UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

DIVISIÓN DE ESTUDIOS DE POSGRADO

"LA PROTECCIÓN DE DATOS PERSONALES EN LA PUBLICIDAD Y EL MARKETING EN: MÉXICO, ESPAÑA Y ARGENTINA"

T E S I S

QUE PARA OBTENER EL GRADO DE:

MAESTRO EN DERECHO

P R E S E N T A:

LIC. ALDO GONZÁLEZ GUTIÉRREZ

DIRECTORA DE TESIS. DRA. SOCORRO APREZA SALGADO

CIUDAD UNIVERSITARIA, 2011.

LA PROTECCIÒN DE DATOS PERSONALES EN LA PUBLICIDAD Y EL MARKETING EN MÉXICO, ESPAÑA Y ARGENTINA

Página

CAPÍTULO III
MARCO NORMATIVO DE LA PROTECCIÓN DE DATOS PERSONALES: MÉXICO, ESPAÑA Y ARGENTINA

CAPÍTULO IV
LA PROTECCIÓN DE DATOS PERSONALES EN LA PUBLICIDAD Y EL MARKETING

CAPÍTULO V
EL IFAI COMO INSTITUCIÓN GARANTE DEL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES: AVANCE O RETROCESO

ABREVIATURAS

- **AEPD.-** Agencia Española de Protección de Datos.
- **CAIPDP.-** Comité de Acceso a la Información y Protección de Datos Personales
- **DERECHOS ARCO.-** Derechos de Acceso, Rectificación, Cancelación y Oposición
- **IFAI.-** Instituto Federal de Acceso a la Información Pública y Datos Personales
- **LEY 25.326.-** Ley De Protección De Datos Personales. Hábeas Data
- **LFPC.-** Ley Federal de Protección al Consumidor
- **LFPDP.-** Ley Federal de Protección de Datos Personales en Posesión de los Particulares
- **LFTAIPG.-** Ley Federal de Transparencia y Acceso a la información Pública Gubernamental
- **LOPD 15 /99.-** Ley Orgánica De Protección De Datos Personales Española
- **LORTAD.-** Ley Orgánica de Tratamiento Automatizado de Datos de carácter Personal
- **OCDE.-** Organización para la Cooperación y el Desarrollo en Europa
- **ONU.-** Organización de las Naciones Unidas
- **SCJN.-** Suprema Corte de Justicia de la Nación
- **TIC's.-** Tecnologías de la Información y las Comunicaciones

INTRODUCCIÓN

Las Tecnologías de la Información y Comunicaciones (en adelante TIC's) constituyen uno de los mayores avances de este siglo, y en ella se basa buena parte del desarrollo económico y social del futuro. Pero, como ocurre en ellas, su utilización comporta una serie de riesgos: el principal, la pérdida absoluta de los datos personales a los que todos tenemos derecho. Frente a ello el ciudadano debe gozar de una serie de derechos, cuyo ejercicio reduzca los riesgos de que sus datos personales figuren sin su conocimiento en ficheros manuales y automatizados.

La posibilidad de cesión y obtención de información, ahora es enorme a través de los mecanismos de las nuevas Tecnologías. Los canales de información permiten obtener una imagen nítida de las personas y captar sus momentos más internos para hacerla participe de los movimientos fraudulentos, ilícitos o comerciales por la cesión de sus datos (la mayoría de las veces sin su consentimiento):

> *"...Resulta que el otro día me compré un coche en el concesionario de mi barrio. Ayer recibí una carta de un proveedor de equipos de aire acondicionado felicitándome por haber comprado el coche X en el concesionario Z y ofreciéndome unos equipos maravillosos y -según el proveedor- baratísimos. Y yo me pregunto: ¿cómo saben que vivo aquí, que me llamo así, que he adquirido este coche y sobre todo... que lo compré sin aire acondicionado!!!?..."*[1]

Ante esas circunstancias, los parlamentos han instaurado en algunos países directrices para el goce de los derechos humanos, empero no es menos cierto que, en algunos momentos todo ha quedado como un cúmulo de intenciones que pretenden proteger el derecho de tercera generación, la autodeterminación informativa.

---

[1] http://www.elmundo.es/sudinero/noticias/act-19-1.html. *Semanario de Economía Familiar, Consumo y Empleo*. No. 19, España, 25 de febrero de 1996.

Pese a ello, países en Europa como España, Suiza, Gran Bretaña y en América Brasil, Colombia Argentina, entre otros han instaurado un sistema de protección frente a los problemas de intromisión en la vida de las personas, concretamente en sus datos personales. El referente que se tiene de estos Estados, ha servido de modulación para futuras regulaciones en la materia, tanto a nivel nacional en sus respectivos países, como internacionalmente en otros puntos de los diversos continentes.

Como fundamento de lo anterior se han adoptado medidas en distintos países como aconteció en mayo de 2009, en que se llevó a cabo en la ciudad de Buenos Aires, Argentina el "Sexto Seminario Internacional de Protección de Datos Personales", aquel evento fue asistido por reconocidos funcionarios de España y Argentina a fin de tratar temas referentes a la protección de datos personales, precisando los retos a los que se enfrentan sus legislaciones, así como la implementación de mejores prácticas para el reconocimiento, y ejercicio de los derechos implicados en la autodeterminación informativa, los temas tratados correspondieron entre otros al desarrollo y modernización de la información crediticia; las buenas prácticas en políticas de privacidad para las bases de datos; políticas de intercambio electrónico de información; Registro Nacional de Reincidencias; Seguridad y protección en Internet; Infraestructura digital en el MERCOSUR que pretende regular: la publicidad, el comercio electrónico, firma digital, identidad digital, protección de datos personales y responsabilidad jurídica.

Además se propuso una normativa para la región del MERCOSUR sobre buenas prácticas en la protección de datos personales, proponiendo la creación de una plataforma que permita sistemas transnacionales (mercado libre, publicidad, oportunidades, pymes, logísticas de distribución, marco regulatorio a nivel regional para el usuario, recepción de productos, recolección de información, páginas web) para comerciar dentro de la región, pero todo ello dentro del marco de la Protección de Datos Personales.

Con gran entusiasmo se desarrollaron las ponencias sobre los temas tratados, mismo que resultaron de gran novedad y trascendencia para las Agencias de Protección de Datos Personales de los países invitados. Países como México no fueron convocados, pues la efímera regulación que mantenía al respecto no lo hacía contar con un sistema de protección de datos personales en posesión de particulares, ni mucho menos con estándares de protección requeridos por las normas internacionales, por lo que difícilmente podían disertar sobre la práctica del sistema, a pesar de que ya se encontraban pendientes algunas iniciativas sobre una Ley de Protección de Datos en el Congreso.

Circunstancias como estas, han motivado al Estado mexicano a querer erigirse sobre la base de un sistema de protección de datos, en el que el individuo sea el centro de la garantía que se pretende proteger, dotando de plena autonomía al derecho individual a la autodeterminación informativa, difuminando cualquier configuración legal de otro derecho constitucional, en este sentido, se da la reforma que adiciona un párrafo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, el 1 de junio de 2009.

De este modo - sostiene la Sentencia 254/1993 del Tribunal Constitucional Español-, *nuestra constitución ha incorporado una nueva garantía constitucional (...) En el presente caso estamos ante ...un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos*.

Los riesgos derivados de las tecnologías de la información y de las comunicaciones, el exceso de errores o el uso incontrolado de información de carácter personal que circula por Internet, no pueden ser afrontados eficazmente por los particulares afectados a causa de una información insuficiente y las pocas medidas de seguridad que hay, pues los ciudadanos se encuentran inermes por la imposibilidad de averiguar qué información sobre sus personas almacenan los distintos sujetos

públicos y privados, premisa indispensable para cualquier ejercicio de los derechos de la autodeterminación informativa (ARCO), menos aun pueden conocerse y prevenir o perseguir el uso desviado o la diseminación indebida de tales datos, ello constituye el capítulo II del presente estudio.

