido autorizados por aquella, salvo la que en cumplimiento de otras disposiciones legales no pueda proporcionarse. Contiene un apartado de infracciones que pueden ser imputables a servidores públicos, recolectores o censores que violen la confidencialidad de los datos que obtienen para los fines estadísticos.

Por su parte, el Reglamento de la Ley de Información Estadística establece los conceptos de dato estadístico confidencial y lo define como los informes cualitativos y cuantitativos proporcionados por los informantes, para fines estadísticos referidos a una unidad de observación.

Desde el punto de vista del uso de las tecnologías de la información, el INEGI tiene un programa integral de seguridad que contempla un sistema de prevención contra ataques internos y externos a la red. Esto es, a través de antivirus, antispam o el faile Web, con eso se resguarda y se protege la integridad de la información que es contenida en bases de datos en las cuales se va integrando aquella información que finalmente va a tener un destino de

información estadística o geográfica.[9]

- El **Instituto Federal Electoral** se encuentra a cargo del padrón electoral y de los datos personales vinculados a la actividad de los partidos políticos, esto es, se habla de un banco de datos con información como nombre, sexo, edad, domicilio, clave de elector entre otros, acumulando más de 75 millones de empadronados. Por la importancia del padrón electoral, su protección y trámite se regula conforme a lo dispuesto por el Código Federal de Instituciones y Procedimientos Electorales (COFIPE), así como en el Reglamento de Transparencia en Materia de datos electorales.

Una de las características que define el Código Federal de Instituciones y Procedimientos Electorales es que los partidos, integrantes de los consejos a nivel general, local y distrital, así como los miembros de las llamadas Comisiones de Vigilancia que son órganos creados ex profesos para vigilar la conformación y veracidad del banco de datos, tienen acceso irrestricto a todos los datos que conforman el padrón electoral y la lista nominal para efectos de control y revisión. Por otra parte, el acceso a la base de datos se encuentra totalmente restringido para aquellos funcionarios que no tengan vinculación con su manejo.

El Registro Federal de Electores cuenta con una plataforma tecnológica que registra electrónicamente cualquier consulta realizada por funcionarios o personal acreditado para efectos de cualquier control, lo que se supone, asegura que en el caso de un mal manejo de dicha información implicaría, entre otras cosas, una

[9] Esta información se encuentra disponible para todo público en la Sección de Transparencia del INEGI, en Internet, bajo el nombre de “Listado de Sistemas de Datos Personales del INEGI” en la página: www.inegi.gob.mx

posible responsabilidad administrativa.

Asimismo el Registro Federal de Electores se encuentra obligado a proporcionar información confidencial en juicios, recursos o procedimientos en que el IFE fuere parte, o bien por un mandato de lo que la ley señala, como juez competente, relativos al Poder Judicial y a las autoridades administrativas, que estén tramitando asuntos de orden legal y se excluye a los Ministerios Públicos locales, federales o a los tribunales administrativos.

- La **Comisión Nacional de los Derechos Humanos** en su carácter de órgano constitucional autónomo y por lo tanto sujeto obligado de las disposiciones de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental ha realizado una serie de acciones en materia de acceso a la información y protección de datos personales, como la realización del Proyecto de Normatividad en el que se establecen los órganos, criterios y procedimientos institucionales para proporcionar a particulares el acceso tanto a los datos personales, como a la información en posesión del ombudsman nacional.

Una vez elaborado dicho proyecto, el Consejo Consultivo de la Comisión Nacional de Derechos Humanos en su sesión ordinaria número 174, celebrada el 8 de abril de 2003, emitió el Reglamento de Transparencia y Acceso a la Información de la Comisión Nacional de Derechos Humanos, mismo que fue publicado en el Diario Oficial de la Federación el 29 de abril de 2003.

El título tercero de este reglamento se refiere a la protección de datos personales, y dentro de las disposiciones más importantes se encuentran las siguientes: sólo los titulares de los datos o sus representantes podrán, previa

acreditación, solicitar a la Unidad de Enlace se les proporcionen los datos que obran en un sistema de datos personales, dicha unidad deberá entregarle al solicitante en un plazo de 10 días hábiles contados desde la fecha en que se presentó la solicitud, la información o bien la respuesta que al respecto remite el área responsable, asimismo se podrá solicitar su modificación que obren en cualquier sistema de datos personales, y para éste caso la Unidad tiene un plazo de 30 días hábiles para comprobar que el área responsable hizo las modificaciones o bien se presente el informe fundado y motivado de las razones por las cuales no procedió lo solicitado, contra la negativa de entrega o modificación de los datos, procede el recurso de revisión al que se refiere el propio reglamento de ésta Comisión.

Con el objeto de informar sobre las políticas de la Comisión Nacional de Derechos Humanos en relación con la protección de datos personales, el 30 de septiembre de 2003 el Consejo Consultivo emitió el acuerdo 7/2003 en el cual se establece que las personas que entreguen información y datos personales a la misma, se les comunicará que la información que proporcionen podrá ser suministrada a un tercero que lo solicite, después de un lapso de 12 años, contados a partir de la fecha en que se resuelve el asunto respectivo. Se establece que el acceso a la base de datos está limitado a un determinado número de funcionarios, quienes en su mayoría lo hacen en la modalidad de consulta, mientras que los responsables de ingresar información o bien realizar modificaciones en caso de que sea necesario, están plenamente identificados. La confidencialidad de la información o documentación relativa a los asuntos de su competencia se encuentra establecida en el artículo 4 de la Ley de la Comisión

Nacional de los Derechos Humanos. Por otra parte señala que desde el año de 1990 se ha ocupado a la seguridad de la información contenida en los distintos sistemas que conforman sus bases de datos, la calve incluye datos personales de los quejosos, agraviados, incluso de presuntos responsables o responsables de las violaciones a derechos humanos. [10]

- Ley Federal del Derecho de Autor. En específico se refiere a la reproducción no autorizada de programas informáticos, regulada en el artículo 11 que establece el reconocimiento del Estado al creador de obras literarias o artísticas, entre las que están los programas de cómputo. La reproducción queda protegida a favor del autor y se prohíbe la fabricación o uso de sistemas o productos destinados a eliminar la protección de los programas.

Asimismo hace alusión al uso no autorizado de programas y de datos; en sus artículos 107 al 110 protege como compilaciones a las bases de datos legibles por medio de máquinas que por razones de disposición de su contenido constituyan obras intelectuales, otorgándole a su organizador el uso exclusivo por cinco años; asimismo, exceptuando las investigaciones de autoridades conforme a los procedimientos respectivos, la información privada de las personas contenidas en bases de datos no podrá ser divulgada, transmitida ni reproducida salvo con el consentimiento de la persona de que se trate.

- Existe también regulación pobre en cuanto a protección jurídica de datos

[10] La página de Internet de ésta Institución para su consulta se encuentra en la dirección www.cndh.org.mx

personales en las llamadas **Sociedades de Información Crediticia**, sociedades particulares cuyo objeto fundamental es el proporcionar información actualizada y veraz sobre la experiencia o comportamiento crediticio de personas físicas y/o morales.

Las reglas aplicables según la información tomada del sitio en Internet de una de estas sociedades [11] son los apartados a y b del artículo 33 de la Ley para Regular a las Agrupaciones Financieras, así como las Reglas Generales para Regular a las Sociedades de Información Crediticia. Cabe mencionar que ninguna de estas disposiciones establece a favor del particular persona física o moral, derecho alguno sobre la posibilidad de que el particular mismo pueda solicitar a la Sociedad de Información Crediticia la rectificación de sus datos personales, que pueda prohibir la interconexión de archivos, el derecho de exigir la cancelación del registro, y cómo única protección a la persona física o moral, establecen que quien solicite información sobre ellos a las Sociedades de Información Crediticia, deberán contar con una autorización por escrito y firmada por el individuo en cuestión.

En el cuerpo de la ley de las Instituciones de Crédito y la Ley del Mercado de Valores, se regula el uso de medios electrónicos para la realización de sus operaciones.

- Entre los servicios que ofrece el **Servicio de Administración Tributaria (SAT)** se encuentra el denominado de Firma Electrónica Avanzada, que resulta

[11] Marzo, 2007, [En Línea] Disponible: http://www.buródecredito.com.mx

ser un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad, sin modificación posterior, del mensaje original, esto es, los datos proporcionados por el contribuyente que permitan acreditar fehacientemente su identidad; esta firma desde al año 1994 se determinó como una obligación de las personas físicas y morales de contar con un certificado de firma electrónica avanzada, básicamente cuenta con dos segmentos de contribuyentes obligados que son personas físicas con actividad empresarial, con ingresos superiores a un millón setecientos cincuenta mil pesos, y un segundo segmento de personas físicas como actividad no empresarial, con ingresos superiores anuales a trescientos mil pesos.

El Servicio de Administración Tributaria tiene la reserva legal de no entregar ni revelar los datos de identidad proporcionados por los contribuyentes conforme a lo estipulado por el artículo 69 del Código Fiscal de la Federación, en donde se guarda absoluta reserva de los datos, no obstante lo anterior, los contribuyentes pueden tener acceso mediante la página del servicio de administración tributaria, proporcionando su Registro Federal de Contribuyentes, contraseña, certificado y punto key y llave privada (que son claves de seguridad que les son asignados al momento de darse de alta ante el SAT).

- **El Código de Comercio** a partir del año 2003 reconoce expresamente la contratación electrónica, regulando la creación de entidades certificadoras para asegurar la autenticidad de mensajes de datos y firma electrónica.

El Código Civil Federal y algunos Estatales, regulan como consentimiento expreso el manifestado por medios electrónicos y equiparan la oferta hecha entre

presentes a la realizada por estos medios.

- Código Penal Federal

En el artículo 167 Fracción VI establece la intervención del correo electrónico, al sancionar con pena privativa de libertad de uno a cinco años y de cien a diez mil días multa, al que dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones alámbricas, inalámbricas o de fibra óptica, sean telegráficas, telefónica o satelitales, por medio de las cuales se transfieran señales de audio, de video o de datos. Tipifica de esta manera el interceptar un correo antes de que llegue a su destinatario, pero no el abrir el buzón o los correos una vez recibidos, esto es, sólo por los datos que las personas envían a través de la red.

Establece en sus artículos 211 bis 1 a 211 bis 7 diversas disposiciones relativas a la protección de datos en general contenidos en sistemas o equipos de informática del Estado o del sistema financiero; a saber:

> Artículo 211 BIS 1. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.
>
> Al que sin autorización conozca o copia información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de 3 meses a 1 año de prisión y de 50 a 150 días multa.
>
> Artículo 211 BIS 2. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de 1 a 4 años de prisión y de 200 a 600 días multa.
>
> Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad se le impondrán de seis meses a dos años de prisión y de 100 a 300 días multa.

