UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

LICENCIATURA EN DERECHO

TRABAJO POR ESCRITO QUE PRESENTA:

PATRICIA RUIZ CORONA

TEMA DEL TRABAJO:

ñVIOLACIÓN A LA GARANTÍA CONSTITUCIONAL DE PROTECCIÒN DE DATOS PERSONALES EN MÈXICOò

EN LA MODALIDAD DE ñSEMINARIO DE TITULACIÓN COLECTIVAò

PARA OBTENER EL TÍTULO DE:

LICENCIADO EN DERECHO

FES Aragón

Nezahualcóyotl, Estado de México 2013

AGRADECIMIENTOS

A Dios por haberme permitido culminar una de mis metas;

A mis padres por su apoyo incondicional;

A mis hermanos por su motivación y aliento para seguir adelante;

A Leonardo porque sin su ayuda, no hubiera sido posible este gran anhelo;

A mi asesora Martha Leticia Ramírez por sus conocimientos y ser mi guía en este proyecto, y;

Principalmente a la Universidad Nacional Autónoma de México

Que me abrió sus puertas, me hizo crecer en todos los sentidos y me dio otra visión del mundo.

Por esto y mucho más

¡¡¡Gracias infinitas a la UNAM¡¡¡

Pág.

CAPÍTULO 3

INTRODUCCIÓN

La era de la informática que se vive actualmente, lejos de ser una etapa pasajera o efímera, tiende y tenderá a incrementarse cada día, mediante el empleo de nuevas técnicas y medios siempre más sofisticados que harán de las comunicaciones una necesidad pública. Frente a esta realidad se hace indispensable modernizar los elementos jurídicos con los que se cuenta para proteger a la persona en su esfera de intimidad.

La regulación de la privacidad y protección de datos personales ha sido abordada a nivel mundial, en México la privacidad y los datos de las personas está contenida en ordenamientos jurídicos a nivel federal. Sin embargo, en la medida en la que se extienda la penetración y uso de internet, se deberá evaluar la posibilidad de fortalecer el marco jurídico para que sea más eficiente la protección de datos y la información proporcionada por los ciudadanos a los órganos gubernamentales cuyos servicios y trámites se ofrecen en línea.

Para lograr dicho objetivo la investigación se ha estructurado de la siguiente manera:

En el Capítulo 1, se define el término Datos Personales de acuerdo a lo establecido en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y también lo señalado por algunos autores, así como su clasificación que se hace de los mismos que es: Datos Personales en General y Datos Sensibles.

También se hace referencia a los Principios Rectores que son una serie de reglas que deben tomar en cuenta tanto los entes públicos como privados en el tratamiento de datos personales, tales como el de licitud, consentimiento, de información, finalidad y vigilancia; que tienen como objetivo principal garantizar el uso adecuado de la información personal.

Por otro lado, se enuncian los derechos que tienen los ciudadanos en relación al tratamiento de sus datos personales, es decir, cualquier operación que se realice con los datos desde su obtención, uso, divulgación, almacenamiento, hasta su cancelación y supresión.

En el Capítulo 2, se enuncian y analizan los principales ordenamientos jurídicos vigentes, como lo es la Constitución Política de los Estados Unidos Mexicanos y la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que aluden al derecho de la protección de datos personales y las sanciones a quienes incumplan con dichos ordenamientos.

Finalmente en el Capítulo 3, se demuestra la vulnerabilidad del que son objeto nuestros datos personales que son recabados con o sin consentimiento por parte de alguna autoridad o entidad gubernamental, así como de los servidores públicos; y la susceptibilidad de ser transferidos a terceras personas ajenas a los mismos con el riesgo de ser utilizados para distintos fines, menos para el objetivo con el cuál fueron recopilados.

En este apartado, se señalan las ventajas y desventajas en la estructura del artículo 22 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, por lo que se determina la necesidad de modificar dicho artículo, para que exista certeza jurídica en la protección de los datos personales de los ciudadanos en poder del Estado en el ejercicio de sus funciones, y de ésta manera garantizar de manera eficaz el derecho constitucional de proteger nuestros datos personales en poder del Estado.

El método utilizado para ésta investigación fue el lógico-deductivo, ya que para determinar nuestro objeto de estudio, se tuvo que partir de conocimientos generales basados en el análisis y síntesis de los mismos para arribar a conclusiones particulares, que ayuden a lograr un resultado para la solución de dicha problemática.

CAPÍTULO 1
LA PROTECCIÓN DE DATOS PERSONALES

En la actualidad, el manejo e intercambio de datos se ha convertido en una práctica habitual como un tipo de comunicación a través de los medios electrónicos entre el Estado y el ciudadano. Estos datos son recogidos y acumulados en una base de datos, ya que para el Estado le es necesaria determinada información de los gobernados para el cumplimiento de sus fines, lo que hace posible que los mismos sean vulnerados y empleados por personas ajenas a los mismos con fines de lucro o para actos delictivos. De ahí la importancia de tener un control sobre las bases de datos en manos de las instituciones gubernamentales, mediante la protección y vigilancia de los mismos. Por lo anterior, se exponen los aspectos principales relativos a ésta garantía consagrada en la Constitución Política de los Estados Unidos Mexicanos.

1.1 DATOS PERSONALES

Actualmente, el uso extensivo de las tecnologías de la información y las telecomunicaciones ha permitido que en muchas ocasiones los datos personales sean utilizados para fines distintos para los que originalmente fueron recabados, y que sean transmitidos a diversas instancias a las que el titular de los datos confió información.

En el año 2002, en México se aprobó la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, la cual tiene como finalidad garantizar la protección de datos personales en posesión de los sujetos obligados como lo es el Poder Ejecutivo Federal, la Administración Pública Federal, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal.

1.1.1 Definición

La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en su artículo 3° señala:

> Datos personales es la información concerniente a una persona física, identificada o identificable.

De lo anterior, se puede inferir que los datos personales es cualquier información relacionada con nuestra persona, por ejemplo: nombre, número de teléfono, domicilio, fotografía o huellas dactilares, así como cualquier otro dato que pueda servir para identificarnos. Este tipo de datos nos permite interactuar con otras personas, o con una o más organizaciones, así como ser sujeto de derechos.

Por consiguiente, es necesario establecer qué es la protección de datos personales. Al respecto Miguel Ángel Dávara Rodríguez señala que:

> ñEs el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidadò[1]

Se interpreta como la necesidad de proteger la esfera privada del individuo, su intimidad de la posible utilización por parte de terceros de su información personal.

1.1.2 Tipos

Pueden clasificarse principalmente en:

---

[1] DÁVARA R., Miguel Ángel. ñManual de Derecho Informáticoò, Aranzandi Editores, España, 1997, p.47. Citado por OVILLA BUENO, Rocío.ò La Protección de Datos Personales en Méxicoò, Porrúa, México, 2005, p. 33.

Datos Personales (en general): Es la información que hace referencia a la persona de existencia física y se refiere a todos aquellos aspectos sobre su personalidad determinada (nombre, dirección, teléfono, edad).

Datos Sensibles: Información personal que revela origen racial, étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, datos acerca de su vida sexual, hábitos personales y sobre su estado de salud física o psíquica.[2]

1.1.3 Principios Rectores

Los principios de protección de datos pueden definirse como una serie de reglas mínimas que deben observar tanto los entes públicos como privados que tratan datos personales, garantizando con ello un uso adecuado de la información personal.

PRINCIPIO	CONTENIDO
1.- DE LICITUD	Es la prohibición para obtener informaciones por medios desleales o ilícitos
2.- DE CONSENTIMIENTO	Es necesario el consentimiento del titular de los datos personales para la obtención de los mismos. Es su derecho de la privacidad, pero este derecho no es ilimitado
3.- DE INFORMACIÓN	Consiste en informar previamente a las personas que sus datos personales van a integrar un archivo automatizado. Y pueden oponerse a tal situación y que tiene un derecho de acceso y de rectificación con respecto a los datos que les conciernen. **Ejemplo de leyenda de información:** **Los datos personales recabados serán protegidos y serán incorporados y tratados en el Sistema de Datos Personales (indicar nombre del sistema), con fundamento en (indicar fundamento**

[2] ANZIT GUERRERO, Ramiro, ñEl Derecho Informático Aspectos Fundamentalesò, Cathedra Jurídica, Argentina, 2010, p.74.