En el capítulo III se muestra el desarrollo que ha tenido el derecho de protección de datos personales, desde su surgimiento en los Instrumentos internacionales hasta la actual Ley Federal de Protección de Datos Personales en Posesión de Particulares en México, sus principios, alcances y defectos, así como su –incipiente- aplicación en los Archivos de datos, su recogida y tratamiento tanto por entes públicos como privados, el comportamiento de las empresas para llegar hasta el público usuario o consumidor a través de las ofertas publicitarias según su perfil de consumo, realizando una comparación con los modelos Argentino y Español, así como las legislaciones conexas que proporcionan un marco de referencia sobre el particular.

El capítulo IV, muestra la influencia de la publicidad y el marketing en los medios de comunicación: Internet, correo electrónico, teléfono y la protección de datos personales en la sociedad de la información; la recopilación de datos personales para hacer llegar al público usuario o consumidor las ofertas, creando previamente perfiles de consumo respecto de sus comportamientos, gustos, aficiones, padecimientos, etc.; las redes sociales constituyen de igual manera herramientas que permiten a los particulares crear bases de datos que posteriormente son utilizadas para promocionar sus objetos de comercialización.

La importancia de preservar los datos personales frente a la publicidad y el marketing, los casos en que pueden ser tratados datos con fines de publicidad y los problemas que la publicidad constituye en un sistema como el nuestro, son parte esencial de este capítulo, los aspectos relevantes de este binomio constituyen los derechos que deben respetarse en el tratamiento de datos en esta actividad, el derecho de acceso y el retiro, bloqueo o cancelación cuando los datos no sean tratados conforme a los fines para los que fueron recopilados, así como la

necesidad de inscripción de las bases de datos en un Registro Nacional hacen de este capítulo el centro neurálgico de nuestra investigación. Los aspectos publicitarios han determinado una cultura impositiva en la que las actividades cotidianas no pueden desarrollarse sin la inclusión de la comercialización en diversos sectores poblacionales, veremos de qué manera ha sido regulada esta actividad, con ello prepararemos el análisis que nos introduzca al V capítulo objeto de estudio.

Finalmente, centraremos nuestra atención en el Instituto Federal de Acceso a la Información Pública y Datos Personales y su competencia, facultado por la reciente Ley de Protección de Datos Personales, verificando si la respuesta al binomio protección de datos personales y las actividades comerciales y de publicidad van en la línea de asegurar el derecho a la autodeterminación informativa. Para ello, examinaremos la Ley Federal de Protección de Datos Personales, cotejándola con estándares internacionales, con el objeto de exponer aciertos y desaciertos de nuestra actual legislación, no sin antes repasar las nuevas facultades que le han sido delegadas al IFAI, y ver si cumplen o no con los estándares expuestos en los capítulos del presente estudio.

Cuanto más avancemos, más camino se vislumbra y cuanto más recorremos, más nos queda por hacer. Vale aquí a modo de estudio, la exposición acerca de la protección de datos personales en México, contrastándolo con los modelos Argentino y Español, que pueden servir como punto de reflexión acerca de la protección y mejoramiento de este derecho en nuestro país.

CAPÌTULO I
EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

1.1. La protección de datos personales como derecho fundamental

- 1.1.1. Delimitación Conceptual en la protección de datos
  - 1.1.1.1. Doctrina Científica
  - 1.1.1.2. Legislación
  - 1.1.1.3. Doctrina jurisprudencial
- 1.1.2. Autodeterminación Informativa o Derecho informático
  - 1.1.2.1. Diferencia

1.2. Principios generales relativos a la protección de datos

- 1.2.1. Seguridad de los datos
- 1.2.2. Calidad de los datos
- 1.2.3. Consentimiento
- 1.2.4. Deber de confidencialidad
- 1.2.5. Transferencia internacional

1.3. Datos Especialmente protegidos

CAPÍTULO I
EL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA

1.1. La protección de datos personales como derecho fundamental

Uno de los aspectos más llamativos del pensamiento jurídico y político de las últimas décadas es la extraordinaria difusión del lenguaje de los derechos. No es exagerado afirmar que los derechos fundamentales se han convertido en el eje central de la discusión sobre los límites y los fines de la acción política. Lo cual no es un hecho singular en la tradición del pensamiento político moderno.

El reconocimiento jurídico positivo de los derechos fundamentales, como reflejo de nuevas demandas sociales, puede ser interpretado como un síntoma de progreso en aquellos Estados que, comprometidos con su entidad constitucional y democrática, pueden afirmar que en los derechos se tiene una línea de continuidad, y que al mismo tiempo, supone una adecuación a su contexto normativo vigente, igualmente supone un beneficio, porque propicia un cambio, estableciendo un nivel de protección y garantía de los derechos actualmente alcanzada, así como su proclamación y aceptación casi universal, traduciéndose en una conquista.

De esta manera, entendemos a los derechos fundamentales como dimensiones básicas de la vida del hombre en sociedad, a bienes de primordial importancia en los que el derecho actúa a través de la atribución de un derecho subjetivo a los individuos en el marco de la satisfacción de necesidades fundamentales de la condición humana o a través de obligaciones que normalmente se establecen por el poder, titular de la soberanía, y que afectan a sectores especialmente importantes para la organización y funcionamiento del Estado y de la sociedad, esto es, se tiene un derecho fundamental cuando una norma jurídica lo reconoce o lo establece dentro del derecho positivo.

Los derechos y deberes fundamentales son un concepto histórico, que se ha ido adaptando a las condiciones sociales, económicas, culturales y políticas que surgen en ese momento, y los podemos entender en opinión de Gregorio Peces Barba, como "el conjunto de normas de un ordenamiento jurídico positivo fundado en la moralidad de la defensa de la dignidad del hombre, de los valores de libertad y de igualdad que representan las normas materiales básicas de ese ordenamiento".[2]

Por su parte, Manuel Aragón Reyes, apunta que "si bien la Constitución utiliza indistintamente diversas denominaciones (derechos fundamentales, libertades públicas, derechos constitucionales, derechos de los ciudadanos, derechos, libertades), la primera de ellas es utilizada predominantemente en el lenguaje jurídico, desde 1978, para designar a todos aquellos derechos que la Constitución garantiza a los ciudadanos como expresión o traducción, en el ordenamiento positivo nacional de los derechos del hombre, derechos humanos –continua el autor-, o derechos inviolables inherentes a la persona (art. 10.1 *Constitución Española*)[3]. De este modo, el Estado democrático de Derecho otorga a estas manifestaciones inmediatas y concretas de la "dignidad de la persona" (art. 10.1 CE) que son los derechos humanos la máxima protección jurídica de que dispone, la Constitución. En este sentido, bien puede decirse que los derechos fundamentales son "derechos constitucionales, es decir, derechos subjetivos, dotados de la fuerza normativa propia de la Constitución que se impone de modo efectivo a todos los poderes públicos y, muy señaladamente, al propio legislador".[4]

Por tanto, a los derechos fundamentales no los crea el poder político, ni la Constitución, los derechos fundamentales se imponen al Estado, la Constitución se

---

[2] Peces-Barba Martínez, Gregorio, *"Derecho y Derechos Fundamentales"*, Centro de Estudios Constitucionales, Madrid, 1993. P. 343

[3] Cabe hacer mención que el citado autor, refiere la Constitución Española, pues si la comparamos con el texto de nuestra Constitución mexicana, según lo dispuesto por el artículo 1, la misma no reconoce derechos fundamentales, sino otorga garantías individuales.

[4] Aragón Reyes, Manuel. *Coordinador. "Temas Básicos de Derecho Constitucional". "Tribunal Constitucional y Derechos Fundamentales".* Tomo III, 1ra. Edición, Madrid, España, 2001. P. 107

limita a reconocer los derechos fundamentales, no se otorgan, la Constitución propugna los derechos fundamentales, pero no los crea.

Queremos decir que el derecho fundamental jurídicamente tiene la estructura normativa de un derecho subjetivo, es decir, que los derechos fundamentales son instituciones jurídicas que tienen la forma del derecho subjetivo. Y la estructura del derecho subjetivo tiene tres elementos: titular del derecho subjetivo, el contenido del derecho subjetivo en el que vamos a distinguir las facultades, por otra parte el objeto del derecho, y un tercer elemento es el destinatario o sujeto pasivo, aquel que está obligado a hacer o no hacer.