Artículo 211 BIS 3. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de 2 a 8 años de prisión y de 300 a 900 días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan se le impondrán de 1 a 4 años de prisión y de 150 a 450 días multa.

Artículo 211 BIS 4. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de 6 meses a 4 años de prisión y de 100 a 600 días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contenga, se le impondrán de 6 meses a 4 años de prisión y de 100 a 600 días multa.

Artículo 211 BIS 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contenga, se le impondrán de 6 meses a 4 años de prisión y de 50 a 300 días multa.

Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de 3 meses a 2 años de prisión y de 50 a 300 días multa.

Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integren el sistema financiero.

Artículo 211 BIS 6. Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 de este Código.

Artículo 211 BIS 7. Las penas previstas en este Capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno.

Integrándose el sistema financiero, conforme al artículo 400 bis séptimo párrafo del Código Penal Federal por las instituciones de crédito, de seguros y de

fianzas, almacenes generales de depósito, arrendadoras financieras, sociedades de ahorro y préstamo, sociedades financieras de objeto limitado, uniones de crédito, empresas de factoraje financiero, casas de bolsa y otros intermediarios bursátiles, casas de cambio, administradoras de fondo de retiro y cualquier otro intermediario financiero o cambiario.

Denotándose de esta forma que por lo que hace al Código en estudio no se prevé conducta y sanción alguna para el que haga uso indebido de los datos personales que se encuentran en registros de Internet o por particulares.

- Código Penal para el Distrito Federal

Por lo que se refiere a éste Código, en relación al uso de la computadora y la manipulación que éstas contienen, se encuentra el artículo 231 Fracción XIV relativo al delito de FRAUDE en donde se establece que se le impondrán las penas previstas en el artículo 230 (específicas para el delito Fraude genérico), a quien:

> "Para obtener algún beneficio para sí o para un tercero, por cualquier medio accese, entre o se introduzca a los sistemas o programas de informática del sistema financiero e indebidamente realice operaciones, transferencias o movimientos de dinero o valores independientemente de que los recursos no salgan de la institución..."

Asimismo en los Capítulos III y IV se hace referencia a la violación de la correspondencia y de la comunicación privada en los artículos 333 y 334 respectivamente que a la letra disponen:

> VIOLACIÓN DE CORRESPONDENCIA.
> Artículo 333. Al que abra o intercepte una comunicación escrita que no esté dirigida a él, se le impondrá de treinta a noventa días multa.

> No se sancionará a quien en ejercicio de la patria potestad, tutela o custodia, abra o intercepte la comunicación escrita dirigida a la persona que se halle bajo su patria potestad, tutela o custodia.
>
> VIOLACIÓN DE LA COMUNICACIÓN PRIVADA
> Artículo 334. A quien intervenga *comunicaciones privadas* sin mandato de autoridad judicial competente, se le impondrán de dos a ocho años de prisión y de cien a mil días multa.
> A quien revele, divulgue utilice indebidamente, o en perjuicio de otro, *información* o imágenes obtenidas en una intervención de *comunicación privada*, se le impondrán de tres a doce años de prisión y de doscientos a mil días multa.

Del análisis de los ordenamientos antes referidos se advierte que ninguna de estas disposiciones hace referencia a la protección de los datos personales como tales, en su aspecto de garantía de privacidad como se ha determinado en el cuerpo del presente estudio.

Así tenemos que en nuestro país, la privacidad y los datos de las personas en las relaciones entre empresas y consumidores, se encuentra regulada en diversas disposiciones sobre privacidad a nivel federal. Sin embargo, en la medida en la que se extienda la penetración y el uso de Internet, se deberá evaluar la posibilidad de crear un marco jurídico más amplio y eficiente que proteja los datos y la información proporcionada por los ciudadanos no sólo a los sitios Web de las empresas comerciales, sino sobre todo a los órganos gubernamentales cuyos servicios y trámites se ofrecerán también en línea en un futuro cercano.

También resulta conveniente que, en sectores altamente sensibles en donde la confidencialidad de la información de las personas es considerada primordial, como son el sector salud, bancario y laboral, se contemple la posibilidad de incluir aspectos puntuales sobre privacidad y protección de datos personales en el ámbito de sus respectivas leyes, reglamentos y ordenamientos.

4.3 INICIATIVAS DE LEY

El Congreso mexicano está llevando a cabo la revisión del Proyecto de Ley Federal de Protección de Datos Personales. Cabe precisar que a la fecha se han expedido tres proyectos de Ley de Protección de Datos Personales, a saber:

1. Proyecto de Ley Federal de Protección de Datos Personales, presentado por el Senador Antonio García Torres del Partido Revolucionario institucional (PRI), ante el Senado de la República del 14 de febrero de 2001;
2. Proyecto de Ley de Protección de Datos Personales presentada por el Diputado Miguel Barbosa Huerta, del grupo parlamentario del Partido de la Revolución Democrática (PRD) en sesión de la Cámara de Diputados, del día 6 de septiembre de 2001 y,
3. Proyecto de la Ley Federal de Protección de Datos Personales presentada ante la Cámara de Diputados por el Diputado Jesús Martínez Álvarez del Grupo Parlamentario de Convergencia en sesión del 1º de diciembre de 2005.

1) Así se observa que la primera Iniciativa es la presentada por el **Senador Antonio García Torres**, del grupo parlamentario del Partido Revolucionario Institucional, en la sesión de la Comisión Permanente del miércoles 14 de febrero de 2001, que fue dictaminada por las comisiones unidas de Puntos Constitucionales y de Estudios Legislativos de la Cámara de Senadores, y fue

firmada por los senadores Manuel Bartlett Díaz en su carácter de Presidente de la Comisión de Puntos Constitucionales y el Senador Fidel Herrera Beltrán en su carácter de Presidente de la Comisión de Estudios Legislativos. [12]

Al igual que la Iniciativa de Decreto que expide la Ley Federal de Protección de Datos Personales, ésta no cuenta con el aval y visto bueno de la sociedad, además de que tiene un serio problema de inconstitucionalidad por haberse originado directamente en la Cámara de Senadores.

El objetivo principal de esta iniciativa es reglamentar las bases a las que estarán sujetas las personas y empresas propietarias de archivos y bases de datos, y guardar el equilibrio entre sus derechos de uso, comercialización o transferencia respecto de su titularidad y los derechos de privacidad de los individuos.[13]

El proyecto de la Ley Federal de Protección de Datos Personales fue aprobado y publicado en la Gaceta Parlamentaria del Senado de la República el 30 de abril del 2002, y publicado en la Gaceta Parlamentaria del 5 de septiembre del 2002; posteriormente fue turnada para su respectivo dictamen a las Comisiones Unidas de Puntos Constitucionales y de Estudios Legislativos.

En septiembre del 2002, esta iniciativa se turnó a la Comisión de Gobernación y Seguridad Pública de la Cámara de Diputados, y en octubre del mismo año se turnó a la Comisión de Comercio y Fomento Industrial, hoy Economía. La entonces Comisión de Comercio de la Cámara de Diputados en noviembre del 2002 presentó al pleno un comentario aduciendo que el contenido

[12] Esta Iniciativa se encuentra disponible en la página del Congreso de la Unión en la siguiente dirección: http://gaceta.cddhcu.gob.mx/
[13] Idem

de esta iniciativa resulta poco claro, ambiguo y su alcance e interpretación genera confusión. De los estudios realizados comenta dicho proyecto legislativo, produciría grandes afectaciones al comercio y al empresariado en general de nuestro país. Se estableció que la iniciativa debería pretender la regulación de la protección de datos de las personas físicas, recopilados, almacenados y procesados en archivos, registros y bases de datos de empresas del sector privado. Señala que se debe considerar la libertad de expresión, cuestiones relativas a regulación, en materia de protección, combate al terrorismo, narcotráfico, lavado de dinero o de alguna orden judicial.

Esta Iniciativa está basada en la Directiva 95/46 sobre Privacidad y Protección de Datos de la Unión Europea. El contenido y ámbito de aplicación de esta Iniciativa son poco claros y demasiado ambiguos en cuanto al registro de bases de datos; contiene reglas bastante estrictas para la transferencia de datos personales a terceros países y establece órganos de vigilancia en la esfera de la administración pública federal que no se han implementado aún y que seguramente impondrán cargas burocráticas excesivas para empresas de tecnologías de la información, de mercadotecnia y publicidad y en general de servicios de información, a este respecto cabe señalar por lo que hace a la prohibición al flujo transfronterizo de datos personales que, las empresas se encuentran en un dilema, puesto por una parte cuentan con socios comerciales con el Tratado de Libre Comercio con América del Norte y por otra parte, tienen la prohibición del libre flujo de datos personales.[14]

Así pues, de ser aprobada por el Poder Ejecutivo, podría traer consigo un

[14] Idem

grave impacto económico en la sociedad mexicana en cuanto a generación de empleos e inversiones que posiblemente podría guiar a algunas empresas a operar clandestinamente o prestar sus servicios en terceros países, inhibiendo en forma considerable el desarrollo del comercio electrónico, las inversiones y la creación de empleos en territorio nacional.

Por otra parte, es indispensable definir si realmente es una Ley de Protección de Datos, que los principios queden muy claros así como los sujetos obligados, porque se habla de organizaciones en donde también se encuentra el Gobierno, hace referencia de unas sociedades de información y se dice que pueden subir datos sensibles como los datos médicos, psiquiátricos y físicos, los que, ni siquiera deberían de recabarse, puesto que no resulta muy benéfico para el mercado que la información de salud de las personas fluya.

El objeto de esta iniciativa de ley es proteger datos y crear sociedades de información. La protección la basa principalmente en el sentido de preguntarle a la persona si está de acuerdo o no en comercializar sus datos; lo que, si bien es cierto que en la exposición de motivos refiere que va a ser benéfico para ambas partes, para las sociedades de información o las empresas que la van a comercializar, se entiende por demás el interés, sin embargo, la ganancia para el titular de los datos, en el sentido de que su información circule, no queda muy claro en sí, ya que sólo podría ser el caso de que reciba ciertos bienes o servicios ad-hoc a sus gustos y necesidades.[15]

La iniciativa por otra parte es ambigua ya que en ocasiones plantea que puede ser el Instituto Federal de Acceso a la Información Pública (IFAI) el órgano

[15] Idem

regulador para posteriormente hacer referencia a algún otro órgano especializado en esto.

