UNIVERSIDAD DEL TEPEYAC

ESCUELA DE DERECHO
CON ESTUDIOS RECONOCIDOS OFICIALMENTE POR
ACUERDO No. 3213-09
DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

"LA PROTECCIÓN JURÍDICA DE DATOS PERSONALES: CASO MÉXICO"

TESIS
QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN DERECHO

PRESENTA
GUILLERMO MORENO CARRASCO

MÉXICO, D.F. 2010

UNIVERSIDAD DEL TEPEYAC

ESCUELA DE DERECHO
CON ESTUDIOS RECONOCIDOS OFICIALMENTE POR
ACUERDO No. 3213-09 CON FECHA 16 – X - 1979
DE LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

“LA PROTECCIÓN JURÍDICA DE DATOS PERSONALES: CASO MÉXICO”

TESIS
QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN DERECHO

PRESENTA
GUILLERMO MORENO CARRASCO

ASESOR DE TESIS
LICENCIADO SERGIO AGUILAR MÉNDEZ
CÉDULA PROFESIONAL No. 1707116

MÉXICO, D.F. 2010

AGRADECIMIENTOS

AGRADECIMIENTOS

Quiero iniciar dando gracias a Dios, por acompañarme en todo momento y permitir que cada día esté rodeado de mis seres queridos y amados.

A mis padres Leopoldo Moreno y Luz María Carrasco, quienes con su amor, dedicación, ejemplo, valores, paciencia y sacrificios lograron hacer de mi, la persona que hoy soy… ¡papá y mamá los amo!

A mi hermano Leopoldo Moreno Carrasco, de quien he aprendido la virtud de la fortaleza; siempre hay que levantarse sin importar quien o que te haga caer, la vida sigue y tenemos que hacerle frente, hermano te quiero, gracias por tu ejemplo.

A mi amada esposa Gabriela Hernández Morgan, quien es la persona más importante en mi vida, de quien estoy y estaré siempre orgulloso, gracias por hacer posible este proyecto que es el de compartir la vida juntos, eres la mayor bendición que Dios me pudo dar, no sé que hice para merecer cruzarme en tu camino, te amo.

A Javier Espinosa, Sergio Zepeda, José Ángel Pichardo, Francisco Martínez, Víctor Tomás López, Oscar Loredo, Juan Luis Muñiz, Carlos Molina, Montserrat Espinoza, Diego Lagunilla, Martha Figueroa, Sra. Zita Morales y al Dr. Guillermo Espinosa (q. e. p. d.), quienes al correr de los años se fueron

convirtiendo en mis cómplices de vida, gracias a todos ustedes porque de una forma u otra siempre están presentes.

A mi asesor Lic. Sergio Aguilar Méndez, pues gracias a su conocimientos y experiencia profesional, logramos terminar el presente trabajo; en verdad muchas gracias Abogado por su tiempo y finas atenciones hacia con mi persona.

A la Escuela de Derecho de la Universidad del Tepeyac, por abrirme sus puertas y brindarme una educación profesional de calidad, a la par de darme la oportunidad de conocer, convivir y aprender de profesores y compañeros de gran valor.

RESUMEN

El desarrollo de la tecnología informática para procesar, almacenar y transferir grandes volúmenes de información impacta sobre la protección de datos personales. Ante ello, resulta inmediato considerar, reflexionar y legislar en la materia.

De la problemática que enfrenta la falta de legislación concreta, específica e integrada sobre la protección de datos personales, no obstante el avance en otras naciones y regiones consideradas de primer mundo, se hace evidente la fragmentación de disposiciones que carecen de orden y aplicación general.

En México, la legislación sobre protección de datos a nivel estatal es limitada, como también se presenta en el ámbito federal cierto desorden y dispersión que favorece la discrecionalidad y vulneración de los derechos fundamentales de dignidad, libertad y privacidad de los integrantes de la sociedad.

Ante ello, el objetivo general del documento se refiere a proponer cambios en las normas actuales que incrementen la eficiencia en la definición, aplicación y ejercicio de los derechos de acceso, rectificación, cancelación y oposición sobre datos personales.

Del desarrollo del tema, desde sus consideraciones generales hasta su contenido jurídico y su relación con la tecnología, las conclusiones apuntan a la necesidad inmediata de legislar sobre la protección de datos personales, pero también a considerar la autorregulación de las instituciones públicas y privadas para el buen uso y en beneficio de la sociedad.

ÍNDICE

ÍNDICE

INTRODUCCIÓN

INTRODUCCIÓN

El registro de datos personales civiles tiene su antecedente en el Concilio de Trento de 1563. Desde entonces y hasta ahora, primero de forma manual y luego de forma electrónica se han venido acumulando una serie de archivos y bases de datos que contienen la información básica o pormenorizada de las personas, de las instituciones e incluso de las naciones.

De forma manual, los datos personales quedaban registrados en actas, documentos oficiales y privados, sujetos al paso del tiempo, al clima y al cuidado en su conservación. El cruce de información personal para fines políticos, económicos, sociales o mercantiles era reducido. La posibilidad de intercambio entre particulares o instituciones significaba una alternativa limitada.

Ante el avance de la tecnología y de la capacidad informática para procesar, almacenar y transferir grandes volúmenes de información en dispositivos al alcance de todos, la situación cambió drásticamente. De ello, se sobrevinieron una serie de condiciones que hoy es necesario considerar, reflexionar e incluso legislar.

De dichas condiciones, los sujetos y su información deben mantener una garantía de protección a su privacidad, publicidad e integridad. El progreso tecnológico también debe asegurar que las reglas mínimas de

información que contengan datos personales sean fijadas, se respeten y tengan un fin lícito.

En la actualidad el cuidado de los datos personales también compromete la seguridad, tranquilidad y bienestar de las personas. Estos en general contienen información sobre múltiples aspectos sociales, familiares y económicos que deben ser administrados de manera responsable y efectiva.

Una persona física identificada contiene información sobre su origen étnico, características físicas, morales o emocionales; sobre su vida afectiva o familiar; sobre su ubicación respecto a domicilio, número telefónico y patrimonio; sobre su posición ideológica y política; sobre sus creencias religiosas o filosóficas; sobre su estado de salud físico o mental; sobre sus preferencias sexuales y su intimidad; sobre sus capacidades profesionales y técnicas; sobre la gente que lo rodea, familiares, amigos, compañeros de trabajo, clientes, proveedores, acreedores, vecinos, etcétera.

En el ambiente internacional se han adoptado iniciativas para regular la administración de datos personales en poder del Estado y de los particulares. Aunque han existido avances en materia de regulación, vigilancia, sanción, cultura y códigos de conducta, es necesario continuar en el proceso de perfección de las legislaciones en materia de protección de datos personales.

En México, hasta la fecha no se dispone de una ley específica para la protección de datos personales. Sin embargo, existen ciertos ordenamientos jurídicos de carácter federal y estatal que de forma dispersa y discrecional regulan aspectos relacionados con la protección.

Entre dichos ordenamientos que mencionan los datos personales se sitúa la Constitución Política de los Estados Unidos Mexicanos, la Ley Federal de Protección al Consumidor, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, Ley de Protección de Datos Personales para el Estado y los Municipios de Guanajuato, entre otras.

No obstante lo anterior, resulta evidente que los ordenamientos antes mencionados, vinculan a los individuos con la protección a sus datos personales, solamente cuando los individuos se ubican en cierto supuesto –como sería el caso de información en poder de entidades e instituciones federales-, y la protección no es genéricamente aplicable a los individuos por el hecho de ser ciudadano.

De ello, las preguntas de investigación que rigen esta tesis son: ¿Cuál es el estado actual en la protección de los datos personales?, ¿Qué condiciones tecnológicas deben considerarse en el tratamiento de los datos personales?, ¿Qué cambios deben proponerse para la integración de una norma específica sobre la protección de datos personales?

Las preguntas anteriores surgen a partir de la falta de protección derivada de las acciones de un sinnúmero de prestadores de servicios, entidades, instituciones y organizaciones, y al hecho de que dicha protección de datos personales recae prácticamente de manera voluntaria en quienes son afectados.

Dando respuesta a estas interrogantes, el objetivo general de la presente investigación es proponer la creación de una Ley específica que

dentro del ámbito federal concentre las normas actuales que existen en materia de protección a los datos personales, así como incremente la eficiencia en la definición, aplicación y ejercicio de los derechos de acceso, rectificación, cancelación y oposición sobre los datos personales, logrando así una verdadera protección jurídica de este tipo de información en nuestro país.

Para lograr lo anterior, este documento se elaboró bajo la técnica de investigación documental, desde un ámbito jurídico y se organizó en cuatro capítulos.

En el primero de ellos se hablará sobre los antecedentes internacionales, en consideración de la Unión Europea, Estados Unidos y lo que sucede actualmente en Latinoamérica.

En el segundo capítulo, relativo a la legislación vigente en México, se desarrollará lo que corresponde al fundamento constitucional, el derecho a la intimidad personal, el marco jurídico federal y el estatal.

En el tercer capítulo, acerca de la problemática, se comenzará estableciendo la relación del tema con la revolución tecnológica actual, aquella que sucede en México, la importancia de las bases de datos y el problema del spam como consecuencia del incremento en el tráfico de información.

Finalmente, en el capítulo cuatro, sobre la protección de datos personales, se tocará lo relativo al tratamiento y la consulta, las iniciativas

recientes sobre el tema y una propuesta que se oriente al incremento de la eficiencia en la protección.

CAPÍTULO 1

ANTECEDENTES INTERNACIONALES

CAPÍTULO 1. ANTECEDENTES INTERNACIONALES

1.1 Consideraciones

El registro formal de datos personales con fines civiles fue a partir del Concilio de Trento (1563), que dictó normas regularizando el modo de llevar los libros parroquiales de bautismos, matrimonios, defunciones, juicios, y otros tipos. Posteriormente, las autoridades civiles crearon los registros civiles y los registros de propiedad (Gregorio, 2005).

Con el paso del tiempo los registros manuales se fueron generalizando, acumulando, destruyendo, clasificándose o utilizándose con diversos fines, hasta la llegada de los medios electrónicos que sistematizaron su información.

La Declaración Universal de los Derechos Humanos (1948) en su preámbulo señala una serie de considerandos relativos a la libertad, la justicia y la paz; la dignidad, los derechos iguales e inalienables; la discriminación; la libertad de palabra y la libertad de creencias; los derechos humanos y el régimen de Derecho; la promoción de las relaciones amistosas entre las naciones; el valor de la persona y la igualdad de hombres y mujeres, entre otros, mismos derechos que están íntimamente relacionados con la persona humana.

A través del texto de la Declaración, se hace énfasis en la libertad y dignidad de la persona y de sus relaciones con los demás, en función de sus derechos fundamentales.

En el artículo primero se indica que todos los seres humanos nacen libres e iguales en dignidad y derechos, debiendo comportarse fraternalmente los unos con los otros.

Particularmente, en el artículo 12 se establece que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Así también, la misma Declaración en su artículo 19 indica que todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

El artículo 29 establece que toda persona tiene deberes respecto a la comunidad. Además, indica que en el ejercicio de sus derechos y en el disfrute de sus libertades, toda persona estará solamente sujeta a las limitaciones establecidas por la ley con el único fin de asegurar el reconocimiento y el respeto de los derechos y libertades de los demás, y de satisfacer las justas exigencias de la moral, del orden público y del bienestar general. De dicha Declaración queda constancia el reconocimiento internacional para la protección de la libertad y dignidad de la persona.

Recientemente en el Naciones Unidas a través de un documento denominado: Un concepto más amplio de la libertad: desarrollo, seguridad y derechos humanos para todos (2005), señala que los seres humanos tienen derecho a ser tratados con dignidad y respeto. También son imprescindibles para lograr un mundo de justicia, oportunidad, estabilidad y desarrollo el respeto por la dignidad humana.

Enfáticamente se indica que ha llegado la hora de que los gobiernos deban rendir cuentas, ante sus ciudadanos y ante los demás gobiernos, del respeto a la dignidad de la persona, que con demasiada frecuencia se limitan a proclamar (Naciones Unidas, 2005a, p. 38).

En la Declaración Americana de Derechos y Deberes del Hombre (OEA, 1948a) se hace referencia al derecho de la persona sobre la vida, a la libertad y a la seguridad de su persona, al derecho de libertad de investigación, opinión, expresión y difusión del pensamiento por cualquier medio, del derecho a la protección a la honra, la reputación personal y la vida privada y familiar, al derecho a la inviolabilidad del domicilio; al derecho a la inviolabilidad y circulación de su correspondencia; al derecho de presentar peticiones respetuosas a cualquiera autoridad competente, ya sea por motivo de interés general, ya de interés particular, y el de obtener pronta resolución.

Por otra parte, la Convención Americana Sobre Derechos Humanos (1969) ratificada por México en 1981, también hace referencia a la protección personal y a la dignidad cuando en el artículo 11 se indica que:

> “Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad; nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación y toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.” (OEA, 1948b)

Hacia 1990, la Organización de Naciones Unidas emite una serie de directrices para la regulación de los archivos de datos personales informatizados, dejando a la iniciativa de cada Estado la sujeción a los siguientes principios (Naciones Unidas, 1990b, p. 1-3):

> “1. Principio de legalidad y lealtad: La información relativa a las personas no debe ser recogida o procesada por métodos desleales o ilegales, ni debe ser utilizada para fines contrarios a los fines y principios de la Carta de Naciones Unidas.
>
> 2. Principio de exactitud: Las personas responsables de la compilación de archivos, o aquellas responsables de mantenerlos, tienen la obligación de llevar a cabo comprobaciones periódicas acerca de la exactitud y pertinencia de los datos registrados.
>
> 3. Principio de especificación de la finalidad: La finalidad a la que vaya a servir un archivo y su utilización en términos de dicha finalidad debe ser especificada, legítima y, una vez establecida, recibir una determinada cantidad de publicidad o ser puesta en conocimiento de la persona interesada, con el fin de que posteriormente sea posible garantizar que todos los datos personales sigan siendo pertinentes; ninguno de los referidos datos personales sea utilizado o revelado, salvo con el consentimiento de la persona afectada y el período durante el que se guarden los datos personales no supere aquel que permita la consecución de los fines especificados.

4. Principio de acceso de la persona interesada: Cualquiera que ofrezca prueba de su identidad tiene derecho a saber si está siendo procesada información que le concierna y a obtenerla de forma inteligible, sin costes o retrasos indebidos; y a conseguir que se realicen las rectificaciones o supresiones procedentes en caso de anotaciones ilegales, innecesarias o inexactas, y, cuando sea comunicada, a ser informado de sus destinatarios.