Atento a lo anterior, podemos decir que los derechos fundamentales, son un conjunto de derechos subjetivos y garantías reconocidos en la Constitución como propios de las personas y que tienen como finalidad prioritaria garantizar la dignidad de la persona, la libertad, la igualdad, la participación política y social, el pluralismo o cualquier otro aspecto fundamental que afecte al desarrollo integral de la persona en una comunidad de hombres libres. Tales derechos no sólo vinculan a los poderes públicos que deben respetarlos y garantizar su ejercicio estando su quebrantamiento protegido jurisdiccionalmente, sino que también constituyen el fundamento sustantivo del orden político y jurídico de la comunidad.

Esto es, que una observación de la realidad jurídica, permite constatar que la incorporación de los derechos fundamentales al Derecho positivo se suele producir por medio de las normas jurídicas de más alto rango en la cadena de validez del ordenamiento, principalmente la Constitución y la ley. Es razonable porque los derechos fundamentales cumplen una función de límite de poder y de guía para el desarrollo del Derecho en todos sus escalones a través de todos los operadores jurídicos.

La identificación del derecho que hoy estudiamos, es un concepto a satisfacer en la aplicación de la norma al caso concreto, puesto que incluye valores, de los cuales no se puede prescindir, en virtud de sus dimensiones.

Lo que hoy nos interesa es la clasificación del derecho fundamental según su contenido, pues de ello, podemos distinguir: derechos individuales, tales como: derecho a la vida, libertad religiosa, de opinión, de expresión, y desde luego, el derecho a la `privacidad e intimidad´.

En este último tópico, centraremos nuestra atención, debido a la configuración que como derecho fundamental pudiere derivarse del derecho a la privacidad, intimidad o la profusa relación que guardare con el derecho a la protección de datos personales, o si por el contrario, la protección de datos personales o autodeterminación informativa, constituye un derecho autónomo e independiente plenamente reconocido.

El derecho a la intimidad como pilar fundamental es la individualidad de la persona cuando puede verse afectada por el conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad y que sobrepasen las fronteras y la soberanía del individuo, por lo que podemos dimensionar a la intimidad como algo profundo de la persona, lo secreto, la no injerencia en esa zona de reserva que no permite traspasar los límites de lo que la persona consentiría, constituye la esfera más pequeña de la confidencialidad humana.

Sin embargo, lejos de generarse normas o acuerdos universales que coincidan jurídicamente en este particular, la tendencia ha sido establecer reglas o pautas de un derecho mínimo según el sistema de cada Estado, que coincida con la voluntad común de esa zona, por lo que no es dable incorporar una tendencia que impere ante la imposibilidad de establecer políticas unitarias.

Lo cierto es que hoy en día la intimidad se ha visto menoscabada por la utilización de los medios tecnológicos e informáticos y, ese es precisamente el

ámbito más extenso de la privacidad, que salvaguarda un bien jurídico diferente, referido a aspectos personales, que si bien, viéndolos de forma aislada, no adquieren especial significación, al ser valorados en su conjunto, revelan el perfil de la personalidad del individuo que tiene el derecho a mantenerse inaccesible al conocimiento de terceras personas.

Se trata de un respeto a la intimidad, en lo que aquello de cada persona se reserva para sí, y a los demás no es lícito invadir. En el caso de la protección de datos, este derecho persigue garantizar al individuo el poder de control sobre sus datos personales, su uso y tratamiento con el propósito de impedir su tráfico ilícito, por lo tanto, se trata de derechos subjetivos constitucionales frente al Estado, para que éste realice acciones positivas fácticas o normativas, que tienen como objeto la delimitación de las esferas de sujetos jurídicos iguales, como así también la imposibilidad y la imposición de esta demarcación.

Al respecto Estadella Yuste, señala "La relación existente entre el derecho a la intimidad y el derecho a la protección de datos personales o a la autodeterminación informativa ha sido analizado de forma diferente por la doctrina. Unos autores han afirmado que los términos "protección de datos" y "protección de la intimidad" son dos nociones diferentes, ya que el interés de proteger la veracidad de los datos y el uso que de ellos se hace no está relacionado necesariamente con la protección de la intimidad individual.[5]

¿Podríamos decir que, el derecho a la protección de datos o la "autodeterminación informativa" se desprende como manifestación del derecho a la intimidad y, como consecuencia, es esta configuración la que hace referencia a la protección de los datos personales de la esfera de la vida privada, o por el contrario, la protección de los datos personales recibe el carácter autónomo de un derecho fundamental?

[5] Estadella Yuste, Olga. *"La protección de la intimidad frente a la transmisión internacional de Datos personales"*, Centre d´Investigació de la COmunicació, Generalitat de Catalunya, Tecnos, Madrid, 1995. P. 81.

En principio cabe afirmar que el derecho a la protección de datos, refleja más que una idea individualista de protección a la intimidad, ya que engloba también los intereses del individuo contra el procesamiento, almacenamiento y recolección de información pero sobre todo otorga al individuo un poder de control sobre el actuar de los responsables en el ejercicio de sus derechos (ARCO). Sin ser necesario abordar profundamente en éste tópico toda la gama de posibilidades que ofrecen los medios tecnológicos para la recogida y el tratamiento de datos personales, ni los indudables riesgos que ello puede generar –tema será tratado en el Capítulo II-, es importante indicar que una persona puede ignorar no sólo cuáles de su datos circulan por los medios tecnológicos, sino que también si los mismos han sido objeto de tratamiento, traslado y con qué finalidad.

Por lo anterior, podemos comprender que el derecho a la intimidad no aporta por sí solo una protección suficiente frente a esta nueva realidad que derive del progreso tecnológico, pues la garantía de la vida privada de la persona y de su reputación poseen una dimensión que excede del ámbito de protección del derecho fundamental a la intimidad, toda vez que el conocimiento de datos de una persona, debidamente relacionados, pueden ofrecer una imagen de ella, sus gustos, aficiones, etc., datos que pueden perjudicar a la persona, no por su falsedad o por el desmerecimiento de su reputación, sino por el sólo hecho de que el individuo no ha consentido su almacenamiento.

Ahora bien, los esfuerzos de protección deben ir encaminados a salvaguardar no sólo la esfera más interna o esencial de la persona, sino también las actividades y ámbitos del individuo que, sin incidir directamente en su intimidad o núcleo de su personalidad, pueden verse afectados (como el ejercicio de los derechos ARCO o los principios a los que debe sujetarse todo tratamiento de datos personales: confidencialidad, consentimiento, calidad, transferencia internacional, etc.) con asombrosa e increíble facilidad, y condicionan el ejercicio de los derechos y el desenvolvimiento adecuado en las relaciones sociales.

Sobre el particular, se han elaborado diversas normas en diferentes países. Los primeros textos internacionales referentes a la protección de datos personales fueron la *Resolución del Comité de Ministros del Consejo de Europa de 1973*, *sobre la Protección de la Vida Privada de las Personas Físicas frente a los Bancos de Datos Electrónicos en el Sector Privado,* a la que le siguió en 1974 otra *Resolución sobre los Bancos de Datos en el Sector Público*. En ellas se recomendaba a los países miembros la adopción de medidas legislativas tendentes a garantizar los siguientes principios:

> a) Reconocimiento del derecho de los interesados a conocer y acceder a las informaciones que les conciernen (Acceso);
>
> b) Obligación de los bancos de datos públicos o privados de corregir la información inexacta y cancelar la obsoleta inapropiada, irrelevante u obtenida por procedimientos ilegales (Rectificación y Cancelación);
>
> c) Adopción de las correspondientes garantías para impedir que la difusión de datos estadísticos permitiera la identificación de sujetos individuales y para evitar la transmisión de datos a personas o entidades no autorizadas (Oposición).