Por otra parte, requiere especificar si existe un derecho de autodeterminación informativa, tiene que definir cuál es su alcance, puesto que por una parte, establece que la persona puede decidir que se transmitan sus datos, sin embargo posteriormente existe un artículo que dice que no se requiere el consentimiento cuando se esté dando mantenimiento de seguridad a la base de datos, con lo cual se puede entender que es en ese momento en que se disminuye el consentimiento o esto sirve para trasmitir de manera transnacional el dato.[16]

*Estructura: e*sta iniciativa consta de 53 artículos en V capítulos, el primero relativo a las disposiciones generales, el segundo a los derechos de los interesados o titulares de los datos, así como a los responsables de los registros, el tercero al Instituto Federal de Protección de Datos Personales, el cuarto a las sanciones, y el quinto a la acción protectora de datos.[17]

En el Capítulo I, se mencionan los objetos de la ley, las expresiones equivalentes, el ámbito de validez, y los principios sobre los cuales descansa la ley, sobresaliendo la circunstancia de que en ningún caso se pueden afectar los archivos, registros, bases o bancos de datos ni las fuentes de información periodísticas.[18]

En el Capítulo II, se regulan los derechos de los interesados, estableciendo un catálogo de obligaciones correspondientes a los organismos públicos y

[16] Idem
[17] Idem
[18] Idem

privados titulares de los datos. De este apartado conviene resaltar los derechos de los interesados para solicitar al Instituto Federal de Protección de Datos Personales la existencia de registros personales, las finalidades y la identidad de los responsables, así como el derecho de pedir a los responsables de archivos, registros, bases o bancos de datos informes, y de pedir de igual manera la inclusión, actualización, complementación, rectificación, reserva, suspensión y cancelación de los registros de datos que les correspondan, siempre que no se lesionen derechos de terceros o se atente contra intereses de carácter general o social.[19]

Asimismo, en este Capítulo II, se habla de las responsabilidades de los titulares de los Registros de las diversas categorías (públicos y privados) de bases o bancos de datos, quienes deben adoptar todas las medidas necesarias para la seguridad y conservación idónea de los datos, imponiéndoseles, incluso, el deber de secreto que se extiende a todos aquellos que hayan intervenido en el tratamiento automatizado de los datos.[20]

En el Capítulo III, se establecen las líneas generales para la creación y operación del organismo que tendrá por objeto el control de los responsables de los registros, bases o bancos de datos, así como sus atribuciones, en las que destaca la facultad de sancionar a los responsables de los archivos o registros por la comisión de violaciones leves y graves a esta ley.[21]

En el Capítulo IV, se propone la regulación específica de las sanciones, que van desde el apercibimiento hasta la cancelación de los registros, archivos, bases

[19] Idem
[20] Idem
[21] Idem

o bancos de datos.[22]

En el Capítulo V, se propone la regulación de un procedimiento especial del que conozcan los juzgados de distrito competentes con relación a causas federales, pues ello persigue que se resuelvan las controversias de manera pronta y sin obstáculos en tiempos más breves que los que corresponden, incluso a los juicios de amparo, pues una administración de justicia que no se otorgue en esos términos, prácticamente inutilizaría el recurso.[23]

Cabe señalar que en la iniciativa referida se señala que éste procedimiento se establece con entera independencia de los procedimientos que correspondan en tratándose de responsabilidad civil, administrativa o penal.[24]

Finalmente, en las disposiciones transitorias se prevé que los archivos, bases o bancos de datos existentes se puedan registrar, conforme lo determine el reglamento, en un lapso posterior al establecimiento del Instituto Federal de Protección de Datos.[25]

La misma iniciativa propone que la garantía procesal tenga por **objeto jurídico** que el interesado pueda acceder a los datos personales que le conciernen; que toda persona pueda acceder a los registros, archivos y bancos de datos públicos o privados de carácter público, y conocer su uso o fin para el que están destinados y, que el interesado pueda pedir la inclusión, actualización, complementación, rectificación, reserva, suspensión y cancelación de los datos

[22] Idem
[23] Idem
[24] Idem
[25] Idem

relativos a su persona.[26]

Bienes protegidos. Los bienes protegidos se identifican con el honor, la intimidad y cualquiera otra garantía del gobernado.[27]

Legitimación activa. Del interesado, esto es, de la persona a la que corresponden o conciernen los datos registrados o archivados, para acceder a ellos, para incluir datos, para actualizarlos, complementarlos, rectificarlos, reservarlos, suspenderlos o cancelarlos. De toda persona para acceder a los registros, archivos o bancos de datos públicos o privados de carácter público, así como para conocer el uso o fin para el que están destinados.

Legitimación pasiva. Son sujetos pasivos del proceso los archivos, registros, bancos o bases de datos públicos o privados en sus diferentes hipótesis.[28]

2) Por otra parte se cuenta con la diversa Iniciativa en relación con el tema de privacidad y protección de datos personales que se originó en la Cámara de Diputados del H. Congreso de la Unión. Fue presentada el día 6 de septiembre del 2001, por el **Diputado Miguel Barbosa Huerta** del Grupo Parlamentario del Partido de la Revolución Democrática (PRD) ante la LVIII Legislatura del H. Congreso de la Unión y publicada en la Gaceta Parlamentaria el 7 de septiembre de 2001.[29]

Está basada en gran medida en la Directiva 95/46 sobre Privacidad y

[26] Idem
[27] Idem
[28] Información tomada de la propia exposición de motivos de la iniciativa de ley en comento.
[29] Esta Iniciativa se encuentra disponible en la página del Congreso de la Unión en la siguiente dirección: http://www.cddhcu.gob.mx/servicios/datorele/cmprtvs/1po2/set/2.htm

Protección de Datos de la Unión Europea y la Ley Orgánica Española de Protección de Datos de Carácter Personal del 13 de diciembre de 1999.[30]

En su momento, fue turnada a la Comisión de Gobernación y Seguridad Pública, contiene una opinión de la Comisión de Comercio y Fomento Industrial de la Cámara de Diputados, sin embargo fue rechazada el 30 de abril de 2002, mismo día que se aprobó la Ley Federal de Transparencia y Acceso a la Información Pública.[31]

Estructura: el texto del proyecto, según la letra de la iniciativa, se integra con una parte general y otra especial. En la parte general se establecen las normas delimitadoras del ámbito de aplicación de la ley, principios reguladores del acopio, registro y uso de datos personales y, sobre todo, garantías de los titulares o afectados.[32]

Así, el ámbito de aplicación se define por exclusión, quedando fuera de él, por ejemplo los datos anónimos, los que constituyen información de dominio público, los que se recogen como información para darla a conocer al público en general o los de uso estrictamente personal. Quedan también fuera del ámbito de la norma aquellos datos que, en virtud de intereses públicos prevalentes, no deben estar sometidos a su régimen cautelar.[33]

Bajo los principios generales de esta iniciativa, se definen las pautas a las que deberá sujetarse la recolección de datos de carácter personal objeto de tratamiento, pautas encaminadas a garantizar tanto la veracidad de la información

[30] Idem
[31] Idem
[32] Idem
[33] Idem

contenida en los datos almacenados como la congruencia y la racionalidad de la utilización de los datos. Este principio de la congruencia y la racionalidad, dice, garantizará que los datos no puedan ser usados, sino cuando lo justifique la finalidad para la que han sido recabados, su observancia es, por ello, esencial para evitar la difusión incontrolada de la información.[34]

Por su parte, el principio de consentimiento, o de autodeterminación, del mismo modo consagrado, otorga a la persona la posibilidad de determinar el nivel de protección de los datos a ella referentes. Su fundamento está constituido por la exigencia del consentimiento consciente e informado del afectado para que la recolección de datos sea lícita. Y ello, a su vez, se refuerza con la definición de lo que se denominan datos sensibles, que comprenden la ideología, las creencias religiosas, la raza, salud y la vida sexual de un individuo. La protección reforzada de estos datos viene determinada porque los primeros de entre los datos mencionados sólo serán disponibles con el consentimiento expreso y por escrito del afectado, y los segundos sólo serán susceptibles de ser recopilados mediante dicho consentimiento o autorización legal expresa, habilitación que, según exigencia del proyecto han de fundarse en razones de interés general. Mientras que en todo caso se establece la prohibición de los ficheros creados con la exclusiva finalidad de almacenar datos personales sensibles.[35]

Indudablemente los derechos que se establecen a favor del titular o afectado constituyen los elementos medulares de la parte general, y se configuran jurídicamente como derechos subjetivos encaminados a hacer operativos los

[34] Idem
[35] Idem

principios genéricos. Son, por ejemplo, los derechos de autodeterminación, de rectificación y de cancelación los que otorgan virtualidad normativa y eficacia jurídica a los principios consagrados en la parte general, principios que, sin los derechos subjetivos aludidos, no rebasarían un contenido meramente programático.[36]

En concreto, los derechos de impugnación de valoraciones, de consulta, de acceso, de rectificación, de cancelación, de oposición y de indemnización que se definen y delimitan en el texto, constituyen las piezas centrales del sistema cautelar que se propone en el proyecto.[37]

Con el objeto de procurar la máxima eficacia de sus disposiciones, en la parte especial del proyecto, se propone la creación del Registro Nacional de Protección de Datos, como el ente encargado de coadyuvar en el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.[38]

Y para la debida articulación de los extremos concretos que han de regir los ficheros de datos, se distinguen distintos tipos de ficheros, según sea su titularidad pública o privada y, simultáneamente, se propone establecer regímenes diferenciados para los ficheros en razón de su titularidad, toda vez que, con toda evidencia, resulta más problemático el control de los de titularidad privada que el de aquellos de titularidad pública.[39]

[36] Idem
[37] Idem
[38] Idem
[39] Idem

Otras disposiciones de la parte especial que son pertinentes destacar son las que se refieren a la cesión o transmisión de los datos objeto de tratamiento. La protección de la integridad de la información personal se concilia, de esta suerte, con el libre flujo de los datos, que constituye una auténtica necesidad de la vida global actual. Y en cuanto a la transmisión internacional de datos se opta por exigir que el país de destino cuente en su ordenamiento con un sistema de protección suficiente para garantizar la integridad de los datos transferidos.[40]

Mención muy especial merece la regulación de la acción de protección de datos personales o *habeas data* (exhibe el dato) como una garantía de toda persona para acceder a la información y a los datos que sobre sí misma obren en registros privados u oficiales; para conocer el uso que se haga de los mismos y de su finalidad, y para solicitar la rectificación o la destrucción de aquellos, si fuesen erróneos o afectaran ilegalmente sus derechos.[41]

Finalmente, se contempla también un capítulo donde se tipifican diversas figuras delictivas, estableciendo severas sanciones, al que insertara o hiciera insertar a sabiendas, datos falsos en un archivo de datos personales; al que proporcione a un tercero a sabiendas, información falsa contenida en un fichero de datos personales; al que sabiendas e ilegalmente, o violando sistemas de confidencialidad y seguridad de datos, accediere de cualquier forma, a un banco de datos personales; y al que revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición

[40] Idem
[41] Idem

de una ley.[42]

Objeto de la ley. (Artículo 1º) Garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de estos derechos fundamentales, así como el acceso a la información que sobre las mismas se recabe, 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. Asimismo las disposiciones de esta ley podrán ser aplicables, en cuanto resulte pertinente, a los datos relativos a personas morales.