	legal) y cuya finalidad es (describir finalidad), el cual fue registrado en el Listado de Sistemas Personales ante el Instituto Federal de Acceso a la Información Pública (www.ifai.org.mx), y podrán ser transmitidos a (indicar receptores de las transmisiones), con la finalidad de (indicar finalidades), además de otras transmisiones previstas en la Ley. La Unidad Administrativa responsable del Sistema de Datos Personales es (indicar nombre de la unidad administrativa responsable), y la dirección donde el interesado podrá ejercer los derechos de acceso y corrección ante la misma es (indicar la dirección de la unidad de enlace). Lo anterior se informa en cumplimiento del Decimoséptimo de los Lineamientos de Protección de Datos Personales, publicados en el Diario Oficial de la Federación (incluir fecha).[3]
4.- DE FINALIDAD	Es una obligación para el recaudador de datos. Las informaciones deben de ser tratadas sólo cuando éstas sean adecuadas, pertinentes y no excesivas en relación con los propósitos para los cuales se hayan obtenido.
5.- DE VIGILANCIA	El controlador de los datos debe asegurar la seguridad de estos datos (evitar que sean hurtados). De lo contrario puede existir una responsabilidad del proveedor del servicio o de acceso o de la empresa que comercializa estos datos.[4]

1.2 INTIMIDAD Y PRIVACIDAD

Cuando se habla del concepto protección de datos se tiende a hablar de los términos intimidad y privacidad. Sin embargo, es necesario hacer la

[3] El derecho a la protección de datos personales en la Administración Pública Federal, disponible en: http://www.itei.org.mx/v3/micrositios/diplomado02/gdl/adjuntos/Sector_Publico_ITEI_18-19-nov-2011.pdf, consultado el 28-Agosto-2012, 8:40 P.M.

[4] Vid. OVILLA BUENO, Rocío. "La Protección de Datos Personales en México", Porrúa, México, 2005, p. 34.

distinción entre estos para delimitar el derecho a la intimidad, privacidad y la protección de datos de carácter personal.

1.2.1 Definición

Según el Diccionario de la Real Academia los define de la siguiente manera:

ñIntimidad. Se debe entender como una zona espiritual íntima reservada de una persona o un grupo, especialmente de una familia.

Privacidad. Es el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisiónò[5]

Entonces se podría decir que en dicha relación la intimidad es un ámbito más reservado que el de la privacidad. La intimidad comprende, por ejemplo, los sentimientos, las creencias (políticas, religiosas y morales), y la información sensible (como la médica o la relativa a la vida sexual); mientras que la privacidad comprende el ámbito (íntimo o no) en el cual un individuo tiene derecho a no recibir intromisión.

En cuanto a la protección de datos, el ámbito de intimidad comprende aquellos datos que bajo ninguna circunstancia proporcionaría un individuo de manera libre y consciente.

Para abordar de manera más clara la distinción entre intimidad y privacidad se dice que se puede recortar el espacio de vida privada de una persona hasta el límite, hasta suprimirlo sin que se destruya la persona, le queda el refugio inaccesible de su intimidad; en cambio sí se destruye la intimidad, la persona se desvanece. En efecto, se puede informar de la vida privada sin que ésta se destruya, en cambio la intimidad se resiste a la información.

---

[5] Diccionario de la Real Academia, Espasa Calpe., Vigésima Segunda edición, España, 2003. Citado por ANZIT GUERRERO, Ramiro, ñEl Derecho Informático Aspectos Fundamentalesò, Cathedra Jurídica, Argentina, 2010, p.71.

1.2.2 Intimidad e Informática

Los aspectos que refieren a la protección de datos requieren un tratamiento especial en el campo de las telecomunicaciones, dado que las mismas conllevan un riesgo adicional, cuanto más las telecomunicaciones electrónicas.

En el siglo XXI ya no es posible concebir la vida de los seres humanos ni su interacción, sin el uso de tecnologías informáticas. Dicha expansión conlleva el intercambio de flujos de información de todo tipo, incluida la relativa a las personas. Hoy en día es posible acceder a información sobre millones de personas y sus actividades en cualquier parte del mundo.

El hecho de que los avances tecnológicos permitan irrumpir silenciosamente en el ámbito de lo privado, vulnera la esfera de uno de los derechos fundamentales de los individuos, el de la intimidad y privacidad. Así pues, se puede afirmar que son violados dichas garantías, ya que sin que las personas se enteren, ni mucho menos otorguen su consentimiento, terceros (sean entes públicos o privados) recaban y transmiten información sobre sus datos personales a través de todo tipo de procedimientos y echan mano de nuevas tecnologías.

La probabilidad de que surjan abusos a la vida privada aumenta hoy como consecuencia del desarrollo de la llamada sociedad de la información. La expansión global de las redes informáticas y de comunicación hace cada vez más frecuentes los casos de robo de identidad o de discriminación a través de la obtención de perfiles que hacen identificables a las personas en sus patrones de consumo y de ahorro, o en sus inclinaciones y preferencias.

Dado que los medios tradicionales de protección de la vida privada son insuficientes en la actualidad, cada vez más países han aprobado leyes de protección de datos personales, tal es el caso de la Constitución española de 1978, que conecta la intimidad y la informática. Dicho texto establece en su artículo 18, entre otras ideas, el derecho a la intimidad, la inviolabilidad del

domicilio, el secreto de las comunicaciones, y establece, en el apartado 4, un encargo al legislador consistente en la limitación por ley del uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.[6]

1.3 DERECHOS RELATIVOS AL TRATAMIENTO DE DATOS PERSONALES

El tratamiento de datos personales se refiere a cualquier operación que se realice con nuestros datos, desde su obtención, uso, divulgación, almacenamiento, hasta su cancelación y supresión. Una vez que estos datos hayan sido recabados, las personas pueden ejercer ciertos derechos para verificar o impugnar el contenido de los archivos que les conciernen. Estos derechos también son conocidos como derechos ARCO.

TIPO	DERECHO A:
DE ACCESO	Obtener previa solicitud y con una frecuencia razonable, la confirmación de la existencia o inexistencia de los datos que le conciernen, la comunicación de dichos datos en forma inteligible, así como información acerca de su origen y en general su utilización. Sin embargo, existen excepciones al derecho de acceso. Estas excepciones suponen la adopción de medidas necesarias para: **a)** la defensa; **b)** las actuaciones penales; **c)** la seguridad pública; **d)** una función de control o de inspección inherente al ejercicio de la autoridad pública; y

[6] Vid. FERNÁNDEZ RODRIGUEZ, José Julio, ñLo público y lo privado en Internet: Intimidad y Libertad de expresión en la Redò, UNAM, México, 2004, p.97.

	e) un derecho equivalente de otra persona y los derechos y libertades de terceros.
DE RECTIFICACIÓN	El titular puede pedir que sus datos personales sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad. Este derecho se aplica a las informaciones inexactas, incompletas, equívocas o caducas. El responsable o usuario de la base de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias. Excepción de los casos en los cuales la supresión pudiese causar perjuicios a derechos o intereses legítimos e terceros, o cundo existiera una obligación legal de conservar los datos.
DE OPOSICIÓN O IMPUGNACIÓN	Si existe una cesión de informaciones o comercialización de archivos, esta cesión debe respetar el principio de respeto de vida privada y poder dar a cada una de las personas concernidas un derecho de impugnación. Una persona puede oponerse, por motivos legítimos, a que las informaciones nominativas que le conciernen sean objeto de un tratamiento automatizado o no. Sin embargo, este derecho de oposición tiene dos limitaciones: - su ejercicio se encuentra subordinado a la existencia de

	un motivo legítimo. - este derecho no se aplica a los tratamientos automatizados creados por las autoridades públicas. .
AL OLVIDO	Las informaciones no deben de ser conservadas bajo una forma nominativa más allá de la duración necesaria prevista en la declaración de obtención de esta información, a no ser que su conservación este autorizada por la autoridad competente.[7]

1.3.1 Sistema Persona

Cada vez que una dependencia o entidad desarrolla un sistema que contenga datos personales, deberá registrarlo en la aplicación informática desarrollada por el Instituto Federal de Acceso a la Información (IFAI) denominada Sistema Persona, que permite a las dependencias y entidades de la Administración Pública Federal cumplir con las obligaciones derivadas de los Lineamientos de Protección de Datos Personales, es decir, esta aplicación apoya en la actualización del listado de los sistemas de datos personales que poseen los sujetos obligados para registrar e informar sobre las transmisiones, modificaciones y cancelaciones de los mismos.

Cada dependencia o entidad debe contar con un administrador y un responsable por cada unidad administrativa que posea sistemas de datos personales.

El administrador es el titular de la dependencia o entidad, registra a las unidades administrativas y administra a los usuarios de la dependencia o entidad.

[7] Vid. OVILLA BUENO, Rocío. op.cit., p.36.

El responsable del sistema de datos personales es el Titular de la Unidad Administrativa cuya función es administrar el sistema de datos personales y las transmisiones de los mismos.

