UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES

ARAGÓN

LICENCIATURA EN DERECHO

TRABAJO POR ESCRITO QUE

PRESENTA:

ANA CELIA BELMONT PÉREZ

TEMA DEL TRABAJO:

"PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES EN INTERNET Y REDES DE CÓMPUTO MEDIANTE LA CREACIÓN DE UNA LEY FEDERAL EN MÉXICO".

EN LA MODALIDAD DE "SEMINARIO DE TITULACIÓN COLECTIVA"

PARA OBTENER EL TÍTULO DE:

LICENCIADO EN DERECHO

FES Aragón

MÉXICO, ARAGÓN, 11 DE ENERO DE 2008

DEDICATORIAS

A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Por el honor que me brindó al dejarme pertenecer a ella, por sus maestros e instalaciones.

A LA FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

Por sus instalaciones y maestros.

A MIS PROFESORES

Por transmitirme todo su conocimiento y sabiduría.

A MIS PADRES

Por su apoyo incondicional, su cariño y brindarme siempre lo mejor.

A MIS HERMANITAS

Por sus consejos y por ser mis mejores amigas.

A TODOS... GRACIAS!

PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES EN INTERNET Y REDES DE CÓMPUTO MEDIANTE LA CREACIÓN DE UNA LEY FEDERAL EN MÉXICO

ÍNDICE

PÁGINA

PÁGINA

CAPÍTULO 2
MARCO JURÍDICO

CAPÍTULO 3
REGULACIÓN JURÍDICA DE LOS DATOS PERSONALES EN INTERNET

INTRODUCCIÓN

Con el presente trabajo de investigación denominado “PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES EN INTERNET Y REDES DE CÓMPUTO MEDIANTE LA CREACIÓN DE UNA LEY FEDERAL EN MÉXICO”, se pretende dar una idea general y actual de las implicaciones y dificultades que la aparición de Internet y el uso de redes de cómputo están generando en la regulación referente a la recolección, tratamiento y cesión de los datos personales.

De ahí que, en el presente texto, nos encontremos frente a las limitaciones y obligaciones que legalmente se están imponiendo con la finalidad de defender distintos derechos, entre los que se encuentra el derecho a la privacidad y la integridad de los datos personales. De tal manera que nos basamos en las leyes vigentes en el momento de hacer la presente investigación utilizando el método deductivo.

Este trabajo de investigación, consta de tres capítulos, los cuales están expuestos de la siguiente manera.

El primer capítulo aborda las generalidades y los conceptos básicos, que ayudarán a comprender el tema a tratar y de igual forma tocará la problemática que nos ocupa; como lo es la privacidad y los datos de las personas.

El segundo capítulo, describe varias disposiciones donde se encuentra regulado el uso de los datos personales, sin embargo, dentro de esta investigación se advierte que en nuestro país, éstas no son suficientes para ofrecer una normatividad idónea y eficaz para regular el uso de Internet y la información de carácter personal que se maneja en los sitios *web.*

Finalmente, el tercer capítulo analiza las iniciativas de ley que ha habido en nuestro país y de las ventajas que traerían consigo si se

aprobaran para el eficaz manejo de los datos de carácter personal en Internet y en las redes de cómputo, por lo que es importante que se implemente un medio de control al respecto, que tutele las garantías individuales de privacidad y el derecho a la intimidad de los ciudadanos.

CAPÍTULO 1
GENERALIDADES

El interés en este capítulo es describir aspectos de importancia para entender la problemática del tema a estudiar, así como algunos conceptos básicos.

1.1 CONCEPTO DE DATO PERSONAL

El ser humano, a lo largo de su existencia, tiene la creciente necesidad de guardar, almacenar información y datos de sus semejantes con distintos objetivos y diversos fines.

Con la influencia de los medios masivos de comunicación a nivel global y los avances tecnológicos de la informática y su libre acceso, han provocado que la información y, en particular los datos de carácter personal, adquieran un valor trascendental, traduciéndose en una nueva forma de poder.

Por lo anterior, para un mayor entendimiento del tema que nos ocupa, se pone a consideración el concepto etimológico y gramatical de la palabra dato, así como la del vocablo personal.

La palabra dato proviene del latín *"datum"*[1] que significa lo que se da. Antecedente necesario para llegar al conocimiento exacto de algo o para reducir las consecuencias legítimas de un hecho. Información dispuesta de manera adecuada para su tratamiento por un ordenador. Mientras que personal, desciende del latín *"personális"*[2], adjetivo perteneciente o relativo a la persona. Propio o particular de ella.

---

[1] Real Academia Española, "Diccionario de la lengua española", Ed. 22, Dirección: www.cargainfo.com, 16 de abril del 2007 18:36 hrs.

[2] *Ídem.*

Analizando los términos anteriormente precisados, se entiende por dato personal o datos de carácter personal, aquellos que contengan cualquier información referente a personas físicas identificadas o identificables, recogida a través de algún procedimiento automatizado, que sea almacenado en ficheros, catálogos o archivos en general.

Por lo anterior, mencionamos que el autor Carlos Correa, señala lo siguiente:

> *"…se entenderá por dato personal toda información acerca de personas naturales que sea susceptible de ser puesta en relación directa o indirecta con individuos determinados."*[3]

Por lo que considerando los conceptos antes precisados, se entiende por dato personal a toda información de personas físicas determinadas o determinables, por lo que estamos a favor del concepto del autor Carlos Correa.

1.1.1 Recopilación de datos personales

Los datos personales empiezan a ser recolectados desde los años setenta, surgiendo numerosos archivos con información de carácter personal, con un conjunto de un mínimo de datos como filiación, fecha y lugar de nacimiento, domicilio particular, estado civil, entre otros; y posteriormente, hasta unos datos aún más específicos como raza, religión, inclinaciones políticas, ingresos, cuentas bancarias, historia clínica, etcétera.

Toda esta información personal, al ser recopilada en diferentes centros de acopio, como lo son los registros civiles y censales, parroquiales, médicos, laborales, académicos, deportivos, ya no exclusivamente por medios manuales, sino por sistemas automatizados, provocan una gran

---

[3] CORREA, Carlos M., "Derecho Informático",editorial Depalma, Buenos Aires, 1987, p. 284.

concentración de información y una instantánea disponibilidad de ésta para diferentes propósitos.

Por lo que en el siguiente punto, se habla de la destinación y de las implicaciones que se le da a esta información.

1.1.2 Destinación e implicaciones

Posteriormente de que se han acopiado los datos personales, éstos se ven vulnerados, dependiendo del manejo del que puedan ser objeto, los cuales pueden ser variados, como los fines publicitarios, comerciales, fiscales y hasta policíacos.

Convirtiéndose de esta forma en un instrumento de opresión y mercantilismo. La pluralidad de supuestos de indefensión ante esta problemática induce a que los individuos puedan estar en un sinnúmero de situaciones que alteren sus derechos fundamentales en sociedad, como puede ser la discriminación, manipulaciones, persecuciones, presiones y asedios, todo ello al margen de un control jurídico adecuado que pueda regularlo.

Esta problemática se incrementa ante el gran número de usuarios del Internet, mediante el uso de servidores que se ofrecen en línea, donde se maneja un sin número de datos incluyendo en estos, claro, los de carácter personal.