Legitimación activa y pasiva para el ejercicio de la acción. (Artículo 30). La acción de protección de los datos personales o de *habeas data* podrá ser ejercida por el afectado o sus representantes, usuarios y encargados de ficheros de titularidad pública o privada destinados a proveer informes.[43]

3) Por último se cuenta con la Iniciativa de "Ley Federal de Protección de Datos Personales"[44] por el **Diputado Jesús Martínez Álvarez,** del Grupo Parlamentario de Convergencia.

Esta iniciativa dice tener por **objeto** garantizar la protección de los datos personales que se encuentren contenidos en documentos, archivos, registros, bancos de datos, o bien en otros medios tecnológicos de procesamiento de datos, sean de carácter públicos o privados, a efecto de proteger los derechos de las personas a la vida privada y a la intimidad, así como el acceso a la información

[42] Idem
[43] Idem
[44] Propuesta visible en la Gaceta Parlamentaria del Jueves 1º de diciembre de 2005.

que sobre las mismas se registre, en términos de los artículos 6, 14 y 16 de la Norma Suprema.[45]

Esta propuesta se divide en ocho capítulos. Las disposiciones generales, se establecen en el primer capítulo, señalando el objeto y leyes aplicables, en lo conducente, a los datos de las personas jurídicas, enfatizando que en ningún caso se podrán afectar los registros y fuentes periodísticas, amén de que los archivos, registros, bases o bancos de datos electorales; los referentes al registro civil, a la prevención, persecución y sanción de los delitos, así como a la ejecución de las sanciones penales; personales concernientes a integrantes de las fuerzas armadas y los cuerpos de seguridad pública o a datos relativos a esos cuerpos y con fines exclusivamente estadísticos se regirán conforme a los ordenamientos aplicables y las excepciones de la ley.[46]

En el Capítulo Segundo se denomina de las definiciones, en donde se precisa que debe entenderse por base de datos, instituto y datos íntimos, entre otros conceptos.[47]

En el Capítulo Tercero se estipulan los principios generales, quedando prohibido el tratamiento de los datos personales que revelen ideologías, origen racial o étnico, convicciones religiosas y no religiosas o de cualquier tipo, hábitos y comportamientos personales, orientación y vida sexual, rasgos físicos y psíquicos, estado de salud, opiniones políticas, afiliación partidaria, salvo que los ordenamientos jurídicos dispongan lo contrario o medie consentimiento de su titular siempre que no sea factible su identificación; los casos en que se podrá

[45] Idem.
[46] Idem.
[47] Idem.

proceder a la recolección y tratamiento de los mismos.[48]

Los derechos de los **titulares** de datos se ubican en el Capítulo Cuarto, detallando entre otros aspectos, que toda persona puede solicitar información al organismo de control relativo a la existencia de archivos, registros, bases o bancos de datos personales, sus finalidades y la identidad de sus responsables, así como la consulta pública y gratuita.[49]

En el Capítulo Quinto, los usuarios y responsables de archivos, registros y bancos de datos destinados a proporcionar informes debiendo inscribirse en el Registro que al efecto habilite el Instituto y los datos mínimos que deberá contener el mismo.[50]

El control, se establece en el Capítulo Sexto, que estará a cargo del Instituto encargado de controlar, organizar, estructurar, evaluar y vigilar la protección de los datos personales, que se encuentren en los bancos de datos, archivos o registros; así como a los responsables de los mismos, regulados por esa Ley, será el que dispondrá la Ley Federal de Transparencia y Acceso a la Información Pública.[51]

En el Capítulo Séptimo está lo relativo a las sanciones, en donde el Instituto podrá apercibir a los usuarios de bases de datos personales cuando incumplan las disposiciones de dicho ordenamiento.[52]

La acción de protección de los datos personales, se encuentra en el Capítulo Octavo, instituyendo que los titulares de los datos personales podrán

[48] Idem.
[49] Idem.
[50] Idem.
[51] Idem.
[52] Idem.

ejercerla, para conocer los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, así como la finalidad de aquellos y para solicitar la rectificación, supresión, confidencialidad o actualización de los datos personales en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en dicha ley.[53]

Al ser éstas iniciativas las propuestas por los diputados y senadores citados con antelación, resulta pertinente que el H. Congreso de la Unión organice una Mesa de Trabajo sobre Privacidad y Protección de Datos Personales, tal y como lo hizo la Comisión de Comercio y Fomento Industrial de la Cámara de Diputados desde principios del año 2003, en las Mesas de Trabajo que organizó sobre comercio electrónico, nombres de dominio, firma electrónica y delitos informáticos. Una mesa de trabajo de esta naturaleza, contaría con la participación de los sectores interesados de la sociedad como son cámaras empresariales, empresas del sector de la publicidad y mercadotecnia, entidades financieras, asociaciones, fedatarios públicos, representantes de la administración pública federal, grupos académicos, entre otros. Mediante un foro de este tipo, se tendría la oportunidad de analizar las aplicaciones tecnológicas más avanzadas de la industria para la protección de la privacidad y la protección de datos, escuchar puntos de vista, analizar propuestas y revisar las disposiciones más controvertidas de la última Iniciativa en comento. Ello llevaría a encontrar un balance apropiado para la adopción de un esquema regulatorio bien estructurado, que por un lado, combine

[53] Idem.

programas de regulación del sector privado y propuestas de los sectores público y académico, protegiendo en la medida de lo posible las garantías constitucionales de los individuos de libertad y privacidad, sin inhibir el desarrollo del comercio electrónico en México.

4.3 EXTRATERRITORIALIDAD.

Para llevar a cabo el presente apartado, me basé principalmente en las conferencias realizadas en el "IV Encuentro Iberoamericano de Protección de Datos Personales", organizado por el Instituto Federal de Acceso a la Información Pública, llevado a cabo tanto en el Salón Don Alberto del hotel "Sheraton Alameda" de esta Ciudad, así como con sede en la Universidad Anáhuac, Campus Norte, Auditorio de Rectoría, celebrado del 2 de noviembre del año 2005, en la mesa denominada *"Las tecnologías de la información y su impacto en la Privacidad: de las computadoras a las telecomunicaciones"* a cargo del Doctor Jesús Rubí Navarrete, Director Adjunto de la Agencia Española de Protección de Datos, del Doctor Alfredo Reyes Kraft, Director de Banca Electrónica de BMW Bancomer y Presidente de la Asociación Mexicana de Internet.

Dentro de dichas conferencias se estableció que la globalización es una realidad, un fenómeno multidimensional que abarca no sólo aspectos económicos, sino también sociales, ideológicos, políticos, culturales, etc. y es que las nuevas tecnologías de la información, el desarrollo de las telecomunicaciones ponen a disposición del usuario todo tipo de información incluida información personal, que es claramente utilizada para fines comerciales y de mercadotecnia, pero la mayoría de las veces estos datos pueden ser manipulados sin el consentimiento

del titular y peor aún si se tiene un total desconocimiento de su tratamiento, uso y destino de dichos datos.

Ante esta situación la persona queda en total indefensión, sin encontrar los mecanismos para acceder a sus datos, solicitar que sea retirada de esas listas de destinatarios o reclamar sobre actos de discriminación derivados del conocimiento por parte de terceros de sus datos personales.

En la mayor parte de los países de América Latina no se ha generado un debate amplio y adecuado sobre los alcances del intercambio generalizado de información, a fin de garantizar un marco de libre flujo de la información, y menos aún para proteger la intimidad o privacidad de las personas.

Existe consenso internacional de que el tratamiento ilegal de datos personales conduce a prácticas comerciales transfronterizas engañosas y fraudulentas.

Ahora bien, la libre circulación de datos personales es un elemento esencial para el desarrollo del comercio internacional. En el caso americano MERCOSUR, por poner un ejemplo, se hace imprescindible que para garantizar la libre circulación de datos exista una regulación que prevea un sistema de garantías, y no sólo en el ámbito de una integración regional, sino también en el comercio que se realice entre unas y otras regiones, entre todos los países, en definitiva el tratamiento de datos y la libre circulación de datos personales que se produzca en un mercado globalizado.

Esto es, si existen países como los europeos en donde los estados se preocupan por proteger los datos personales de sus ciudadanos, es justo que si quieren hacer negocios con otros países y en especial con México, se les otorgue

el mismo nivel de protección.

La Criminología sostiene que tanto el factor espacio como el tiempo constituyen elementos de riesgo que el delincuente tendrá en cuenta al momento de cometer la acción ilícita. En los delitos informáticos estos dos factores se ven altamente disminuidos.

En los delitos cometidos a través de medios informáticos encontramos también las características de los delitos a distancia, entendidos estos como aquellos en los cuales puede disociarse espacialmente la conducta delictuosa del resultado. Esta extensión plantea problemas como la determinación de la competencia, extradición, prueba extranjera, entre otros.

Por ejemplo: un *software* puede ser programado en cualquier lugar del planeta y puede producir sus efectos en cualquier otra parte. Ayuda a esto la interconexión cada vez mayor que se da entre computadoras, como en el caso de los virus informáticos que se suelen encontrar en los ordenadores personales son hechos en su mayoría en el exterior, por personas que residen ahí y producen sus efectos en nuestro país.

En las leyes estatales norteamericanas sobre delitos informáticos, y que se detallaron con anterioridad, el capítulo de competencia es lo bastante amplio como para poder permitir juzgar el delito informático en cualquier estado, para el efecto de evitar dilaciones en el trámite de la causa, esto es conocido como *long arm statutes*, es decir, leyes de gran alcance, buscando evitar los efectos de las redes informáticas.

Otras leyes son más extensas en su jurisdicción y tienden a aplicarse incluso más allá de sus fronteras. Por ejemplo, la Ley de Delitos Informáticos de

Malasia del año 1997 establece, bajo el título de ámbito territorial, que la ley se aplicará a cualquier individuo, con independencia de su nacionalidad e incluso que la ley tendrá efectos fuera de Malasia.

Lo cierto es que estos problemas de extraterritorialidad del delito serán cada vez más frecuentes hasta en tanto no se determine a nivel global las leyes aplicables al caso específico conforme a los tratados internacionales existentes entre los países.

Al respecto, la Convención de Naciones Unidas, relativa precisamente al crimen transnacional, contempla la temática de las bases de datos y, en concreto y vinculado con todas la temática del lavado de dinero y además, del narcotráfico, la cuestión de la cooperación judicial o la cooperación entre los estados.

No se podrá cumplir con ninguno de los objetivos u obligaciones de los propios estados, de no darse una normatividad precisamente que sea acorde a estas necesidades que por un lado tienen, lo que es el derecho a la privacidad y los derechos humanos de la persona y, por el otro lado, la tecnología que ha sobrepasado a varios estados en su legislación interna y el esfuerzo de la comunidad internacional por controlar y regular debidamente y que se realicen en el campo de lo lícito y no de lo ilícito varias actividades y comportamientos que desgraciadamente no se han sujetado a control.