En el Sistema Persona se registra e informa sobre las transmisiones, modificaciones y cancelaciones de los sistemas de datos personales, así como información general de éstos relativa:

1) Al nombre de la base de datos personales;
2) La unidad administrativa en la que se encuentra;
3) Al nombre, cargo, teléfono y correo electrónico del responsable;
4) La finalidad de la base de datos;
5) La normatividad aplicable.

La finalidad es que toda persona pueda conocer qué tipo de datos están en posesión del gobierno.

La consulta es pública y gratuita y basta con agregar el nombre de la dependencia o entidad de la Administración Pública Federal para realizar la búsqueda.

1.3.2 Lineamientos de Protección de Datos Personales

Publicados por el IFAI el 30 de Septiembre de 2005, tienen como finalidad establecer las políticas y procedimientos que deben observar las dependencias y entidades de la Administración Pública Federal para garantizar al titular de los datos la facultad de decidir sobre el uso y destino de su información, a fin de asegurar su adecuado tratamiento e impedir su transmisión ilícita y lesiva.

Conceptualizan los principios que rigen el tratamiento de datos personales que se deben observar en la Administración Pública Federal, y establecen las condiciones y requisitos mínimos para el manejo y custodia de los sistemas de datos personales en poder de la Administración Pública Federal.

De conformidad con dichos lineamientos, ñUn sistema de datos personales constituye el conjunto ordenado de datos personales que estén en posesión de una dependencia o entidad, con independencia de su forma de acceso, creación, almacenamiento u organizaciónò

Existen sistemas físicos y automatizados, definiéndose de la siguiente manera:

- **Sistemas físicos**: Conjunto ordenado de datos contenidos en registros manuales, impresos, sonoros, magnéticos, visuales u holográficos.
- **Sistemas automatizados**: Conjunto ordenado de datos que por su naturaleza, requieren de una herramienta tecnológica específica para su acceso, recuperación o tratamiento.[8]

Por lo tanto, el ejercicio de las atribuciones de las dependencias y entidades de la Administración Pública Gubernamental implica recabar datos personales para los fines establecidos en las disposiciones aplicables, por lo que los servidores públicos deben ser los primeros obligados al cumplimiento de la ley, para promover el uso responsable de las nuevas tecnologías de la información, atendiendo los principios de protección de datos personales de: licitud, calidad, de información al titular sobre el uso y destino de su información, de seguridad, custodia y consentimiento para su transmisión; principios que no limitan la utilización de la informática en el ámbito público, sino que se trata de hacerla compatible con los derechos de los ciudadanos.

[8]Vid. Guía Práctica para la Gestión de las Unidades de Enlace y Comités de Información en las dependencias y entidades de la Administración Pública Federal, disponible en: http://www.resi.org.mx/icainew/images%5CBiblioteca%5CPublicaciones%5CGPUETomoII.pdf, consultado el 01-Octubre-2012, 7 P.M.

CAPÍTULO 2
REGULACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES EN LA LEGISLACIÓN VIGENTE

2.1 CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS

En México, hay que contemplar de un lado la protección de la vida privada a través del derecho de la privacidad y de intimidad y por otro, la existencia de un marco legislativo de la protección de datos personales. El objeto del derecho a la intimidad es la protección de los datos e información personal, propias del ser humano. Este derecho va a evitar toda intromisión en la esfera privada del mismo.[9]

La protección expresa de los datos personales en la Constitución Política de los Estados Unidos Mexicanos, así como la legislación expedida al respecto en ordenamientos secundarios, se integraron al marco jurídico mexicano de manera relativamente reciente, en 1977 se reconoció la garantía del derecho a la información con la adición del artículo 6° de la Constitución Federal. 30 años después, México tiene en materia de derecho de información una práctica normativa a nivel federal y local, que se inicia a partir de la publicación en el Diario Oficial de la Federación la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

El 20 de Julio de 2007 se publicó en el Diario Oficial de la Federación, la adición de un segundo párrafo con siete fracciones, concretamente nos referiremos sólo a las fracciones II Y III y que textualmente dice:

> **Artículo 6.**
> **Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:**
>
> **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.**

[9] Vid. OVILLA BUENO, Rocío. op.cit., p.27.

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 estos.

El artículo que antecede:

- Refiere a las bases y principios que rigen la actuación de la Federación, los Estados y el Distrito Federal para el ejercicio del derecho de acceso a la información.
- Privilegia el principio de la publicidad y mantiene la reserva para la información que con tal carácter así establezcan las leyes.
- Establece que la vida privada y los datos personales serán tutelados en términos de lo que establecen las leyes, la gratuidad de la información, libera de la justificación del interés legítimo para la solicitud de información y su procedencia.

Por otra parte, existe en el cuerpo constitucional un precepto que fue adicionado en el año de 2009 relativo a la protección de datos personales, el cual se encuentra contenido en el párrafo segundo del artículo 16, pero que también es de vital importancia el primer párrafo que señala lo siguiente:

Artículo 16. 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.
Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Constituye el derecho de que ningún ciudadano puede ser molestado en cuanto a su persona, familia, domicilio, papeles o posesiones, a menos que sea por medio de un mandamiento por escrito de la autoridad competente, y que funde y motive la causa legal de su actuar.

También se reafirma el derecho que tienen los ciudadanos a que se protejan sus datos personales, en los términos que fije la ley, a través de los derechos conocidos como ARCO, de los cuales se hablaron en el capítulo anterior. Sin embargo se señalan algunas excepciones a dichos principios, tal es el caso de que el ciudadano no podrá negarse a la obtención y tratamiento de sus datos para el Catastro, la CURP, la credencial de elector, el Registro Público de la Propiedad, el Registro de Inmatriculación de Vehículos, o para las Actas del Registro Civil.

También los datos que estén dirigidos a autoridades y se cuente con autorización judicial, prevalece el valor de la seguridad pública sobre el derecho de privacidad.

El gobernado tampoco puede oponerse a la transferencia de sus datos si se trata de transferencias entre administraciones públicas que tengan una finalidad estadística o científica, y se trate de datos sobre la salud, además de ser necesarios para atender alguna circunstancia emergente o para estudios epidemiológicos, sólo por mencionar algunas.

En resumen, se señalan que son los preceptos contenidos en la Constitución Federal, tanto en el artículo 6 como en el 16, enmarcados en el contexto de las garantías de libertad, que establecen con mayor claridad y precisión la protección de datos personales, de tal forma que sea un límite al abuso que so pretexto del ejercicio de la garantía de acceso a la información, provoque afectaciones directas sobre la persona, es decir, que vulnere la protección de su intimidad, por lo que deben considerarse confidenciales, así como la información que se refiera a su vida privada.

2.2 LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL

Ésta ley es imprescindible ya que todo individuo, si bien es cierto pertenece a una sociedad determinada, éste debe de respetar la parte privada e

íntima de toda persona, por lo que se le debe otorgar seguridad jurídica, ser protegido por la legislación y el Estado contra la invasión de su intimidad y privacidad, a conocer, rectificar, suprimir y prohibir la divulgación de determinados datos, especialmente los sensibles, y que la información que él proporcione tenga el destino exclusivo para el que fue otorgado.

Dicha ley fue publicada en el Diario Oficial de la Federación el 11 de Junio de 2002, y su finalidad se establece en el art. 1° que a la letra dice:

> **Artículo 1°. La presente Ley es de orden público. 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.**

Al respecto es de resaltar que cuando se refiere el texto a ñtoda personaò se alude a que debe ser sin ningún tipo de discriminación social, política, económica, por edad, de género, etc.; y que dicha información se encuentre en posesión de los Poderes de la Unión u órganos constitucionales autónomos tales como el Instituto Federal Electoral, la Comisión Nacional de Derechos Humanos, el Banco de México, las Universidades y demás instituciones de educación superior a las que la ley otorgue autonomía y cualquier otro establecido en la Constitución Política de los Estados Unidos Mexicanos.

En el artículo 4° fracción III se establece uno de los objetivos más importantes de esta ley en relación a este tema y que es:

> **Artículo 4. Son objetivos de esta Ley:**
> **Ié**
> **III. Garantizar la protección de los datos personales en posesión de los sujetos obligados;**

Esta protección de los datos personales deberá llevarse a cabo por los sujetos obligados que se encuentran establecidos en el artículo 3° fracción XIV, que son:

> **Artículo 3. Para los efectos de esta Ley se entenderá por:**
> **Ié**
> **XIV. Sujetos obligados:**

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.

En pocas palabras, cualquier autoridad de alguna dependencia o entidad gubernamental se considera sujeto obligado.