Es por eso que, en el siguiente tema abordaremos el concepto de Internet y lo referente a los servicios que en él se ofrecen, al mismo tiempo que tiene una gran importancia para el presente trabajo de investigación.

1. 2 DEFINICIÓN DE INTERNET

Existen diversos conceptos y definiciones para describir a la Internet, aunque para el presente trabajo de investigación basta con resumir que

Internet es una red de ordenadores compuesta por un gran número de subredes interconectadas entre sí, formando una malla que hoy en día se extiende por más de cien países y que es usada por unos treinta millones de usuarios por todo el mundo, permitiendo que éstos se pongan en contacto unos con otros o que todos ellos puedan acceder a determinados recursos comunes, como base de datos, servicios de información, etcétera.

Al respecto, para mayor entendimiento del término, el autor José A. Carballar Falcón, define al Internet de la siguiente manera:

> "…es una red formada por la interconexión cooperativa de redes de ordenadores. Dicho de otra forma, Internet es una red de redes. De hecho, el término Internet procede de las palabras inglesas *interconnection* y *network*; esto es, interconexión y red. Esto viene a significar que Internet son miles de redes interconectadas…"[4]

Por lo que, considerando la definición antes anotada, en síntesis, se entiende por Internet a la red de redes, formada por la interconexión de redes de ordenadores, por lo que estamos de acuerdo con el concepto manejado por el autor.

Ahora bien, en los siguientes temas se señalarán elementos integrantes de la computadora para entender su funcionamiento.

1. 3 SISTEMA INFORMÁTICO

Para mayor entendimiento, es de importancia señalar algunos aspectos básicos de la computadora y su funcionamiento a nivel estructural, explicando brevemente lo que son los elementos *hardware* y el *software.*

[4] CARBALLAR FALCÓN, José A., "Internet Libro del Navegante", Ediciones RA-MA, Tercera Edición, España, 2002, p. 6.

1.3.1 *Hardware*

El *hardware* está constituido por las partes mecánicas, electrónicas y electromecánicas, como lo es la estructura física de las computadoras, encargada de la captación, almacenamiento y procesamiento de la información, así como la obtención de resultados; es decir, el *hardware* es la base física en la cual existe el software y es la que abarca todas las piezas de la computadora como el teclado, el monitor, etc.

1.3.2 *Software*

En cambio el *software,* se refiere a los programas y datos almacenados en una computadora, constituye la estructura lógica que permite la ejecución del trabajo que se ha de realizar; por medio de los datos y programas, que son los que dan instrucciones para realizar tareas al *hardware*.

1.5. SERVIDORES

Los servidores o servicios en línea, han proporcionado a los usuarios de Internet diversos métodos para intercambiar mensajes, archivos y opiniones, entre otros tipos de información. Estos servidores incluyen organizaciones como *American Online, Prodigy, Yahoo, Hotmail* entre otros; dentro de los cuales a su vez se ofrece el servicio de correo electrónico.

Ahora bien, para mayor abundamiento e interés del tema en estudio, es necesario describir qué es un correo electrónico y sus características.

1.5.1 De correo electrónico

El correo electrónico es uno de los servicios más utilizados de los que se ofrecen en Internet, al correo electrónico se le conoce también como *e-*

mail o simplemente *mail* (correo en inglés). La finalidad de este servicio es la de permitir el intercambio de mensajes entre los usuarios de la red.

El correo electrónico consiste en el intercambio de mensajes entre los usuarios de la red, mediante el cual cualquier usuario puede comunicar sus ideas claramente como lo haría por medio de una carta y tan rápido como lo haría mediante una llamada telefónica.

Con el correo electrónico no sólo se pueden enviar textos, sino también audio, video, gráficos y archivos de cualquier tipo.

1.5.2 El correo electrónico como dato personal y su problemática

El servicio del correo electrónico es un claro ejemplo de la problemática en estudio y de las consecuencias que trae consigo la recopilación y el almacenamiento de los datos personales en un servidor y de la vulnerabilidad en la que se ve expuesta nuestra privacidad al no haber un sistema jurídico adecuado que regule tal situación.

Como ha quedado precisado, el correo electrónico o *e-mail,* es un servicio que permite la creación y transmisión de mensajes entre sus usuarios, convirtiéndose así en un medio de comunicación muy eficaz, económico y de los más utilizados en Internet.

Sin embargo, no se garantiza que los mensajes lleguen siempre a su destino correcto, ni que se informe de este hecho al remitente o que éste último sea quien dice ser.

Por otro lado, es igual de alarmante saber que la dirección de correo electrónico es la forma más frecuente de registrar la identidad de una persona en Internet, la cual puede ser observada en múltiples lugares de la red y conseguirse fácilmente sin nuestro conocimiento, pues es importante recordar, que al momento de obtener nuestra dirección de correo electrónico

se requiere llenar un cuestionario donde proporcionamos una serie de datos, donde se incluyen los de carácter personal.

Su aspecto más inquietante se fundamenta en que pueda servir de base para la confección de perfiles personales (temas de interés, inclinaciones políticas o culturales o de ideología, orientación sexual) a partir de nuestra pertenencia a grupos de distribución o de discusión. En este caso, nos exponemos a que los datos proporcionados puedan ser recopilados sin informar al afectado y sin obtener su consentimiento utilizándolos para otros fines.

De la misma forma, el uso del *e-mail* o correo electrónico, puede desencadenar problemas en las relaciones profesionales y laborales, es así que el autor Aníbal Pardini considera:

> *"Las amenazas a la privacidad son más sutiles y se han planteado, generalmente, en el uso de los e-mails (aunque cada vez se ponga más énfasis en la privacidad de la navegación por Internet); al respecto, pueden ser establecidos algunos límites, cuya elección tendrá como parte del análisis a quienes intervengan relacionándose mediante esta forma de comunicación. De esta manera las relaciones establecidas entre un alumno y su profesor no requerirán el mismo nivel de seguridad que las efectuadas entre un abogado y su cliente…"*[5]

El autor se refiere con esto a que, en el caso del abogado con su cliente, se requiere de mayor diligencia por parte del profesional, o la autorización de su cliente para utilizar este vulnerable medio de comunicación.

---

[5] PARDINI, Aníbal A., "Derecho de Internet", Ediciones La Roca, Buenos Aires, 2002, pp. 67 y 68.

Por lo antes visto, es de importancia observar que este tipo de comunicación entre personas sea protegido y regulado, ya que quedamos en una total indefensión al ser posibles víctimas del abuso del que pudiera ser objeto la información que proporcionamos en este servicio, de tal manera que en el siguiente tema se abordará la estrecha relación que existe entre éste servicio, que es el correo electrónico y la privacidad, considerada un derecho por la ley.

1.6 DERECHO A LA PRIVACIDAD

El derecho a la privacidad es el derecho fundamental de la personalidad, el cual consiste en la facultad que tienen los individuos para no ser interferidos por persona o entidad alguna, en las actividades que legítimamente han decidido mantener fuera del conocimiento público; este derecho se materializa al momento de proteger del conocimiento ajeno el hogar, la oficina o el ámbito laboral, los expedientes médicos, legales y personales, las conversaciones y reuniones privadas, la correspondencia, la intimidad sexual y todas aquellas que se llevan a cabo en lugares no públicos.

Este derecho a la vida privada, surge por el desarrollo de los medios de información, del aumento de datos y hechos noticiosos.