Ante lo cual, cuando la legislación no es lo suficientemente clara para definir al “juez natural” que deberá conocer del asunto, le corresponderá a la jurisprudencia sentar los principios para su determinación.

Los países deberían de instrumentar, como mínimo, los lineamientos sobre protección de la privacidad y flujos transfronterizos de datos personales de la

Organización de Cooperación y Desarrollo Económico, en donde se establece que el manejo de los datos personales debe de ser primeramente, simple y tecnológicamente neutro, o sea que se puedan utilizar diversas tecnologías, no estar sujetos únicamente a algún tipo de tecnología.

En América Latina hay una gran diversidad de enfoques en materia de protección de datos, en materia de “habeas data” que llevan precisamente a una consecuencia negativa que es que la terminología utilizada, incluso los conceptos que muchas veces son hasta contradictorios y conspiran precisamente con la finalidad que debe tener todo sistema de protección de datos, que es por supuesto que haya una claridad conceptual, que haya una claridad terminológica, y por supuesto, que se simplifique al máximo todo lo que tiene que ver con su regulación, por supuesto no dejando de lado regulaciones fundamentales.

Los medios de protección legislativos parten de tres fuentes fundamentales. La primera son los convenios o los convenios regionales. En América Latina, no tenemos todavía una convención americana sobre la protección de datos, aunque hay proyectos en la Organización de los Estados Americanos al respecto, y de algún modo los trabajos de la Red Iberoamericana de Protección de Datos Personales están tendiendo a esta concreción.

Luego vienen las constituciones, que en el caso de América Latina a partir de la década de los 80’s se creó lo que se llamó el Habeas Data con distintos matices en cada uno de los países. Este es uno de los motivos por los cuales hay una gran diversidad, no solamente en terminologías en legislaciones y conceptuales, sino en los proyectos que hoy están en los parlamentos de los distintos países latinoamericanos que todavía no tienen ley de protección de

datos, como en el caso de México.

Por último, se encuentran los medios de protección de datos y otras normas que no son leyes generales de protección de datos, pero que contribuyen a la misma finalidad, siendo que en el caso de nuestro país se han detallado las diferentes leyes que hablan al respecto, incluyendo al Código Civil, el Código Penal Federal, la de Instituciones de Crédito, la Ley Federal de Defensa del Consumidor, la Ley de Información Estadística y Geográfica, la Ley de Transparencia y Acceso a la Información Pública, entre otras.

Sin embargo, resulta indispensable que haya una autoridad única que, de algún modo, establezca criterios uniformes, porque si la legislación no es clara se puede producir una serie de discordancias en el ordenamiento interno que no es aconsejable, por lo menos en lo que respecta a la protección que se debe proporcionar a los ciudadanos. Por ejemplo, el concepto de “habeas data” que se usaba como derecho en realidad no lo es, sino se trata de una garantía de otros derechos. En los proyectos de Colombia en la doctrina de la Corte Constitucional se usa la palabra derecho de habeas data como la primera frase que tiene que ver con el acceso y después a la segunda frase se llama derechos conexos de rectificación.

No obstante, el sentido inicial del “habeas data” fue una acción procesal constitucional que nació en una constitución brasileña del año 1988 y que tenía como finalidad actuar sobre los datos personales para tutelar la integridad física, el derecho a la vida, porque se trataba en la idea de los contribuyentes, que el acceder a los bancos de datos oficiales se podrían crear futuras discriminaciones.

En algunos países como en el caso de Argentina, Chile y España, sólo por

citar algunos, se ha determinado como un medio de protección judicial la vía civil, a falta de la ley de protección de datos, con el efecto de obtener una indemnización. Las sanciones civiles están propiciadas desde el orden internacional, el principio octavo de las directrices de la Organización de las Naciones Unidas, el artículo 23 de la directiva europea 95-46, un documento del año de 2004 del Grupo del artículo 29 de la Unión Europea, el artículo 23 de la ley chilena, el artículo 19 de la ley española, por mencionar algunas.

De ahí, que para tener uniformidad, por lo menos en América Latina, sobre la protección de datos personales, resulta indispensable la existencia de una autoridad independiente, en cuanto al nivel último de decisión, ya que si bien pudieran haber otras autoridades que pueden aplicar los principios de protección de datos, esto ha traído determinadas formas de regulación, por ejemplo en el Derecho Comparado tenemos el Privacy & Comisional de Canadá, el garante de la privacidad en Italia, la Agencia Española de Protección de Datos que es una autoridad independiente; en el caso argentino existe la Dirección Nacional de Protección de Datos que depende del Ministerio de Justicia, en la ley chilena el Registro Civil e Identificación; el Servicio del Registro Civil de Identificación en la ley uruguaya, comisión que depende del Ministerio Económico y Finanzas; y en el caso de México vemos una diversificación ya que se cuenta con el Instituto Federal de Acceso a la Información (IFAI); sin embargo, únicamente para la protección de datos personales que obran en dependencias gubernamentales como se señaló con anterioridad; existiendo así diversas formas de controlar los datos, conforme a algunas instituciones de fracción parlamentaria, otras de extracción ejecutiva y otras autoridades independientes.

El carácter totalmente descentralizado y no jerárquico de Internet, el hecho de no estar bajo ninguna autoridad o control es la mayor ventaja de la red respecto de los usuarios. Pero desde el punto de vista legal, ello constituye un grave problema "la ley penal se caracteriza por su aplicación territorial y choca con la dimensión transnacional de Internet" [54]

Lo anterior en razón de que Internet no reconoce límites geográficos y que los delitos traspasan fronteras se ha tomado conciencia de la necesidad de cooperación conjunta para combatir el delito informático.

En la Unión Europea existe preocupación por el fenómeno de la delincuencia a través de redes informáticas globales. Así, en la Iniciativa Europea de comercio electrónico se sostiene que:

> "Un problema que cada día preocupa más es la aparición de la "*ciberdelincuencia*", con delitos como el lavado electrónico de dinero, las actividades de juego ilegal, la piratería informática o la violación de la propiedad intelectual. La cooperación internacional está ya muy avanzada en determinadas áreas fundamentales, como la lucha contra la delincuencia internacional organizada que se sirve de las nuevas redes de comunicación. Ante las nuevas formas de delincuencia informática y tecnológica que han aparecido en las redes mundiales[55] (los delitos de piratería informática registrados están experimentando un crecimiento anual del 100%), las autoridades públicas han reaccionado enérgicamente... En Europa (Europol), así como en un contexto internacional más amplio, se han creado grupos especiales y se ha reforzado la cooperación transfronteriza en áreas tan importantes como la "localización y seguimiento" (trap and trace) de delincuentes en línea y la "búsqueda y confiscación" (search and seize) de pruebas digitales. También se están haciendo esfuerzos para armonizar la legislación penal en materia de delitos informáticos y evitar la aparición de paraísos digitales. A raíz del Consejo de Dublín, se creó un Grupo de Alto Nivel que está ultimando un plan de acción para luchar contra la ciberdelincuencia. Estos esfuerzos revisten una

[54] PALAZZI, Pablo A. op. Cit. P. 81

[55] La *Federal Trade Comisión* de los EE.UU. y la *Gendarmerie Royale* de Canadá tienen un "Web site" cada una para informar al público de los diferentes tipos de abusos y operaciones ilegales en Internet. Véase http://www.ftc.gov y http://www.rcmp-grc.gc.ca/html/scams-f.htm

importancia fundamental para incrementar la confianza en el comercio electrónico internacional". [56]

Este movimiento internacional fue coronado en abril de 2000 con la reciente propuesta del Consejo de Europa de crear un tratado sobre delitos informáticos. El tratado no sólo incluye armonización de figuras penales sino también distintas formas de cooperación entre las autoridades nacionales, tales como intercambio de datos en línea y acuerdos de extradición más efectivos.

Con esto se busca evitar lo que ocurrió con un virus informático en Filipinas y que afectó a ordenadores en los Estados Unidos y Europa, Filipinas carecía de leyes sobre delitos informáticos, lo que obstaculizó la posibilidad de investigar el caso.

Por lo anterior, se hace necesario destacar la importancia de contar con una institución independiente en cualquier sistema de protección para lograr mayor seguridad a los datos de la ciudadanía.

4.5 PROPUESTA DEL DELITO QUE ATENTE CONTRA LA PRIVACIDAD DE LOS DATOS PERSONALES EN INTERNET.

El inexorable avance de la tecnología ha rebasado con mucho la regulación civil, penal y administrativa relacionada con el intercambio de datos personales existentes en nuestro país.

La protección de datos personales y la confidencialidad de la información en Internet, son temas de capital importancia en la sociedad de la información y cada día requieren de mayor atención por parte de la comunidad mundial de Internet,

[56] Comunicación al Parlamento Europeo, el Consejo, el Comité Económico y Social y el Comité de las Regiones, del 12/4/97.

desde los proveedores de servicios de Internet, los responsables o administradores de páginas y sitios Web, los dueños de las empresas con sitios Web, así como los millones de usuarios alrededor del mundo que deben considerar un código ético en el manejo de la información confidencial a la que tienen acceso y contemplar los ordenamientos jurídicos existentes.

Lo más importante es que, al proteger los datos personales y su confidencialidad, se protege a su titular, de ahí que cuidar la información y hacer un buen uso de ella, es una garantía para proteger a las personas, lo cual se integra dentro de los derechos fundamentales.

En México para el año 2007 existen aproximadamente 20 millones de cibernautas, ocupando un aproximado de 17 millones de equipos de cómputo, entre los cuales casi el 73 por ciento son jóvenes y jóvenes adultos que van de los 13 a los 34 años. Estos grupos poblacionales son especialmente vulnerables a un mal manejo de sus datos personales en la transacción de bienes y servicios en línea. [57]

Uno de los delitos que se está expandiendo más hoy en día es el robo de identidad principalmente por el escaso nivel de seguridad con que cuentan las bases de datos personales, logrando con ello fraudes cibernéticos por ejemplo, ante lo cual se deben establecer penas muy fuertes en ese sentido así como criterios de custodia de todos aquellos datos que puedan servir para identificar a las personas, que acrediten de alguna manera directa o indirecta la identidad.[58]

Otro delito es el que se ha denominado “fishing” que son correos

[57] Fuente: INEGI 2007.
[58] PALAZZI Pablo A. Op cit. P. 57

electrónicos falsos solicitando información financiera, lo que conlleva los fraudes, a través de correos de bancos en los cuales solicitan números de tarjetas, números de cuentas, etc. lo que conlleva a fraudes cuantiosos. Otro ejemplo es el de la "carta nigeriana" realizada claro está, por nigerianos quienes mandaban una solicitud de que le guarden dinero a un riquísimo rey nigeriano en el exilio que necesita poner su dinero en alguna cuenta, para eso requieren la cuenta bancaria con la promesa de grandes ganancias, y con ese número evidentemente viene el fraude.[59]

También se captan los datos personales de los cibernautas con los servicios financieros que se ofrecen, esquemas de trabajo en casas, ofertas de trabajos, empresas petroleras que ofrecen trabajos de tres meses en el Mar del Norte ganando miles de dólares al mes, venta de títulos y grados académicos sin estudiar por supuesto, paquetes vacacionales, toda la parte de la pornografía, adquisición de música y juegos entre otros.