5. Principio de no discriminación: Sin perjuicio de los casos susceptibles de excepción restrictivamente contemplados en el principio 6, no deben ser recogidos datos que puedan dar origen a una discriminación ilegal o arbitraria, incluida la información relativa a origen racial o étnico, color, vida sexual, opiniones políticas, religiosas, filosóficas y otras creencias, así como la circunstancia de ser miembro de una asociación o sindicato.

6. Facultad para hacer excepciones: Las excepciones a los principios 1 a 4 solamente pueden ser autorizadas en caso de que sean necesarias para proteger la seguridad nacional, el orden público, la salud pública o la moralidad, así como, entre otras cosas, los derechos y libertades de otros, especialmente de personas que estén perseguidas (cláusula humanitaria), siempre que tales excepciones estén especificadas de forma explícita en una ley o norma equivalente promulgada de acuerdo con el sistema jurídico interno, que expresamente establezca sus límites y prevea las salvaguardas adecuadas.

Las excepciones al principio 5, relativo a la prohibición de la discriminación, además de estar sujetas a las mismas salvaguardas que las prescritas para las excepciones a los principios 1 a 4, solamente podrán autorizarse dentro de los límites establecidos en la Carta Internacional de Derechos Humanos y en el resto de instrumentos aplicables en el campo de la protección de los derechos humanos y la prevención de la discriminación.

7. Principio de seguridad: Deben adoptarse medidas adecuadas para proteger los archivos tanto contra peligros naturales, como la pérdida o destrucción accidental, como humanos, como el acceso no autorizado, el uso fraudulento de los datos o la contaminación mediante virus informáticos.

8. Supervisión y sanciones: El derecho de cada país designará a la autoridad que, de acuerdo con su sistema jurídico interno, vaya a ser responsable de supervisar la observancia de los principios arriba establecidos. Esta autoridad ofrecerá garantías de imparcialidad, independencia frente a las personas o agencias responsables de procesar y establecer los datos, y competencia técnica. En caso de violación de lo dispuesto en la ley nacional que lleve a la práctica los principios anteriormente mencionados, deben contemplarse condenas penales u otras sanciones, junto con los recursos individuales adecuados.

9. Flujo transfronterizo de datos: Cuando la legislación de dos o más países afectados por un flujo transfronterizo de datos ofrezca salvaguardas similares para la protección de la intimidad, la información debe poder circular tan libremente como dentro de cada uno de los territorios afectados. En caso de que no existan salvaguardas recíprocas, no deberán imponerse limitaciones indebidas a tal circulación, sino solamente en la medida en que lo exija la protección de la intimidad.

10. Campo de aplicación: Los presentes principios deben hacerse aplicables, en primer lugar, a todos los archivos informatizados públicos y privados, así como, mediante extensión optativa y sujeta a los ajustes correspondientes, a los archivos manuales.”

Hasta la fecha Naciones Unidas no ha hecho un pronunciamiento expreso sobre la protección de datos personales, no obstante autoridades respectivas en cada país miembro de la Conferencia Internacional de

Autoridades de Protección de Datos y Privacidad, hacia 2008 resolvieron la urgente necesidad de proteger la privacidad en un mundo sin fronteras, necesitando para ello una propuesta conjunta de estándares internacionales sobre la privacidad y protección de los datos personales emitida por la ONU.

De los miembros participantes en dicha Conferencia se tiene a:

- La Comisión Nacional de la Informática y de las Libertades (Francia)
- El Comisionado Federal para la Protección de Datos (Alemania)
- El Garante para la Protección de Datos Personales (Italia)
- La Oficina del Comisionado de Información (Reino Unido)
- La Inspección Estatal de Protección de Datos (Lituania)
- La Oficina para la Protección de los Datos Personales (Rep. Checa)
- La Autoridad Griega de Protección de Datos
- La Autoridad Holandesa de Protección de Datos
- El Inspector General para la Protección de Datos Personales (Polonia)
- El Comisionado de Protección de Datos de Irlanda
- La Comisión Nacional de Protección de Datos (Portugal)
- El Director Nacional de Protección de Datos Personales (Argentina)
- El Comisionado de Protección de Datos de Guernsey
- El Comisionado de Privacidad de Nueva Zelanda
- La Agencia de Protección de Datos de Andorra
- El Supervisor Europeo de Protección de Datos

- El Comisionado para la Protección de Datos de Berlín (Alemania)
- La Agencia Catalana de Protección de Datos
- La Agencia de Protección de Datos de la Comunidad de Madrid
- La Agencia Vasca de Protección de Datos
- La Red Iberoamericana de Protección de Datos (RIPD)
- Las Autoridades de Protección de Datos de Europa Central y del Este (CEEDPA).

A través de la 31ª Conferencia Internacional de Protección de Datos y Privacidad celebrada en España a finales de 2009, se buscó establecer las bases de trabajo y fijar los estándares internacionales que deben conformar la Carta universal de la ONU sobre el respecto. (Martí, 2009)

1.2 La protección de datos personales en la Unión Europea

El Parlamento Europeo, el Consejo y la Comisión, bajo la Carta de los Derechos Fundamentales de la Unión Europea (2000) expresan en su artículo primero que la dignidad humana es inviolable, misma que será respetada y protegida.

En el artículo 11 de la misma carta, acerca de la libertad de expresión y de información se señala que toda persona tiene ese derecho. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras.

Por su parte, en el artículo 42 se señala el derecho de acceso a los documentos cuando todo ciudadano de la Unión o toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro tiene derecho a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión.

Así mismo, en el artículo 44, sobre el derecho de petición se indica que todo ciudadano de la Unión o toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro tiene el derecho de petición ante el Parlamento Europeo.

De lo anterior, puede observarse el compromiso de la Unión por reconocer el derecho de protección a la dignidad, la libertad de expresión, de comunicar y recibir, de pedir y tener acceso a la información contenida en documento del Parlamento Europeo, del Consejo y de la Comisión.

Desde 1995 hasta la fecha, la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 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 constituye el texto de referencia, a escala europea, en materia de protección de datos personales.

A través de esta Directiva se establece el marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE), fijando límites estrictos para la recogida y utilización de los datos personales. De igual forma, solicita la creación en cada Estado

miembro de un organismo nacional independiente encargado de la protección de los datos personales.

La misma Directiva en el artículo dos señala algunas definiciones pertinentes sobre los datos personales, tales como (Directiva 95/46/CE, 1995):

> a) “«datos personales»: toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social;
>
> b) «tratamiento de datos personales» («tratamiento»): cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción;
>
> c) «fichero de datos personales» («fichero»): todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica;
>
> d) «responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por

disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario;

e) «encargado del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento;

f) «tercero»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento;

g) «destinatario»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que reciba comunicación de datos, se trate o no de un tercero. No obstante, las autoridades que puedan recibir una comunicación de datos en el marco de una investigación específica no serán considerados destinatarios;

h) «consentimiento del interesado»: toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan."

Dichas definiciones establecen el alcance y las limitaciones de acción de la Directiva, así como también se indica en sus 72 considerandos y 34 artículos aspectos sobre:

- Condiciones generales para la licitud del tratamiento de datos personales: principios relativos a la calidad de los datos; principios relativos a la

legitimación del tratamiento de datos; categorías especiales de tratamientos; información del interesado; derecho de acceso del interesado a los datos; excepciones y limitaciones; derecho de oposición del interesado; confidencialidad y seguridad del tratamiento; notificación de:

- Recursos judiciales, responsabilidad y sanciones:
- Transferencia de datos personales a países terceros
- Códigos de conducta
- Autoridad de control y grupo de protección de las personas en lo que respecta al tratamiento de datos personales
- Medidas de ejecución comunitarias
- Disposiciones finales

El estado que guarda la aplicación de dicha Directiva, en términos de la Comunicación de la Comisión al Parlamento Europeo y al Consejo, de 7 de marzo de 2007, se establece que hasta ahora la Directiva no requiere cambios, que la aplicación mejoró y que todos los Estados miembros han tomado en cuenta la Directiva. (Comisión de las Comunidades Europeas, 2007)

1.3 La protección de datos personales en los Estados Unidos de Norteamérica

Los Estados Unidos cuentan con un marco jurídico amplio en materia de privacidad. Igualmente, han adoptado una política de autorregulación que ha estado a cargo en gran medida del sector privado, respondiendo 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.

> “El modelo americano de privacidad descansa sobre la fuerza de la ley y en la capacidad de la judicatura para limitar las acciones de un Estado que pudiera resultar invasor y totalitario. Esta construcción de la privacidad es una limitación sucesiva para impedir que leyes —dictadas dentro de los procedimientos constitucionales— terminen asignado al Estado poderes que no debe tener” (Gregorio, 2005, p. 306).

Dicha primera enmienda señala que el Congreso no aprobará ninguna ley con respecto al establecimiento de religión alguna, o que prohíba el libre ejercicio de la misma o que coarte la libertad de palabra o de prensa; o el derecho del pueblo a reunirse pacíficamente y a solicitar del Gobierno la reparación de agravios (Constitución de los Estados Unidos de América, 2009).

La política de regulación de los Estados Unidos ha evolucionado para ocuparse más de legislar aquellos sectores que se consideran más sensibles y vulnerables para la sociedad, como son el sector salud y la protección y confidencialidad de la información que proporcionen niños menores de edad a sitios en Internet.

Estados Unidos han adoptado una política 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 porque saben que el gobierno está 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 permiten que las pequeñas y medianas empresas puedan realizar actividades de comercio electrónico en todos los niveles.

A través de la Comisión Federal del Comercio se ha asumido la vigilancia y supervisión de la privacidad en las comunicaciones electrónicas comerciales, hecho que ha motivado al organismo a participar como observador en foros, conferencias y otros mecanismos de estudio y cooperación en materia de protección de datos personales.

Entre las normativas que la Comisión difunde entre los consumidores para proteger su identidad está la Ley de Informe Justo de Crédito (*Fair Credit Reporting Act, FCRA*), misma que le concede derechos específicos a un sujeto cuando sea o crea ser víctima de un robo de identidad.

Entre los derechos que se refieren a los datos personales se encuentran (FTC, 2009):

1. “Tiene derecho a pedir que las agencias de informes al consumidor a nivel nacional coloquen “alertas de fraude” en su expediente para hacer saber a posibles acreedores y otros que puede ser una víctima de robo de identidad.

2. Tiene derecho a obtener copias gratuitas de la información en su expediente. Una alerta de fraude inicial le da derecho a una copia de toda la información en su expediente en cada una de las tres agencias nacionales.

3. Tiene derecho a obtener documentos referentes a transacciones fraudulentas realizadas o cuentas abiertas utilizando su información personal.

4. Tiene derecho a obtener información de un cobrador de deuda.

5. Si cree que la información en su expediente es el resultado de un robo de identidad, tiene derecho a pedir que una agencia de informes del consumidor bloquee esa información de su expediente.

6. Evitar que empresas reporten información sobre usted a agencias de informes del consumidor si considera que la información es resultado de un robo de identidad.”

Otras normas relativas a la privacidad son (Gregorio, 2005, p. 307):

- “Electronic Communications Privacy Act, de 1986, 18 USC 2510-2520, 1994 & Supp. 1997
- Omnibus Safe Streets and Crime Control Act de 1967, 18 USC 2510-2520, 1968
- Video Privacy Protection Act, 18 USC 2710, 1994
- Telephone Consumer Privacy Act, 47 USC 227, 1994
- Bank Secrecy Act, 31 USC 5313, 1994
- Drivers Privacy Protection Act, 18 USC 2721-25 1994

- Children’s Online Privacy Protection Act, 15 USCA 6501-6506, 1998
- Aunado a otras leyes estatales y locales.”

A nivel regional, el interés de Estados Unidos de Norteamérica en la participación como observador en la Red Iberoamericana de Protección de Datos busca nuevos mecanismos de cooperación con las autoridades de otros países latinoamericanos para proteger la privacidad y los derechos fundamentales a fin de desarrollar políticas activas en favor de la comunidad hispanohablante y de la población en general de los Estados Unidos.

1.4 La protección de datos personales en Latinoamérica

La Red Iberoamericana de Protección de Datos con sede en España pero donde la mayoría de sus 14 países miembros se encuentran en América Latina, se crea mediante la Declaración del Encuentro Iberoamericano de Protección de Datos celebrado en Guatemala el 6 de junio de 2003.

En dicha Declaración expresan la necesidad de protección de datos personales como un auténtico derecho fundamental de las personas, a su intimidad y de su facultad de control y disposición sobre los mismos, reconociendo que aun existen situaciones que impiden o dificultan el ejercicio efectivo de tal derecho.

Declaran que el tratamiento de datos personales puede impulsar el desarrollo de los Países Iberoamericanos, en el marco de la Sociedad de la Información, reconociendo los beneficios de las nuevas tecnologías de la información y las comunicaciones (Declaración de la Antigua, 2003, p. 1).

A través de la adopción de medidas que garanticen un elevado nivel de protección de datos, así como la idoneidad de contar con marcos normativos nacionales en armonía con los principios esenciales de protección de datos reconocidos en los instrumentos internacionales, se estima alcanzar avances en las iniciativas regulatorias que se han puesto en marcha en diversos Países Iberoamericanos.

Esta iniciativa de los responsables institucionales, académicos, judiciales y del sector privado involucrados en la protección de datos en Iberoamérica contó con un apoyo político expresado en la Declaración Final de la XIII Cumbre de Jefes de Estado y de Gobierno de los países iberoamericanos de 2003.

En su organización se establece que podrán solicitar ser miembros con voz y voto de la Red los representantes de las Instituciones y Autoridades nacionales con competencias en materia legislativa y de Supervisión de Protección de Datos y Hábeas Data (tales como los Parlamentos, las Defensorías del Pueblo, las autoridades Independientes de Supervisión y las autoridades Judiciales), y los Centros Administrativos y Gubernamentales, así mismo de ámbito nacional, con competencia reglamentaria y con capacidad para implementar y poner en práctica medidas de protección de datos dentro de la esfera de sus atribuciones.

También se establece con el mismo carácter de los anteriores, podrán ser miembros asociados de la Red los representantes de organismos públicos que actúen en la esfera de la privacidad y protección de datos personales, las universidades que desarrollen actividades docentes o de

investigación en el ámbito de la protección de datos, y las entidades privadas con interés en el ámbito de la privacidad y protección de datos.