El derecho a la privacidad, contiene algunas características que el autor Ernesto Villanueva puntualiza:

“a) es un derecho esencial del individuo, ya que se trata de un derecho inherente al individuo con independencia del sistema jurídico que lo tutela.

b) es un derecho extrapatrimonial, porque no se puede comerciar o intercambiar como los derechos de crédito, ya que forma parte de la personalidad del individuo, por lo que también es intransmisible e irrenunciable, y

c)es un derecho imprescriptible e inembargable, ya que ha dejado de ser un tema exclusivo de la doctrina para pasar a formar parte del derecho positivo."[6]

En resumen, la vida privada es un derecho intransmisible, irrenunciable, imprescriptible e inembargable propio del individuo, que nació a consecuencia del desarrollo de los medios de información; pero para abundar en este aspecto, en el siguiente tema se define a la privacidad y su relación con los datos de carácter personal.

1.6.1 Concepto de privacidad

Con relación al tema anterior y al estudio de los datos de carácter personal, debemos precisar el concepto de privacidad, la que está íntimamente ligada con el tema en estudio.

La privacidad esta definida por tres grandes sistemas jurídicos como lo son el derecho romano, el derecho germánico y el *common law*[7].

La privacidad, para el derecho romano es el derecho a comunicarse libremente con cualquier persona sin el temor a ser vigilado; para el derecho germánico es el derecho a controlar el acceso de la información personal y para el *common law*, la privacidad es el derecho a disfrutar de la vida privada libre, sin interrupciones o intromisiones indeseadas.

Por ello, es de suma importancia ver que cada vez más, se recopilan datos personales en las empresas comerciales y privadas, y de igual forma es empleada en los órganos gubernamentales, cuyos servicios y diversos trámites se ofrecen en línea; donde los datos proporcionados por los

---

[6] VILLANUEVA, Ernesto, "Temas Selectos de Derecho de la Información", Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, Primera Edición, México, 2004, p.p. 37 y 38.

[7] **Término usado para referirse al grupo de normas y reglas de carácter jurídico no escritas, pero sancionadas por la costumbre o la jurisprudencia, que son fundamento ineludible del derecho de los países anglosajones.**

ciudadanos, instituciones y empresas depositan al llevar a cabo trámites gubernamentales.

Por lo que día a día, más asuntos se gestionan y gradualmente se llevarán a cabo trámites gubernamentales completamente en línea y toda la información generada, estará contenida, en su totalidad, en sistemas electrónicos y bases de datos “propiedad” del gobierno.

Es así, que el individuo esta constantemente en una total indefensión, al verse sin una figura jurídica en la cual poder respaldarse y aplicar, la cual vele por el derecho a la privacidad, en el caso de que se utilice la información proporcionada por éste para fines distintos para los cuales fueron requeridos.

Por lo que en el siguiente tema se describen los principios básicos que se deben tomar en cuenta antes de legislar sobre los datos personales.

1.6.2 Principios básicos de la legislación de datos personales

El estudio comparado que han hecho varios autores sobre la materia, permitió detectar diez principios básicos para la regulación de los datos personales, como los describe Correa:

1. *Principio de la justificación social,* el cual instituye que la recolección de datos deberá tener un propósito general y usos específicos.

2. *Principio limitación de la recolección,* establece que los datos deberán ser recolectados por medios lícitos, es decir, el individuo de su consentimiento y tenga conocimiento del fin que tendrán los datos proporcionados, los cuales tendrán que limitarse al mínimo necesario para el designio perseguido por el acopio.

Lo cual quiere decir, por ningún motivo, salvo casos justificables, se deberán conservar datos relativos a circunstancias totalmente personales,

como lo son la raza, religión, opiniones políticas, salud, relaciones sexuales etcétera.

3. *Principio calidad y fidelidad de la información,* con él, los datos recolectados deberán ser exactos, actuales y completos.

Con este principio se pretende evitar algún tipo de error que resulte por los datos mal registrados, de ahí el interés que éstos sean rectificados, actualizados o cancelados en su caso.

4. *Principio de especificación del fin,* el cual establece que en el momento de la recolección de datos se especifiquen los fines para los cuales son registrados.

5. *Principio de confidencialidad,* instituye que el acceso a estos datos a terceros sólo se hará con el consentimiento del sujeto de los datos o con una autorización legal.

6. *Principio de salvaguarda de la seguridad,* de conformidad con él, que es obligación de la entidad responsable del registro de los datos de carácter personal, el adoptar medidas de seguridad adecuadas para protegerlos contra posibles pérdidas, alteraciones, destrucciones o acceso no autorizado.

7. *Principio de política de apertura,* garantiza la transparencia de acción de la administración pública y privada con relación al procesamiento de datos personales. Esta transparencia queda asegurada por el conocimiento del público de su existencia, sus fines, métodos de operación de los registros y usos.

8. *Principio de la limitación en el tiempo,* de conformidad con este principio, los datos no se deben conservar más tiempo del que se requiere para el objeto con los que fueron recolectados.

9. *Principio de control,* establece que conviene la existencia de un órgano de control, que sea responsable de la seguridad de los principios antes mencionados.

10. *Principio de participación individual,* establece el derecho de acceso a los datos que se concede al individuo, los cuales consisten en:

a) obtener datos que le atañan de la entidad responsable,
b) debe ser informado dentro de un tiempo razonable,
c) oponerse a cualquier dato que le pertenezca, el cual debe quedar registrado,
d) obtener datos de su persona,
e) que se le informen las razones de porque se le deniega su derecho de acceso,
f) oponerse a la negativa.[8]

De esta manera, se puede observar en nuestro siguiente tema que, los principios básicos expuestos, no son considerados por lo que hace al almacenamiento y acopio de información personal en el correo electrónico o el también llamado *e-mail*.

1.7 FIGURAS JURÍDICAS APLICABLES

Son variadas las figuras de índole jurídico con las que se ha intentado regular en distintos países este aspecto, preocupados por el mal uso que tienen los datos personales en la web y redes de cómputo.

Tocante a ello, en el ámbito internacional se encuentran la Declaración Universal de los Derechos Humanos, los cuales consideran que es un derecho la vida privada, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos y la Convención de Derechos del Niño; consideradas por el artículo 133

[8] CORREA, Carlos M., "Derecho Informático", Editorial Depalma, Buenos Aires, 1987, pp. 257-262.

Constitucional Ley Suprema de la Unión. Los derechos personales, los derechos patrimoniales, libertades públicas y privadas en Francia y derecho a la privacidad en los países anglosajones; derecho a la intimidad y al honor en las personas en España, y en particular en nuestro país, las garantías individuales y sociales, así como los denominados “Lineamientos de Protección de Datos Personales”, y en específico en el Estado de Colima existe la llamada “Ley de de Protección de Datos Personales del Estado de Colima”, cuyo contenido se analizará en el capítulo siguiente.

Al respecto, debe considerarse que, lo verdaderamente importante es el hecho de 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, como se a anotado, es un derecho fundamental.

Es así que, al hablar de derechos por consiguiente se debe hacerlo también de sus respectivas excepciones, como se observa en el punto siguiente.