Es indispensable incorporar figuras como la autorización del titular de los datos personales, a efecto de poder disponer de ellos y la correlativa prohibición de usarlos con las sanciones penales y la determinación de la responsabilidad civil en caso de incumplimiento.

La información tendrá que ser manejada con un contenido eminentemente ético, respetuoso de las garantías individuales y reservado, toda vez que afecta la esfera de intimidad de las personas y puede dar lugar a la lesión de la honra, fama pública o consideración que la sociedad tenga de determinada persona.

No se trata de una simple reforma que pueda ser incorporada a un Código

[59] Idem p. 58

Civil o Penal, se trata de todo un cambio en la percepción jurídica de estos aspectos tanto a nivel federal, como local. Deberán ser leyes especializadas sobre la materia que, inclusive, tipifiquen delitos en caso de trasgresión y establezcan los parámetros para determinar la responsabilidad civil que un indebido manejo de datos personales pueda ocasionar.

El campo de protección podría ser también amplio, ya que los medios electrónicos invaden aspectos tales como domicilio, número telefónico, ocupación, preferencia sexual, salud, todo tipo de información que pueda afectar la esfera de privacidad de un individuo. Las empresas que usen o más aún que comercialicen este tipo de información deben estar reguladas y supervisadas por órganos gubernamentales para efecto de prohibir la comercialización, ya que sería ir en contra del mercado y el avance tecnológico impedir esa situación.

Necesitamos todo un marco jurídico incluyente que involucre a los sectores público, privado y social en la protección de datos personales, donde se garantice la protección de la privacidad sin descuidar los aspectos económicos, tecnológicos, de mercado que han detonado la expansión de esta actividad.

Por otra parte, cabe señalar que resulta indispensable establecer qué Institución podría ser la encargada de resguardar y controlar las bases de datos existentes en México y que circulan por Internet, resultando como principal candidato para tal efecto, el propio Instituto Federal de Acceso a la Información Pública quien deberá contar con facultades para contener los datos contenidos en el sector tanto público como privado, el cual deberá ser un organismo autónomo, esto es, de contar el Estado con el resguardo de la protección de los datos personales del sector privado, no existe la seguridad de que el mismo estado

pueda hacer uso de la información proporcionada para un control excesivo de los ciudadanos.

Así pues, tomando en consideración lo expuesto en el presente trabajo propongo que el tipo penal que debería incluirse en nuestra legislación vigente es la inclusión de diversos artículos que se contemplen dentro del Título Noveno bajo el Capítulo II denominado “Acceso ilícito a sistemas y equipos de informática” del Código Penal Federal y precisamente es en esta legislación, en virtud de que, al ser los datos personales que circulan por Internet los que se pretenden proteger es que se requiere mayor protección jurídica que el que pudiera contener únicamente el Distrito Federal, máxime que este medio de comunicación es usado en toda la República Mexicana y no solamente en esta Entidad; por otra parte como se mencionó con anterioridad resultan indispensables los tratados internacionales para la protección requerida, lo cual un Código local no puede contemplar. Aunado a lo anterior de que no existe legislación relativa a la PROTECCIÓN DE DATOS PERSONALES.

PROPUESTA:

“Se impondrá sanción de un mes a tres años de prisión:

I. Al que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales;

II. Al que a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

III. Al que obtenga los datos personales sin el

consentimiento expreso del interesado cuando éste sea requerido;

IV. Al que recoja datos de carácter personal de forma engañosa y fraudulenta;

V. Al que comunique o ceda los datos de carácter personal, fuera de los casos en que estén permitidos;

VI. Al que recabe y trate los datos de carácter personal especialmente protegidos cuando no medie el consentimiento expreso del afectado o no lo disponga una Ley, tratándose de ficheros dedicados exclusivamente a la recolección de datos relacionados con la ideología, afiliación sindical, religión, creencias, origen racial o étnico, vida o preferencia sexual de las personas, así como los que hayan sido recabados para fines policiales;

VII. Al que vulnere el deber de guardar secreto sobre los datos de carácter personal relacionados con la ideología, afiliación sindical, religión, creencias, origen racial o étnico, vida o preferencia sexual de las personas, así como los recabados para fines policiales sin el consentimiento de las personas afectadas;

Asimismo, se impondrán de uno a cuatro años de prisión al que:

I. Realice la transferencia temporal o definitiva 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 sin autorización del Instituto Federal de Acceso a la Información;

II. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley;

III. No atienda u obstaculice de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición a los datos personales cuando esto proceda legalmente;

IV. Mantenga archivos, registros, bases o bancos de datos, equipos o herramientas sin las condiciones mínimas de seguridad requeridas por las disposiciones aplicables.

Además de la pena impuesta en los artículos precedentes, se condenará al responsable del pago de indemnización de daño moral en caso de comprobarse.

Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el tiempo similar al de la prisión impuesta.

Este ilícito se seguirá por querella."

De la propuesta señalada se advierte la existencia de los siguientes elementos OBJETIVOS, SUBJETIVOS Y NORMATIVOS a saber:

ELEMENTOS OBJETIVOS.

CONDUCTA. "La conducta es el primer elemento básico del delito y se define como el comportamiento humano, voluntario, positivo o negativo, encaminado a un propósito". [60] Esto es, sólo los seres humanos pueden cometer conductas positivas o negativas, ya sea una actividad o inactividad respectivamente. Es voluntario dicho comportamiento porque es decisión libre del sujeto y es encaminado a un propósito, porque tiene una finalidad al realizarse la acción u omisión. La acción en sentido estricto, es la actividad voluntaria realizada por el sujeto, consta de un elemento físico y de un elemento psíquico, el primero es el movimiento y el segundo es la voluntad del sujeto; esta actividad voluntaria produce un resultado y existe un nexo causal entre la conducta y el resultado.

Por otra parte, este ilícito en algunas de sus hipótesis también resulta ser de omisión, consistente en "la inactividad voluntaria cuando existe el deber jurídico de obrar" [61] Así pues, los delitos de omisión consisten en la abstención del sujeto, cuando la ley ordena la realización de un acto determinado.

[60] LOPEZ Betancourt, Eduardo. Teoría del Delito, Editorial Porrúa, Cuarta Edición, 1997, México, p. 73

[61] CUELLO Calón, Eugenio. Derecho Penal. Parte General, tomo I, 9ª Ed., Editora Nacional, México, 1961, p. 288.

Ahora bien, una vez establecido lo anterior, del tipo penal propuesto se advierte la presencia de diversas hipótesis por las cuales se puede generar el ilícito, como son:

De la fracción I se desprenden:

* Al que insertara a sabiendas datos falsos en un archivo de datos personales ó,

* Al que…. hiciera insertar a sabiendas datos falsos en un archivo de datos personales;

De la fracción II:

* Al que a sabiendas e ilegítimamente… accediere, de cualquier forma, a un banco de datos personales ó bien,

* Al que… violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

De la fracción III se advierte:

* Al que obtenga los datos personales sin el consentimiento expreso del interesado cuando éste sea requerido;

Fracción IV:

* Al que recoja datos de carácter personal de forma engañosa y fraudulenta;

Fracción V:

* Al que comunique… los datos de carácter personal, fuera de los casos en que estén permitidos; o bien,

* Al que… ceda los datos de carácter personal, fuera de los casos en que estén permitidos;

Fracción VI:

* Al que recabe y trate los datos de carácter personal especialmente protegidos cuando no medie el consentimiento expreso del afectado… tratándose de ficheros dedicados exclusivamente a la recolección de datos relacionados con la ideología, afiliación sindical, religión, creencias, origen racial o étnico, vida o preferencia sexual de las personas, así como los que hayan sido recabados para fines policiales;

* Al que recabe y trate los datos de carácter personal especialmente protegidos cuando… no lo disponga una Ley tratándose de ficheros dedicados exclusivamente a la recolección de datos relacionados con la ideología, afiliación sindical, religión, creencias, origen racial o étnico, vida o preferencia sexual de las personas, así como los que hayan sido recabados para fines policiales;

Fracción VII:

* Al que vulnere el deber de guardar secreto sobre los datos de carácter personal relacionados con la ideología, afiliación sindical, religión, creencias, origen racial o étnico, vida o preferencia sexual de las personas, así como los recabados para fines policiales sin el consentimiento de las personas afectadas;

Por otra parte se advierte la presencia de un tipo penal que previene una mayor sanción en los siguientes casos:

Fracción I:

* Realice la transferencia temporal… de datos de carácter personal que hayan sido objeto de tratamiento… con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Instituto Federal de Acceso a la Información;

* Realice la transferencia… definitiva de datos de carácter personal que hayan sido objeto de tratamiento… con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Instituto Federal de Acceso a la Información;

* Realice la transferencia temporal… de datos de carácter personal que… hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Instituto

Federal de Acceso a la Información;

* Realice la transferencia… definitiva de datos de carácter personal que… hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Instituto Federal de Acceso a la Información;

Fracción II:

* Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley;

De la Fracción III y IV se advierte la presencia de hipótesis que establecen conductas de omisión:

* No atienda… de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición a los datos personales cuando esto proceda legalmente;

* …obstaculice de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición a los datos personales cuando esto proceda legalmente;

Fracción IV:

* Mantenga archivos, registros, bases o bancos de datos, equipos o herramientas sin las condiciones mínimas de seguridad requeridas por las disposiciones aplicables.

BIEN JURÍDICO TUTELADO POR LA NORMA. Como se ha establecido con antelación, el bien jurídico resulta ser el derecho de las personas a LA PRIVACIDAD.

RESULTADO. El resultado de la acción debe ser sancionado por la ley penal, es

decir, deberá configurar un delito descrito y penado por la ley, será intrascendente que lesione intereses jurídicos protegidos por la ley o sólo los ponga en peligro según lo requiera el tipo penal. Maggiore define al resultado como la "consecuencia de la acción, que la ley considera decisiva para la realización del delito, o lo que es lo mismo, la realización del tipo de delito fijado por la ley, así, el resultado es el efecto voluntario en el mundo exterior o más precisamente, la modificación del mundo exterior como efecto de la actividad delictuosa." [62] En el caso a estudio, nos encontramos ante la presencia de un ilícito de RESULTADO FORMAL, esto es, para su configuración no se requiere de ninguna materialización, puesto que la afectación que produce precisamente resulta ser en la PRIVACIDAD de las personas.