Sin duda el texto internacional más importante, es el Convenio 108 del Consejo de Europa, en donde se ubican varios principios, por el que la información no debe recogerse por procedimientos desleales e ilícitos,[6] el principio de publicidad por el que debe mantenerse un registro público de los ficheros automatizados existentes, y el principio de acceso individual, por el que cualquier persona tiene derecho a conocer si sus datos son objeto de tratamiento automatizado, y si los hubiere, el titular del derecho puede obtener la rectificación o la destrucción de los mismos, nos referimos al *Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal,* adoptado por el Comité de Ministros del Consejo de Europa en

[6] Convenio 108 del Consejo de Europa de 1981, para la protección de personas con respecto al tratamiento automatizado de datos de carácter personal, (ví: 15 de abril de 2008). http://www.monografías.com/trabajos/eu

septiembre de 1980 y abierto a la firma de los Estados miembros a partir del 28 de enero de 1981.

En 1985 se creó una *Declaración sobre Flujos Transfronterizos de Datos*, sin embargo, la legislación sobre este derecho en el sistema comunitario, se realizó a través de una serie de directivas, y más tarde por el propio TCEE (Tratado Consultivo de la Comunidad Económica Europea) y el TUE (Tratado de la Unión Europea) y legislación concordante. Este derecho aparece por primera vez en una directiva en 1995, la *Directiva 95/46/CE*, en cuyo sentido se considera a la protección de datos personales en relación con el derecho a la vida privada; nuevamente en 1997 surge otra directiva, y en 1998 la OCDE, aprobó una *Declaración sobre la protección de la intimidad en las redes globales*; en 2002 se da la creación de otros instrumentos de carácter internacional y organismos internacionales como la Organización para la Cooperación y el Desarrollo en Europa; en el marco de la OCDE se aprobaron tres importantes instrumentos sobre este asunto.

Por su parte, la *Declaración Universal de los Derechos Humanos,* adoptada por la Resolución de la Asamblea General de la Organización de las Naciones Unidas en 1948, sostuvo en su artículo 12, *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, domicilio o 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".*

Damos cuenta de que en este numeral, se sostiene el derecho a la vida privada, claro está, que no hay que dejar de lado el contexto en el que se promulga dicha Declaración, pues el mundo venía saliendo de los estragos de una Guerra, y lo que se pretendía era precisamente el dar una mayor amplitud y generalidad para que los países la aplicaran, sin embargo, los Asambleístas de la ONU, no pronosticaron que los adelantos científicos y tecnológicos requerirían de una mayor protección legal, y que el concepto de privacidad, no aseguraba la protección de datos

personales. Así, tenía que adaptarse a las exigencias de una sociedad informatizada, y con ello adoptar modalidades de protección jurídica en lo que refiere a los datos personales.

Misma configuración legal que ha ido en desarrollo a tal grado de quedar constituida como un derecho a título propio, independiente del derecho a la intimidad en Europa dentro de la *Carta de Derechos Fundamentales de la Unión Europea* de 2000 en su artículo 8º.[7]

En Alemania, la protección de datos personales, se ha articulado a través de la categoría jurídica del derecho a la autodeterminación informativa que fue consagrada constitucionalmente por el Tribunal Constitucional Federal Alemán en su famosa sentencia sobre la *Ley del Censo de Población* de 15 de diciembre de 1983, aunque ya era utilizada por los Tribunales ordinarios[8].

En dicha sentencia se establece que este derecho consiste en la facultad del individuo de decidir básicamente cuándo y dentro de qué límites procede relevar situaciones referentes a la propia vida, haciendo necesaria la protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitadas de los datos concernientes a la persona .

Pese a que los rudimentarios sistemas de registro, propios de la etapa anterior a la computadoras, ya auguraban los riesgos que implicaba un fichero con datos incompletos, falsos o utilizados para otros propósitos, "el derecho a la protección de datos", pertenece al contenido de la era informática, proyectándose hacia la cuarta generación de Derechos Humanos, y repensando la condición humana de la

[7] El artículo 8º señala: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratan de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legitimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

[8] Schwabe, Jürgen. *Jurisprudencia del Tribunal Constitucional Federal Alemán. Extractos de las sentencias más relevantes.* Sentencia BVerfGE 65, 1 [Censo de Población]. Ed. Konrad Adenauer Stiftung, Alemania, 2009. P. 94.

sociedad tecnológica e informatizada en un intento por consolidar un derecho de 4ª Generación; señalaba Estadella Yuste, "resulta atrevido afirmar que esta compleja disciplina legal estuviera ya implícita en las referencias generales al derecho a la intimidad inserta en cuerpos normativos de ámbito nacional e internacional de la era preinformática".[9]

El reconocimiento del derecho fundamental a la protección de datos personales, ha cobrado su importancia, sobre todo en el Derecho Comunitario, en la jurisprudencia, en la legislación y su aplicación.

En el plano jurisprudencial comunitario, se ha enfrentado con cuestiones relativas al derecho a la protección de datos personales, antes de que existiera alguna legislación al respecto. Los órganos comunitarios, reconocieron que el derecho a la intimidad, plasmado en el artículo 8 de la Convención Europea de Derechos Humanos y derivado de las tradiciones constitucionales a los Estados miembros, es uno de los derechos fundamentales protegidos en el ordenamiento comunitario.

Un paso más lo constituye la sentencia del Tribunal de Justicia de las Comunidades Europeas de 12 de noviembre de 1969, Erich Stauder vs Stadt Ulm-Sozialamat, en donde el Tribunal decidió el hecho de supeditar el suministro de mantequilla con precios reducidos al hecho de que suministrara a los vendedores previamente el nombre de los beneficiarios. Aunque el recurrente, no alegó expresamente el derecho a la protección de datos personales, sin embargo, es un primer antecedente.

Hasta aquí hemos podido constatar que la doctrina mayoritaria Europea distingue entre el derecho a la intimidad y a la protección de datos personales, pudiendo concluir que el derecho fundamental a la intimidad es la de proteger al individuo de cualquier injerencia en su esfera, tanto personal como familiar por las

9 Estadella Yuste, "La protección de la intimidad", citada por R. Puccinelli, Oscar en *"Protección de datos de carácter personal",* Astrea, Buenos Aires, 2004. P. 12

intromisiones de terceros en contra de su voluntad, a diferencia del derecho fundamental a la protección de datos, que aunque en medida comparten el objetivo de ofrecer una protección de la vida privada y familiar, atribuye a su titular un poder de control jurídico para imponer a terceros la realización u omisión de determinados comportamientos dispuestos en la ley, debiendo imponer medidas de seguridad en la utilización de los medios tecnológicos, a fin de respetar el derecho fundamental a la protección de datos. La peculiaridad de este derecho respecto de aquél es su distinta función, lo que trae por consecuencia que su objeto y su contenido difieran.

El derecho fundamental a la protección de datos personales garantiza un poder de disposición de esos datos, prohibiendo a los entes públicos y privados convertirse en fuentes de información, de ahí la singularidad de este derecho, por un lado, su objeto es más amplio que el derecho a la intimidad que constitucionalmente es establecido en los países como esfera de los bienes jurídicamente tutelados de la personalidad; el derecho a la protección de datos amplía esa esfera constitucional a aquéllos datos relevantes en el ejercicio de los derechos de la persona, sean o no constitucionales y sean o no relativos a la intimidad.

1.1.1. Delimitación Conceptual en la protección de datos

1.1.1.1. Doctrina Científica

A nivel internacional, principalmente en el Derecho Europeo, la protección de datos personales es considerada como un derecho fundamental a título propio, distinto a otros derechos como el derecho a la intimidad.

Con la aparición de una nueva era tecnológica de la información, muchos datos relativos a la vida privada de las personas, que en otra época no tenían relevancia, en la actualidad se han visto como potenciales medios para crear bienes de gran cotización en las llamadas sociedades de mercado o sociedades de

marketing, lo que ocasionó que en la doctrina se pronunciara al respecto, identificando la agresión al derecho fundamental, al igual que en la legislación internacional.