1.7.1 Derechos y excepciones

Es cierto que al hablar de una regulación jurídica implica a su vez mencionar establecidos derechos y excepciones muy particulares como lo son:

a) Derecho de acceso.- Permite a los interesados conocer las instituciones y el tipo de información que disponga sobre su persona.

b) Derecho de rectificación.- Es el que admite solicitar al individuo una modificación en los términos de alteración o ampliación, o una eliminación o cancelación de aquella información o datos que, referidos a su persona, considere como inexactos o irrelevantes.

c) Derecho del uso conforme al fin.- Consiste en que las personas tienen el derecho a exigir que su información nominativa sea destinada para los fines por los que la proveyó.

d) Derecho para la prohibición de interconexión de archivos.- Este derecho se refiere a que ninguna base de datos pueda consultarse y vincularse con otras.

El incumplimiento a estos derechos puede generar sanciones ya sea de carácter administrativo, civil e incluso penal, dependiendo de los casos en particular.

En cuanto a las excepciones a estos derechos, Julio Téllez indica que:

> *"son las 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, entre otros."*[9]

Es decir, que si la seguridad del Estado en ámbitos como lo son la economía, la salud y persecución de delitos, dependiera del incumplimiento a los derechos antes mencionados, se deberá aplicar una excepción, lo que se considera óptimo, siempre y cuando sea en beneficio de la sociedad.

Es por ello que en lo sucesivo, se analizan diversos lineamientos y leyes ya existentes en diversas naciones, que deberán de tomarse como base y fundamento para en su momento, hacer una ley eficaz en nuestro país que regule y proteja los datos personales y nuestra privacidad.

---

[9] TELLEZ VÁLDEZ, Julio, "Derecho Informático", Editorial Mc Graw Hill, Tercera Edición, México, 2003, p. 62.

CAPÍTULO 2
MARCO JURÍDICO

En este capítulo, se mencionan diversas regulaciones que existen sobre la protección de los datos de carácter personal a nivel internacional, así como de los organismos interesados en la problemática y el marco constitucional que consagra el bien jurídico de la privacidad en nuestro país.

2.1 LEGISLACIÓN INTERNACIONAL

En el ámbito internacional existe la figura de la Organización para la Cooperación y Desarrollo Económicos (OCDE)[10], aquel es un organismo multilateral que a elaborado importantes lineamientos y políticas sobre la privacidad y protección de datos, siendo referentes al contexto del comercio electrónico, entre los más importantes. Estos lineamientos no son de carácter obligatorio para muchos países en la esfera del derecho internacional público, sin embargo, son principios generalmente aceptados como recomendaciones de carácter voluntario en algunos gobiernos, empresas, organizaciones y usuarios individuales de países miembros de la OCDE, como lo es México.

Los principios de la OCDE que regulan la protección de la privacidad y los flujos transfronterizos de datos personales del 23 de septiembre de 1980, contienen ocho principios de aplicación nacional y cuatro de aplicación internacional que son considerados como los estándares mínimos a seguir para la obtención, el procesamiento de datos y el libre flujo transfronterizo de datos para los sectores público y privado.

Los ocho principios de aplicación a nivel nacional son los siguientes:

1. El principio de "Límite de Obtención", consiste en la imposición de límites para la obtención de datos personales mediante medios apropiados y

[10] CORREA, Carlos M., Derecho Informático, Editorial Depalma, Buenos Aires, 1987, p. 266.

legales haciéndolo del conocimiento y teniendo el consentimiento del individuo; lo cual impide que el responsable del acopio de la información se exceda en el acopio de la información requerida por éste y además sin carecer del consentimiento de la persona.

2. El principio de "Calidad de los Datos", advierte la importancia de asegurar la exactitud, totalidad y actualización de los datos; es decir, que la información almacenada debe ser fidedigna.

3. El principio del "Propósito de Descripción", consiste en especificar el propósito de recabar información en el momento en el que se lleva acabo la recolección y el subsecuente uso limitado del cumplimiento de dicho propósito u otros que no sean incompatibles con aquellos propósitos especificados en cada ocasión; es decir, que se debe comunicar al individuo de la intención con que se hace el almacenamiento de la información y que uso se le dará en el futuro.

4. El principio del "Límite de Uso", indica que no se deben divulgar los datos personales o aquellos utilizados para propósitos distintos a los contemplados en el principio anterior, excepto:

a) el consentimiento sobre la materia de datos;
b) mediante una autoridad contemplada en ley.

5. El principio de "Protección a la Seguridad", consiste en proteger los datos personales e información, mediante mecanismos razonables de seguridad en contra de riesgos tales como pérdida, acceso no autorizado, destrucción, utilización, modificación o divulgación de datos;

6. El principio de "Imparcialidad", establece políticas generales de imparcialidad sobre desarrollos, prácticas y políticas con respecto a los datos personales, asegurando la transparencia en el proceso de obtención de información y estableciendo los propósitos para su utilización;

7. El principio de "Participación Individual", consiste en el derecho que tiene un individuo de: obtener del controlador de datos la confirmación de tener o no los datos del individuo; que el controlador de datos se lo haya comunicado en un tiempo y forma razonable; obtener respuesta del controlador de datos si una solicitud le ha sido negada y tener la posibilidad de impugnarla; tener la posibilidad de impugnar datos personales y si la impugnación resulta exitosa solicitar que los datos sean eliminados, modificados, rectificados o complementados; y

8. El principio de "Responsabilidad", señala la responsabilidad del controlador de datos de cumplir efectivamente con medidas suficientes para implementar los siete principios anteriores.

De tal manera que, bien aplicados estos principios y tomados como pilar principal en la creación de leyes y en específico una ley federal en México, se cubrirían en gran medida las necesidades y lagunas existentes por el avance tecnológico que atraviesa el país, que esta muy por encima del jurídico.

Los cuatro principios de aplicación internacional son los siguientes:

1. Que los países miembros tomen en cuenta las implicaciones que tiene el procesamiento doméstico y la re-exportación de datos personales para otros países miembros;

2. Que los países miembros tomen las medidas apropiadas y razonables para asegurar que los flujos transfronterizos de datos personales incluyendo el tránsito a través de un país miembro sea ininterrumpido y seguro;

3. Que un país miembro se abstenga de restringir los flujos transfronterizos de datos personales entre sí mismo y otro país miembro, excepto cuando este último no haya observado estos lineamientos o cuando la reexportación de dichos datos contravenga su legislación interna de

privacidad. Un país miembro podrá imponer restricciones en relación a ciertas categorías de datos personales para las cuales su legislación doméstica de privacidad incluya regulaciones específicas en vista de la naturaleza de aquellos datos y para los cuales el otro país miembro no proporcione protección equivalente.

4. Los países miembros deberán evitar el desarrollo de leyes, políticas y prácticas en nombre de la protección de la privacidad y las libertades individuales que pudieran crear obstáculos a los flujos transfronterizos de datos personales que pudieran exceder requisitos para dicha protección.

Por lo anterior, nos damos cuenta que el contenido de estas guías sobre privacidad y protección de datos, proveen principios y reglas determinadas a seguir para que los gobiernos adopten políticas de regulación efectivas sobre privacidad y protección de datos, las cuales sirven de base y fundamento para la creación de leyes en materia de privacidad que permitan evitar el mal uso de la información y de los datos personales.

2.1.1 Unión Europea

La privacidad y la protección de datos personales en Internet son temas que internacionalmente se están estudiando y analizando con más detenimiento para su legislación.