> “Hacia 2004 los miembros países que se habían integrado a la red eran Argentina, Brasil, Chile, Costa Rica, Colombia, El Salvador, Ecuador, España, México, Nicaragua, Perú, Panamá, Portugal, Uruguay y Venezuela. Asimismo, se han sumado como observadores, representantes de la Comisión Federal del Comercio de los Estados Unidos” (Red Iberoamericana de Protección de Datos, 2005, p. 9).

De las decisiones tomadas se ha llegado a acordar la formación de grupos de trabajo por temas reconociendo la necesidad de estudiar separadamente las materias y preparar documentos formados por Grupos de Trabajo temporales o permanentes de acuerdo con las actividades que desarrollen.

De los avances hasta ahora logrados por Red se tiene:

- Ofrecer asistencia técnica y transferencia de conocimientos a los países iberoamericanos que así lo soliciten;
- Impulsar la edición y publicación de documentos de trabajo y de las obras que permitan difundir y dar a conocer los resultados obtenidos en el desarrollo de sus actividades;
- Promover la cooperación interinstitucional y el diálogo entre actores claves para el desarrollo de iniciativas y políticas de protección de datos;
- Propiciar alianzas con instituciones públicas o privadas que permitan el desarrollo y ejecución de proyectos de su interés;

- Potenciar el establecimiento de políticas, tecnologías y metodologías tendentes a garantizar una mejor protección del derecho fundamental a la protección de datos personales;
- Participar en foros internacionales;
- Dar transparencia y difusión universal a todas las actividades de la Red.

De los retos que se han identificado lo son la búsqueda de soluciones normativas armonizadas y adaptadas a la tradición legislativa de cada país, mayor difusión y formación a los ciudadanos.

En cuanto a la mayor armonización, ésta se logrará accediendo a la experiencia de los miembros cualificados expertos y responsables directos en materia de protección de datos que conocen perfectamente la realidad legislativa de sus respectivos países.

Acerca de difundir y educar en el respeto a la protección de datos, es necesario enfatizar en la privacidad y protección de datos mediante un Observatorio de Protección de Datos el cual se encargará de recopilar y analizar la información que permita medir el desarrollo y los avances de los países de Iberoamérica en el área de la Protección de Datos, así como elaborar indicadores del desarrollo de la materia.

CAPÍTULO 2

LEGISLACIÓN VIGENTE EN MÉXICO

CAPÍTULO 2. LEGISLACIÓN VIGENTE EN MÉXICO

2.1 Fundamento constitucional

Hacia 1977 se adicionó al artículo 6° de la Constitución Federal para consagrar en su texto, de acuerdo a la Declaración Universal de los Derechos del Hombre de 1948, el derecho a la información, como una garantía individual.

El fundamento constitucional sobre la persona, su dignidad, libertad, su privacidad y la información que se deriva de ella está contenido actualmente en diversos artículos a lo largo de la Carta Magna, tales como los artículos 1, 6, 7, 16 y 20.

El artículo primero de la Constitución Política de los Estados Unidos Mexicanos establece que queda prohibida toda discriminación motivada por origen étnico o nacional, el género, la edad, las discapacidades, la condición social, las condiciones de salud, la religión, las opiniones, las preferencias, el estado civil o cualquier otra que atente contra la dignidad humana y tenga por objeto anular o menoscabar los derechos y libertades de las personas.

Para el ejercicio del derecho de acceso a la información, según el artículo 6, la Federación, los Estados y el Distrito Federal, incluyen para su actuación lo siguientes principios:

I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.

II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.

IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.

V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.

VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.

VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.

En el artículo 7, al imponer los límites a la libertad de escribir y publicar escritos sobre cualquiera materia e indicar que ninguna ley ni autoridad puede establecer la previa censura, ni exigir fianza a los autores o impresores, ni coartar la libertad de imprenta, señala a la vida privada, a la moral y a la paz pública.

El artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, en relación a la persona, indica que 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.

Igualmente, el precepto anterior manifiesta que las comunicaciones privadas son inviolables. Para ello, establece que la ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas.

Así mismo, se indica que en ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley. 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, excepto para las materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor. Así también, se indica que la correspondencia que bajo cubierta circule por las estafetas estará libre de todo registro, y su violación será penada por la ley.

Acerca del proceso penal, en el artículo 20, inciso C, apartado V, De los derechos de la víctima o del ofendido, se señala que la víctima tiene derecho al resguardo de su identidad y otros datos personales en los siguientes casos: cuando sean menores de edad; cuando se trate de delitos de violación, secuestro o delincuencia organizada; y cuando a juicio del juzgador sea necesario para su protección, salvaguardando en todo caso los derechos de la defensa.

Así también, el Ministerio Público deberá garantizar la protección de víctimas, ofendidos, testigos y en general todas los sujetos que intervengan en el proceso. Los jueces deberán vigilar el buen cumplimiento de esta obligación.

2.2 Derecho a la intimidad personal

El derecho a la intimidad se ubica en la primera generación de derechos humanos, en virtud de que corresponde a los derechos de protección y fue anterior a la conformación de los derechos sociales.

> “En la actualidad el derecho a la protección de la intimidad personal cobra relevancia en virtud de los avances tecnológicos, electrónicos y de comunicaciones, que hacen cada vez más vulnerables a los individuos frente a las intromisiones en su vida privada” (Celis, 2006, p. 72).

La importancia del derecho a la intimidad radica en el reconocimiento de que, no es suficiente proteger los derechos tradicionales, sino que también es necesario promover el disfrute de una vida plena, sin intromisiones ni obstáculos de ninguna especie.

En particular, la Constitución mexicana no reconoce de manera expresa el derecho a la intimidad. No obstante, manifiesta algunos derechos asociados con el mismo, tal como la libertad de imprenta cuando el ejercicio de ésta afecte el respeto a la vida privada; la prohibición a la autoridad de realizar actos de molestia sin mandamiento escrito de autoridad competente debidamente fundado y motivado; la inviolabilidad de las comunicaciones privadas y la libertad de correspondencia.

Así, en el marco jurídico mexicano el derecho a la intimidad sólo se encuentra parcialmente protegido y no está reconocido como tal en la

Constitución, “lo que genera un vacío normativo y deja la puerta abierta a la impunidad en los casos de violaciones a ese derecho” (Celis, 2006, p. 72).

> “Etimológicamente, la palabra ‘intimidad’ viene del latín *intus* que da idea de algo interior, algo recóndito, profundo del ser y por lo mismo oculto, escondido, de manera tal que se trata de un ámbito individual de existencia personal, en el cual el sujeto decide su forma de ser y estar, de verse él mismo, para gozar de su soledad o convivencia tranquila a fin de encontrarse en aptitud de reflexionar, analizar, pensar crear, trabajar, amar, soñar; en fin, para sentirse anímicamente dueño de sí y mantener su libertad como suprema aspiración humana” (Celis, 2006, p. 73).

> “Se identifican dos tipos de amenazas contra la intimidad: la acción o intrusión en un espacio o zona propia, y el conocimiento o intromisión informativa sobre hechos, datos o aspectos relativos a la vida privada de una persona. Puede hablarse en consecuencia, de una intimidad territorial y de una intimidad de información, que también puede llamarse confidencialidad” (Carbonell, 2005, p. 452-455).

El derecho a la intimidad encuentra su justificación en la necesidad de separar el ámbito de lo privado y lo público. Conforme al derecho estadounidense, referente de la intimidad a través de *right of privacy,* puede hablarse de violaciones a la intimidad al menos en los siguientes casos (Carbonell, 2005, p. 452-455):

- “Cuando se genere una intrusión en la esfera o en los asuntos privados ajenos.
- Cuando se divulguen hechos embarazosos de carácter privado.
- Cuando se divulguen hechos que suscitan una falsa imagen para el interesado a los ojos de la opinión pública.

- Cuando se genere una apropiación indebida para provecho propio del nombre o de la imagen ajenos.
- Cuando se revelen comunicaciones confidenciales, como las que se pueden llevar a cabo entre esposos, entre un defendido y su abogado, entre un médico y su paciente o entre un creyente y un sacerdote.”

De ello, puede indicarse que la información sobre el origen familiar, social y racial; las convicciones o preferencias políticas, las creencias y filiaciones religiosas; las ideas y creencias en general; la vida amorosa y las preferencias sexuales; los aspectos ocultos de la vida familiar son parte de la intimidad.

Aunado a lo anterior, también la información reservada implica los defectos y anomalías físicas o psíquicas no ostensibles; el comportamiento y trato social y personal que de conocerse sería criticable; las afecciones de salud que menoscaban apreciaciones sociales y profesionales; las comunicaciones de tipo personal; la vida pasada del sujeto; los momentos penosos y de extremo abatimiento del individuo.

Siendo lo anterior violaciones a la intimidad cuando son puestas a disposición de la opinión pública o simplemente van más allá de la propia persona y 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.

Ante ello, la intimidad es también una facultad subjetiva reconocida a favor de la persona física, de no permitir la intromisión de extraños, en lo que respecta al ámbito de su reserva individual, sin perjuicio de las limitaciones

normativas que de manera expresa se establezcan o de costumbres y usos sociales prevalecientes en una época y lugar determinados.

Dentro del derecho a la privacidad, se comprenden tres aspectos (Muñoz de Alba, 2002, p. 39):

- “Derecho de reserva o confidencialidad: que tiene por finalidad la protección de la difusión y revelación de los datos pertenecientes a la vida privada.
- El respeto a la vida privada: que tiene como objeto la protección contra intromisiones ilegítimas en ese espacio.
- El derecho de excluir la intromisión de terceros en aquello que constituye la zona nuclear de la personalidad, que comprende lo privado, lo reservado, lo íntimo.”

De lo expuesto se puede indicar que se distinguen como características del derecho a la intimidad: ser innato, ser vitalicio, ser absoluto, ser extrapatrimonial y ser inalienable e intransferible.

El derecho a la intimidad se relaciona con la ausencia de intervención de las comunicaciones, y la protección contra el conocimiento por parte de otras personas de información personalísima, independiente de los medios en que se dé a conocer, la ausencia de injerencias no deseadas en lugares y actividades privadas de los individuos.

Como se ha mencionado, en el artículo 16 Constitucional, se establecen algunos aspectos incluidos en el derecho a la intimidad, tales como el

derecho a no ser molestado arbitrariamente por parte de las autoridades y la inviolabilidad de las comunicaciones y de la correspondencia. Sin embargo, ello es insuficiente para considerar que este derecho es considerado expresamente determinante, suficiente y efectivamente protegido en la Carta Magna mexicana como un derecho fundamental.

Respecto al tema de la intimidad en materia penal, de acuerdo con los artículos 210 y 211 del Código Penal Federal se sanciona “al que sin justa causa, con perjuicio de alguien y sin consentimiento del que pueda resultar perjudicado, revele algún secreto o comunicación reservada que conoce o ha recibido con motivo de su empleo, cargo o puesto” (Código Penal Federal, 2009).

A este delito penal, se señala la ausencia de motivos que justifiquen la comunicación, el perjuicio sufrido, la falta de consentimiento, el acto de comunicar algo que está reservado y el abuso de poder por su ubicación jerárquica.

En el ordenamiento penal también se establecen como delitos la difamación y la calumnia. La variante del delito de calumnia que guarda cierta relación con el derecho a la intimidad, es la que consiste en imputar a otro un hecho determinado y calificado como delito por la Ley, si este hecho es falso, o es inocente la persona a quien se imputa. Así se está en el entendido que esta imputación es ante algún medio de comunicación o difundiendo esa imputación de alguna otra forma.

Derivado del derecho constitucional a la inviolabilidad de comunicaciones privadas del artículo 16, se establece, en el artículo 211 bis del Código Penal el delito cuya conducta consiste en “revelar, divulgar o utilizar indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada” (Código Penal Federal, 2009).

De ello, en la legislación punitiva el único delito que guarda relación directa con el derecho a la intimidad es la divulgación o utilización de información derivada de la intervención indebida de las comunicaciones privadas. Aunque este precepto tiene como fin preponderante la protección de la actividad económica y la industria, así como regular el desempeño ético de los profesionistas cuando el sujeto activo recibió la información con motivo de su empleo, cargo o puesto.

El derecho a la intimidad no se tutela integralmente por la legislación penal federal, por lo que las violaciones a este derecho, al menos en materia penal, pueden quedar materialmente impunes.

Por lo que la protección de este derecho viene a quedar supeditada a una interpretación favorable de la legislación penal, y la habilidad de los litigantes, lo que no es admisible cuando se trata de una prerrogativa fundamental, como el respeto a la intimidad de la vida privada.

Lo dicho con anterioridad también es aplicable a la legislación penal de las entidades federativas, las cuales contemplan prácticamente las mismas

disposiciones en la materia que la normatividad federal, lo que es de igual forma insuficiente.

Por otra parte, en la legislación civil se encuentra cierta tibieza en lo que se refiere a la protección del derecho a la intimidad, tal como la utilización de una figura particularmente importante que permite salvaguardar ese derecho: el daño moral.

De acuerdo con el artículo 1916 del Código Civil Federal, por daño moral se entiende como la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspectos físicos, o bien en la consideración que de sí misma tienen los demás. De igual forma, el precepto en cuestión indica que se presumirá que hubo daño moral cuando se vulnere o menoscabe ilegítimamente la libertad o la integridad física o psíquica de las personas.

Dicho artículo, en el Código Penal Federal, establece también que cuando un hecho u omisión ilícitos produzcan un daño moral, el responsable del mismo tendrá la obligación de repararlo mediante una indemnización en dinero, con independencia de que se haya causado daño material, tanto en responsabilidad contractual como extracontractual (Código Penal Federal, 2009).

Derivado de la ambigüedad de la disposición anterior se presenta la dificultad de acreditar el daño moral, mediante la comprobación de que un acto de invasión a la intimidad ha causado un daño subjetivo, aunado al criterio para establecer la cuantía del daño. Otro problema es que la figura del

daño moral opera *ex post facto*; es decir, no tiene por objeto la restitución en el goce del derecho violado, sino una satisfacción posterior, vía indemnización, de los daños causados.

Como puede observarse, la legislación civil federal es aún más deficitaria que la penal en materia de protección de la intimidad de las personas, lo que genera todavía mayor insuficiencia para la tutela de los derechos de los individuos.