López-Ayllón, define a los datos personales como una información que concierne a una persona física, identificada o identificable, y cualquiera que sea el soporte en que se encuentre (número, gráfico, alfabético, acústico, etc.). Entre los datos personales enumera el nombre asociado a las características físicas o emocionales, el estado de salud, la cuenta de correo electrónico, el patrimonio, la religión, la huella digital, la fotografía o el número de seguridad social de una persona. Lo importante es la asociación de dos o más datos que permitan referirlos a una persona física específica e identificable.[10]

Por su parte, Oscar Puccinelli, hace la distinción entre "derecho de la protección de datos" y "derecho a la protección de datos", entendiendo al primero como el conjunto de normas y principios que, destinados o no a tal fin, y con independencia de su fuente, son utilizados para la tutela de los diversos derechos de las personas que pudieran verse afectados por el tratamiento de datos de carácter personal[11].

Por otro lado, el derecho a la protección de datos es la facultad conferida a las personas para actuar per se y para exigir la actuación del Estado con el fin de obtener la tutela de los diversos derechos que pudieran verse afectados en virtud de aquellas operaciones de tratamiento de los datos de carácter personal que le concierne.[12]

Puccinelli reconoce la facultad de individuo para ejercitar al aparato estatal a fin de proteger los diversos derechos que pudieren derivarse del tratamiento de datos personales. Debemos destacar que en la definición, no se señala a qué

[10] En Salazar Ugarte, Pedro. *Coordinador*."*El derecho de acceso a la información en la Constitución Mexicana: razones, significados y consecuencias"*. UNAM/IFAI, México, 2008. Pp. 17-18
[11] R. Puccinelli, Oscar. *"Protección de Datos de carácter personal",* Astrea, Buenos Aires, 2004. P. 8
[12] Idem. P. 9

derechos se refiere en el tratamiento de esos datos, recordemos que en el tópico anterior, reconocemos la variedad de derechos que pueden ser objeto de agresión por parte de terceros en la recogida o tratamiento de la información, sean íntimos o no, y la definición no limita el resguardo a los derechos, ya que pueden ser incluso los derivados del propio tratamiento (acceso, rectificación, cancelación y oposición).

Lucas Murillo, sostiene que el derecho a la protección de datos personales o autodeterminación informativa –según el autor es más conveniente llamarle-, tiene como objeto preservar la información individual (íntima y no íntima) frente a su utilización incontrolada, arrancando precisamente, donde termina el entendimiento convencional del derecho a la vida privada.

Pese a que la definición precedente incluye la preservación de la información individual sea íntima o no, considerando con ello que el derecho a la autodeterminación informativa constituye un aspecto más amplio que el derecho a la intimidad, adolece de otros elementos considerados por la doctrina y la jurisprudencia, esto es que, el derecho a la protección de datos no es exclusivo para la preservación de la información, sino de cualquier otro derecho involucrado en la recogida y tratamiento del mismo, como el acceso, rectificación, cancelación y oposición, y no sólo la confidencialidad, ya que como lo establecimos anteriormente, la peculiaridad de este derecho fundamental es el objeto y su contenido.

Miguel Ángel Dávara Rodríguez, define a la protección de datos personales como 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 intimidad.[13]

[13] *"Manual de Derecho Informático"*. Aranzandi Editores, Madrid, España, 1997. P. 47

El jurista español, reduce la protección de datos personales al derecho a la intimidad, restándole la autonomía de un derecho fundamental que aunque en cierta medida ambos comparten el objetivo de ofrecer una salvaguarda, en el derecho a la protección de datos pueden ser íntimos o no. Igualmente, considera este derecho a la posible utilización por terceros en forma no autorizada de datos personales susceptibles de tratamiento automatizado, sin embargo, el derecho no refiere únicamente a la utilización de los datos, sino a los derechos denominados ARCO que se deriven de la recogida y el tratamiento; además, el autor hace alusión exclusivamente al tratamiento automatizado de datos, dejando de lado los archivos manuales que también constituyen fuentes de información que permiten identificar al titular del dato. Por lo tanto, la definición adolece de serias deficiencias.

En la Semana Nacional de Transparencia 2005, llevada a cabo en el IFAI, Isabel Dávara, sostenía que existen entre "150 y 200 datos personales". Si bien es cierto, todos ellos no pueden quedar cuantificados en una definición, hay elementos que deben ser insertados en la propia concepción en algunos casos expresamente, en otros siendo alusivos o encontrarse inmersos en aquellos o bien por analogía, por lo que atendiendo a la aparición de las nuevas tecnologías, ha sido necesario que el concepto de protección de datos personales se modifique, toda vez que se traduce en un derecho de control sobre los datos relativos a su persona, por lo que atendiendo a este criterio, propongo la siguiente definición:

"El derecho fundamental de protección de datos personales es la facultad jurídica del individuo de disponer y controlar sus datos sean íntimos o no, sensibles o no, y en general cualquiera que estos sean: además de imponer la obligación a terceros de omitir o realizar actos que importen peligro al titular de aquéllos frente al tratamiento automatizado o manual, en archivos públicos o privados, que identifiquen o permitan la identificación de su persona".

Un sector reducido de la doctrina científica se ha manifestado haciendo alusión a la protección de datos personales como manifestación del derecho a la

intimidad; sin embargo, yo no coincido con ella y me identifico con el sector mayoritario que se pronuncia a favor de la autonomía plena del derecho. Veamos como ha regulado el Derecho a la protección de datos la normativa comparada: México, España y Argentina.

1.1.1.2. Legislación

El derecho de protección de datos personales ha sido recogido por legislaciones que han ido adoptando su normativa a los Tratados, Convenios y Directivas Internacionales. Como punto de partida esta España, que es pionera entre los países a estudio, siguiendo con la República Argentina, la cual adoptó este derecho mediante su artículo 43 constitucional y en su Ley reglamentaria 25.326 de Hábeas Data y su Decreto Reglamentario 1558/01, y finalmente México que se incorpora tardíamente a la tendencia internacional.

En el Derecho Comunitario, el Estado Español, lo prevé en el artículo 18 de su Constitución y lo desarrolla en la *Ley Orgánica 15/1999*, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Posee un organismo encargado de velar el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, cancelación y oposición de datos. Este organismo es la AGENCIA ESPAÑOLA DE PROTECCION DE DATOS (AEPD), Ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada, adscrito al Ministerio de Justicia, pero que actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones.

Por su parte la Ley 15/99, esgrime en su artículo 1º, que el objeto de la ley es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y el artículo 3º, inciso a) define al dato personal como cualquier información concerniente a personas físicas identificadas o identificables, ello bajo la

interpretación de la Sentencia 292/2000 de 30 de noviembre, en donde se reconoce el derecho como autodeterminación informativa o libre disponibilidad de los datos de carácter personal.

La República Argentina, lo regula en el artículo 43 Constitucional, que establece: "...Toda persona podrá interponer esta acción (Hábeas Data) para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos...".

La *Ley Nº 25.326 de Hábeas Data y su Decreto 1558/01,* establecen que el objeto de la ley, es la protección integral de los datos personales, asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a los establecido por el artículo 43, párrafo tercero de la Constitución Nacional...", lo mismo que su Decreto en alcance a dicha ley.

En México, la reforma constitucional de 1 de junio de 2009, que adiciona un segundo párrafo al artículo *16 de la Constitución Política de los Estados Unidos Mexicanos,* reconoce el derecho a la protección de datos personales en los siguientes términos *"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."*[14]

[14] DECRETO por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Diario Oficial de la Federación, 1 de junio de 2009.

Por su parte la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental* (en adelante LFTAIP), define a los datos personales como "la información concerniente a una persona física, identificada o identificable, entre otras, la relativa a su origen étnico, racial, o que esté referida 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 la intimidad.[15]

La Ley de Protección de Datos Personales para el Distrito Federal de 3 de octubre de 2008, define de forma amplia el concepto, al establecer como datos personales 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 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.

Por último, la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* (en adelante LFPDP) de 6 de julio de 2010, concreto en lo siguiente: "Cualquier información concerniente a una persona física identificada o identificable".

En principio, parece que en México, el tema de Protección de Datos Personales, ha dejado de ser una tarea pendiente, al efectuarse las reformas a los artículos 6º y 16 Constitucionales, éste último que dispone por vez primera el derecho de Hábeas Data que refiere al derecho que tiene todo ciudadano a la protección de sus datos personales con los denominados derechos ARCO, sin

[15] Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. IFAI, 2007

embargo, también establecen los casos de excepción a dichos derechos por razones de orden, salud, y seguridad jurídica o para proteger los derechos de terceros.