OBJETO. Sobre el cual recae la conducta del activo lo son los datos personales resguardados por las personas, que, con o sin su consentimiento se encuentren en un Banco de datos o registros remitidos a través de Internet.

SUJETOS. Es necesario tomar en consideración que en Internet, aparecen sujetos específicos, tales como la operadora de telecomunicaciones, el proveedor de acceso a Internet o el proveedor de servicios de Internet, que para el desarrollo de su actividad y la prestación de sus servicios requieren del tratamiento de los datos de los usuarios, y que por tanto, quedan sometidos a la normativa sobre protección de datos en general y específica en el

[62] MAGGIORE, Giuseppe, Derecho Penal. I. 5ª Ed., Ed. Temis, Bogotá, 1989, p. 357

sector de las telecomunicaciones.

La protección de datos en Internet se convierte en una obligación para quienes tratan datos de los usuarios y en una garantía para éstos últimos. Si bien dicha protección habrá de ser el resultado de una combinación entre las disposiciones legales, recordando que no todos los ordenamientos jurídicos tratan la cuestión de la misma forma, y las diferentes soluciones tecnológicas que desde la industria del hardware y el software se desarrollen para dar soluciones específicas a ésta cuestión. Para esto se requiere que se obligue a los que recaban datos a cumplir la normativa y a los usuarios que los proporcionan, se encuentren mejor informados para poder tomar las decisiones oportunas.

Así pues, tomando en consideración las características del delito que se propone, se advierte que los sujetos ACTIVOS podrían serlo investigadores privados, empresas de *marketing*, agencias de informes crediticios y de solvencia patrimonial, los denominados “piratas informáticos” o hackers, los propios usuarios (en el caso de los robos de identidad), empresas que realizan competencia parasitaria, entre otros.

Y por otra parte, como sujetos PASIVOS puede serlo desde el Estado, entidades financieras y en sí, cualquier persona que opere con ordenadores y que se encuentre obligada a proporcionar sus datos personales, puede ser víctima del delito informático.

INTERVENCIÓN. Jiménez de Asúa [63] afirma que en un ilícito penal, no siempre habrá la intervención de un solo agente; también puede ser cometido por varios individuos que se ponen de acuerdo y dividen entre sí el esfuerzo para realizar el hecho criminal. En nuestra legislación dicha intervención se encuentra detallada en el artículo 13 del Código Penal Federal.

Así pues, por las modalidades en que se pueden obtener los datos personales, éste ilícito puede ser cometido por uno o varios sujetos.

AGRAVANTES. Estableciendo para éste ilícito únicamente en el caso de que el sujeto activo se trate de un servidor público se contempla la destitución e inhabilitación de su cargo por el mismo tiempo que se señaló para la privativa de libertad.

ELEMENTOS SUBJETIVOS.

DOLO. Entendido como la conciencia de violar la norma, el dolo se caracteriza en querer la conducta, ante lo cual nos encontramos ante la presencia de un DOLO DIRECTO, esto es, el saber que es un delito el adquirir, transferir o cualquiera de las hipótesis previstas, sin el consentimiento de las personas o de forma ilegal, y aún así quiere el resultado jurídicamente prohibido. Por lo que atendiendo a las características del delito propuesto, únicamente acepta la realización dolosa y no culposa del actor.

[63] JIMÉNEZ de Asúa, Luis, Principios de Derecho Penal. La Ley y el Delito, 3ª ed., Ed. Sudamericana, Buenos Aires, 1990, p. 365

ELEMENTOS NORMATIVOS. Relativos a cuestiones de índole meramente cultural, estos elementos se determinarán conforme a la hipótesis por la cual se pudiera ejercitar acción penal, como pudiera ser los conceptos de privacidad, banco de datos, datos personales, confidencialidad, transferencia, secreto, entre otros.

4. CONCLUSIONES

PRIMERA. Los datos personales son un derecho fundamental que debe permitir a la persona tener el control sobre su uso, tratamiento, destino y acceso en el momento en que lo requiera, esto es, darle a la persona el poder de disposición sobre sus datos personales.

SEGUNDA. La protección a la vida privada es necesaria para garantizar el respeto a la dignidad personal, y desde mi perspectiva existe un doble propósito en la protección de la intimidad. Por una parte se trata de asegurar la libertad individual, y por otra se intenta restringir o prohibir el uso indebido de información confidencial.

TERCERA. Hablar de protección de datos personales, hablar de tomar conciencia como persona que tengo estos derechos, es en última instancia un reconocimiento de la libertad humana, y un reconocimiento de que todo ser humano tiene y debe proteger su capacidad de razonar y de escoger. Creo que ésta es, en alguna medida, la esencia del tratamiento especial que le debemos dar a los datos personales que nos llevan a la necesidad de una definición clara, de previsiones normativas que se cumplan en todas las fases del proceso, recolección, tratamiento, transmisión, almacenamiento de datos y acceso a los archivos de los mismos y claro está, a sanciones específicas que realmente sean capaces de disuadir al trasgresor.

CUARTA. Es de vital importancia que los gobiernos tomen las medidas correspondientes para regular este aspecto, más allá de los beneficios comerciales que represente o por cumplir con tratados internacionales suscritos, sino más bien con el convencimiento que está legislando a favor del ciudadano.

QUINTA. El mayor desafío de las democracias de América Latina y principalmente de México es, por un lado, garantizar el acceso a la población a todas las fuentes de información disponibles y las nuevas tecnologías; pero también, por otro lado, garantizar el respeto de los derechos humanos fundamentales, específicamente los derechos que tienen que ver con estas materias.

SEXTA. En nuestro país no contamos con un marco normativo comprensivo que considere tanto al sector público como al privado en su conjunto, sobre la protección de los datos personales; por tanto, es imprescindible el diseño de una ley de protección de los datos personales. Una ley de esta naturaleza deberá hacerse cargo de proteger al individuo en su dimensión de consumidor y, al mismo tiempo, proteger al mercado, a fin de asegurar una economía que pueda objetivamente basarse en la confianza documentada.

SÉPTIMA. Es necesario distinguir conceptual y normativamente que la naturaleza de los datos puede ser diversa y por tanto su recolección, tratamiento y

transmisión suponen medidas acordes al impacto que puede llegar a tener su difusión o mal uso de los mismos. El objetivo de una ley de datos personales consiste en reglamentar, sin entorpecer, las formas de circulación, garantizando siempre y por encima de todo, el derecho a la privacidad de los individuos; esto es, la regulación del derecho a la autodeterminación informativa de las personas, estableciendo su ámbito de aplicación en las bases de datos, estén o no automatizadas.

OCTAVA. Sin una protección adecuada de los datos personales, todos perdemos un derecho fundamental: la privacidad, misma que siempre irá de la mano de la libertad, ambas condiciones para la democracia.

NOVENA. En sectores altamente sensibles en donde la información de las personas es considerada primordial, como el sector salud o el laboral, se contemple la posibilidad de incluir aspectos de privacidad y protección de datos en el ámbito de sus respectivas leyes y reglamentos, en la medida en que se vaya incrementando el uso del Internet en México y de acuerdo a las necesidades específicas que la sociedad vaya requiriendo.

DÉCIMA. Resulta indispensable crear conciencia en la ciudadanía sobre los riesgos que existen al no existir un control adecuado de los datos personales que circulan en Internet, debiendo incluir el conocimiento previo informado que algunos sectores como la industria no están interesados en preservar la ley.

DÉCIMA PRIMERA. Es emitente incluir como bien jurídico dentro del Código Penal a la privacidad y a los demás derechos personalísimos y las diversas formas de afectación que existen, por lo que se debe tipificar como delito el acceso ilegítimo a sistemas informáticos, así como penalizar los casos de tratamiento y uso ilegítimo de información personal sensible.

DÉCIMA SEGUNDA. Se debe crear conciencia entre la ciudadanía de la importancia del resguardo real que deben tener sus datos personales, así como de los riesgos que acarrea el uso indiscriminado de éstos.

5. ANEXO ÚNICO.

Tomado del artículo publicado por Jorge Machado, Vladimir Levin, autor del más grande fraude electrónico:[1]

Vladimir Levin, un graduado en matemáticas de la Universidad Tecnológica de San Petesburgo, Rusia, fue acusado de ser la mente maestra de una serie de fraudes tecnológicos que le permitieron a él y la banda que conformaba, substraer más de 10 millones de dólares, de cuentas corporativas del Citibank.

En 1995 fue arrestado por la Interpol, en el aeropuerto de Heathrow, Inglaterra, y luego extraditado a los Estados Unidos.

Las investigaciones establecieron que desde su computadora instalada en la empresa AO Saturn, de San Petersburgo, donde trabajaba, Levin irrumpió en las cuentas del Citibank de New York y transfirió los fondos a cuentas aperturadas en Finlandia, Israel y en el Bank of America de San Francisco.

Ante las evidencias y manifestaciones de sus co-inculpados, Vladimir Levin se declaró culpable. Uno de sus cómplices, Alexei Lashmanov, de 28 años, en Agosto de 1994 había hecho alarde entre sus conocidos, en San Petersburgo, acerca de sus abultadas cuentas bancarias personales en Tel Aviv, Israel.

Estos conspiradores habían obtenido accesos no autorizados al Sistema de Administración de Dinero en Efectivo del Citibank (The Citibank Cash Management System), en Parsipanny, New Jersey, el cual permite a sus clientes acceder a una red de computadoras y transferir fondos a cuentas de otras

[1] En línea] Disponible: http://www.perantivirus.com/sosvirus/hackers/index.htm, 15 de enero de 2006.

instituciones financieras, habiendo realizado un total de 40 transferencias ilegales de dinero.

Lashmanov admitió que él y sus cómplices había transferido dinero a cinco cuentas en bancos de Tel Aviv. Incluso trató de retirar en una sola transacción US $ 940,000 en efectivo de estas cuentas.

Otros tres cómplices, entre ellos una mujer, también se declararon culpables. Esta última fue descubierta "in fraganti" cuando intentaba retirar dinero de una cuenta de un banco de San Francisco. Se estima en un total de 10.7 millones de dólares el monto substraído por esta banda.

Las investigaciones y el proceso tuvieron muchas implicancias que no pudieron ser aclaradas ni siquiera por los responsables de la seguridad del sistema de Administración de Dinero en Efectivo, del propio Citibank. Jamás se descartó la sospecha de participación de más de un empleado del propio banco.

A pesar de que la banda substrajo más de 10 millones de dólares al Citibank, Levin fue sentenciado a 3 años de prisión y a pagar la suma de US $240,015.00 a favor del Citibank, ya que las compañías de seguros habían cubierto los montos de las corporaciones agraviadas.