Es necesario señalar que la ley no es una ley que permita tener acceso a toda clase de documentos de carácter administrativo que pertenezcan a la Administración Pública Federal. Sólo en ciertos casos, definidos como excepciones por la propia ley, la información que poseen las dependencias y entidades podrá clasificarse como reservada o confidencial, establecidos en los siguientes artículos:

Artículo 13. Como información reservada podrá clasificarse aquélla cuya difusión pueda:
I. Comprometer la seguridad nacional, la seguridad pública o la defensa nacional;
II. Menoscabar la conducción de las negociaciones o bien, de las relaciones internacionales, incluida aquella información que otros estados u organismos internacionales entreguen con carácter de confidencial al Estado Mexicano;
III. Dañar la estabilidad financiera, económica o monetaria del país;
IV. Poner en riesgo la vida, la seguridad o la salud de cualquier persona, o
V. Causar un serio perjuicio a las actividades de verificación del cumplimiento de las leyes, prevención o persecución de los delitos, la impartición de la justicia, la recaudación de las contribuciones, las operaciones de control migratorio, las estrategias procesales en procesos judiciales o administrativos mientras las resoluciones no causen estado.

Del artículo anterior, se establecen los supuestos en que se encuadra la información clasificada como reservada, un ejemplo es la relativa a la seguridad nacional cuya información trate de acciones destinadas a proteger la integridad, estabilidad y permanencia del Estado Mexicano, la defensa exterior y la

seguridad interior de la Federación, orientadas al bienestar general de la sociedad que permitan el cumplimiento de los fines del Estado.

> **Artículo 14. También se considerará como información reservada:**
> **I. La que por disposición expresa de una Ley sea considerada confidencial, reservada, comercial reservada o gubernamental confidencial;**
> **II. Los secretos comercial, industrial, fiscal, bancario, fiduciario u otro considerado como tal por una disposición legal;**
> **III. Las averiguaciones previas;**
> **IV. Los expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio en tanto no hayan causado estado;**
> **V. Los procedimientos de responsabilidad de los servidores públicos, en tanto no se haya dictado la resolución administrativa o la jurisdiccional definitiva, o**
> **VI. La que contenga las opiniones, recomendaciones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos, hasta en tanto no sea adoptada la decisión definitiva, la cual deberá estar documentada.**
> **Cuando concluya el periodo de reserva o las causas que hayan dado origen a la reserva de la información a que se refieren las fracciones III y IV de este Artículo, dicha información podrá ser pública, protegiendo la información confidencial que en ella se contenga.**
> **No podrá invocarse el carácter de reservado cuando se trate de la investigación de violaciones graves de derechos fundamentales o delitos de lesa humanidad.**

En ésta última es en donde se protege la confidencialidad de los datos personales, que requieren el consentimiento de los individuos para su difusión, distribución o comercialización.

Dicha información puede permanecer bajo estas características hasta por un período de 12 años, pasado este tiempo la información podrá ser revelada

En cuanto a la información confidencial se refiere, se estará a lo que establece el artículo 18:

> **Artículo 18. Como información confidencial se considerará:**
> **I. La entregada con tal carácter por los particulares a los sujetos obligados, de conformidad con lo establecido en el Artículo 19, y**
> **II. Los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta Ley.**

No se considerará confidencial la información que se halle en los registros públicos o en fuentes de acceso público.

Dicho artículo considera como información confidencial, con el carácter de confidencial, entregada a los sujetos obligados por los ciudadanos, y que se requiere el consentimiento de los mismos para que pueda ser difundida, distribuida o comercializada.

También considera que la información contenida en registros públicos no es confidencial, sin embargo, la ley no establece ninguna definición sobre qué es un registro público, a efecto de facilitar una interpretación que proteja la privacidad de datos personales

El Capítulo IV titulado Protección de Datos Personales se refiere a responsabilidades, prohibiciones, deberes y acciones, encaminados a la protección de la información de los individuos contenida en los datos personales, es decir, de la información concerniente a una persona física, identificada o identificable, cuya posesión se encuentra a disposición de los sujetos obligados, que son según la ley, los órganos integrantes de los Poderes de la Unión, los constitucionales autónomos, los Tribunales Administrativos Federales, y en general cualquier otro de carácter Federal.

Específicamente el artículo 20, establece las responsabilidades de los sujetos obligados en cuanto a los datos personales, que son:

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.

Los sujetos obligados son los principales encargados de que se cumplan cabalmente los lineamientos en cuanto a la protección de datos personales, mediante mecanismos y procedimientos de acceso y corrección de datos, informándole a los ciudadanos el propósito para el cual han sido recabados y que estos datos sean exactos y actualizados garantizando el buen uso de los mismos.

Asimismo, es indispensable que los servidores públicos estén capacitados para poder manejar adecuadamente la información a fin de poder recibir y responder las solicitudes de acceso y corrección de datos personales requeridos por los ciudadanos.

El artículo 21 establece que:

Artículo 21. 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.

Los responsables del manejo de los datos personales, según la ley, son los sujetos obligados, específicamente los obliga a la corrección, protección, tratamiento, disposición (para los individuos), actualización, sustitución, rectificación, complementación y garantizar la seguridad de los mismos, estableciéndose la prohibición de difundir, distribuir o comercializar, los contenidos en sus respectivos sistemas de información, desarrollados en el ejercicio de sus funciones, excepto cuando exista un consentimiento previo y expreso.

Respecto del manejo de la información referida de los datos personales, la Ley señala algunas excepciones, a decir de estas:

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.

En cuanto a la obtención de datos personales debe ser mediante el consentimiento de los interesados, de lo contrario podría ser considerado como un acto ilícito, sin embargo, estos supuestos de excepción se encuentran no del todo justificadas, ya que el hecho de que el ciudadano no pueda oponerse a su obtención no implica que sus datos personales se puedan utilizar para fines distintos a los previstos.

También una de las obligaciones de los sujetos obligados, es el que se establece en el artículo 23, que es el de reportar al IFAI el listado actualizado de los sistemas de datos personales que posean por cualquier título.

Artículo 23. Los sujetos obligados que posean, por cualquier título, sistemas de datos personales, deberán hacerlo del conocimiento del Instituto o de las instancias equivalentes previstas en el Artículo 61, quienes mantendrán un listado actualizado de los sistemas de datos personales.

Asimismo, el artículo 24 de dicha ley, faculta a los interesados o sus representantes, para actuar en relación en sus datos personales ante los sujetos obligados en los siguientes supuestos:

1. Solicitar que les sean proporcionados de manera gratuita, en un plazo de 10 días hábiles, a partir de la fecha de la solicitud de los mismos.

2. Solicitar la modificación de los que consten en el sistema de datos personales respectivo, señalando las modificaciones y aportando la documentación.
3. La posibilidad de interponer un Recurso de Revisión ante la autoridad competente por la negativa de entregar o corregirlos.

Artículo 63. Serán causas de responsabilidad administrativa de los servidores públicos por incumplimiento de las obligaciones establecidas en esta Ley las siguientes:
I. Usar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar, total o parcialmente y de manera indebida información que se encuentre bajo su custodia, a la cual tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;
II. Actuar con negligencia, dolo o mala fe en la sustanciación de las solicitudes de acceso a la información o en la difusión de la información a que están obligados conforme a esta Ley;
III. Denegar intencionalmente información no clasificada como reservada o no considerada confidencial conforme a esta Ley;
IV. Clasificar como reservada, con dolo, información que no cumple con las características señaladas en esta Ley. La sanción sólo procederá cuando exista una resolución previa respecto del criterio de clasificación de ese tipo de información del Comité, el Instituto, o las instancias equivalentes previstas en el Artículo 61;
V. Entregar información considerada como reservada o confidencial conforme a lo dispuesto por esta Ley;
VI. Entregar intencionalmente de manera incompleta información requerida en una solicitud de acceso, y
VII. No proporcionar la información cuya entrega haya sido ordenada por los órganos a que se refiere la fracción IV anterior o el Poder Judicial de la Federación.

La responsabilidad a que se refiere este Artículo o cualquiera otra derivada del incumplimiento de las obligaciones establecidas en esta Ley, será sancionada en los términos de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.

La infracción prevista en la fracción VII o la reincidencia en las conductas previstas en las fracciones I a VI de este Artículo, serán consideradas como graves para efectos de su sanción administrativa.

En cuanto al artículo antes referido, se señalan las causas de responsabilidad administrativa de los servidores públicos en caso de usar, sustraer, destruir, ocultar, inutilizar, divulgar o alterar de manera total o parcialmente y de manera indebida la información que se encuentre bajo su resguardo; o que actúen intencionalmente de manera irresponsable en la

sustanciación de las solicitudes de acceso a la información o en la difusión de dicha información; o entregar incompleta información requerida en dichas solicitudes.

También incurrirán en responsabilidad en caso de que nieguen de forma intencional información que no es clasificada como reservada o no considerada como confidencial, clasificar como reservada, con el fin de perjudicar, información que no cumpla las características señaladas por la ley como se mencionó anteriormente; así como entregar información considerada como reservada o confidencial a persona ajena a la misma, o no proporcionar información solicitada por alguna autoridad.