Diversas naciones, como algunos estados miembros de la Unión Europea, han considerado los temas de privacidad y protección de datos personales como asuntos prioritarios para legislar, con el propósito de no sólo hacer un alto a bloques comerciales como lo son el TLCAN y el MERCOSUR[11], sino también para tener una medida proteccionista para salvaguardar los derechos y libertades de las personas físicas, en particular del derecho a la intimidad y la libre circulación de datos personales,

[11] TLCAN, Tratado de Libre Comercio de América del Norte y el MERCOSUR, Mercado Común del Sur, es un bloque económico compuesto por Argentina, Brasil, Paraguay y Uruguay.

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.

Por ello, 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", la cual es mejor conocida como la Directiva sobre Privacidad y Protección de Datos, entró en vigor el 25 de octubre de 1998 y su objetivo primordial es proporcionar un marco general de referencia para los países miembros. Esta Directiva establece reglas muy estrictas para la protección del derecho a la privacidad en relación a la obtención y procesamiento de datos personales.

En el artículo 25 de la Directiva, se establece la prohibición de transferir datos de carácter personal a países que no tengan la seguridad adecuada para la protección de estos y, aun y cuando algunos países puedan proporcionar o satisfacer un adecuado nivel de seguridad y protección de los datos personales, dicha Directiva impone obligaciones y restricciones adicionales bastante estrictas para llevar a cabo la transferencia de datos a terceros países.

Esta Directiva, ha sido aceptada en su mayoría, sin embargo ha encontrado muchas dificultades de implementación por parte de algunos estados miembros, por lo que en enero de 2000, la Comisión Europea decidió llevar a cabo procedimientos administrativos para sancionar a países como Francia, Alemania, Holanda, Irlanda y Luxemburgo por no haber comunicado a tiempo las medidas que tomaron para efectuar esta Directiva.

La Comisión Europea, en mayo del 2002, elaboró un cuestionario para enviarlo a los países miembros y estos a su vez le remitieran sus propuestas para una mejor implementación de la Directiva.

Reino Unido, envió parte de sus respuestas a estas interrogantes y sus propuestas, entre otras, fueron principalmente:

1) Que se revisen las definiciones de "datos personales", “datos sensibles”[12] y "sistema de aplicación de datos personales", con el objeto de mejorarlas y hacerlas más estables al momento de ponerlas en práctica;

2) Revisar los arreglos de acceso en la materia, para encontrar un equilibrio entre los intereses de los individuos que proporcionan datos personales y los intereses de los organismos controladores de datos;

3) Mejorar las normas sobre procesamiento de datos personales;

4) Examinar las reglas relacionadas con la transferencia de datos personales a terceros países y establecer criterios más simples y flexibles.

A nivel Internacional, esta Directiva también ha tenido serios problemas de aceptación en países que han adoptado políticas de regulación distintas a los países miembros de la Unión Europea, como es el caso de los Estados Unidos y alguno países Asiáticos.

Por ello, nuestros legisladores deben ser muy cuidadosos al pretender adoptar medidas de protección europeas, las cuales afectarían no solo el comercio exterior sino también las inversiones que se realizan dentro del país y los empleos que generan.

[12] Se consideran los referentes a raza, opiniones políticas, filosóficas o religiosas, pertenencia a sindicatos, antecedentes penales, salud.

2.1.2 Alemania Federal

En la Alemania Federal existe la Ley Federal para la Protección Contra el Uso Ilícito de Datos Personales y entró en vigor un 27 de enero de 1977.

Esta ley esta dividida en seis capítulos, de los cuales el primero contiene las definiciones y normas de carácter general. El segundo capítulo consiste en los registro de la administración pública. El tercero de ellos se refiere a los registros del sector privado, distinguiendo que estos se hacen por cuenta propia o por parte de un tercero del que nos habla el cuarto capítulo. Y por último, el quinto y sexto se refieren a las sanciones penales y administrativas.

Esta ley es aplicable a los registros tanto automáticos como manuales que procesen datos personales.

Los aspectos más importantes de esta ley son la prohibición de la habilitación de un registro si este no cuenta con autorización expresa del interesado; que las entidades del sector público no pueden utilizar los datos sino para las funciones que les son propias y uno de los que considero más importantes es que el registro de datos debe ser comunicado al ciudadano y debe ser publicado en el boletín oficial de aquel país. De esta obligación están exentos los registros que hacen las autoridades del Ministerio Federal de la Defensa y el procedimiento será vigilado por “un delegado federal para la protección de los datos personales”, el cual no podrá desempeñar ningún otro cargo público ni privado.

Esta ley, se considera una de las más eficaces, ya que regula tanto almacenamiento manual como en sistemas automáticos en el sector público y en el privado, aunque se advierte que no contempla a las personas morales.

2.1.3 Austria

La ley austriaca fue sancionada el 18 de octubre de 1978 y es aplicada al procesamiento y acopio de datos personales que se llevan a cabo por medio de sistemas automáticos en el sector público y privado.

Esta ley es dividida en dos capítulos; el primero establece disposiciones constitucionales que otorgan a la protección de datos, un derecho fundamental de toda persona física o moral y le confiere al gobierno federal competencia para legislar sobre la materia.

Mientras el capítulo segundo se divide en siete secciones, las cuales la primera describe disposiciones generales y definiciones; la segunda y tercera se refieren respectivamente, al sector público y al privado; en la cuarta se regula el tráfico internacional de los datos personales; la quinta esta inclinada hacia la reglamentación de los órganos creados por esta ley y las últimas dos, contienen disposiciones penales y transitorias.

Igualmente que la anterior ley de Alemania Federal, ésta establece que los organismos públicos sólo podrán recolectar o procesar datos de carácter personal cuando exista una autorización expresa por parte del interesado, o bien, cuando sea indispensable para el cumplimiento legítimo del organismo; siempre y cuando se le informe al Registro de Elaboración de Datos creado por la misma ley.

Esta ley prevé excepciones a sus disposiciones como:

a) Que se protejan a las instituciones constitucionales y a la administración de la justicia penal,
b) Aseguramiento del ejército federal,
c) Defensa general del país, previa disposición reglamentaria en audiencia del Consejo de Protección de datos.

El Consejo de Protección de datos es un organismo asesor entre cuyas funciones se encuentra el vigilar las consecuencias de la informática y los efectos de la aplicación de esta ley, tiene potestad reglamentaria, es independiente y posee competencia judicial.

Esta ley, contiene sanciones penales de privación de la libertad y multa para los casos de violación de secreto, intervenciones no autorizadas en la elaboración de datos e incumplimiento de las obligaciones que impone; así como en los asuntos materia de flujo de datos transfronterizos se exige la autorización de la Comisión de protección de datos y respetando los convenios internacionales que existieran al respecto.

Esta ley, se distingue de las demás analizadas por ser una de las más completas; teniendo un órgano rector que vela por los efectos de su ley reglamentaria y el cual es independiente.

2.1.4 Francia

En el caso de Francia, su ley relativa a la informática, los ficheros y las libertades entró en vigor el 6 de enero de 1978. Esta ley esta dividida en siete capítulos de los cuales el primero se refiere a los principios y definiciones; el segundo de ellos habla de la Comisión Nacional de la Informática y las Libertades; el tercer capítulo consiste en los trámites previos a la puesta en práctica de tratamientos automatizados, el cuarto de ellos alude a la colecta, registro y conservación de informaciones nominativas; el quinto describe las reglas para el derecho de acceso; el sexto capítulo señala las sanciones penales y el séptimo diversas disposiciones.