Los técnicos tuvieron que mejorar sus sistemas de seguridad contra "crackers" y Vladimir Levin ahora se encuentra en libertad.

6. BIBLIOGRAFÍA:

1. ANIBAL A. Pardini Derecho de Internet, Ed. La Rocca, 2002.

2. ARAGÓN REYES Manuel y Fernández Esteban María Luisa. Incidencia de Internet en los Derechos Fundamentales. Edita Banco Santander Central Hispano – Asesoría Jurídica del Negocio – C/ Alcalá 49 – 28014 Madrid.

3. BERLO, David K. El proceso de la comunicación*;* Biblioteca Nuevas Orientaciones de la Educación, Buenos Aires, Argentina, 1973.

4. BINI, Rafael, El Internet, Ed. Sagitario, España, 1997.

5. BRIGGS, Asa. De Gutemberg a Internet, Narrativa y ensayo. Ed. Taurus, El Colegio de México, 2007, p. 95

6. CANALES MENDEZ, G. Javier, Gran Diccionario Jurídico De Los Grandes Juristas, 1ª Ed. México.

7. CASAS, Fray Bartolomé de las, El Memorial, México, FCE, 1974.

8. CUELLO Calón, Eugenio. Derecho Penal. Parte General, Tomo I, 9ª Ed., Editora Nacional, México, 1961.

9. DAVARA RODRÍGUEZ, Miguel Ángel, Manual de Derecho Informático. Ed. Arazandi, Pamplona España, 1993.

10. DIAZ DEL CASTILLO, Bernal, Historia verdadera de la conquista de la Nueva España, 3 v., México, Robredo, 1939. Véase además la edición preparada por J. Ramírez Cabañas, 2 v., México, Porrúa, 1955. Hay otras ediciones.

11. GODED, Jaime, *Antología sobre la comunicación humana;* Lecturas universitarias, México, Núm. 25.

12. JIMENEZ de Asúa, Luis, Principios de Derecho Penal. La Ley y el Delito, 3ª ed., Ed. Sudamericana, Buenos Aires, 1990.

13. LEON-PORTILLA, Miguel, La Visión de los Vencidos, 26ª reimpresión, UNAM, México, 2005.

14. LEÓN PORTILLA, Miguel, La Filosofía náhuatl, estudiada en sus fuentes, México, Instituto Indigenista Interamericano, 1956.

15. LOPEZ Betancourt, Eduardo. Teoría del Delito, Editorial Porrúa, Cuarta Edición, 1997, México.

16. LOPEZ DE GÓMARA, Francisco, Historia de la conquista de México, introducción y notas de Joaquín Ramírez Cabañas, 2v., México, Editorial Robredo, 1943.

17. LOZANO, José Maria, Estudio Del Derecho Constitucional Patrio, Porrúa, México, 1987.

18. MAGGIORE, Giuseppe, Derecho Penal. I. 5ª Ed., Ed. Temis, Bogotá, 1989.

19. MÁRQUEZ RÁBAGO Sergio R. Evolución Constitucional Mexicana, Porrúa, México, 2002.

20. MARTINEZ BULLE GOYRI Víctor M. Genética Humana y Derecho a la Vida Privada, UNAM, México, 2004.

21. MEJAN, C. Manuel, El Derecho a la intimidad, Ed. Porrúa, México, 1996.

22. NORIEGA CANTU, Alfonso, Lecciones de Amparo. Porrúa, México, 1980.

23. PALAZZI, Pablo A. Delitos Informáticos, Ad-Hoc, Buenos Aires, 2000.

24. PALAZZI, Pablo Andrés, El Derecho y la sociedad de la información, la importancia de Internet en el mundo actual, Ed. Porrúa, México, 2007, p. 46

25. PÉREZ Luño, Antonio E. *Informática y protección de datos personales*, Centro de Estudios Constitucionales, Madrid, 1993 (Cuadernos y Debates, núm. 43).

26. PISCITELLI Alejandro, Internet la imprenta del siglo 21, Ed. Gedisa Mexicana, ed. 2005, Colección Cibercultura/Gedisa

27. STEFANO, Rodotá, Democracia y protección de datos, Italia, 2004, Traducción revisada por José Luis Piñar Mañas.

28. ROMERO COLOMA, Aurelia Ma. Derecho a la Información y la Libertad de Expresión. Ed. Bosh, Madrid, 1984.

29. ROJAS CABALLERO, Ariel Alberto, Las Garantías Individuales en México, Porrúa, México, 2002.

30. SÁEZ, CAPEL José, El derecho a la intimidad y las intervenciones telefónicas, en JA, 22/7/98.

31. TÉLLEZ VALDÉZ Julio, Derecho Informático, Mc Graw-Hill. México, 2003.

32. TENA RAMÍREZ, Felipe, Leyes Fundamentales de México, 1808-1991, 16a. ed., Porrúa, México, 1991.

33. WALKER, Andy. Seguridad, Spam spyware y virus, Ed. Anaya.

34. WIENER, Norbert. Cibernética y sociedad, FCE, México, 1980.

7. LEGISLACIÓN:

1. Constitución Política de los Estados Unidos Mexicanos
2. Constitución del Estado de México
3. Ley Federal de Acceso a la Información Pública
4. Ley de informática, estadística y geografía
5. Ley Federal del Derecho de Autor
6. Ley Federal de Protección al Consumidor
7. Ley de Protección de datos personales del Estado de Colima
8. Ley de Protección de datos personales del Estado de Jalisco
9. Ley de Protección de Datos Personales para el Estado y los Municipio de Guanajuato.
10. Ley de Transparencia y Acceso a la Información Pública del Estado de México
11. Ley de Transparencia y Acceso a la Información Pública del Estado de Sinaloa
12. Ley de Transparencia y Acceso a la Información Pública del Estado de Coahuila
13. Ley del Servicio Postal Mexicano
14. Ley de Vías Generales de Comunicación.
15. Ley de Imprenta
16. Código Penal Federal
17. Código Penal para el Distrito Federal
18. Código de Procedimientos Civiles en el Distrito Federal.
19. Código de Comercio
20. Código Federal de Instituciones y Procedimientos Electorales
21. Reglamento de Transparencia en materia de datos personales

22. Reglamento de Transparencia y Acceso a la Información de la Comisión Nacional de Derechos Humanos.

23. Ley Orgánica de Protección de Datos de España.

24. Declaración América de Derechos del Hombre.

25. Declaración Universal de Derechos Humanos.

26. Convención Internacional sobre los Derechos del Niño.

27. Pacto Internacional de Derechos Civiles y Políticos

8. PROYECTOS DE LEY:

1. Proyecto de Ley Federal de Protección de Datos Personales, presentado por el Senador Antonio García Torres del Partido Revolucionario institucional (PRI), ante el Senado de la República del 14 de febrero de 2001.

2. Proyecto de Ley de Protección de Datos Personales presentada por el Diputado Miguel Barbosa Huerta, del grupo parlamentario del Partido de la Revolución Democrática (PRD) en sesión de la Cámara de Diputados, del día 6 de septiembre de 2001.

3. Proyecto de la Ley Federal de Protección de Datos Personales presentada ante la Cámara de Diputados por el Diputado Jesús Martínez Álvarez del Grupo Parlamentario de Convergencia en sesión del 1º de diciembre de 2005.

9. PUBLICACIONES:

1. CANTOR, Damián: “Investigan la venta de bases de datos de la ANSeS y la D. G. I.” Y PALAZZI, Pablo: “Las leyes no dan cuenta de los cambios de los delitos”, ambos publicados en el diario *Buenos Aires Económico,* del 12/I/98.

2. *Derecho y Nuevas Tecnologías*, Año 1, No. 0, Ad-Hoc, Buenos Aires, 1998.

3. Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca, Revista Jurídica Ius Et Praxis *“DERECHO A LA AUTODETERMINACIÓN INFORMATIVA Y LA ACCIÓN DE HABEAS DATA EN IBERO AMÉRICA”,* Chile 1997, año 3, No. 1.

4. *Informática y Derecho,* vol. 6, Depalma, Buenos Aires, 1998.

10. SITIOS DE INTERNET:

1. Cristos Velasco San Martín y otro “Spyware, el software espía”, marzo de 2005 (En línea). Disponible: www.enterate.unam.mx/Articulos/dos/enero/protecci:htm

2. DAVARA RODRÍGUEZ, Miguel Ángel, “Privacidad y Protección de datos personales en Internet” Octubre, 2003, [En Línea] Disponible: http://www.davara.com/, Febrero 2005.

3. *“La privacidad de los menores y el marketing a través de Internet”* disponible en noticias.jurídicas.com, @rea Digital –APTICE.

4. MACHADO, Jorge, Vladimir Levin, autor del más grande fraude electrónico., [En línea] Disponible: http://www.perantivirus.com/sosvirus/hackers/index.htm, 15 de enero de 2006

5. MENDOZA LUNA, Amílcar. *“Los cookies: ¿amenaza a la privacidad de información en la Internet?* www.derecho.org/redi

6. ROJAS Angélica, Protección de la Privacidad, Octubre 2001 (En línea). Disponible: www.utem.d/cyt/derecho/proteccion.html

10.1 SITIOS OFICIALES:

7. Directiva 95/46 del Parlamento Europeo y del Consejo del 24 de Octubre de 1995 en la siguiente dirección: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=es&numdoc=31995L0046&model=guichett

8. The Freedom of Information and Protection of Privacy Act de la Provincia de British Columbia (La libertad de información y Protección de la privacidad. Ley de la provincia de la Columbia Británica) se encuentra disponible en la siguiente dirección: http://www.legis.gov.bc.ca/37th3rd/3rd_read/gov07-3.htm

9. OCDE en la siguiente dirección: **http://www.oecd.org/EN/document/0,,EN-document-44-1-no-24-320-44,00.html**

10. http://microasist.com.mx/noticias/tp/jodtp2607.shtml.

11. http://microasist.com.mx/noticias/.

12. http:/www.perantivirus.com/sosvirus/hackers/index.htm

13. www.micasa.gob.mx

14. www.cndh.org.mx

15. http://www.buródecredito.com.mx

16. ucs@profeco.gob.mx

17. www.profeco.gob.mx

Páginas del Congreso de la Unión:

18. senado.gob.mx/index.php

19. diputados.gob.mx/leyinfo/compila/reflix.htm

20. http://gaceta.cddhcu.gob.mx

21. http://www.cddhcu.gob.mx/servicios/datorele/cmprtvs/1po2/set/2.htm

22. http://www.ftc.gov y http://www.rcmp-grc.gc.ca/html/scams-f.htm

Esta tesis se concluyó en el mes de julio de 2007, bajo la dirección del LIC. MARIO ALBERTO MARTELL GOMEZ, Profesor de la Escuela de Derecho de la Universidad Salesiana.