De ello, las carencias que en el ordenamiento mexicano existen en materia de protección a la intimidad son (Celis, 2006, p. 102):

- "La falta de reconocimiento expreso en la Constitución Federal del derecho a la intimidad como un derecho fundamental.
- La falta de protección contra la obtención de documentación o información que pueda ser usada en juicio contra los individuos, tal como los antecedentes generales, familiares, de salud, académicos, laborales, financiera, patrimonial, etcétera.
- La falta de protección contra injerencias indebidas en decisiones íntimas, de pareja o familiares.
- La falta de protección contra la invasión física a la intimidad, como puede ser las grabaciones, fotografías o filmes en el domicilio privado de las personas o en lugares públicos sin el consentimiento de las personas.
- La falta de protección de publicaciones falsas o sobre información privada de las personas, cuando ésta no se difunda a través de un medio escrito."

En materia de medios de comunicación masiva, el derecho a la intimidad puede verse ultrajado en los siguientes supuestos (Celis, 2006, p. 103):

- “La falta de protección contra el uso de la imagen, nombre o firma de una persona, para fines publicitarios o comerciales sin su consentimiento.
- La falta de protección efectiva de los datos que circulan por Internet.
- La falta de mecanismos para proteger la intimidad de los padres en la educación de sus hijos.
- Prohibición de revelar información profesional que se refiera a la vida privada de las personas, cuando ésta no es considerada un secreto.
- La falta de protección a la divulgación de las tendencias sexuales.
- La falta de protección contra el oportunismo de la prensa o de agentes de medios de comunicación masivos.
- El hostigamiento de persona por medio de la acechanza, la observación, con llamadas telefónicas.
- La falta de tutela del derecho al olvido de las personas que se han retirado de la vida pública.”

De ello, la protección a la intimidad y la información de los sujetos es un hecho que deja vulnerable a la persona y sus seres cercanos, no habiendo hasta el momento alguna norma jurídica capaz de detener las intromisiones a la tranquilidad.

2.3 Marco jurídico federal

Con fecha 30 de abril del año 2002, los Diputados integrantes del Grupo Parlamentario del Partido Acción Nacional presentaron una iniciativa para la

expedición de una ley reglamentaria federal para garantizar que las personas tengan acceso a una información veraz, suficiente y oportuna, en términos del artículo 6 Constitucional.

Como resultado de dicha iniciativa, el Congreso de la Unión aprobó la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y ésta fue publicada en el Diario Oficial de la Federación en junio de 2002. Dicha ley tiene como finalidad proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal.

Para los efectos de esta Ley, en el artículo 3 se indica entiende como datos personales a la información concerniente a una persona física, identificada o identificable, entre otra, la relativa a su origen étnico o racial, o que esté referida a las características físicas, morales o emocionales, a su vida afectiva y familiar, domicilio, número telefónico, patrimonio, ideología y opiniones políticas, creencias o convicciones religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad.

Así también se define como Sistema de datos personales al conjunto ordenado de datos personales que estén en posesión de un sujeto obligado, siendo éste último:

- El Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República;

- El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos;
- El Poder Judicial de la Federación y el Consejo de la Judicatura Federal;
- Los órganos constitucionales autónomos;
- Los tribunales administrativos federales, y cualquier otro órgano federal.

Dentro de la información reservada y en atención de los datos personales, el artículo 13 menciona aquella que ponga en riesgo la vida, la seguridad o la salud de cualquier persona. El artículo 18 señala como información confidencial sobre la persona, la entregada con tal carácter por los particulares a los sujetos obligados, los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta Ley.

En el Capítulo IV, acerca de la Protección de datos personales del artículo 20 al 25 se indica la responsabilidad de los sujetos obligados y el derecho de los interesados para solicitar modificaciones.

En seguida se transcriben algunos elementos de consideración:

“Artículo 20. Los sujetos obligados serán responsables de los datos personales.

Artículo 21. Los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información.

Artículo 22. No se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:

I. (Se deroga). Fracción derogada DOF 11-05-2004

II. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;

III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;

IV. Cuando exista una orden judicial;

V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y

VI. En los demás casos que establezcan las leyes.

Artículo 23. Los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlo del conocimiento del Instituto.

Artículo 24. Sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales.

Artículo 25. Las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales."

Hacia septiembre de 2005, el Pleno del Instituto Federal de Acceso a la Información Pública (IFAI), con fundamento en lo dispuesto por los artículos 37 fracción IX de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, y 2 fracción III, 47 y 62 fracciones I y II de su Reglamento presentó los Lineamientos de Protección de Datos Personales.

Bajo dichos lineamientos, en su artículo primero el IFAI señala que éstos tienen el objeto de establecer las políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal para garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales, con el propósito de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva para la dignidad y derechos del afectado.

Entre los principios que deberán regir en la protección de datos personales se mencionan la licitud, calidad, acceso y corrección, de información, seguridad, custodia y consentimiento para su transmisión. (IFAI, 2005, p. 4-5)

- "Licitud: La posesión de sistemas de datos personales deberá obedecer exclusivamente a las atribuciones legales o reglamentarias de cada dependencia o entidad y deberán obtenerse a través de los medios

previstos en dichas disposiciones. Los datos personales deberán tratarse únicamente para la finalidad para la cual fueron obtenidos. Dicha finalidad debe ser determinada y legítima.

- Calidad de los datos: El tratamiento de datos personales deberá ser exacto, adecuado, pertinente y no excesivo, respecto de las atribuciones legales de la dependencia o entidad que los posea.
- Acceso y corrección: Los sistemas de datos personales deberán almacenarse de forma tal que permitan el ejercicio de los derechos de acceso y corrección previstos por la Ley, el Reglamento y los Lineamientos emitidos por el Instituto.
- De Información: Se deberá hacer del conocimiento del Titular de los datos, al momento de recabarlos y de forma escrita, el fundamento y motivo de ello, así como los propósitos para los cuales se tratarán dichos datos.
- Seguridad: Se deberán adoptar las medidas necesarias para garantizarla integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado.
- Custodia y cuidado de la información: Los datos personales serán debidamente custodiados y los Responsables, Encargados y Usuarios deberán garantizar el manejo cuidadoso en su tratamiento.
- Consentimiento para la transmisión: Toda transmisión de datos personales deberá contar con el consentimiento del Titular de los datos, mismo que deberá otorgarse en forma libre, expresa e informada.”

Paralelo a la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, existen otros ordenamientos federales que incluyen normas sobre datos personales, tal como la Ley de Seguridad Nacional, Ley para Prevenir y Sancionar la Trata de Personas, Reglamento de la Ley del Instituto del Fondo Nacional de la Vivienda para los Trabajadores en Materia

de Transparencia y Acceso a la Información, el Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones, entre otros.

Enseguida se muestran los artículos relativos sobre datos personales:

- Ley de Seguridad Nacional, 2005:

Artículo 6. Información gubernamental confidencial: los datos personales otorgados a una instancia por servidores públicos, así como los datos personales proporcionados al Estado Mexicano para determinar o prevenir una amenaza a la Seguridad Nacional.

Artículo 63.- Los datos personales de los sujetos que proporcionen información, serán confidenciales. Artículo 64.- En ningún caso se divulgará información reservada que, a pesar de no tener vinculación con amenazas a la Seguridad Nacional o con acciones o procedimientos preventivos de las mismas, lesionen la privacidad, la dignidad de las personas o revelen datos personales.

- Ley para Prevenir y Sancionar la Trata de Personas, 2007:

Artículo 14.- Las autoridades federales adoptarán políticas y programas a fin de:

III. Recopilar e intercambiar los datos y las estadísticas delictivas de la trata de personas, respetando la confidencialidad de los datos personales de las víctimas.

Artículo 18.- La protección a las víctimas u ofendidos del delito de trata de personas comprenderá, además de lo previsto en el Apartado B del artículo 20 de la Constitución, y de lo contemplado en los Capítulos I, II, III y IV de esta Ley, los siguientes rubros:

I. Proteger la identidad de la víctima y de su familia, con la finalidad de asegurar que sus nombres y datos personales no sean divulgados en ningún caso;

- Reglamento de la Ley del Instituto del Fondo Nacional de la Vivienda para los Trabajadores en Materia de Transparencia y Acceso a la Información, 2006

Artículo 1. El presente ordenamiento tiene por objeto reglamentar las obligaciones de transparencia, acceso a la información y a los datos personales, su corrección, y la organización de archivos a cargo del Instituto del Fondo Nacional de la Vivienda para los Trabajadores, así como garantizar el acceso a la información en posesión de dicho Instituto.

- Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones, 2009

Artículo 44. Los concesionarios de redes públicas de telecomunicaciones deberán:

Los concesionarios deberán conservar copias fotostáticas o en medios electrónicos de los documentos necesarios para dicho registro y control; así

como mantener la reserva y protección de las bases de datos personales, las cuales no podrán ser usadas con fines diferentes a los señalados en las leyes.

De lo expuesto, se estima que la administración pública federal y sus dependencias o empresas privadas sujetas a la norma federal deben establecer mecanismos de protección de datos personales, desde casos que implican la seguridad nacional hasta la contratación de servicios diversos.

Por otra parte, la Cedula Única de Registro de Población (CURP) permite registrar en forma individual a todas las personas que residen en el territorio nacional, así como aquellas que radican en el extranjero. Tiene la particularidad de asegurar una correspondencia biunívoca entre claves y personas. Es autogenerable a partir de los datos básicos de la persona (nombre, sexo, fecha y lugar de nacimiento), que se encuentran en el acta de nacimiento, documento migratorio, carta de naturalización. (SEGOB, 2006)

Dicho sistema de identificación tiene la particularidad de que confiere un código único a cada ciudadano, del que se pueden inferir múltiples datos personales; por ello, esto puede atentar contra los principios de seguridad y de consentimiento al revelar datos sobre fecha y lugar de nacimiento.

El marco jurídico del comercio electrónico en México es relativamente reciente. Acerca de la protección de datos personales ya se encuentra regulada en la Ley Federal de Protección al Consumidor, donde se contempla la posibilidad de que los proveedores y consumidores puedan celebrar transacciones a través de medios electrónicos.

La fracción I del artículo 76 bis de dicha ley 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 o que exista un requerimiento de alguna autoridad.

Así también, 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.

Adicionalmente, algunas disposiciones sobre privacidad se encuentran contempladas en otros ordenamientos jurídicos como son la Ley de Imprenta, la Ley Federal del Derecho de Autor, la Ley del Instituto Nacional de Estadística, Geografía e Informática y el Código Penal Federal, Ley para regular las Sociedades de Información Crediticia, entre otros.

2.4 Marco jurídico estatal

A la fecha, “sólo cuatro estados de la República cuentan con una ley que proteja los datos personales de sus habitantes, mientras que aún se encuentran en rezago el gobierno federal y 28 entidades federativas, reveló la comisionada del Instituto Federal de Acceso a la Información (IFAI), María Marván” (Velasco, 2009, p. 12).

En respuesta a la necesidad de modernización derivado del avance tecnológico acelerado y sin detrimento de los derechos de protección a los datos personales, diversos Estados tienen una ley que protege los datos personales. Entre las primeras entidades que han adoptado una ley en la materia, están Colima, Guanajuato, Tlaxcala y el Distrito Federal.

El Estado de Colima, con fecha de mayo de 2002 expidió la Ley de Protección de Datos Personales del Estado de Colima. En su primer artículo señala que la presente Ley es de orden público e interés social, tiene por objeto reglamentar la fracción VI del artículo 1º de la Constitución Política del Estado Libre y Soberano de Colima, a fin de proteger y garantizar los derechos de protección de los datos de carácter personal, como uno de los derechos humanos fundamentales.

En su artículo 2 indica que la presente Ley será aplicable a los datos de carácter personal que sean registrados en cualquier soporte físico que permita su tratamiento, tanto por parte del sector público como privado dentro del Estado.

La estructura de dicha ley es la siguiente:

- Disposiciones generales
- De los datos de carácter general
- De la Creación de Protección de los Datos Personales
- De los Archivos
- De la Comisión
- De las Infracciones y Sanciones
- Transitorios

Por otro lado, en el Distrito Federal la denominada Ley de Protección de Datos Personales para el Distrito Federal fue publicada en la Gaceta Oficial del Distrito Federal el 3 de octubre de 2008.

En su artículo 2 define datos personales como la información numérica, alfabética, gráfica, acústica o de cualquier otro tipo concerniente a una persona física, identificada o identificable. Tal y como son, de manera enunciativa y no limitativa: el origen étnico o racial, características físicas, morales o emocionales, la vida afectiva y familiar, el domicilio y teléfono particular, correo electrónico no oficial, patrimonio, ideología y opiniones políticas, creencias, convicciones religiosas y filosóficas, estado de salud, preferencia sexual, la huella digital, el ADN y el número de seguridad social, y análogos.

La interpretación de esta ley se realizará conforme a la Constitución Política de los Estados Unidos Mexicanos, la Declaración Universal de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana sobre Derechos Humanos, y demás instrumentos internacionales suscritos y ratificados por el Estado Mexicano y la interpretación que de los mismos hayan realizado los órganos internacionales respectivos, tal como indica el artículo 3.

La estructura de dicha ley es la siguiente:

- Disposiciones comunes para los Entes Públicos
- De la tutela de los datos personales
  - De los principios
  - De los sistemas de datos personales

De las medidas de seguridad
Del tratamiento de datos personales
De las obligaciones de los entes públicos

- De la Autoridad Responsable del Control y Vigilancia
- De los Derechos y del Procedimiento para su ejercicio
- De las responsabilidades
- Transitorios

Como se observa, la aplicación de la ley se refiere a las obligaciones de los entes públicos en el manejo y disposición de los datos personales y las bases de datos que los contengan, de lo que se desprende la necesidad de una regulación que se aplique también a los particulares y las empresas que tengan datos personales, los acumulen y sean poseedores de bases de datos.

Así también se estima la necesidad de un ente regulador especializado que vigile el cumplimiento de la ley, que sancione a los infractores y que establezca una serie de procedimientos y reglas para la vigilancia de los derechos de los particulares, de las empresas y de la información del Estado, en cuanto a datos personales de empleados, funcionarios y cualquier persona en general.