La ley se enfoca a los registros automatizados que contengan datos sobre personas físicas, tanto del sector privado como del sector público.

Para que el sector público habilite un registro, necesita la autorización de la Comisión Nacional de la Informática y las Libertades y en el caso de que el registro pertenezca al sector privado, sólo se necesita hacer una

declaración ante la Comisión, la cual es un organismo que aplica esta ley y tiene potestad reglamentaria y funciones de supervisión e información al público.

La Comisión es una autoridad administrativa independiente, integrada por 16 miembros, entre los cuales están representantes del Parlamento, del Consejo de Estado y de la Corte. Esta Comisión está obligada a poner a disposición del público una lista de todos los registros existentes y debe entregar un informe anual al presidente de Francia.

El derecho de acceso en esta ley, indica que debe ser un acceso directo del individuo, salvo en el caso de que sean registros de carácter de seguridad o defensa del Estado, a los cuales sólo accede de la Comisión.

La ley prohíbe la recolección y conservación de información sobre datos sensibles, salvo conformidad expresa del interesado y establece la forma de recolectar, usar, conservar y difundir los datos personales.

Como en las dos leyes anteriores, en esta se prevén sanciones de multa y prisión para quienes infrinjan las disposiciones legales.

Al igual que la ley de Alemania Federal, esta ley no contempla a las personas morales, pero como la austriaca tiene un órgano independiente con competencia judicial y que posee autonomía.

2.1.5 Noruega

La ley noruega fue puesta en vigor el 9 de junio de 1978, la cual establece un sistema de licencias o autorizaciones previas.

Contiene once capítulos, los cuales están organizados de la siguiente manera: el primero de ellos se refiere a la competencia, el segundo alude a la inspección de datos, el tercer capítulo determina las reglas generales, el cuarto establece la obligación de solicitar autorización para el crear registros

de personas, el quinto se refiere a la información de personas y de solvencia, el capítulo sexto regula a las empresas de servicios informáticos, el séptimo nos establece acerca del reparto de documentos y tráfico de direcciones, el capítulo octavo legisla sobre encuestas de opinión y prospecciones de mercado, el noveno regula sobre la transferencia de datos personales al extranjero, el décimo capítulo se refiere a las sanciones penales y el último capítulo a las disposiciones transitorias.

Esta ley es aplicable tanto a registros manuales como a los automáticos que contuvieran datos acerca de personas físicas y morales.

Como regla general, esta ley establece que se debe contar con la autorización del rey para la creación de un registro de datos electrónico y para los manuales que contengan informaciones sensibles; también esta ley faculta al rey para que establezca excepciones al requisito de autorización previa. Esta competencia y la de conceder la autorización han sido delegadas en la Inspección de Datos, la cual es un organismo especial dependiente del rey, encargado de la aplicación de esta ley.

La inspección de datos lleva un catálogo de todos los registros que requieren autorización.

Por lo que esta ley es de considerarse una de las más completas ya que contempla tanto a personas físicas como morales y es aplicable a registros manuales y automáticos.

2.1.6 Suecia

La ley sueca de protección de datos personales del 1 de julio de 1973, fue la primera en su tipo en Europa.

Contiene veintiocho artículos, normas generales que establecen un sistema de licencias y autorizaciones al igual que la ley noruega.

El ámbito de aplicación de esta ley se dirige a los registros automáticos públicos y privados que contengan datos relativos a una persona física.

Para la habilitación de un registro de datos de carácter personal se requiere una licencia, la cual consiste en una certificación que otorga la autoridad competente para la aplicación de la ley y una autorización de la misma si el registro contiene información sensible.

Cada registro tiene una responsable de éste, la cual responderá en caso de pérdida, destrucción o acceso no autorizado de los datos y a su posterior cancelación si estos no corresponden con los fines para los cuales fueron registrados.

Además, está obligado a conceder el acceso a la persona registrada y proceder a las modificaciones o ratificaciones que le fueran solicitadas por ella.

Asimismo, esta ley contempla sanciones pecuniarias y de privación de la libertad para los casos de incumplimiento de las disposiciones y de resarcimiento en el caso de que se hubiese causado un daño a la persona registrada.

2.1.7 Dinamarca

En Dinamarca el procesamiento de los datos personales se encuentra regulado dentro de dos leyes, una destinada al sector público y otra para el sector privado. Ambas fueron puestas en vigor el 8 de junio de 1978.

La primera de ellas se denomina la Ley de Registros de Autoridades Públicas, se divide en nueve capítulos, siendo el primero destinado para la regulación al ámbito de aplicación, el segundo se refiere a la creación de registros, el tercer capítulo a la conservación de datos, el cuarto regula el derecho de acceso, el quinto a la difusión de datos a particulares, el capítulo

sexto está destinado a las autoridades públicas, el séptimo a la inspección de registros, el octavo capítulo a las sanciones penales y el noveno a las disposiciones transitorias.

Esta ley es aplicada a los registros electrónicos de datos que son almacenados por la administración pública, con excepción de los que son llevados por servicios de información policíaca y encargados de la seguridad pública.

Para la habilitación e interconexión de registros se debe contar con la autorización del ministro competente y con el ministro de Hacienda.

La entidad responsable del registro sólo puede conservar los datos que le son útiles para sus funciones, quedándole prohibido el registro de datos relativos a circunstancias personales como, raza, religión opiniones políticas etc.

La segunda ley se llama Ley de Registros Privados, es dividida en ocho capítulos, siendo el primero dedicado para la regulación de la competencia, el segundo se refiere a las empresas mercantiles, el tercero a las oficinas de información sobre la solvencia, el cuarto capítulo regula a las empresas dedicadas al tráfico de datos, el quinto a las oficinas de servicios informáticos, el capítulo sexto se refiere al tratamiento electrónico de datos en el extranjero, el séptimo a las sanciones penales y el octavo capítulo a disposiciones transitorias.

Para el caso de registros privados a diferencia de los públicos, no se requiere de autorización especial, salvo casos muy especiales.

Esta ley se aplica a los registros electrónicos y manuales con excepción de los que se lleven con fines científicos o estadísticos.

Las dos leyes anteriores prevén sanciones pecuniarias y de prisión en el caso de no cumplir con sus disposiciones legales.

2.1.8 E.U.A.

En cambio, los Estados Unidos de América, a diferencia de los países europeos no cuenta con una ley general que regule la protección de datos personales, sin embargo, cuenta con un marco jurídico bastante amplio consistente en legislaciones específicas para determinados sectores de ésta actividad y principalmente en materia de privacidad.

En 1966 se aprobó la *"Freedom of information act"*, referente a la libertad de la información, que velaba por el libre acceso al pueblo norteamericano en los documentos públicos, es decir, a los de la administración pública, con algunas excepciones entre las cuales se hallan las informaciones relativas a la vida privada de las personas.

Existe otra ley referente a las informaciones sobre la vida privada, la llamada *"Privacy Act",* encargada de regular aspectos sobre la vida privada de las personas físicas contenidas en registros ya sean manuales o electrónicos del gobierno federal.

Por otro lado, cabe destacar que la política de regulación de los Estados Unidos ha evolucionado de tal forma que en la actualidad se ha ocupado más de legislar sobre los sectores que consideran más vulnerables para sus ciudadanos como lo es el sector salud y la protección y confidencialidad de la información que puedan proporcionar menores de edad a sitios en Internet.