En caso de reincidencia en cualquiera de las conductas anteriores serán consideradas como graves.

De conformidad con el artículo 63 de la Ley, las sanciones aplicables a los servidores públicos que incurran en responsabilidad administrativa por el incumplimiento de las obligaciones derivadas de los preceptos de la misma, será en términos de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos establecidas en su artículo 13 que dice:

> **Artículo 13.- Las sanciones por falta administrativa consistirán en:**
> **I.- Amonestación privada o pública;**
> **II.- Suspensión del empleo, cargo o comisión por un período no menor de tres días ni mayor a un año;**
> **III.- Destitución del puesto;**
> **IV.- Sanción económica, e**
> **V.- Inhabilitación temporal para desempeñar empleos, cargos o comisiones en el servicio público. Cuando no se cause daños o perjuicios, ni exista beneficio o lucro alguno, se impondrán de tres meses a un año de inhabilitación.**
> **Párrafo reformado DOF 05-06-2012**
> **Cuando la inhabilitación se imponga como consecuencia de un acto u omisión que implique beneficio o lucro, o cause daños o perjuicios, será de un año hasta diez años si el monto de aquéllos no excede de doscientas veces el salario mínimo general mensual vigente en el Distrito Federal, y de diez a veinte años si excede de dicho límite. Este último plazo de inhabilitación también será aplicable por conductas graves de los servidores públicos.**

Las sanciones administrativas para los servidores públicos irán desde una amonestación pública o privada hasta la suspensión del empleo o cargo o la destitución definitiva de su puesto, así mismo tendrán una sanción económica las cuales podrán ser de hasta tres veces de los beneficios o lucros obtenidos o de los daños o perjuicios causados, pero en ningún caso podrá ser menor o igual al monto de los beneficios o lucro obtenidos o de las daños o perjuicios causados.

> **Artículo 64. Las responsabilidades administrativas que se generen por el incumplimiento de las obligaciones a que se refiere el Artículo anterior, son independientes de las del orden civil o penal que procedan.**

Esto es, que además de las responsabilidades que pueda tener establecidas en la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, también tendrán responsabilidad civil o penal.

En cuanto al orden civil, se refiere al daño moral que pueda producir el Estado y sus servidores públicos a cualquier persona, tal como lo establece el artículo 1916 del Código Civil Federal:

> **Artículo 1916.- Por daño moral se entiende la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspecto físicos, o bien en la consideración que de sí misma tienen los demásé**
>
> **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,é así como el Estado y sus servidores públicos...**

Es decir, cuando alguna persona sufre alguna afectación en sus sentimientos, afectos, creencias, decoro, honor, reputación o vida privada, como es el caso de los datos personales que son recabados por alguna entidad gubernamental y ésta haya hecho mal uso de ellos, como ya se mencionó anteriormente, se dice que hay un daño moral y el responsable, en este caso el Estado o sus servidores públicos, deberán de reparar el daño mediante una indemnización en dinero a la persona afectada.

Por lo que respecta al ámbito penal, se aplicará lo establecido en el Código Penal Federal en la que se tipifican los supuestos relativos a la materia de datos personales que se encuentran en posesión de entidades gubernamentales, en los siguientes artículos:

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.
Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Artículo 211 bis 3.- Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa.
Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa.

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

Aquí se señalan las sanciones penales a la que son acreedores, al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado y que están protegidos por un sistema de seguridad, se le impondrá de 1 a 4 años de prisión y de 200 a 600 días de multa; y al que sin autorización conozca o copie información contenida en los sistemas antes mencionados, se le impondrá de 6 meses a 2 años de prisión y de 150 a 400 días de multa.

Por otro lado, el que cuente con autorización para acceder a sistemas y equipos de informática del Estado, y que indebidamente modifique, destruya o provoque pérdida de información contenidos en ellos, se impondrán de 2 a 8 años de prisión y de 300 a 900 días de multa; y al que estando autorizado para acceder a los sistemas y equipos de informática del Estado e indebidamente copie información contenida en los mismos, se impondrá de 1 a 4 años de prisión y de 150 a 450 días de multa.

Sin embargo, estas penas podrán aumentar hasta en una mitad cuando la información obtenida sea utilizada para beneficio propio o de alguna persona ajena.

Finalmente el derecho a la información, expresa el derecho que tiene toda persona a ejercer el control de la circulación de la información relacionada con asuntos de naturaleza pública, pero también la privada, es el caso de los datos personales, el difícil dilema de poder conjugar la información concerniente a lo esencial de la vida, pero manteniendo al mismo tiempo la relación social, los vínculos y la vida privada libre de intromisiones externas; sin embargo, con el desarrollo de la tecnología y la creciente demanda de información de nuestros días, esto parece ser imposible.

Esta consideración tiene una doble explicación, ya que por un lado puede tratarse de la inseguridad que representa el almacenamiento, recopilación o transmisión de datos, en las redes internas de las entidades públicas, o bien, a pesar de la seguridad, debido al ingenio que poseen algunas personas que por diversas razones manipulan sistemas informáticos ajenos; ya sea por una u otra de las razones, la vida privada de las personas se encuentra susceptible de ser vulnerada.

CAPÍTULO 3

VIOLACIÓN A LA GARANTÍA CONSTITUCIONAL DE PROTECCIÓN DE DATOS PERSONALES

El avance de la tecnología ha traído mayores niveles de bienestar social, al tiempo que ha puesto contra la pared algunos derechos fundamentales como lo es el derecho a la privacidad consagrado en el artículo 16 Constitucional, la protección de datos personales ha estado presente desde hace varios años, mediante los avances en materia de informática algunas instituciones públicas tienen un amplio conocimiento de nuestra información personal, para el mejor desempeño de sus funciones.

En el contexto que actualmente aqueja a la población mexicana, debido a la enorme inseguridad que nos invade, el tema de protección de datos personales viene a ser trascendental, ya que la tecnología permite obtener, modificar o alterar, borrar, extraer, tratar, ordenar, generar, difundir y almacenar datos personales de manera ilimitada, tanto de forma legal como ilegal.

Es importante que no se pase por alto este derecho, porque todos quedamos vulnerables al no contar con los derechos mínimos de protección a nuestra intimidad, a través de la propagación que se hace de nuestra información de carácter personal como lo es el nombre, domicilio, edad, salario y distintas preferencias desde las comerciales, religiosas, hasta políticas o sexuales; todos estos datos pueden tener distintos usos y la posibilidad de que estos cambien del destinatario original a otro, es muy alta. [10]

En México, la privacidad de los datos personales, como ya se mencionó en el capítulo anterior, se encuentra regulada en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, derivada de la Constitución Política de los Estados Unidos Mexicanos como una nueva

[10] Vid. Datos Personales, Estudio de Derecho Comparado a nivel Estatal e Internacional, así como de Opiniones Especializadas (segunda Parte). Disponible en: http://www.diputados.gob.mx/cedia/sia/spi/SPI-ISS-25-09.pdf, consultado el 05 de Agosto de 2012, 5 P.M.

garantía ciudadana básica del siglo XXI. Sin embargo, en la medida de que se extienda la penetración y uso de internet, se deberá de contar con un marco jurídico más eficiente que proteja los datos y la información proporcionada por los ciudadanos a los órganos gubernamentales cuyos servicios y trámites se ofrecen en línea; así como herramientas tecnológicas más seguras. Es por ello, que resulta relevante saber qué harán estas entidades y dependencias de los tres niveles de gobierno con esta información y datos proporcionados por los ciudadanos, al llevar a cabo dichos trámites.

Asimismo, la evolución tecnológica, hace posible la vulneración de derechos fundamentales con gran facilidad, como lo es el derecho a la intimidad y privacidad; un ejemplo de ello es que, el Poder Ejecutivo Federal administra grandes bases de datos con información muy variada de las personas, ya sea para el ejercicio de sus atribuciones o para la adecuada aplicación de las leyes.

Es el caso de la base nacional de datos de la Clave Única del Registro de Población (CURP), la base de datos del Servicio de Administración Tributaria (SAT) sobre contribuyentes, los sistemas de expedientes clínicos del Sector Salud en el que se alojan millones de expedientes de derechohabientes, incluso las bases de datos generados en materia de seguridad pública que utilizan herramientas tecnológicas que permiten renovar y modernizar la acción policial, también los obtenidos a través de trámites diversos como la obtención de la credencial de elector, el registro vehicular y las licencias de conducir, entre otros, han sido vulnerados y transferidos a terceros; lo que viola el derecho a la protección de datos consagrada en nuestra Carta Magna.