CAPÍTULO 3

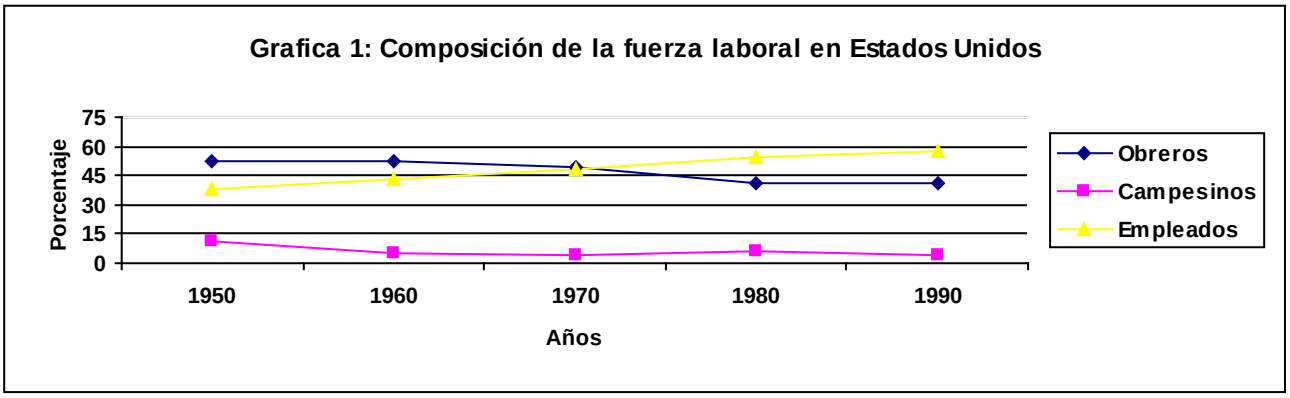
LA PROBLEMÁTICA

CAPÍTULO 3. LA PROBLEMÁTICA

3.1 La revolución tecnológica

La revolución tecnológica de las economías se ha hecho evidente con el aumento de la urbanización y la disminución de las actividades rurales. Tomando como ejemplo a Estados Unidos, el 70% de sus trabajadores está dedicado a labores de ventas, educación, salud, servicios financieros, servicios legales, entre otros, generando el 75% del Producto Nacional Bruto. (Laudon y Laudon, 2001, p. 25)

La siguiente gráfica muestra la evolución de este acontecimiento indicando una declinación desde 1950 a 1990 de la fuerza laboral representada por obreros y campesinos, aunado a una tendencia en el aumento de empleados administrativos.



Fuente: Adaptado de U.S. Department of Commerce, Bureau of the Census, Statistical Abstract of the United States, 1994. Table 644 and Historical Statistics of the United States, Colonial Times to 1970, Series D 182-232 en Laudon, Kenneth. Laudon, Jane. *Management Information Systems*. USA. 2001.

Lo anterior, es sólo un reflejo de la importancia y uso de la información como un medio para generar un cambio estructural en un país que está orientado hacia el uso de los datos procesados, como una forma de ejercer un papel protagónico en el mundo.

En cuanto a México, se calcula que cerca de 10 millones de usuarios de Internet (51% del total) ha comprado algún producto o pagado algún servicio vía electrónica. De estas compras o pagos, el 60% se ha realizado en portales mexicanos y el restante en portales internacionales. Las principales empresas de comercio electrónico en nuestro país son “Mercado Libre, empresa asociada con E-Bay que recibe 2 de cada 3 visitas a un sitio de comercio electrónico, De Remate y otras” (Contreras, 2001, p. 15).

> “Los artículos más vendidos por Internet son cámaras digitales, memorias portátiles, computadoras portátiles, cables USB para celulares y camisetas de equipos de fútbol. Cerca de 25,000 empresas mexicanas están relacionadas

> de alguna forma con el comercio electrónico mercado que tiene mucho espacio para crecer en los próximos años.” (Loperena, 2005, p. 46)

Paralelo a las transformaciones como nación, las empresas y el Estado experimentan nuevas oportunidades y retos de corto plazo. Por ello, ahora deben estructurarse de tal manera que promuevan la descentralización, la flexibilidad, la interdependencia, la disminución de costos, la motivación y el trabajo en equipo. Estas formas de organización, aunado al manejo más eficiente de la información sistematizada les permite permanecer, sobrevivir, tener más clientes, mayor número de electores o mayor o menor calificación de los gobernantes

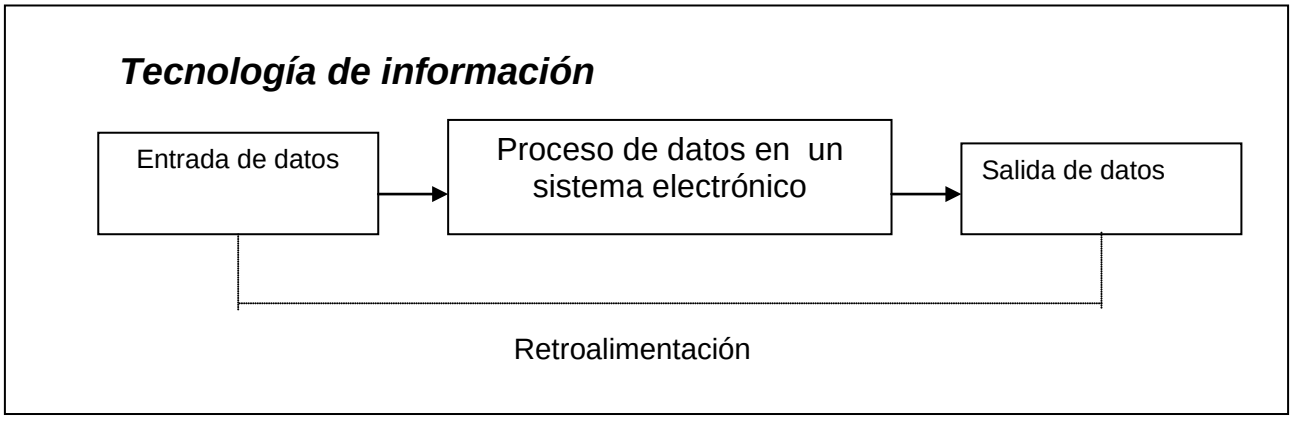
Actualmente, un sistema efectivo de información debe incluir al menos tres elementos: “una estructura organizacional, una administración y una tecnología de información de vanguardia.” (Instituto de Estudios Mediales, 2006, p. 83). La coordinación de estos elementos permite obtener, acceder y utilizar la información interna y externa sobre múltiples procesos, productos y los datos de las personas.

Específicamente, la información cuando es reunida, procesada, almacenada y distribuida por medios electrónicos genera lo que se conoce como Tecnología de Información. La Tecnología de Información tiene la finalidad de proporcionar herramientas para el control y toma de decisiones. Adicionalmente, esta información es utilizada por empresarios, gobernantes y la sociedad civil para analizar problemas y crear alternativas de solución tales como mejores servicios, mejores procesos administrativos y productivos,

nuevos productos, comportamientos sociales, y justificación de necesidades de infraestructura, educación, empleo, vivienda, salud, seguridad, etcétera.

De esta forma, la Tecnología de Información contiene datos sobre personas, lugares, operaciones y diversos temas de interés nacional, empresarial o social. Una vez que estos datos son ordenados y sistematizados producen información para tomar decisiones.

Así, para que estos datos participen sistemáticamente en los procesos, es condición necesaria que entren al sistema y finalmente salgan formando parte del conjunto; es decir; interrelacionados con otros datos para permitir a su vez la retroalimentación necesaria que alimente de manera eficiente al sistema de información, tal como se muestra en el siguiente gráfico:



Cabe señalar que un Sistema de Información (SI) va más allá del uso de computadoras. Aún cuando los datos sean procesados y convertidos en información a través de un medio electrónico, su efectiva utilización depende de una serie de relaciones humanas y de estructuras organizacionales que deben funcionar como complemento. Un SI es un “conjunto de formas,

procedimientos, relaciones interpersonales, donde se envían y reciben mensajes internos y externos.” (Laudon y Laudon, 2001, p. 9)

Por lo anterior, la Tecnología de Información es un medio, junto con el Sistema de Información para lograr un objetivo: proporcionar información que encamine a sus usuarios más allá de su posición actual y antes de que la competencia haga lo mismo.

La Tecnología de Información (TI) en los países desarrollados es una herramienta estratégica en todos los procesos administrativos y productivos, nacionales e internacionales. Sin embargo, en los países en vías de desarrollo, como México, la TI se ha limitado a apoyar la administración financiera y las operaciones productivas básicas.

Con ello, una empresa o gobierno que desconoce la tendencia anterior, por lo regular desea introducir o mejorar su TI careciendo de una estrategia definida claramente. Muchas empresas y gobiernos consideran equivocadamente que sistematizar las herramientas de proceso y control es en sí una estrategia, pensando que al hacerlo les proporcionará una ventaja competitiva.

La TI, vista como un medio para alcanzar un objetivo competitivo, “es una herramienta integradora, capaz de implementar una estrategia corporativa de forma sistematizada, considerando al personal que ejecuta, el control que evalúa y retroalimenta, la toma de decisiones proactiva y el tiempo de respuesta a las acciones tomadas.” (OIT, 2006, p. 17)

Una vez que se ha automatizado el proceso de datos, es posible mejorar la productividad individual y grupal por medio de la utilización de herramientas que permitan la confección de documentos y el acceso a datos para construir modelos de análisis de sensibilidad con diversos escenarios en distintas áreas.

Quizá uno de los usos estratégicos más interesantes, novedosos y poco conocidos de la TI es su relación con la Tecnología de Telecomunicaciones e Internet. En términos de negocios, Internet: la red mundial de información, abre una oportunidad inédita para todas aquellas entidades que teniendo o no recursos económicos suficientes deseen mantener comercio electrónico interactivo, ofrecer información en línea, facilitar gestiones, informar, proponer, denunciar, comunicar sin tener fronteras de tiempo, presupuesto y alcance.

El reto para las empresas, gobiernos y sociedad civil que participen en la red interactiva es “el de conjugar su experiencia con las nuevas dimensiones y requerimientos que exige un medio en línea que le permite al usuario estar al menos dos segundos en cada pantalla.” (Ramiro, 2005, p. 34). Es decir, Internet exige cambios en la forma de ver al cliente, al usuario, al gobernante, al gobernado, a la sociedad en general, tanto en la forma de darle información como obtener información de él, incluso de sus datos personales.

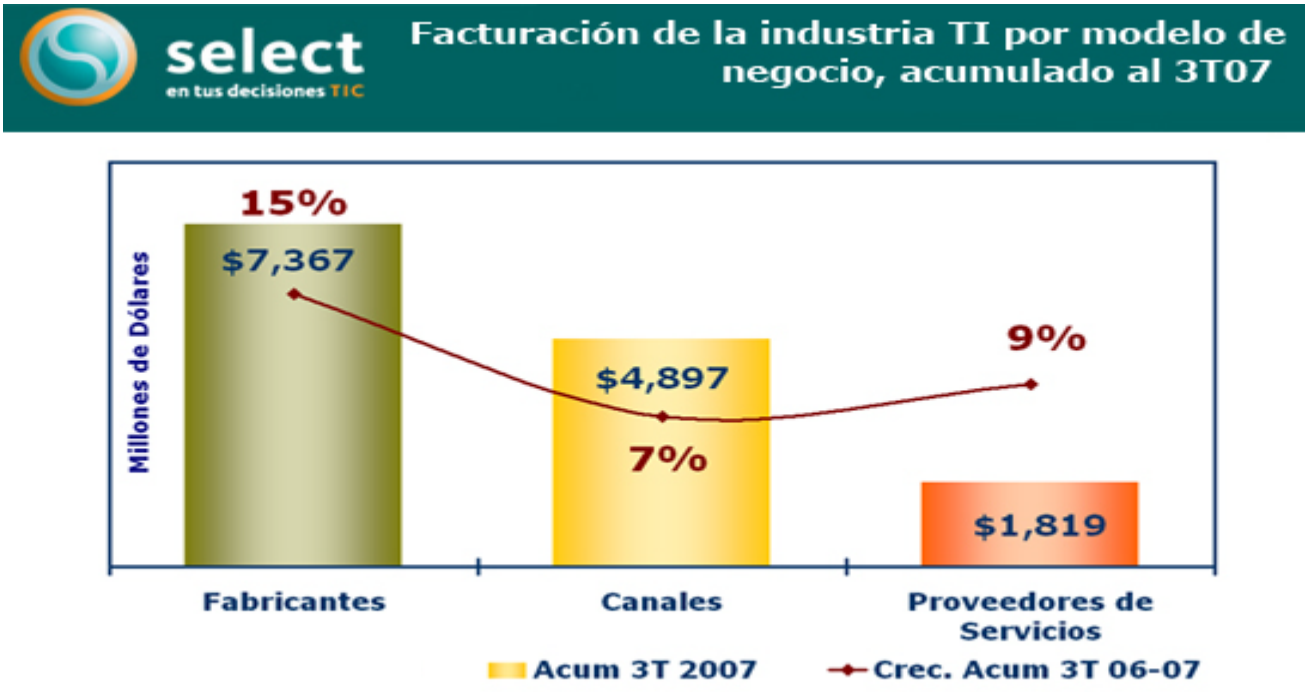
3.2 Tecnología de información en México

Como anteriormente se ha señalado, la Tecnología de Información (TI) incluye el HW, el SW, las telecomunicaciones y los dispositivos de almacenamiento. Así, también, se ha anotado que a mayor volumen y necesidades de procesamiento, la complejidad de la TI resulta ser una labor que debe ser realizada por especialistas que tomen en cuenta las necesidades de los usuarios operativos.

En México, las condiciones anteriores se han dado de forma acelerada en términos de la globalidad y sus exigencias por procesar cada vez más información que fundamente la toma de decisiones de individuos, empresas y gobierno.

Según datos de la consultora de Servicios de Estrategia en Electrónica (SELECT), citado por Pérez (2004) señala que el mercado de computadoras personales (PC) en México registró un crecimiento del 30% en términos de volumen a finales de 2007. De ello, destaca la mayor demanda de equipo por parte de pequeñas y medianas empresas, estudiantes y computadoras para el uso doméstico. En valor, los datos reportados por SELECT son los siguientes:

Grafica 3.1. Facturación de la Industria de la Tecnología de Información por Modelo de Negocio.



Fuente: Select, Noviembre 2007.

En México, como en el resto del mundo, los procesadores de información están marcando la pauta en la evolución de la TI y estos a su vez están condicionado el desarrollo de Internet. Cabe mencionar que INTEL en México, observando el desarrollo del mercado introduce por lo menos cada dos o tres años una nueva línea de procesadores para PC´s de escritorio y estaciones de trabajo, respectivamente (Mastermagazine, 2004, p. 57). Con estos nuevos productos, las empresas mexicanas, los gobiernos estatales, municipales y el federal están posibilitados para iniciar una serie de cambios relacionados con su forma de operar.

Paralelo a estos elementos, la tendencia de los proveedores de servicios es complementar y muchas veces ofrecer al mercado mexicano soluciones de integración de sistemas, networking y outsourcing[1] junto con el HW, las telecomunicaciones requeridas y los dispositivos de almacenamiento que sean compatibles.