Esta reforma constitucional, constituyó el fundamento para la creación de la Ley Federal sobre Protección de Datos Personales en Posesión de los Particulares, colocando a nuestro país a la vanguardia en la protección de este derecho de tercera generación.

Por su parte, el Instituto de Acceso a la Información Pública (en adelante IFAI), como organismo descentralizado de la Administración Pública, expidió un Decreto sobre el cual se crean políticas generales y procedimientos que deberán observar las dependencias y entidades de la Administración Pública Federal, a fin de garantizar a la persona la facultad de decisión sobre el uso y destino de sus datos personales a saber constituyen los siguientes:

- *Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares.*
- *Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental que formulen los particulares, así como en su resolución y notificación, y la entrega de la información en su caso, con exclusión de las solicitudes de acceso a datos personales y su corrección.*
- *Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos.*
- *Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal para notificar al Instituto el listado de sus sistemas de datos personales.*
- *Lineamientos de protección de datos personales.*
- *Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales.*

A nivel local, los Estados de Colima, Guanajuato, Morelos, Coahuila y el Distrito Federal, cuentan con una Ley de Protección de Datos Personales, y de igual manera Municipios de los Estados mencionados, así como Sinaloa, Durango, Estado de México, cuentan con Reglamentos para la protección de este derecho.

A modo de conclusión, podemos referir que aunque el Estado Español en principio establezca la disyuntiva de que los artículos 18.1 y 18.4 Constitucionales que establecen a la protección de datos como un derecho de configuración legal de la intimidad, la doctrina jurisprudencial (en sentencia de 30 de noviembre de 2000, 292/00, del Tribunal Constitucional, la que referiremos más adelante), se pronuncia a favor de la postura de un nuevo derecho fundamental, donde deja claro la autonomía de la protección de datos personales.

La ley 15/99 de Protección de Datos es considerada como un estándar internacional, que ha servido de referente para la creación de otras leyes como la Ley Argentina 25.326, por lo que podemos considerar a la Legislación española como fundamento normativo. Pese a ello la legislación Argentina, también ha marcado un hito en la historia de la Protección de Datos Personales en América, su normativa actualiza los altos estándares de calidad para la Protección de los datos, al amparo también de su decreto 1558/01, que reglamenta a su Ley de Habeas Data.

En México la legislación en materia de datos personales ha ido en evolución gracias a las exigencias sociales, y recientemente a la creación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, la cual pretende introducir a México a un nivel adecuado de protección de datos con otros países, derivado de la red de Tratados comerciales con lo que nuestro país cuenta y sobre todo por las limitantes que prevén al respecto otros tratados comerciales como el TLCAN, y evitar el desinterés del comercio con otros países de la Unión Europea, que exigen cierto grado de protección en la materia.

Pese a la adopción de la norma internacional al sistema jurídico mexicano, los avances en este tópico deben de ir en incremento, ya que ante las nuevas modalidades de tecnologías de la información, se requiere la adecuación de medidas de seguridad que garanticen el derecho fundamental de la autodeterminación informativa.

Las insuficiencias que la LFPDP contenga deberán ser subsanadas por el órgano encargado de aplicarla, conjuntamente con los Lineamientos que al efecto se expidan y la estructura que se forme por la necesidad de garantía sobre el derecho, ya que el ejercicio de los derechos ARCO, en materia de publicidad no se encuentra regulado específicamente, remitiendo a otros sectores de la Administración Pública para reglamentar los aspectos comerciales, mismos que se encuentran pendientes.

Aunado a ello, la falta de regulación sobre el tratamiento automatizado, y la ausencia de un Registro Nacional de Bases de Datos, constituyen argumentos sólidos para la implementación de reformas, adiciones, mejores prácticas, programas, políticas, recomendaciones, etc., que permitan y complementen el derecho del hombre, y al mismo tiempo, aporten al país una reducción de distancias entre las potencias comerciales y México.

1.1.1.3. Doctrina Jurisprudencial

No puede obviarse que estamos frente a un auténtico derecho fundamental, cuyo contenido el Tribunal Constitucional Español ha terminado de perfilar en la Sentencia 292/2000, de 30 de noviembre,[16] denominándolo derecho de autodeterminación informativa o de libre disponibilidad de los datos de carácter personal. En dicha sentencia se indica que este derecho fundamental *"persigue garantizar a esa persona el poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado"*.

Declara en cuanto a su ámbito, que *"el objeto de protección del derecho fundamental a la protección de datos no se reduce sólo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo*

[16] Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

conocimiento o empleo por tercero pueda afectar a sus derechos sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 de la Constitución Española otorga, sino los datos de carácter personal."

La jurisprudencia de la Corte Suprema Argentina, que refiere a la protección de datos personales, puede clasificarse antes y después[17] de la Ley 25.326 de Hábeas Data., sin embargo, cabe destacar la que dejó fundamento para la interpretación del derecho a la protección de datos personales:

En el caso Suárez Mason del 13 de agosto de 1998,[18] la Corte Suprema de Justicia sostuvo que el artículo 43, párrafo tercero del a Constitución Nacional, ha incorporado un nuevo derecho a la protección de los datos personales frente a cualquier intromisión arbitraria o abusiva que pudiera implicar una violación a la intimidad.

En México, el Poder Judicial de la Federación ha emitido diversos criterios a través de sus órganos, principalmente la Suprema Corte de Justicia se ha pronunciado en materia de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (así como los criterios pronunciados por el Comité de Acceso a la Información y de Protección de Datos Personales, en adelante CAIPDP), de la Suprema Corte de Justicia de la Nación (en adelante SCJN), durante los años 2003 a 2008,[19] de los cuales cabe resaltar:

---

[17] FALLOS ANTERIORES A LA LEY: *Steifensand, Egbert Friederich Kaspar c/Cablevisión SA s/amparo; Súarez Mason S/Homicidio y privación Ilegal de la Libertad; Urteaga, Facundo Raúl c/Estado Nacional-Estado Mayor Conjunto de las Fuerzas Armadas s/amparo Ley 16.986; Matimport SA s/medida precautoria, y otros.* FALLOS RESUELTOS DESPUÉS DE DICTADA LA LEY: *Lazcano Quintana Guillermo Víctor c/Veraz SA s/Habeas Data; González Juan Carlos c/BCRA y otros s/hábeas data; Paolini, Nicolás Agustín c/Registro del estado Civil y Capacidad de las Personas s/Hábeas Data.*
SUÁREZ MASON S/HOMICIDIO Y PRIVACIÓN ILEGAL DE LA LIBERTAD. Fallos, 319:71 http://www.csjn.gov.ar/consultaexp/documentos/expedientes/cons_expe.jsp

[19] Al respecto pueden consultarse todos los criterios establecidos en *Compilación de normas y criterios en materia de Transparencia, Acceso a la Información Pública y Protección de Datos Personales de la Suprema Corte de Justicia de la Nación*. Quinta edición, SCJN, México, 2009.

CRITERIOS EMITIDOS POR LA SCJN:

Transparencia y Acceso a la Información Pública Gubernamental. El artículo 14, fracción I, de la Ley Federal relativa, no viola la garantía de Acceso a la Información.[20] En tal criterio, el Pleno de la Suprema Corte de Justicia de la Nación refiere que el artículo en comento, no viola el ejercicio del derecho a la información del artículo 6º constitucional, porque es *jurídicamente adecuado que en las leyes reguladoras de la materia, el legislador federal o local establezca las restricciones correspondientes y clasifique a determinados datos como confidenciales o reservados, con la condición de que tales límites atiendan a intereses públicos o particulares y encuentren justificación racional en función del bien jurídico a proteger,* es decir que exista proporcionalidad y congruencia entre el derecho fundamental de que se trata y la razón que motive la restricción.