3.1 AUTORIDAD RESPONSABLE DE LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

El Instituto Federal de Acceso a la Información y Protección de Datos es la autoridad garante en materia de protección de datos personales. La ley le ha otorgado la facultad de difundir el conocimiento de este nuevo derecho entre la

sociedad mexicana, de promover su ejercicio y vigilar su debida observancia por parte de los entes públicos o privados que poseen datos personales.

Con el propósito de coadyuvar con el Instituto en la debida aplicación de la ley, dependencias de la Administración Pública Federal, colaborarán con el IFAI en la emisión de la regulación que corresponda. Entre ellas están las Secretarías de Economía, Salud, Comunicaciones y Transportes, Hacienda y Crédito Público, Educación; las cuales deberán emitir normas específicas para la protección de datos personales en los sectores económico, de salud, telecomunicaciones, financiero y educativo.

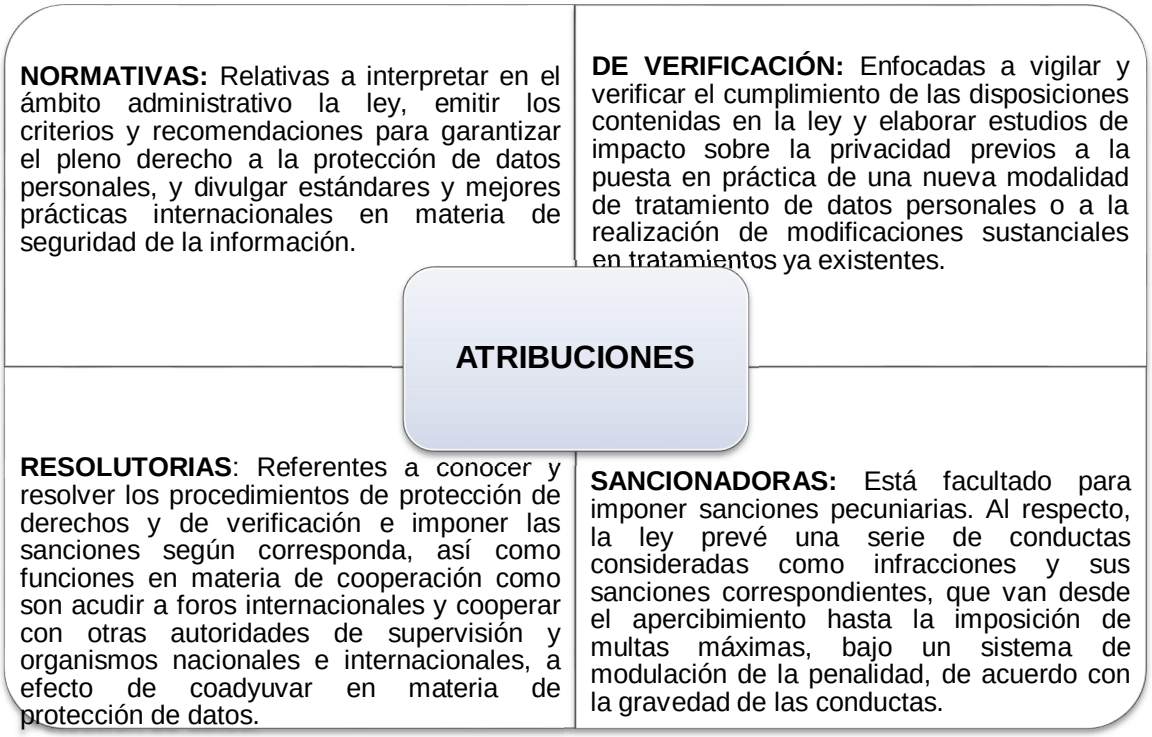
3.1.1 Instituto Federal de Acceso a la Información y Protección de Datos

La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), contempla en el artículo 33, la creación del Instituto Federal de Acceso a la Información y Protección de Datos Personales, el cual comenzó a operar oficialmente en Junio de 2003 gozando desde entonces con autonomía operativa, presupuestaria y de decisión.

El IFAI está encargado de cumplir y hacer cumplir la LFTAIPG en el ámbito del Poder Ejecutivo Federal, y es la instancia encargada de promover y difundir el ejercicio del derecho de acceso a la información y de resolver la negativa de las autoridades de dar respuesta a las solicitudes de acceso a la información. Asimismo, desde el año 2010, el IFAI es la autoridad garante del derecho a la protección de datos personales, derecho de tercera generación. Igualmente, se dota al Instituto de facultades informativas, normativas, de verificación, resolutorias y sancionadoras que en su conjunto garantizarán la plena vigilancia del cumplimiento de dicha ley, y por consiguiente será el IFAI el que vele por el debido respeto de este nuevo derecho.[11]

A decir de sus atribuciones, se tienen las siguientes:

[11] Vid. Introducción al Instituto Federal de Acceso a la Información y Protección de Datos. Disponible en: http://www.privacyconference2011.org/includes/IntroduccionalIFAIEspanol.pdf, consultado el 01-Agosto-2012, 7:00 P.M.



Para la imposición de la sanción, el Instituto deberá tomar en cuenta factores como la naturaleza del dato, la notoria improcedencia de la negativa del responsable para realizar los actos solicitados por el titular, el carácter intencional o no de la acción u omisión constitutiva de la infracción, la capacidad económica del responsable y la reincidencia.

Lo anterior, en virtud de que la ley debe desincentivar conductas contrarias a lo establecido por la misma, y al tratarse de un derecho fundamental reconocido a nivel constitucional, debe garantizarse al ciudadano una vez que ha sido violado su derecho, habrá una consecuencia para el responsable que actuó con negligencia o dolo en el debido tratamiento de su información, máxime cuando éste fuere sensible.[12]

[12]Vid. Autoridad Garante, disponible en: http://www.ifai.org.mx/buscador_ifai/buscar.do?type=all&spell=true&lemmatize=true&fuentes=4&queryStr=FUNCIONES%20DEL%20IFAI, consultado el 28-Agosto-2012, 12:00 P. M.

Es importante destacar que para efectos de sus resoluciones, el IFAI no está subordinado a autoridad alguna, ya que es un organismo descentralizado de la Administración Pública Federal, no sectorizado por lo que goza de autonomía operativa, presupuestaria y de decisión. Es una institución al servicio de la sociedad.

3.2 VULNERABILIDAD EN LA TRANSFERENCIA DE DATOS PERSONALES

La falta de una legislación efectiva y de una cultura de protección de datos personales, favorece prácticas como el tráfico de datos personales con fines comerciales o delictivos. El avance tecnológico al tiempo que da seguridad a algunos, produce la inseguridad de muchos más.

Actualmente, no existen muchas barreras para dificultar el acceso por terceros al conocimiento de la vida ajena. Los medios electrónicos hacen posible la intromisión no autorizada en la vida privada de los individuos y permiten el acopio de todo tipo de información relativa a una persona identificada o identificable y pueden utilizarla sin su consentimiento.

De ahí la importancia de contar con mecanismos eficientes que eviten que sean transgredidos los derechos fundamentales consagrados en nuestra Carta Magna, así como sancionar de manera eficaz y severa a los sujetos obligados encargados de velar dicha protección de datos personales de los ciudadanos.

A continuación, algunos ejemplos que demuestran claramente la violación de esta garantía constitucional.

3.2.1 Instituto Federal Electoral

En México, en materia política, una modalidad del flujo de información y su trascendencia puede advertirse en el proceso de revisión del padrón electoral bajo varios ángulos:

a) Los ciudadanos otorgan determinados datos al IFE para obtener su credencial para votar y, a su vez, para la integración de dicho documento; en tanto,
b) Los partidos políticos, en ejercicio de la libertad de información y de fiscalización del proceso electoral, participan en la actualización de dicho padrón, con lo cual, consecuentemente, acceden a tales datos.

De esta manera, los datos de millones de ciudadanos que forman parte de él son manejados por los partidos políticos, lo cual incluye, desde luego, el que éstos conozcan determinada información personal o de la vida privada de los ciudadanos.

Esto es, el mismo sistema democrático exige que los ciudadanos mexicanos otorguen alguno de sus datos personales para poder ejercer el derecho fundamental de votar y, a la vez, autoriza a los partidos políticos a revisar esos datos, en el proceso de revisión del padrón.

Durante la campaña electoral por la presidencia de México para el período 2006-2012, el Partido Acción Nacional (PAN) creó una red de apoyo de simpatizantes a la candidatura de Felipe Calderón Hinojosa.

Para el desarrollo de esta red, se creó un procedimiento de registro de simpatizantes en el sitio de internet del candidato presidencial, en el cual, para inscribirse, el sistema pedía aportar el nombre como aparece en la credencial para votar e, incluso, la fecha de nacimiento, si ello no era así, el sistema electrónico no permitía el registro.