Hoy en México la perspectiva de soluciones integrales en TI constituye la demanda principal de los clientes. Así, el enfoque de los proveedores tecnológicos es producir lo que el consumidor requiere, dejando atrás la idea de imponer esquemas tecnológicos que no contribuyen a acercar a las empresas al logro de sus objetivos.

Ciertamente, en México la TI está impulsada por las exigencias del mercado y el poder de proveedores de HW, SW y telecomunicaciones. Además, el papel de los administradores de sistemas también está evolucionado hacia una participación más activa y decisiva en las acciones, lo cual implica que la TI adquiera mayor influencia en los sistemas de información de las organizaciones.

Conforme a todo lo anterior, la TI representa una herramienta indispensable para la evolución y permanencia. La falta de ella o su aplicación sin tomar en cuenta los objetivos de las entidades podría ser contraproducente. Los elementos que la componen deben integrarse a una

[1] Nota: Networking, se refiere a redes de trabajo orientadas a un objetivo común. Pueden ser internas o externas. Las primeras se relacionan a procesos donde intervienen diferentes áreas funcionales y complementarias. Las externas involucran proveedores, clientes, gobierno e incluso a la competencia. Outsourcing, se refiere a la subcontratación de servicios para resolver una situación donde la empresa carece de los conocimientos, experiencia, contactos, equipo o recursos humanos necesarios y suficientes o simplemente desea concentrar su atención sobre actividades prioritarias y relacionadas con su giro de negocios inicial.

estrategia donde también incluya la participación de la gente. Finalmente, una buena TI siempre debe considerar que aunque se logre sistematizar la información, son las personas las que toman acciones y decisiones con ella, pero también que la sensibilidad, privacidad y calidad de la información personal debe ser respetada, tanto como los sistemas manuales lo hacían.

3.3 Las bases de datos

En mayo de 2003 se puso al descubierto que la empresa Choice Point vendió al gobierno de Estados Unidos bases de datos de uso privativo del Estado mexicano en el que se incluía información de 58 millones de votantes mexicanos.

Dicha base de datos, perteneciente al Instituto Federal Electoral, puso en evidencia la falta de control sobre la información personal de las personas y la necesidad de regular de manera integral el uso de la información de datos personales contenida en diversas bases de datos en poder del Estado y de los particulares.

Ya en 2003 el IFE demandó a los implicados en la venta bajo los cargos de revelación de secreto, delitos de carácter electoral y de traición a la patria. Al año de 2006 el Segundo Tribunal Unitario en Materia Penal del Primer Circuito, acusó de delito continuado y la agravante de pandilla a una trabajadora de la empresa Soluciones Mercadológicas en Bases de Datos, por su implicación en la venta del padrón electoral a la empresa

estadounidense Choice Point, determinando una reparación del daño e indemnización de mil 658 millones de pesos.

El 9 de Febrero de 2009, la Secretaría de Comunicaciones y Transportes publicó en el Diario Oficial de la Federación un Decreto por el que se reforman y adicionan diversas disposiciones de la Ley Federal de Telecomunicaciones.

Ese decreto, que entró formalmente en vigor el pasado 9 de Abril, crea un Registro Nacional de Usuarios de Telefonía Móvil cuyo objetivo es combatir los delitos de secuestro, extorsión y delincuencia organizada que se han venido dando últimamente en México.

El decreto establece como obligación a todos los concesionarios de redes públicas de telecomunicaciones de llevar un registro y control de usuarios de líneas de teléfonos móviles contratadas en las modalidades de plan tarifario y de prepago mediante la recopilación de una serie de datos personales como son el nombre, domicilio, nacionalidad, número telefónico, los datos contenidos en la credencial para votar y otros requisitos como son la comprobación del domicilio actual del usuario conforme a un comprobante e inclusive la toma e impresión de su huella dactilar, ya sea en tinta, o en forma electrónica o digital.

Asimismo, la reforma prevé las siguientes obligaciones a cargo de las empresas de telefonía celular y móvil: (i) conservar las copias fotostáticas o en medios electrónicos de los documentos utilizados para llevar a cabo el registro y control y la reserva y protección de las bases de datos personales

en donde se encuentre dicha información; (ii) conservar un registro y control de comunicaciones, tales como transmisión de voz, buzón vocal, conferencia, datos, reenvío o transferencia de llamadas o servicios de mensajería o multimedia, fecha, hora y duración de la comunicación, la ubicación geográfica de las líneas telefónicas; (iii) entregar dentro de las 72 horas, los datos al Procurador General de la República o Procuradores Generales de Justicia de las Entidades Federativas, cuando lleven a cabo investigaciones sobre delitos de extorsión, amenazas, secuestro, en cualquiera de sus modalidades o de algún delito grave o relacionado con la delincuencia organizada; (iv) bloquear de inmediato las líneas contratadas bajo cualquier modalidad, reportados por los clientes o usuarios como robados o extraviados, entre otras.

Al respecto, resulta cuestionable que dicha base de datos de usuarios ayude a reducir drásticamente los delitos de extorsión telefónica y delincuencia organizada en el secuestro de personas. Así también, resulta preocupante una lista de datos personales que estarán en posesión de las empresas telefónicas, sus empleados y en sus respectivas bases de datos las cuales gozarán de cierta libertad y discrecionalidad en su uso, al no estar todavía reglamentadas por una ley específica en la materia.

Asimismo, no deja de preocupar el hecho de que toda la información de los ciudadanos que cuenten con un teléfono móvil contenida en el registro estará disponible para las procuradurías federales y estatales cuando tengan que hacer investigaciones relacionadas con la comisión de delitos graves o en materia de delincuencia organizada.

En materia de las bases de datos que contiene el Estado, el 16 de abril de 2009 se publicó en el Diario Oficial de la Federación (DOF) el Reglamento de Transparencia, Acceso a la Información Pública y Protección de Datos Personales.

El documento señala que es innecesario recabar el consentimiento para el procesamiento de los datos personales, cuando se divulguen para el cumplimiento de obligaciones legales, medie una orden de autoridad competente o figuren en fuentes de libre acceso y su procesamiento, no implique quebranto de derechos y libertades fundamentales del interesado, entre otros.

Apunta que cualquier titular de datos incluidos en los sistemas de datos personales, tiene derecho a otorgarlos, negarse a otorgarlos, consultarlos, ser informado de la posible inclusión de sus datos personales por otra fuente, así como rectificarlos y oponerse a su procesamiento y cancelarlos.

“Las personas a quienes se soliciten datos personales deben ser previamente informadas de la existencia de una base de datos en la que se debe incluir la información y la finalidad de la obtención de éstos” (Mejía, 2009, p. 22), señala el reglamento.

A la fecha no se tiene cuantificado en México el número de bases de datos entre particulares y el Estado. De ello, sí se reconoce la existencia de un mercado de piratería de bases de datos que circula por Internet y se ofrece mediante correos electrónicos, aunque no se ha precisado su alcance.

> “Tomando como referencia a Argentina, en ese país se estima que circulan prácticamente sin control más de 100,000 bases de datos personales, donde ahora no existe una normativa que regule el uso de esa información sin el consentimiento de los involucrados” (Dinatale, 2003, p. 16).

En México, como en otros países, dichas bases de datos incluyen desde informes crediticios ilegales hasta las ventas de bases de datos a gobiernos extranjeros, pasando por el telemarketing sin consentimiento de quienes reciben las consultas y el envío de e-mails masivos sin detalles de procedencia.

“En México hace falta fortalecer la disciplina con la que se levantan bases de datos con fines comerciales, así como actualizarlas y limpiarlas, siendo un área y mercado de oportunidad, según la Asociación Mexicana de Mercadotecnia Directa e Interactiva (Directa)” (Ulloa, 2008, p. 16).

Dicha asociación señala que “al elaborar las bases de datos, las empresas se enfrentan con el problema de que la gente no quiere proporcionar sus datos personales (nombre, dirección, teléfono, conducta o gustos de compra), aunque no se trata de aspectos sensibles (como antecedentes médicos o preferencias sexuales). Además aún hace falta crear avisos de privacidad, donde la empresa informe al consumidor que usará sus datos y para qué” (Ulloa, 2008, p. 16).

3.4 El spam

Internet ha permitido rebasar fronteras y tener al alcance muchos tipos de información, sin embargo uno de los medios más utilizados como lo es el e-mail (correo electrónico), frecuentemente es aprovechado por personas o empresas mal intencionadas que hacen envíos de correo masivos a personas que no lo han solicitado.

El llamado “spam” ocasiona congestionamientos en los servidores de correo ocasionando una disminución en el espacio disponible para sus usuarios, causando una perdida en el nivel de calidad del servicio. Cabe mencionar que este tipo de comunicaciones no deseadas pueden ser transmitidos por distintas vías, no solamente por correo electrónico, sino también en mensajes de texto vía teléfonos celulares y programas de mensajería instantánea, como el Messenger.

Este correo comercial no solicitado o chatarra, actualmente es uno de los grandes problemas que afectan a los consumidores que navegan en Internet puesto que su utilización y difusión por parte de las empresas e individuos representa un problema significativo de costo y pérdida de tiempo y recursos para las personas que utilizan el correo electrónico.

Generalmente, el spam es enviado por empresas de mercadotecnia o simplemente por individuos contratados específicamente por empresas ilegítimas que se especializan en elaborar listas de distribución de correos electrónicos para enviarlos directamente a las carpetas de los usuarios y

dichos mensajes comúnmente se filtran cuando el usuario no cuenta con las herramientas necesarias para identificar, controlar y eliminar el spam.

Aún y cuando el usuario cuenta con las herramientas para controlar el spam, muchas veces los mensajes normalmente se filtran a las carpetas conocidas como “bulkmail”. Es a través del spam, que muchas empresas y proveedores de bienes y servicios llevan a cabo prácticas comerciales engañosas y fraudulentas hacia los consumidores y sobre todo ahora se ha convertido en un conducto para cometer otros ilícitos tales como el robo de identidad. El problema más importante que hay con el correo electrónico es que la gente usurpa las identidades, pues manda un correo que podría corresponder a alguien conocido, pero sin que exista algo que asegure que es real.

Algunas cifras permiten considerar que “tres cuartas partes (75 por ciento) del correo electrónico mundial es spam; de ese porcentaje, 63% se produce en Estados Unidos; 21% en la región Asia Pacífico; 13% en Europa, y 3% en América del Sur” (Téllez, 2006, p. 7).

En México, los principales correos basura de contenido engañoso (scam) que llegan a México son las ofertas de trabajo fácil en casa para ser millonario, productos milagrosos para bajar de peso, la carta nigeriana y la venta de títulos profesionales piratas. El primer tipo de fraude se presenta como una oferta de trabajo del esquema piramidal, donde los miembros van reclutando nuevos miembros a la empresa hasta volverse millonario, sin embargo, para conocer el plan de negocios las personas tienen que pagar entre 200 y 300 dólares y nunca reciben la información.

Tabla 3.2. Tipos de Spam

TIPO DE SPAM	DESCRIPCIÓN
Productos	Son los e- mail que ofrecen o aconsejan usar un determinado producto. Ejemplos: Servicios de investigación, maquillajes, prendas de vestir...
Financieros	Son los e- mail que contienen ofertas relacionadas con dinero. Ejemplos: Inversiones, préstamos, inmuebles...
Adultos	Son los emails que contienen o se refieren a productos o servicios dirigidos a personas mayores de edad (+18 años); suelen ser contenidos ofensivos o inapropiados. Ejemplos: Porno, anuncios personales, consejos matrimoniales...
Salud	Son los e- mails que ofrecen o aconsejan productos y/o servicios relacionados con la salud. Ejemplos: Farmacéuticos, tratamientos médicos, remedios con hierbas medicinales...
Engaños	Son los reconocidos como fraudulentos, intencionadamente equivocados, o conocidos para una actividad ilegal por parte del emisor. Ejemplos: Cartas nigerianas, esquemas piramidales, cartas en cadena...
Internet	Son los que específicamente ofrecen o aconsejan servicios o productos de o para Internet. Ejemplos: Servicios de hosting, diseño web, programas de filtrado de spam...
Ocio	Son los que ofrecen premios, descuentos en actividades de ocio, etc. Ejemplos: Ofertas de vacaciones, casinos on-line, juegos...
Fraudes	Son los emails que aparentan ser de compañías bien conocidas, pero no lo son. Esto es conocido como "Phising". Estos mensajes suelen usar trucos para revelar información personal de los usuarios, como la dirección de e-mail, información financiera, contraseñas, etc. Ejemplos: Verificación de tarjetas de crédito, notificación de cuentas, actualizaciones de facturación.
Políticos	Son los mensajes que aconsejan una campaña de un candidato político, piden que dones dinero a un partido o a una causa política, ofrecen productos relacionados con la campaña o figura del partido. Ejemplos: Partidos políticos, elecciones, donaciones...
Religión	Son los e-mails con información o servicios religiosos o evangelización espiritual. Ejemplos: Psíquicos, Astrología, religión organizada...
Otros	Son los e-mails que no pertenecen a ninguna de las anteriores categorías

Fuente: Téllez Valdés, 2006

Desde finales de 2003, la Procuraduría federal de Protección al Consumidor (PROFECO) colaboró activamente con países miembros del comité de políticas del consumidor (CCP) para la elaboración de un documento titulado Background Paper on Spam.

Posteriormente, como resultado de las reformas a la LFPC del 4 de Febrero del 2004, la PROFECO reforzó y mejoró el marco jurídico en los siguientes rubros: (i) las prácticas de mercadotecnia y de publicidad con el objeto de proteger al consumidor mexicano de los mensajes no solicitados que constantemente envían empresas de telemercadeo y publicidad por correo electrónico; (ii) veracidad de la información sobre bienes y servicios para evitar prácticas abusivas o engañosas por parte de empresas y proveedores; (iii) celebración de contratos de adhesión por vía electrónica y servicios adicionales o conexos no previstos en el contrato original; (iv) la presentación de denuncias por vía electrónica por incumplimiento a las disposiciones de la LFPC, la Ley Federal de Metrología y Normalización, normas oficiales mexicanas y demás disposiciones aplicables; y (v) las notificaciones de PROFECO por vía electrónica u otro medio similar previa aceptación por escrito del consumidor.

Las reformas más importantes en materia de prácticas publicitarias y de mercadotecnia se presentaron en los artículos 17, 18 y 18 BIS de la Ley Federal de Protección al Consumidor, relativos a la publicidad que se envía a los consumidores en forma electrónica y el registro público a cargo de la PROFECO sobre los consumidores que no desean recibir dicha información o publicidad por parte de las empresas.