Transparencia y Acceso a la Información Pública Gubernamental. Los artículos 3º, fracción II, y 18, fracción II, de la Ley Federal relativa, no violan la garantía de igualdad, al tutelar el Derecho a la Protección de Datos Personales sólo de las personas físicas.[21] Esta tesis sustenta que el derecho a la protección de datos personales se refiere únicamente a las personas físicas por estar encausado respecto de un derecho personalísimo, como es el derecho a la intimidad, del cual derivo aquél y por lo tanto no existe igualdad jurídica entre las personas físicas y las morales.

En este criterio, la Suprema Corte de Justicia sostiene que el derecho a la protección de datos personales constituye una derivación del derecho a la intimidad; en el mismo sentido lo declara en la siguiente interpretación:

---

[20] Amparo en revisión 50/2008. Rosario Liévana León. 12 de marzo de 2008. *Semanario Judicial de la Federación y su Gaceta,* Novena Época, Tomo XXVII, abril de 2008, Segunda Sala, p. 733, Tesi, 2ª XLIII/2008, IUS: 169772.

[21] Amparo en revisión 191/2008. Grupo Senda Autotransporte S.A. de C.V. 7 de mayo de 2008. *Semanario Judicial de la Federación y su Gaceta,* Novena Época, Tomo XXVII, julio de 2008, Segunda Sala, p. 549, Tesi, 2ª XCIX/2008, IUS: 169167.

Transparencia y Acceso a la Información Pública Gubernamental. Los artículos 3o, fracción II, y 18, fracción II, de la Ley Federal relativa, no violan la garantía de igualdad, al tutelar el derecho a la protección de datos personales sólo de las personas físicas. El presente criterio señala que si se toma en cuenta que la garantía constitucional indicada no implica que todos los sujetos de la norma siempre se encuentren en condiciones de absoluta igualdad, sino que gocen de una igualdad jurídica traducida en la seguridad de no tener que soportar un perjuicio (o privarse de un beneficio) desigual e injustificado, se concluye que los artículos 3o., fracción II, y 18, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, al tutelar sólo el derecho a la protección de datos personales de las personas físicas y no de las morales, colectivas o jurídicas privadas, no violan la indicada garantía contenida en el artículo 1º de la Constitución Política de los Estados Unidos Mexicanos, pues tal distinción se justifica porque el derecho a la protección de los datos personales se refiere únicamente a las personas físicas por estar encausado al respeto de un derecho personalísimo, como es el de la intimidad, del cual derivó aquél. Esto es, en el apuntado supuesto no se actualiza una igualdad jurídica entre las personas físicas y las morales porque ambas están en situaciones de derecho dispares, ya que la protección de datos personales, entre ellos el del patrimonio y su confidencialidad, es una derivación del derecho a la intimidad, del cual únicamente goza el individuo, entendido como la persona humana.[22]

CRITERIO EMITIDO POR EL CAIPDP:

Nombramientos y Avisos de Baja de los Servidores Públicos de la Suprema Corte de Justicia de la Nación. El Documento en el que consten es público, con excepción de los datos personales que contengan, los que constituyen información confidencial que debe

[22] Novena Época, Instancia: Segunda Sala, Fuente: Semanario Judicial de la Federación y su Gaceta, XXVIII, Julio de 2008, Página: 549,Tesis: 2a. XCIX/2008, Tesis Aislada Materia(s): Administrativa, Constitucional.

suprimirse de la versión pública que se genere.[23] En dicho criterio, se sostiene que los documentos relativos a los nombramientos y avisos de baja de los servidores públicos de la Suprema Corte, constituyen información pública, toda vez que se trata de actos administrativos relativos al manejo de su personal, y por ende justifican parte del ejercicio del presupuesto asignado. En ese sentido debe generarse una versión pública que suprima datos personalísimos y confidenciales como son: el domicilio, el estado civil o el teléfono particular del servidor público.

En diciembre de 2009, salió publicado en el Semanario Judicial de la Federación uno de los criterios más recientes del Poder Judicial sobre datos personales en los términos siguientes:

Transparencia y Acceso a la Información Pública Gubernamental. Al resolver la oposición del tercero interesado a una solicitud de acceso a sus datos personales, la autoridad debe explicar, de considerarla fundada, por qué estima que la difusión de éstos daña innecesariamente a la persona o, en caso contrario, cuáles son los beneficios que con ello se generan al interés público. De los artículos 24, 25, 40 y 50 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y 40 y 41 de su reglamento, se advierte la posibilidad de que el titular de la información (en su carácter de tercero interesado) se oponga ante la autoridad, dependencia o entidad, a una solicitud de acceso a sus datos personales y alegue lo que a su derecho convenga, ya sea en la primera etapa de ese procedimiento -que se desarrolla ante la unidad de enlace correspondiente-, o en la segunda al tramitarse el recurso de revisión. Así, el ejercicio de la garantía de audiencia, en ambas etapas, tiene como propósito que la resolución sobre acceso a información pública cumpla con las formalidades previstas en los ordenamientos mencionados, necesarias para oír en defensa al tercero titular de la información afectado quien puede manifestar su conformidad u oposición con la divulgación de

[23] Clasificación de Información 10/2006-A, derivada de la solicitud de Acceso a la Información presentada por Aldo González Gutiérrez, 11 de abril de 2006. *Íbidem*. Pág. 565-566.

la información, en el entendido que en el último caso deberá demostrar que la divulgación anotada genera un daño específico al valor jurídicamente protegido. De lo anterior se concluye que al resolver la oposición del tercero interesado a una solicitud de acceso a sus datos personales, la autoridad debe explicar, de considerarla fundada, por qué estima que la difusión de éstos daña innecesariamente a la persona, lo cual justificaría clasificar la información como reservada o confidencial o, en caso contrario, cuáles son los beneficios que con ello se generan al interés público para que ciertos datos sean difundidos a pesar de la afectación a los secretos tutelados.[24]

Hasta aquí, considero que el derecho a la protección de datos personales tiene particularidades que no pueden reducirse sólo al derecho a la intimidad, puesto que con la intromisión de terceros a la esfera de privacidad del individuo, pueden ser objeto de agresión otros datos personales que no necesariamente son íntimos, ya que también se alcanza aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento ajeno, no escapan al poder de control y disposición del titular porque así lo garantiza su derecho a la protección de datos (derechos ARCO), por consiguiente no comparto el criterio de las Cortes Argentina y Mexicana, ya que reducen la protección de datos personales a la esfera de la intimidad, y el derecho de protección de datos va más allá de datos puramente íntimos, sirviendo como fundamento el Convenio para la Protección de las Personas respecto al Tratamiento Automatizado de Datos de Carácter Personal, la Carta de Derechos Fundamentales de la Unión Europea y la Directiva del Parlamento Europeo 95/46/CE.

[24] Amparo en revisión 248/2009. Promotora Azucarera, S.A. de C.V. 1o. de octubre de 2009. Unanimidad de votos. Ponente: Jesús Antonio Nazar Sevilla. Secretaria: Indira Martínez Fernández. Novena Época, Instancia: Tribunales Colegiados de Circuito, Fuente: Semanario Judicial de la Federación y su Gaceta XXX, Diciembre de 2009, Página: 1658, Tesis: I.4o.A.688 A, Tesis Aislada, Materia(s): Administrativa.

.

Ahora bien, si es evidente que, al menos en parte, coinciden el derecho a la intimidad y el derecho a la autodeterminación informativa, ya no lo es tanto que puedan considerarse incluidas en el primero las exigencias relacionadas con la protección de los datos de carácter personal no encuadrables en la noción de intimidad en sentido estricto.

1.1.2. Autodeterminación Informativa o Derecho informático

1.1.2.1. Diferencia

El derecho informático, ha sido analizado desde diversas perspectivas. Por un lado el Derecho Informático se define como un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el Derecho y la informática. Por otro lado hay definiciones que establecen que es una rama del derecho especializado en el tema de la informática, sus usos, sus aplicaciones y sus implicaciones legales. El término "Derecho Informático" (Rechtinformatik) fue acuñado por el Prof. Dr. Wilhelm Steinmüller, académico de la Universidad de Regensburg de Alemania, en los años 70´s. Sin embargo, no es un término unívoco, pues también se han buscado una serie de términos para el Derecho Informático como Derecho Telemático, Derecho de las Nuevas Tecnologías, Derecho de la Sociedad de la Información, Iuscibernética, Derecho Tecnológico, Derecho del Ciberespacio, Derecho de Internet, etc.