Por tal razón, la entonces Coalición Por el Bien de Todos (integrada por el PRD, Convergencia y PT) presentó la denuncia ante el Consejo General del IFE en contra del PAN por:

a) La utilización indebida del padrón electoral o de las listas nominales de electores, y;

b) Violación a la confidencialidad de los datos personales contenidos en los documentos señalados.

La autoridad electoral declaró fundada la queja y le impuso al partido denunciado una sanción económica equivalente a $252,850 (doscientos cincuenta y dos mil, ochocientos cincuenta pesos), pero sólo por la primera de las faltas.

El PRD pidió, fundamentalmente, que no sólo se sancionara al PAN por el uso indebido del padrón electoral, sino por violar la confidencialidad de los datos personales de los ciudadanos inscritos.[13]

En resumen, es cuestionable el cumplimiento de uno de los objetivos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, consistente en que todos los sujetos obligados por la Ley, entre ellos el Instituto Federal Electoral, deben garantizar la protección de datos personales que se encuentren en sus sistemas en el ejercicio de sus funciones, por lo que es evidente que a pesar de la reforma constitucional al artículo 16, no existe esta protección constitucional pues como se puede inferir se deja desprotegido a tal derecho fundamental al ser vulnerado por sujeto que se supone deben salvaguardar.

3.2.2 Registro Nacional de Usuarios de Telefonía Móvil (RENAUT)

El 19 de Febrero del año 2009, se publicó un Decreto en el Diario Oficial de la Federación en el que se reformaron y adicionaron diversas disposiciones de la Ley Federal de Telecomunicaciones, ordenando a las compañías de telefonía móvil a registrar los datos personales de todos los usuarios de líneas celulares antes del 10 de Abril de 2010; es decir, se establece la creación del

[13]Vid. El Procedimiento Administrativo Sancionador. Utilización indebida del padrón electoral, disponible en: http://www.te.gob.mx/documentacion/publicaciones/Serie_comentarios/26_procedimiento.pdf, consultado el 8-Septiembre-2012, 7 P.M.

Registro Nacional de Usuarios de Telefonía Móvil (RENAUT), como una medida para coadyuvar en la prevención, investigación y persecución de delitos como el secuestro y la extorsión, en los que frecuentemente utilizan teléfonos celulares.

El RENAUT debía conformarse con el nombre, número telefónico y la clave única del registro de población (CURP) de los usuarios de telefonía móvil; siendo responsable del resguardo y manejo de estos datos la Secretaría de Gobernación a través del Registro Nacional de Población (RENAPO).

En dicha ley se establecía que transcurrido el plazo legal para el registro de los usuarios, se procedería a la cancelación de las líneas telefónicas con incumplimiento de esta disposición, sin responsabilidad alguna para el proveedor de los servicios.

La principal crítica al RENAUT fue que no se establecieron las medidas de seguridad técnicas y organizativas, que garantizaran la confidencialidad, integridad y disposición de los datos personales en la transmisión de éstos a las autoridades competentes; lo que se evidenció en el mes de Junio de 2010, al presentarse una grave violación a las garantías de privacidad y seguridad, ya que la base de datos del RENAUT fue ofertada en sitios de internet, a bajo costo, con información ñ100% fiableò.

Ante lo expuesto, a un año de la operación del RENAUT, algunos senadores y diputados, así como integrantes de la sociedad civil, se pronunciaron públicamente contra este mecanismo, aludiendo un fracaso, debido a que no se cumplió con el objetivo principal de coadyuvar en la prevención, investigación y persecución de los delitos en los que se utilizan teléfonos celulares, ni se dió cabal cumplimiento a la integración de los datos así como tampoco se contaba con las herramientas necesarias para validar los datos proporcionados por los usuarios y se carecía de las medidas de seguridad básicas para el manejo de la información contenida en la base de datos del registro.

El 1° de Marzo del presente año, la Cámara de Diputados aprobó el Decreto por el que se deroga el Registro Nacional de Usuarios de Telefonía Móvil (RENAUT), por falta de utilidad y fallas en la operatividad.[14]

Sin embargo, no hay seguridad de que esos datos no hayan sido transferidos a terceras personas, con anterioridad a la destrucción de las bases de datos, ya sea para obtener o no un lucro.

3.3 MODIFICACIÓN AL ARTÍCULO 22 FRACCIONES II, IV, V Y VI DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL

El objetivo principal establecido en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental es garantizar la protección de los datos personales en posesión de los sujetos obligados, evitando la exposición de la misma a personas ajenas a ella, que podrían causar algún tipo de afectación a los derechos titulados por la Constitución; pero sabemos que en realidad dicho propósito no se ha cumplido cabalmente. Si bien es cierto, contamos con disposiciones jurídicas y un organismo garante encargado de velar por nuestros derechos en cuanto a esta garantía se refiere, la información personal de los ciudadanos se encuentra desprotegida ya que la ley no específica qué datos personales están protegidos y que no serán entregados por el gobierno a otros individuos que nada tienen que ver con los mismos.

Según la ley, los datos personales son confidenciales y su titular debe otorgar previamente su consentimiento para que el gobierno pueda divulgarlos, distribuirlos o comercializarlos; asimismo, la información confidencial, como lo son los datos personales, permanece reservada a menos que el titular de la misma otorgue su consentimiento para ser revelada.

---

[14]Vid. Caso: El Registro Nacional de Usuarios de Telefonía Móvil y el Derecho a la Protección de Datos Personales, disponible en: http://derecom.com/numeros/pdf/renaut.pdf, consultado el 15- Agosto- 2012, 3 P.M.

Sin embargo, las entidades gubernamentales tienen facultades para entregar datos personales a terceros sin autorización del titular, como es el caso de que la información personal que provenga de fuentes o registros públicos disponibles para los ciudadanos, no es confidencial y, por lo tanto puede ser publicada; aunque la ley no es clara en cuanto a qué es un registro público o qué datos se deben contener en los mismos.

También, la información que sea necesaria para fines estadísticos, científicos o de interés general, la que se transfiere entre dependencias gubernamentales o la solicitada por un tribunal, el gobierno la puede transferir sin la autorización del ciudadano titular de la misma, tal como lo establece el artículo 22 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

A continuación se enuncia cómo se encuentra actualmente dicho artículo y la propuesta de modificación.

ACTUAL	PROPUESTA
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**	**Artículo 22. 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 la ley,** **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. A terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales. Dichos terceros**

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.**	**no podrán utilizar los datos personales para propósitos distintos a aquéllos para los cuales se les hubieren transmitido, y** **V. En los demás casos que establezcan las leyes.** **Se exceptúan de las anteriores cuando exista una orden judicial, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas.**

He aquí la problemática a dichas excepciones, porque ponen en riesgo la información personal al permitir el acceso de datos personales tanto a personas autorizadas o no y que puedan ser transferidas a terceros y que sean utilizados para fines distintos para lo cual fueron recopilados, ya que no existen límites para restringir el acceso a los mismos, por lo que no hay certeza de que sean utilizados responsablemente. Como ya mencionamos anteriormente, en teoría se establecen diferentes tipos de sanciones o responsabilidades para quien haga la transferencia de dicha información y que la misma sea utilizada para otros fines, pero la realidad es que esto no es impedimento para hacer mal uso de los mismos.

Por ejemplo, aludiendo a la fracción II del artículo vigente, que establece que no es necesario el consentimiento del ciudadano para la obtención de sus datos personales por razones estadísticos, la información que se recaba en las encuestas del INEGI con fines estadísticos, al momento de que se solicitan no hay de por medio algún aviso en el que se nos informe que van a ser protegidos esos datos personales y mucho menos que van a ser incorporados a algún sistema de datos personales, tal como lo establecen los principios rectores de los mismos

En lo que se refiere a la fracción III, que tampoco se requiere tal consentimiento 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, es el caso del padrón electoral y la lista de electores que contiene datos personales que los ciudadanos entregan al Registro Federal de Electores del Instituto Federal Electoral, lo cual obliga a la autoridad a mantener su confidencialidad y no podrán comunicarse o darse a conocer, mucho menos hacer transferencia de los mismos.

Quién no ha recibido correos electrónicos de candidatos a la Presidencia de la República en las pasadas campañas electorales, invitándolos a votar por determinado candidato, sin que se nos haya solicitado previamente nuestro nombre o correo electrónico, por lo que es necesario cuestionarse: ¿Dónde obtuvieron nuestros datos personales? ¿Quién es el que autorizó o realizó la transferencia de los mismos? ¿Cuál es el fin de la obtención y transferencia de los datos?, lo que se traduce en una invasión total a nuestra esfera privada.