CAPÍTULO 4

DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES: CONTENIDO

CAPÍTULO 4. DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS PERSONALES: CONTENIDO

4.1 Derecho a saber el tratamiento que se dará a los datos personales

Existen algunos ordenamientos Federales que regulan el tratamiento de datos personales, tales como el Código Civil Federal, la Ley Federal del Derecho de Autor, la Ley Federal de Telecomunicaciones, la Ley General de Vías de Comunicación, la Ley de Información Estadística y Geográfica y su reglamento, la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, el Código Penal, la Ley contra la Delincuencia Organizada, El Código de Comercio, la Ley de Instituciones de Crédito, la Ley para Regular Agrupaciones Financieras.

Así también se refieren al tratamiento de datos personales la Ley General de Población, la Ley Orgánica de la Administración Pública Federal, el Código Fiscal de la Federación, la Ley Federal de Imprenta, la Ley Federal de Radio y Televisión, la Ley para Regular Sociedades de Información Crediticia, el Código Federal de Instituciones y Procedimientos Electorales, la Ley Federal de Protección al Consumidor, la Ley General de Salud y su reglamento.

De lo anterior, puede observarse que existen leyes que aplican para distintas organizaciones públicas y privadas. Así pueden encontrarse regulación para organizaciones privadas, tales como las financieras; para órganos constitucionales autónomos, tal como el Instituto Federal Electoral o para situaciones en donde intervienen particulares e instituciones, tal como lo relativo a la salud pública.

No obstante ello, se reconoce que no existe un marco normativo específico para la protección de datos personales, mismo que no diluye el derecho de (Gómez y Ornelas, 2006, p. 3):

- “Que el titular conozca qué información tienen las sociedades y organismos privados o particulares, centralizados, descentralizados o autónomos.
- Que los datos que tengan en poder las instituciones sean manejados con absoluta confidencialidad.
- Que la información no sea utilizada para fines distintos al ejercicio de sus funciones.
- Que el titular tenga derecho a revisar la veracidad de los datos personales contenidos en los registros.
- Que el acceso a sus datos personales tenga el previo consentimiento del titular.”

Como un avance parcial y relativamente reciente en el tratamiento de la información de los datos personales en poder del Ejecutivo Federal, se tiene la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (2006), publicada en el Diario Oficial de la Federación el 11 de junio de 2002 y su texto vigente reformado hacia mitades del 2006.

Dicha ley señala en su Capítulo IV Protección de datos personales del artículo 20 al 26 aquello que aplica a los sujetos obligados, que en su mismo artículo tercero entiende como:

a) El Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República;

b) El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos;

c) El Poder Judicial de la Federación y el Consejo de la Judicatura Federal;

d) Los órganos constitucionales autónomos;

e) Los tribunales administrativos federales, y

f) Cualquier otro órgano federal.

Así, según el artículo 20, los sujetos obligados serán responsables de los datos personales y, en relación con éstos, deberán:

I. Adoptar los procedimientos adecuados para recibir y responder las solicitudes de acceso y corrección de datos, así como capacitar a los servidores públicos y dar a conocer información sobre sus políticas en relación con la protección de tales datos, de conformidad con los lineamientos que al respecto establezca el Instituto o las instancias equivalentes previstas en el Artículo 61;

II. Tratar datos personales sólo cuando éstos sean adecuados, pertinentes y no excesivos en relación con los propósitos para los cuales se hayan obtenido;

III. Poner a disposición de los individuos, a partir del momento en el cual se recaben datos personales, el documento en el que se establezcan los

propósitos para su tratamiento, en términos de los lineamientos que establezca el Instituto o la instancia equivalente a que se refiere el Artículo 61;

IV. Procurar que los datos personales sean exactos y actualizados;

V. Sustituir, rectificar o completar, de oficio, los datos personales que fueren inexactos, ya sea total o parcialmente, o incompletos, en el momento en que tengan conocimiento de esta situación, y

VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

Asimismo, el artículo 21 indica que los sujetos obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, desarrollados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso, por escrito o por un medio de autenticación similar, de los individuos a que haga referencia la información.

En cuanto al consentimiento, el artículo 22 señala que no se requerirá el consentimiento de los individuos para proporcionar los datos personales en los siguientes casos:

I. (Se deroga).

Fracción derogada DOF 11-05-2004

II. Los necesarios por razones estadísticas, científicas o de interés general previstas en ley, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran;

III. Cuando se transmitan entre sujetos obligados o entre dependencias y entidades, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos;

IV. Cuando exista una orden judicial;

V. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y

VI. En los demás casos que establezcan las leyes.

En cuanto a la solicitud, el artículo 24 menciona que sin perjuicio de lo que dispongan otras leyes, sólo los interesados o sus representantes podrán solicitar a una unidad de enlace o su equivalente, previa acreditación, que les proporcione los datos personales que obren en un sistema de datos personales. Aquélla deberá entregarle, en un plazo de diez días hábiles contados desde la presentación de la solicitud, en formato comprensible para el solicitante, la información correspondiente, o bien, le comunicará por escrito que ese sistema de datos personales no contiene los referidos al solicitante.

La entrega de los datos personales será gratuita, debiendo cubrir el individuo únicamente los gastos de envío de conformidad con las tarifas aplicables. No obstante, si la misma persona realiza una nueva solicitud respecto del mismo sistema de datos personales en un periodo menor a doce meses a partir de la última solicitud, los costos se determinarán de acuerdo con lo establecido en el Artículo 27.

Acerca de la modificación de datos, el artículo 25 establece que las personas interesadas o sus representantes podrán solicitar, previa acreditación, ante la unidad de enlace o su equivalente, que modifiquen sus datos que obren en cualquier sistema de datos personales. Con tal propósito, el interesado deberá entregar una solicitud de modificaciones a la unidad de enlace o su equivalente, que señale el sistema de datos personales, indique las modificaciones por realizarse y aporte la documentación que motive su petición. Aquélla deberá entregar al solicitante, en un plazo de 30 días hábiles desde la presentación de la solicitud, una comunicación que haga constar las modificaciones o bien, le informe de manera fundada y motivada, las razones por las cuales no procedieron las modificaciones.

4.2 Derecho de consulta a los registros que contengan datos personales

Dentro de las normas federales en las cuales existe algún derecho sobre los datos personales en cuanto a acceso, rectificación se encuentra la 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 que su articulado establece:

- Que los datos que los informantes proporcionen con fines estadísticos serán manejados, para efectos de esta ley, bajo la observancia de los principios de confidencialidad y 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, a que se refiere dicha norma, sólo podrá proporcionarse a particulares, organismos o gobiernos extranjeros por conducto de la desaparecida Secretaría de Programación y Presupuesto (cuyas funciones fueron atraídas por la actual Secretaría 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 pueda proporcionarse.
- Que los informantes, podrán exigir, previa presentación de solicitud ante la misma autoridad que capturó la información registrada, que sean rectificados los datos que les conciernan, al demostrar que son inexactos, incompletos, equívocos u obsoletos, y denunciar ante las autoridades administrativas y judiciales todo hecho o circunstancia que demuestre que se ha desconocido el principio de confidencialidad de los datos o la reserva establecida por disposición expresa, en el ejercicio de las facultades que esta ley confiere a las unidades que integran los sistemas nacionales.
- Que para proteger los intereses del solicitante, cuando proceda, deberá entregársele un documento en donde se certifique el registro de la modificación o corrección.
- Que a las personas a quienes se les requieran datos estadísticos o geográficos deberán ser informadas de:
    - El carácter obligatorio o potestativo de sus respuestas;
    - Las consecuencias de la falsedad en sus respuestas a los cuestionarios que se les apliquen;
    - La posibilidad del ejercicio del derecho de rectificación;
    - La confidencialidad en la administración de la información estadística que proporcionen, y

- La forma en que será divulgada o suministrada la información.

Por otra parte, existe también en México regulación limitada en cuanto a protección jurídica de datos personales se refiere, sobre 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.

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 no 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.

Como 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 mismo orden de ideas, la Ley Federal del Derecho de Autor, en su articulado prevé la protección jurídica a las bases de datos. Establece que el acceso a información de carácter privado relativa a las personas contenidas en las bases de datos a que se refiere el artículo anterior, así como la publicación, reproducción, divulgación, comunicación pública y

transmisión de dicha información, requerirá la autorización previa de las personas de que se trate.

De lo anteriormente revisado, se tiene presente que si bien en algunas leyes se hace referencia al acceso y la rectificación de datos personales, no se menciona lo relativo a cancelación y oposición, derechos que son limitados en la legislación actual.

Un antecedente de lo anterior resulta expuesto en una iniciativa presentada en 2001 ante la Cámara de Diputados, relativa a las reformas constitucionales para consagrar en el artículo 16 el Habeas Data, y así dar fundamento y a un ordenamiento jurídico que consagrara la protección jurídica de los datos personales; y también una iniciativa de Ley Federal de Protección de Datos Personales. De la letra de las iniciativas se transcriben en lo conducente información ilustrativa sobre acceso, rectificación, cancelación y oposición.

1. Que el interesado pueda acceder a los datos personales que le conciernen.
2. 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.
3. Que el interesado pueda pedir la inclusión, actualización, complementación, rectificación, reserva, suspensión y cancelación de los datos relativos a su persona.

En congruencia con los proyecto de reforma constitucional aludidos, está el correspondiente a la reforma del artículo 73 constitucional que tiene

por objeto dotar de facultades al Congreso Federal para legislar en materia de protección de datos en posesión de los particulares.

Al esfuerzo realizado en torno a la protección de datos, también se ha sumado la Suprema Corte de Justicia de la Nación con las reformas del 12 de diciembre de 2007 al Reglamento de la Suprema Corte de Justicia de la Nación y del Consejo Instituto Federal de Acceso a la Información Pública de la Judicatura Federal para la aplicación de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

En dichas reformas se establece que en los documentos contenidos en los expedientes que no sean reservados o confidenciales, se suprimirán los datos personales de las partes.

> “Las sentencias ejecutorias y demás resoluciones públicas dictadas en expedientes de cualquier materia que por su naturaleza puedan afectar de algún modo la dignidad personal o causar un daño irreparable, se difundirán en una versión impresa o electrónica de la que se supriman los datos personales de las partes” (IFAI, 2008, p. 11).

4.3 Iniciativa reciente al derecho de acceso, rectificación, cancelación y oposición

Como una de las iniciativas más representativas, encontramos la presentada por el entonces Diputado Federal Luis Gustavo Parra Noriega miembro de la Sexagésima Legislatura del Congreso de la Unión e integrante del Grupo Parlamentario del Partido Acción Nacional, de fecha 7 de octubre de 2008,

con la que se busca crear la Ley de Protección de Datos Personales en Posesión de Particulares. De ella se indica, entre otros elementos, en materia de acceso, rectificación, cancelación y oposición en el Capítulo III los derechos de los titulares y en el Capítulo IV el procedimiento para el ejercicio del derecho de particulares.

En seguida se muestra el texto de la propuesta:

Capítulo III Derechos de los Titulares de Datos Personales.

Artículo 19. Cualquier titular, o en su caso su representante, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la Ley. Los datos personales deben ser almacenados de tal manera, que permitan el ejercicio de los derechos mencionados en este artículo.

Artículo 20. Todo titular tiene derecho a conocer si sus datos personales se encuentran almacenados en una base de datos, y a solicitar su rectificación o cancelación de conformidad con lo señalado en esta ley.

Dicho derecho se ejercerá en forma gratuita, y en consultas no menores a seis meses, previa acreditación de su identidad ante el responsable de la base de datos o el particular titular de la misma.

El acceso puede consistir en la consulta de los archivos contenidos en la base de datos, o en la indicación de los datos objeto de tratamiento, a efecto de que el titular:

I. Conozca si existen datos personales en una base de datos;

II. Solicite información sobre las fuentes y los medios a través de los cuales se obtuvieron los datos;

III. Solicite los fines para los cuales sus datos personales fueron recabados;

IV. Se le informe respecto de si la base de datos se encuentra inscrita en el registro que al efecto administra la Comisión.

Artículo 21. En caso de que los datos personales pretendan ser transferidos o cedidos a otra persona u organización nacional o extranjera, el particular deberá obtener el consentimiento del titular; y en caso de haberlo obtenido, deberá asegurarse que el receptor de los datos personales, protegerá la información con al menos, los mismos principios previstos en esta Ley.

Artículo 22. Los titulares podrán oponerse a proporcionar sus datos personales, salvo que exista obligación proveniente de una disposición legal, de una relación contractual o por resolución de una autoridad competente.

Artículo 23. El titular podrá solicitar al responsable de una base de datos, que se cancelen sus datos personales que se encuentren en la misma, obtenidos sin su consentimiento, en los términos previstos en esta Ley. La cancelación deberá realizarse de manera gratuita.

Capítulo IV Procedimiento para el Ejercicio de los Derechos ante el Particular

Artículo 24. El Titular podrá ejercer ante el Particular, los derechos de acceso, rectificación o cancelación reconocidos en esta ley, mediante el siguiente procedimiento:

I. Se solicitará al Particular en el domicilio que al efecto haya designado o por la vía que se haya previsto en el aviso de privacidad respectivo, el ejercicio de alguno de los derechos previstos en la ley;

II. El Particular tendrá un plazo máximo de 5 días hábiles para determinar sobre la procedencia de la solicitud, y en su caso, permitir el acceso o llevar a cabo la rectificación o cancelación de los datos personales. Si es procedente, le informará al titular sobre dicha determinación, y en un plazo máximo de 48 horas, deberá permitir al titular el acceso a los datos personales, o realizar la rectificación o cancelación de los mismos.

Artículo 25. El Particular podrá negarse a permitir el acceso a los datos personales, o a realizar la rectificación o cancelación de los mismos, cuando se surta cualquiera de las siguientes hipótesis:

I. Cuando el solicitante no sea el titular de los datos personales, o el representante debidamente acreditado para ello;

II. Cuando en su base de datos, no se encuentren los datos personales del solicitante;

III. Cuando se lesionen los derechos de un tercero;

IV. Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación o cancelación de los mismos;

V. Cuando la rectificación o cancelación, haya sido previamente realizada;

En todos los casos anteriores, el particular deberá justificar su decisión y notificársela al titular de los datos, en un plazo máximo de tres días hábiles, por el mismo medio por el que se llevó a cabo la solicitud, acompañando, en su caso, las pruebas que resulten pertinentes.