2.2 El marco constitucional

En el marco jurídico vigente en México existen diversas disposiciones que regulan las consecuencias de los ataques o invasiones a la vida privada de las personas en materias como la civil, penal y de responsabilidad

administrativa del Estado, las cuales tienen como objetivo proteger al individuo de injerencias ilegales en su vida privada; cabe señalar que a estas últimas, no se les a dado difusión suficiente para que el individuo las utilice y las conozca.

Tocante a ello hay que recordar que en los artículos 6 y 7 de la Constitución Política de los Estados Unidos Mexicanos establecen como límite a la manifestación de las ideas y a la libertad de imprenta, respectivamente, el ataque a los derechos de tercero y el respeto a la vida privada, así como la libertad de expresar o publicar pensamientos, tiene la restricción de que cuando con ello se menoscabe a la persona. Asimismo, el artículo 6 consagra el derecho a la información, el cual será garantizado por el Estado y que para efectos de los Lineamientos de Protección de Datos Personales, mencionados en temas anteriores, se interpreta como el derecho del individuo a tener acceso a la información sobre sí mismo que obra en bancos de datos y a que sus datos no sean manejados de manera indebida.

De igual forma, el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos representa el marco jurídico de la privacidad en nuestro país. El primer párrafo que a la letra dice:

> *"Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento."*

Este numeral consagra una de las garantías individuales más importantes que es el derecho que tenemos a no ser molestados en nuestra persona, familia, domicilio, papeles o posesiones, sino en virtud de un mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento y en el penúltimo párrafo de este mismo

artículo, se contempla que la correspondencia que bajo cubierta circule por las estafetas, deberá estar libre de todo registro y su violación será penada por la ley.

Es decir, estos artículos constitucionales consagran el bien jurídico personal que es: la privacidad.

Por lo anterior, se puede observar que esta garantía de seguridad jurídica es suficiente para garantizar el derecho a la privacidad de los individuos en nuestro país.

Además, en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en su capítulo tercero llamado “información reservada”, regula la información que no puede hacerse pública y tiene un periodo de reserva de doce años y la que es confidencial al tratarse de datos de los particulares. Y el capítulo tercero esta dedicado a la protección de los datos personales, estos son manejados por entidades y dependencias, la cual es conservada con carácter de confidencial porque hacen referencia a las a características personales de sus empleados. Sólo pueden tener acceso a ellos los interesados o sus representantes legales.

En este capítulo se estipulan las responsabilidades que tienen las dependencias con respecto a los datos personales, así como los derechos y obligaciones que los ciudadanos tienen en caso de que quiera conocer los propios o modificarlos; sin embargo estos capítulos no son suficientes para alcanza a abarcar el sin número de cuestiones que pueden surgir en el ámbito del uso de los datos personales ya sea por dependencia gubernamentales o empresas de carácter privado.

CAPÍTULO 3
REGULACIÓN JURÍDICA DE LOS DATOS PERSONALES

En el presente capítulo se estudiarán las iniciativas de ley en nuestro país a cerca de la protección jurídica de los datos personales en Internet y de la necesidad y las ventajas que traerían al ser aprobadas.

3.1 INICIATIVAS DE LEY SOBRE PROTECCIÓN DE DATOS PERSONALES MÉXICO

En Iberoamérica sólo existen nueve países con un apartado en su sistema de régimen legal o jurídico de protección de datos personales. Argentina, Colombia, Costa Rica, Chile, España, México, Perú, Portugal y Uruguay son los estados nacionales que han previsto una discusión sobre su importancia.

En el caso de México, se tiene contemplada la Iniciativa de la Ley Federal de Protección de Datos Personales, que señala principalmente la necesidad de contener los efectos nocivos de las nuevas tecnologías sobre los tres derechos fundamentales de las personas, que son: la autonomía, la inviolabilidad y la dignidad de la persona.

1.-Iniciativa de decreto que expide la Ley Federal de Protección de Datos Personales; esta iniciativa fue la primera en relación a la protección de datos personales y la privacidad, la cual se originó en la Cámara de Diputados del H. Congreso de la Unión. Se presento el 6 de septiembre del 2001, por el diputado Miguel Barbosa Huerta, del Partido de la Revolución Democrática, ante la LVIII Legislatura, la que fue publicada el 7 de septiembre del mismo año. La iniciativa esta basada en la Directiva 95/46, sobre la privacidad y 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.

La iniciativa se turno a la Comisión de Gobernación y Seguridad Pública y actualmente se encuentra detenida por no contar con el aval y visto bueno de sectores como el público, privado y académico.

2.- Iniciativa de Ley Federal de Protección de Datos Personales; esta iniciativa fue presentada por el senador Antonio García Torres y aprobada en el Senado en abril de 2002 y publicada en la Gaceta Parlamentaria en septiembre del mismo año; posteriormente fue turnada para su respectivo dictamen a las Comisiones Unidas de Puntos Constitucionales y de Estudios Legislativos y subsecuentemente a la Cámara de Diputados.

Al igual que la Iniciativa de Decreto que expide la Ley Federal de Protección de Datos Personales, esta Iniciativa no cuenta con el aval y visto bueno de la sociedad. Igualmente esta basada en la Directiva 95/46 sobre Privacidad y Protección de Datos de la Unión Europea; su contenido es muy confuso, 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 que pertenecerían a la administración pública, lo que traería consigo cargas burocráticas excesivas para empresas de tecnologías de la información, de mercadotecnia y publicidad y en general de servicios de información.

3.2 LA NECESIDAD DE PROTECCIÓN JURÍDICA A LOS DATOS PERSONALES EN INTERNET Y REDES DE CÓMPUTO

Como se ha anotado, es de suma importancia que nuestros legisladores se preocupen por regularizar el flujo, uso y recopilación de los datos de carácter personal en los registros automatizados y en específico en los de Internet, acopiados por el sector público y privado; para el mejoramiento de las relaciones de los ciudadanos con estos sectores y evitar la vulnerabilidad a la que se ve expuesta su privacidad día con día al proporcionar datos personales sin que a la fecha tengan una defensa o

amparo en alguna ley específica en el caso de que se ocupen con fines distintos para los que le fueron solicitados.

La creación de una secretaría de informática y desarrollo, o un “Instituto Federal de Datos Personales” como lo propone el diputado Barbosa Huerta, con una adecuada reglamentación, aparte de traer consigo empleos, de igual manera, permitiría el buen manejo de los datos personales, así como vigilar y cuidar la privacidad de todos los ciudadanos.

Con la creación de un organismo adecuado, nacerían diversos derechos y obligaciones para ambas partes, tanto para los individuos que proporcionen datos personales como para las instituciones públicas y privadas que conserven estos datos, por ejemplo el informarle a las personas datos de tanta importancia como quien es el responsable de los registros o del tratamiento de los datos personales proporcionados, del uso y el tiempo de duración que conservará el registro de sus datos.

3.3 LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

El interés por legislar adecuadamente los avances tecnológicos que crecen a pasos agigantados es ya mundial y por ello la Asamblea General de las Naciones Unidas convocó a la Cumbre Mundial sobre la Sociedad de la Información que tuvo lugar del 10 al 12 de diciembre de 2003 y en Túnez en noviembre de 2005, para proyectar y formular procedimientos indispensables para lograr que la sociedad se tome conciencia al respecto.