Por lo que respecta a la fracción V que establece que tampoco se requiere el consentimiento de los individuos para proporcionar los datos personales a terceros cuando se contrate la prestación de un servicio que requiera el tratamiento de datos personales, y estos no podrán ser utilizados para propósitos distintos para los cuales se les hubieren transmitido; es importante resaltar que es complicado que se tenga un control sobre terceras personas quienes son contratadas con el fin de realizar labores de tratamiento de datos personales y mucho menos que estos no sean utilizados con fines distintos para los cuales se hubieren transmitido; lo que hace necesario el consentimiento de los ciudadanos no sólo para la obtención de sus datos personales sino también si autorizan o no la transferencia de los mismos a terceras personas.

De aquí surge la necesidad de establecer restricciones o límites a estas excepciones, pues como se puede apreciar, es una puerta abierta para aquellas autoridades o servidores públicos que por un descuido o de manera intencional, transfieren información de carácter personal, justificándose en alguna de las excepciones antes señaladas.

Con tal modificación se reconoció a nivel constitucional la protección de datos personales y confiere a las personas la posibilidad de hacer valer cualquier afectación en la esfera de datos personales, sin embargo, queda claramente determinado que hay una violación a la garantía de la protección de datos personales en posesión del gobierno por lo que la ciudadanía debe de contar con mecanismos efectivos para poder ejercer este derecho y que los sujetos obligados que incurran en responsabilidad sean severamente sancionados porque hasta el momento esto no ha ocurrido, a pesar de que existen varios hechos que dejan de manifiesto la vulnerabilidad y violación de esta garantía, por lo que se requiere de manera pronta una reforma constitucional a dicho artículo en comento.

CONCLUSIONES

PRIMERA.- Actualmente en México, como en muchas partes del mundo, el manejo e intercambio de datos a través de los medios electrónicos entre el Estado y el ciudadano, se ha convertido una práctica habitual. La recolección de datos personales realizada por el gobierno para un mejor desempeño de sus funciones, hace posible que los mismos sean vulnerados y utilizados por personas ajenas a los mismos empleándolos para fines diferentes para la cual fueron recabados, faltando así a lo establecido por la Constitución Política de los Estados Unidos Mexicanos en su artículo 16 que se ha venido enunciado en el cuerpo del presente trabajo.

SEGUNDA.- Se deberá de entender por datos personales lo que dispone la propia Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que dice que es toda información concerniente a una persona física, identificada o identificable, es decir, cualquier información relacionada con nuestra persona como lo es el nombre, número de teléfono, domicilio, fotografía o huellas dactilares, así como cualquier información que pueda identificarnos. Estos se clasifican principalmente en dos categorías: Datos Personales en General, que es la información que refiere aquellos aspectos sobre su personalidad determinada tales como el nombre, dirección, teléfono y edad; y los Datos Sensibles, que es la información que revela su origen racial, étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, datos sobre su vida sexual o estado de salud física o psíquica.

TERCERA.- El artículo 22 de la ley antes mencionada, establece que no se requiere el consentimiento de los particulares para proporcionar sus datos personales cuando se trate por razones estadísticas, científicas o de interés general, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran, cuando se transmitan entre sujetos obligados o entre dependencias o entidades gubernamentales siempre y cuando los datos se utilicen para el ejercicio de sus facultades; cuando exista una orden judicial; a terceros cuando se contrate la prestación de un servicio

que requiera el tratamiento de datos personales y estos no podrán utilizar los datos personales para fines distintos para los cuales se le transmitieron.

CUARTA.- La problemática en dicho artículo es que no hay ninguna restricción para el acceso a datos personales por parte de las autoridades o servidores públicos que escudándose en las excepciones, puedan acceder a datos personales de manera indebida y más aún que puedan ser transferidos a terceros y ser usados con fines distintos para los cuales fueron recabados, el artículo indica que no se requiere el consentimiento cuando se trate por razones estadísticas, científicas o de interés general, previo procedimiento por el cual no puedan asociarse los datos personales con el individuo a quien se refieran; sin embargo, no se señala cuál es ese procedimiento previo para no asociar datos personales a un individuo.

QUINTA.- Otro inconveniente de dicho artículo, es que no determina el uso de la leyenda de Información en los datos personales que son recabados con fines estadísticos hechos por el INEGI, por ejemplo, y mucho menos que van a ser incorporados a algún sistema de datos personales, con lo que se vulnera totalmente lo establecido en los principios rectores de los mismos y no hay certeza de que sean utilizados responsablemente; y el riesgo es mayor cuando se transfieren estos datos entre dependencias o entidades gubernamentales en el ejercicio de sus atribuciones o a terceros.

SEXTA.- El objetivo principal de la modificación al artículo 22 en sus fracciones II, IV, V Y VI, es que no se transgreda el derecho que tienen los ciudadanos a la protección de sus datos personales en poder del Estado consagrado en la Constitución Política de los Estados Unidos Mexicanos, manteniendo siempre informado al ciudadano el por qué y para qué son recabados sus datos personales a través del uso en todo momento de la leyenda de Información, otorgando en la mayoría de las veces su consentimiento para dicho propósito y más aún para el caso de que sean transferidos a otra dependencia o a un tercero; sin olvidar que pueden ejercer los derechos llamados ARCO, en el tratamiento de los mismos.

SÉPTIMA.- La modificación al artículo en comento, reduciría el riesgo de que se vulnere la confidencialidad de los datos personales de los ciudadanos y la obtención de los mismos sin su consentimiento por parte de alguna autoridad o entidad gubernamental así como por funcionarios públicos, evitando hacer mal uso de los mismos y mucho menos que sean transferidos a personas ajenas, estableciendo también algunas salvedades estrictamente necesarias y así cumplir con lo establecido en la Constitución Mexicana en el artículo 16 segundo párrafo.

FUENTES CONSULTADAS

- ANZIT GUERRERO, Ramiro. et al., El Derecho Informático, ñAspectos Fundamentalesò, Cathedra Jurídica, Argentina, 2010.
- DÁVARA R., Miguel Ángel. Manual de Derecho Informático, Aranzandi Editores, España, 1997.
- FERNÁNDEZ RODRIGUEZ. José Julio, Lo público y lo privado en Internet: Intimidad y Libertad de expresión en la Red, UNAM, México, 2004.
- OVILLA BUENO, Rocío. La Protección de Datos Personales en México, Porrúa, México, 2005.
- Bases técnico metodológicas para la realización de trabajos de investigación en la carrera de derecho**,** UNAM, 2006.
- DICCIONARIO PORRÚA DE SINÓNIMOS Y ANTÓNIMOS, Porrúa, Decimoséptima edición, México, 2005.
- Constitución Política de los Estados Unidos Mexicanos
- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental
- Ley Federal de Responsabilidades Administrativas de los Servidores Públicos
- Código Civil Federal
- Código Penal Federal
- El derecho a la protección de datos personales en la Administración Pública Federal, disponible en: http://www.itei.org.mx/v3/micrositios/diplomado02/gdl/adjuntos/Sector_Publico_ITEI_18-19-nov-2011.pdf, consultado el 28-Agosto-2012, 8:40 P.M.
- Guía Práctica para la Gestión de las Unidades de Enlace y Comités de Información en las dependencias y entidades de la Administración Pública Federal, disponible en: http://www.resi.org.mx/icainew/images%5CBiblioteca%5CPublicaciones%5CGPUETomoII.pdf, consultado el 01-Octubre-2012, 7 P.M.

- Datos Personales, Estudio de Derecho Comparado a nivel Estatal e Internacional, así como de Opiniones Especializadas (segunda Parte). Disponible en: http://www.diputados.gob.mx/cedia/sia/spi/SPI-ISS-25-09.pdf, consultado el 05 de Agosto de 2012, 5 P.M.
- Introducción al Instituto Federal de Acceso a la Información y Protección de Datos. Disponible en: http://www.privacyconference2011.org/includes/IntroduccionalIFAIEspanol.pdf, consultado el 01-Agosto-2012, 7:00 P.M.
- Autoridad Garante, disponible en: http://www.ifai.org.mx/buscador_ifai/buscar.do?type=all&spell=true&lemmatize=true&fuentes=4&queryStr=FUNCIONES%20DEL%20IFAI, consultado el 28-Agosto-2012, 12:00 P.M.
- El Procedimiento Administrativo Sancionador. Utilización indebida del padrón electoral, disponible en: http://www.te.gob.mx/documentacion/publicaciones/Serie_comentarios/26_procedimiento.pdf, consultado el 8-Septiembre-2012, 7 P.M.
- Caso: El Registro Nacional de Usuarios de Telefonía Móvil y el Derecho a la Protección de Datos Personales, disponible en: http://derecom.com/numeros/pdf/renaut.pdf, consultado el 15- Agosto-2012, 3 P.M.