Artículo 26. El Titular de los datos podrá solicitar ante la Comisión una declaración administrativa de infracción en un plazo máximo de tres meses contado a partir de que se cumpla cualquiera de los siguientes supuestos:

I. En caso de que no hubiere recibido la notificación señalada en el artículo anterior;

II. Cuando habiendo recibido la notificación a que se refiere la fracción anterior, no estuviere de acuerdo con su contenido;

III. En el supuesto de que el particular no hubiere permitido el acceso o realizado la rectificación o cancelación, en los términos y condiciones previstos en esta Ley.

De aprobarse esta reglamentación, que hasta abril del 2009 permanecía en estudio en el Congreso, se regulará el flujo de información de datos personales en posesión de particulares y de empresas; además se establecerán obligaciones a la iniciativa privada y particulares en el manejo de los datos.

Igualmente, al aprobarse esta ley se tendrá observancia nacional y para garantizar su cumplimiento se propone que sea el IFAI la autoridad encargada de hacerla cumplir, en virtud de que este organismo tiene marco jurídico, carácter legal y criterios para hacer el balance de transparencia de información y protección de datos.

4.4 Propuesta

Retomando algunos elementos de la propuesta anterior, a manera de incrementar la eficiencia en la definición, aplicación y ejercicio de los derechos de acceso, rectificación, cancelación y oposición, se propone lo siguiente:

- El ejercicio del derecho de acceso, rectificación, cancelación y oposición constituye el máximo objetivo en el tratamiento de los datos personales en poder de autoridades federales, estatales y municipales, como también de empresas y particulares que dispongan de bases de datos sobre personas.
- El titular de los datos o su representante podrán ejercer el derecho de acceso sin limitaciones de ninguna naturaleza.
- El poseedor de la base de datos deberá dar todas las facilidades para que el titular acceda a todos sus datos sin excepción.
- Ante el acceso integral de los datos personales contenidos en la base de datos requerida, se podrá ejercer el derecho de rectificación, cancelación u oposición.
- No es condición acceder antes de pedir rectificación, cancelación u oposición, siempre que se tengan elementos que motiven el derecho.
- El ejercicio del derecho de acceso no puede ser impugnado por el tenedor de la base de datos personales en cuestión. Ante la negativa de acceso, el titular podrá solicitar una restricción de uso de sus datos personales.
- El ejercicio del derecho de acceso será gratuito, expedito, extrajudicial y administrativo. Ante una solicitud deberá emitirse una respuesta, la que representará el inicio del proceso en el derecho de acceso.

- La negación del acceso, la falta de respuesta al ejercicio del derecho, el cobro, la tardanza y la necesidad de ejercer el derecho de acceso por medio de una instancia judicial, será motivo para que la autoridad correspondiente ordene al tenedor de la base de datos el acceso inmediato del titular.
- En cuanto al derecho de rectificación, el titular podrá en los mismos términos que el acceso, solicitar que el tenedor de la base datos modifique los datos personales, a fin de que estos reflejen la verdad, la oportunidad y la objetividad de su persona.
- Será necesario que el titular de los datos, ofrezca elementos de prueba para que el tenedor de la base de datos inicie un procedimiento de rectificación y depuración de los datos.
- Será obligación del tenedor de la base de datos emitir una comunicación de cambio, modificación o rectificación de datos cuando así lo solicite el titular.
- En cuanto al derecho de cancelación, el titular de los datos deberá solicitar, en los mismos términos que el acceso, la cancelación de sus datos por considerar que así conviene a sus intereses, porque no tienen ninguna relación directa o indirecta con el tenedor de la base de datos o porque el uso de su información personal transgrede su derecho de privacidad, intimidad, seguridad y bienestar.
- La cancelación de los datos personales deberá realizarse de forma gratuita, expedita, extrajudicial y administrativamente, de no hacerse así y de requerir un proceso judicial, la autoridad deberá recibir las motivaciones del titular y del tenedor de la base de datos, considerando para su resolución que los derechos del titular están por encima de su inclusión en la base de datos respectiva.

- Cuando la inclusión de los datos personales se haya realizado sin el consentimiento del titular, cuando estos se hayan obtenido de forma ilícita o fraudulenta, la cancelación procederá de manera inmediata y el tenedor de la base de datos deberá realizarla sin mediación de la autoridad.
- Si el tenedor de la base de datos se negare a hacer la cancelación, la autoridad podrá hacer una revisión que implique resolver la controversia limitando la base de datos que estime que fue obtenida ilícitamente o fraudulentamente.
- En relación a la oposición, el titular de los datos personales podrá oponerse a proporcionar información parcial, general o específica sobre su persona, incluso a una autoridad, sin un motivo o mandato judicial.
- También podrá oponerse a que la base de datos que contienen sus datos personales sea vendida, cedida, prestada, o cualquier otra forma de transmisión a una autoridad federal, estatal, municipal, institución privada o particular, nacional o extranjero sin su consentimiento previo.

CONCLUSIONES

CONCLUSIONES

En términos del objetivo general propuesto para esta investigación, relativo a proponer cambios en las normas actuales que incrementen la eficiencia en la definición, aplicación y ejercicio de los derechos de acceso, rectificación, cancelación y oposición sobre datos personales, se han organizado las conclusiones en dos partes: 1) la que corresponde al contexto jurídico y técnico sobre el problema, y 2) sobre el estado actual de la legislación en México.

Ambas partes coinciden en señalar que el avance tecnológico, el uso y abuso de la técnica como medio mercantil indiscriminado de datos individuales, colectivos y acumulados en bases de datos, sobrepasa la capacidad de los ciudadanos, sus gobiernos y las mismas empresas.

La facilidad con que es posible la transmisión de datos vía electrónica, en línea y sin límites de distancia, implica un esfuerzo conjunto de autoridades nacionales e internacionales para definir el concepto, la norma, y la forma de sanción para aquellos que transgredan el derecho natural de la privacidad e intimidad de los sujetos.

Igualmente, cabe indicar que más allá de la intromisión del Estado, de la necesidad de acumular datos específicos para la toma de decisiones públicas, como también de la libre competencia entre empresas sin distinción de

nacionalidad, es necesario apelar a la corresponsabilidad y la autorregulación como una forma de solventar el problema y atender de manera inmediata las demandas de protección de datos personales.

En consideración de lo anterior, las conclusiones sobre el contexto jurídico y técnico del problema en el manejo de los datos personales, son:

- La libertad, la dignidad y la privacidad son derechos humanos universales sobre los cuales se fundamenta la protección de la información personal.
- La información personal, constituye un patrimonio que debe ser garantizado, protegido, resguardado y sancionado, correspondiendo al sujeto la potestad de publicarlo, expresarlos o restringirlo.
- Los principios que prevalecen en la protección de datos personales, independientemente de su fuente manual o electrónica se refieren a la legalidad y lealtad, exactitud, finalidad, acceso, no discriminación, hacer excepciones, seguridad, emitir sanciones, flujo transfronterizo de datos y el campo de aplicación.
- La autorregulación, más que el control del Estado, como en el caso de Estados Unidos, es una estrategia que promueve la competencia y el desarrollo tecnológico, a la vez que limita las acciones indeseables autoritarias sobre el manejo de la información de datos personales.
- De la experiencia internacional, y dada la pulverización de los avances en telecomunicaciones, la colaboración entre naciones resulta indispensable para establecer un marco definitorio y jurídico para la permanente protección de los datos personales.

Acerca de las conclusiones sobre el estado actual de la legislación en México se concluye que:

- A nivel federal existe una fragmentación de la regulación sobre datos personales. Dicha situación implica falta de control de las autoridades y nula autorregulación de las instituciones que tienen bases de datos con información de la población.
- Igualmente, la fragmentación favorece la aplicación indiscriminada según situaciones concretas, lo que desprotege a aquellos que no están contemplados en las leyes existentes.
- A nivel estatal, el rezago en materia de protección es alto, hasta la fecha sólo cuatro entidades protegen a través de la ley los datos personales. Esto exige la atención de quienes ven afectados los derechos fundamentales que trastocan su dignidad, seguridad y privacidad.
- Es conveniente que se transite de la definición al establecimiento de normas específicas que engloben situaciones generales. Más aun, es necesario que se instrumenten los mecanismos de sanción aplicables a quien por medios ilícitos, de forma abusiva y vulnerando los derechos de dignidad y privacidad, comercializan la información sobre datos personales.

Con fecha del 2001, 2005, 2006, 2008, 2009 y recientemente en el 2010 la Comisión de Gobernación de la Cámara de Diputados ha presentado a LXI Legislatura una iniciativa de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, misma que a la fecha aun no ha sido aprobada. De todo lo anterior, el tema de la protección de datos personales continua vigente y en proceso de legislación.

BIBLIOGRAFÍA

BIBLIOGRAFÍA

Legislación:

Honorable Congreso de la Unión. (2009). Código Civil Federal. México

Honorable Congreso de la Unión. (2009). Código Penal Federal. México

Honorable Congreso de la Unión. (2009). Constitución Política de los Estados Unidos Mexicanos. México

Constitución Política del Estado Libre y Soberano de Colima. (2005). UNAM. México

Honorable Congreso de la Unión. (2009). Ley de Información Estadística y Geografía. México

Ley de Protección de Datos Personales del Estado de Colima. (2003). México

Ley de Protección de Datos Personales para el Distrito Federal. (2008). México

Honorable Congreso de la Unión. (2009). Ley de Seguridad Nacional. México

Honorable Congreso de la Unión. (2009). Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. México

Honorable Congreso de la Unión. (2008). Ley Federal del Derecho de Autor. México

Honorable Congreso de la Unión. (2009). Ley para Prevenir y Sancionar la Trata de Personas. México

Honorable Congreso de la Unión. (2008). Ley para Regular a las Agrupaciones Financieras. México

Honorable Congreso de la Unión. (2006). Reglamento de la Ley del Instituto del Fondo Nacional de la Vivienda para los Trabajadores. México

Fuentes bibliográficas:

Carbonell Sánchez, M. (2005). Los derechos fundamentales en México. México. Universidad Nacional Autónoma de México. Porrúa. CNDH.

Celis Quintal, M. (2006). “La protección de la intimidad como derecho fundamental de los mexicanos”. En Cienfuegos Salgado, D. y Macías Vázquez, M. (Coordinadores). Estudios en homenaje a Marcia Muñoz de Alba Medrano. Protección de la persona y derechos fundamentales. Universidad Nacional Autónoma de México.

Gómez-Robledo Alonso y Lina Ornelas Núñez. (2006). Protección de Datos Personales en México: El caso del Poder Ejecutivo Federal. UNAM. México.

Gregorio Carlos G. (2005). Protección de datos personales: Europa vs. Estados Unidos, todo un dilema para América latina. En Márquez Romero, Raúl. (Coordinador). Transparentar al Estado: la experiencia mexicana de acceso a la información. UNAM. México.

Laudon, Kenneth. Laudon, Jane. (2001). Management Information Systems. USA.

Muñoz De Alba Medrano, M y Cano Valle, A. (2002). *Derechos de las personas con Síndrome de Inmunodeficiencia Adquirida*. México. Cámara de Diputados. Universidad Nacional Autónoma de México.

Scalvini, E, y Leyva, C. (2002). *Las medidas precautorias y la tutela efectiva del derecho a la intimidad: Derecho a la información, habeas data e Internet*. La Rocca. Buenos Aires.

Téllez Valdés, Julio. (2006). Regulación del Spam en México. ITESM. México.

Fuentes hemerográficas

AMD e Intel, (2004). Mastermagazine. España.

Contreras, Oscar F., (2001). Martin Kenney y James Curry“. Internet y Desarrollo Regional en el Noroeste de México”. En Comercio Exterior, Vol. 51. Núm. 4, abril.

Dinatale, Martín. (2003). Circulan casi sin control las bases de datos personales: la dependencia que fiscaliza el manejo de la información privada está colapsada. En La Nación. Argentina. 28 de julio

Loperena, Félix. (2005) “Comercio electrónico” En Grupo Fórmula. México. Junio 22

Martí Font, J. M. (2009) “España promueve una Carta de la ONU para velar por la privacidad Expertos internacionales en protección de datos elaboran los criterios básicos” En El País. España. Enero 13

Mejía, José G. (2009). Publican reglamento para acceso y protección de datos personales. En El Universal. México. Abril 6

Pérez Fajardo, Judith. (2007). “Crece la base instalada de PC en el hogar.” En El Universal. septiembre 20

Ramiro Visser, Alexandra. (2005). Retos del B2B en España: concienciación pública e internacionalización. En Compras y Existencias Nº 137. Marzo-Abril. España

Ulloa, Aida. (2008) ¿Una base de datos segura? En El Universal. México. Marzo 26

Fuentes electrónicas:

Constitución de los Estados Unidos de América. Rivera García, Ignacio (Traductor). LexJuris. Puerto Rico. Tomado en http://www.lexjuris.com/lexuscon.htm el día 13 de marzo de 2009

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 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. Unión Europea. Bruselas. 2007 tomada de http://europa.eu/scadplus/leg/es/lvb/l14012.htm el 12 de marzo de 2009

Otras:

Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos. (2007). Comisión de las Comunidades Europeas. Bruselas Marzo 7.

Declaración de La Antigua (Guatemala) con motivo del II Encuentro Iberoamericano de Protección de Datos Personales. (2003). Guatemala.

El impacto de las tecnologías de la información en las empresas chilenas respecto a España y Estados Unidos. (2006). Instituto de Estudios Mediales. Chile.

FTC. (2009) “Remediando los Efectos del Robo de Identidad”. Consumer Response Center Washington, D.C.,

Instituto Federal de Acceso a la Información Pública. (2008). La protección de datos personales en México: una propuesta para deliberar. IFAI. México.

Naciones Unidas. (2005). Informe: Un concepto más amplio de la libertad: desarrollo, seguridad y derechos humanos para todos. ONU. Nueva York.

Naciones Unidas (1990). Directrices para la regulación de los archivos de datos personales informatizados. Adoptadas mediante resolución 45/95 de la Asamblea General, de 14 de diciembre de 1990. ONU. Nueva York.

OIT. (2006). Las tecnologías de la información, comunicación y la formación profesional. CINTERFOR. Organización Internacional del Trabajo. Uruguay.

Organización de Estados Americanos. (1969). Convención Americana sobre Derechos Humanos. OEA. Costa Rica.

Organización de Estados Americanos. (1948). Declaración America de Derechos y Deberes del Hombre. OEA. Washington.

Red Iberoamericana de Protección de Datos. (2005). Documento Estratégico Sobre la Red Iberoamericana de Protección de Datos. México.