En México, va creciendo la preocupación de legislar sobre la protección de los datos personales, tomando en cuenta el avance tecnológico de las redes informáticas, como el Internet.

Si bien es cierto, la protección de los datos personales es un tema que en México apenas comienza a ser objeto de debate y discusión, prácticamente no se cuenta con un marco jurídico sólido para tal fin.

Como se observó en el capítulo anterior, en la actualidad el sistema jurídico mexicano cuenta con la Ley Federal de Acceso a la Información Pública Gubernamental, en donde en un breve apartado regula la protección de los datos personales derivada de los archivos que se manejan para hacerlos públicos a los interesados y de la cual deriva la mencionada Ley de protección de datos personales del estado de Colima, en la que dentro de su contenido específica entre otras cosas que son los datos personales, quien los registra y los responsables de estos registros en el sector público y privado, de las sanciones e infracciones, etcétera, la cual consideramos muy completa y que, de ser el caso, debe tomarse como base en el momento de crearse una ley de carácter federal.

De igual manera, existen los Lineamientos de Protección de Datos Personales, los cuales son de poco manejo y deficiente difusión de su contenido para la población en general y que también procede de la Ley Federal de Acceso a la Información Pública Gubernamental. En esta ley se establece el ámbito de aplicación, los elementos de los datos personales, los principios rectores de la protección de los datos personales, que fueron analizados en el capítulo primero de esta investigación.

En la jurisprudencia emitida por los Tribunales federales, el avance es muy poco en el ámbito de la protección jurídica de los datos personales.

3.3.1 Proyecto de Ley Federal de Protección de Datos Personales

El proyecto de ley que se propone se pensó esencialmente por la ya mencionada inexistencia de un marco jurídico eficaz de esta naturaleza en México, se buscó principalmente que la ley que se aprobará fuera protectora y no prohibitiva; y que diera las herramientas necesarias para hacer valer los derechos que en ella se contenían.

Es por ello, que en el presente texto se propone, una ley de este tipo, ya que a lo largo de la investigación se detectó la preferencia por legislar de manera genérica, tratando de configurar las conductas delictivas dentro de

una visión general, evitando legislar de manera específica para los aspectos electrónicos o digitales.

La ley que se propone, deberá contener el ámbito de aplicación y las excepciones a ésta; las definiciones de importancia para la ley como el concepto de lo que es archivo o base de datos, archivos de acceso público, datos de carácter personal, encargado del tratamiento o responsable de los datos personales, etcétera; lineamientos y principios de la protección de datos, como el consentimiento, el tratamiento de la información, confidencialidad entre otros; prerrogativas de los titulares.

Esta ley deberá ser regulada por un juez civil del orden común, del domicilio del actor, o del demandado. Este juez tendría que resolver el procedimiento que surja de controversias por el abuso de los datos personales, mediante la acción de protección de datos de carácter personal, la cual podrá ser ejercitada por el afectado o sus representantes. Este procedimiento será igual al establecido para los juicios ordinarios civiles en la legislación aplicable en cada entidad federativa.

Se hará mediante demanda por escrito, donde el actor expondrá los motivos por los que entiende que en determinado archivo se encuentra información de él que considera discriminatoria, falsa o inexacta.

El responsable del fichero, archivo o banco de datos, tendrá que ser requerido por el juez para que le remita la información que le concierne al actor y de la documentación relativa a la recolección de la misma.

También, el responsable del archivo tendrá que exponer en su informe o contestación de demanda los motivos por los que tiene en su poder determinada información que no le fue proporcionada por el individuo a quien le concierne y tendrá la obligación de dar los datos del tercero que le proporciono los datos del actor.

Respecto a las sanciones, se hará con la reparación del daño y en su caso de pena corporal en casos que a consideración del juez sean graves.

Finalmente, es por ello que nos parece apremiante la necesidad de la creación de una ley federal que sea congruente con las legislaciones internacionales y que se encuentre dentro de los parámetros y principios fundamentales de la protección de los datos de carácter personal contenida en redes de cómputo e Internet, por los motivos expuestos a lo largo de la investigación.

CONCLUSIONES

PRIMERA.- Los datos personales, son aquellos que contienen información de personas físicas o morales, los cuales son recopilados a través de sistemas automáticos y almacenados en archivos o ficheros.

SEGUNDA.- El Internet es la red de redes que permite la interconexión de éstas y que es utilizada por unos treinta millones de usuarios en más de cien países.

TERCERA.- El libre acceso y la inexistencia de una regulación eficaz al respecto, permite que los datos proporcionados en el correo electrónico puedan servir de base para la confección de perfiles personales sin obtener el consentimiento del afectado.

CUARTA.- Existen instituciones que consiguen auxiliar al respecto como los Derechos Humanos y en particular en nuestro país, los denominados Lineamientos de Protección de Datos Personales, y en específico en el Estado de Colima la Ley de de Protección de Datos Personales del Estado de Colima.

QUINTA.- Existen principios y ordenamientos dedicados a la regulación de la protección de los datos personales, formulados por la Organización para la Cooperación y Desarrollo del cual México es un país miembro.

SEXTA.- En Europa existen grandes avances en materia de legislación de la protección de los datos personales y la privacidad, legislación que bien podría servir de base para en su momento la creación de una ley al respecto en el país.

SEPTIMA.- En México los artículos 6, 7 y 16 constitucionales son el marco jurídico de la privacidad. Asimismo, se encuentran otras disposiciones y ordenamientos a nivel federal que regulan sobre privacidad y la protección de datos personales.

OCTAVA.- Se debe crear una ley federal para la debida regulación del uso, acopio y conservación de los registros de los datos de carácter personal, para evitar la vulnerabilidad de nuestra privacidad y confidencialidad, además de que esta ley traería consigo beneficios no sólo para los particulares sino también para el país, implementando un control para los registros del sector público y del sector privado para que éstos usen únicamente los datos para los fines para los que le fueron proporcionados, es decir, no prohibiendo el manejo de los datos personales sino regulando su uso para protegerlos.

FUENTES CONSULTADAS

1.- CARBALLAR FALCÓN, José A., "Internet Libro del Navegante", Ediciones RA-MA, Tercera Edición, España, 2002.

2.- CORREA, Carlos M., "Derecho Informático", Ediciones Depalma, Buenos Aires,1987.

3.- PALAZZI, Pablo A., "Delitos Informáticos", Editorial Ad-Hoc, Buenos Aires, 1988.

4.- PARDINI, Aníbal A., "Derecho de Internet", Ediciones La Roca, Buenos Aires, 2002.

5.- TELLEZ VÁLDEZ, Julio, "Derecho Informático", Editorial Mc Graw Hill, Tercera Edición, México, 2003.

6.- VILLANUEVA, Ernesto, "Temas Selectos de Derecho de la Información", Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, Primera Edición, México, 2004.

FUENTES LEGISLATIVAS

1.- Constitución Política de los Estados Unidos Mexicanos

2.- Código Penal Federal

3.- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

4.- Ley de Protección de Datos Personales del Estado de Colima.

FUENTES ELECTRÓNICAS

1.- www.jurídicas.unam.mx, 8 de marzo del 2007,

2.- http://es.wikipedia.org/wiki/Hacker, 7 de mayo de 2007.

3.- Real Academia Española, "Diccionario de la lengua española", Ed. 22 www.cargainfo.com, 3 de mayo del 2007

4.- www.ifai.org.mx, 11 de mayo de 2007.