Se considera que el Derecho Informático es un punto de inflexión del Derecho, puesto que todas las áreas del derecho se han visto afectadas por la aparición de la denominada Sociedad de la Información, cambiando de este modo los procesos sociales y, por tanto, los procesos políticos y jurídicos. Es aquí donde hace su aparición el Derecho Informático, no tanto como una rama sino como un cambio.

El Derecho informático o Derecho de la informática constituye el sector normativo de los sistemas jurídicos contemporáneos integrado por el conjunto de disposiciones dirigido a la regulación de las nuevas tecnologías de la información y

la comunicación, es decir, la informática y la telemática. Así mismo integran el Derecho informático, las proposiciones normativas, es decir, los razonamientos teóricos del Derecho que tienen por objeto analizar, interpretar, exponer, sistematizar o criticar el sector normativo que disciplina la informática y la telemática. Las fuentes y estructura temática del Derecho informático afectan a las ramas de derecho tradicionales.

Así se inscriben en el ámbito del derecho público: el problema de la regulación del flujo internacional de datos informatizados, que interesa al derecho internacional público; la libertad informática, o defensa de las libertades frente a eventuales agresiones perpetradas por las tecnologías de la información y la comunicación, objeto de especial atención por parte del derecho constitucional y administrativo; o los delitos informáticos, que tienden a configurar un ámbito propio en el derecho penal actual, mientras que inciden directamente en el derecho privado cuestiones tales como en los contratos informáticos.

Ese mismo carácter interdisciplinario que distingue al derecho informático, ha suscitado un debate teórico sobre: si se trata de un sector de normas dispersas pertenecientes a diferentes disciplinas jurídicas; o constituye un conjunto unitario de normas, dirigidas a regular un objeto bien delimitado, que se enfoca desde una metodología propia, en cuyo supuesto entrañaría una disciplina jurídica autónoma.

Por su parte, Antonio Enrique Pérez Luño,[25] señala que el derecho a la autodeterminación informativa, es una construcción de la doctrina y la jurisprudencia germana equivalente a la libertad informática, tiene una importancia decisiva en las sociedades tecnológicas del presente. Su función se cifra en garantizar a los ciudadanos unas facultades de información, acceso y control de los datos que le conciernen. Pero esa forma de intimidad no se concibe como un valor intrasubjetivo, sino como autodeterminación del sujeto en el seno de sus relaciones con los demás ciudadanos y con el poder público. La *Grundgeset* de

[25] *Ensayos de Informática Jurídica*. Distribuciones Fontamara, México, 1996. P. 14

la República Federal Alemana proclama el libre desarrollo de la personalidad en su artículo 2.1: mientras que la vigente Constitución española de 1978 lo hace en su artículo 10.1. Este valor se desglosa, según la doctrina germana, en las dos libertades básicas: la libertad general de acción, entendida como libertad para decidir la realización u omisión de determinados actos y la consiguiente facultad para comportarse o actuar de acuerdo con esa decisión; y la autodeterminación informativa.

Así pues, Ana Isabel Herrán Ortiz, define a la autodeterminación informativa como: "La libre capacidad de decisión que todo individuo ostenta respecto a la difusión, utilización y cesión de la información que le concierne".[26]

La propia expresión "autodeterminación informativa" facilita en cierto modo la definición del contenido de este derecho: facultad del individuo a *determinar* por sí mismo la línea de actuación en relación a la *información* relativa a su persona.

El concepto de autodeterminación informativa, se construye a partir del concepto de privacidad, dicho concepto nos remonta a la Sentencia emitida por el Tribunal Constitucional Alemán de 15 de diciembre de 1983,[27] que declaró inconstitucionales algunos artículos de la Ley del Censo de la República Federal Alemana, ha marcado un hito en la defensa de los derechos de la persona a preservar su vida privada.

> *"El recurso contra dicha Ley fue interpuesto por simpatizantes del movimiento de "los verdes", quienes obtuvieron una resolución cautelar del Tribunal Constitucional el 13 de abril de 1983, por la que se suspendió la entrada en vigor de la Ley del Censo y posteriormente la decisión definitiva sobre el fondo del recurso. En esta sentencia el Tribunal Constitucional germano señala que la proliferación de centros de datos ha permitido,*

[26] Herrán Ortiz, Ana Isabel. *"La violación de la Intimidad en la Protección de Datos Personales"*, Dykinson, Madrid, 1999. P. 89
[27] Schwabe, Jürgen. *Jurisprudencia del Tribunal Constitucional Federal Alemán. Ob. Cit.* P. 94

gracias a los avances tecnológicos producir "una imagen total y pormenorizada de la persona respectiva -un perfil de la personalidad-, incluso en el ámbito de su intimidad, convirtiéndose así el ciudadano en hombre de cristal".

El Tribunal Federal ha sido rotundo en su decisión de que la persona posee un derecho de libre decisión y libre disposición sobre sus datos personales y que puede decidir qué es lo que otros pueden saber sobre él.

La sentencia del tribunal Constitucional alemán señala que las limitaciones a este derecho a la autodeterminación informativa sólo son admisibles en el marco de un interés general superior y suscitan un fundamento legal basado en la Constitución. El legislador, en su regulación, debe observar el principio de proporcionalidad y tiene que adoptar, asimismo, precauciones de índole organizativa y de derecho procesal susceptible de contrarrestar el peligro de vulneración del derecho a la salvaguardia de la personalidad. Declara ilícitos, entre otros, los preceptos relativos al cotejo de datos para ser utilizados contra las personas obligadas a suministrar esa información"[28].

De la precedente sentencia del Tribunal Constitucional Alemán, cabe destacar los siguientes aspectos:

1. Las limitaciones de este derecho a la "autodeterminación informativa" sólo son admisibles en el marco de un interés general superior y necesitan un fundamento legal basado en la Constitución, que debe corresponder al imperativo de claridad normativa inherente al Estado de Derecho.

2. En la Ley Fundamental se encuentra el valor y la dignidad de la persona, que actúa con libre autodeterminación como miembro de una sociedad libre. El derecho general de la personalidad abarca la facultad del individuo derivada de la autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué

[28] http://www.informatica-juridica.com/autodeterminacion_informativa.asp

límites procede revelar situaciones referentes a la propia vida: la libre eclosión de la personalidad presupone en las condiciones modernas de la elaboración de datos de protección del individuo contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona.

3. El derecho fundamental garantiza, en efecto, la facultad del individuo de decidir básicamente por sí solo sobre la difusión y utilización de sus datos personales.

4. La elaboración automática de datos ha ampliado en una medida hasta ahora desconocida las posibilidades de indagación e influencia susceptibles de incidir sobre la conducta del individuo, siquiera sea por la presión psicológica que supone el interés del público en aquélla. La autodeterminación del individuo presupone que se conceda al individuo la libertad de decisión sobre las acciones que vayan a realizar o, en su caso a omitir. El que no pueda percibir con seguridad suficiente qué informaciones relativas a él son conocidas en determinados sectores de su entorno social y quién de alguna manera no sea capaz de aquilatar lo que puedan saber de él sus posibles comunicantes puede verse sustancialmente cohibido en su libertad de planificar o decidir por autodeterminación. Quien sepa de antemano que su participación, por ejemplo, en una reunión o iniciativa cívica va a ser registrada por las autoridades y que podrán derivarse riesgos para él, por este motivo renunciará presumiblemente a lo que supone un ejercicio de los correspondientes derechos fundamentales.

En consecuencia, el reconocimiento y la conceptualización del derecho a la autodeterminación informativa ha significado el inicio de un intenso debate entre los juristas españoles, que todavía hoy continúa, sobre la oportunidad de su reconocimiento como derecho fundamental, su naturaleza y contenido así como respecto a la expresión más adecuada en torno a la que se pueda resumir la técnica de protección de datos personales.

En cambio, el concepto de Derecho informático hace alusión preferentemente a la sistematización de la información automatizada en la creación, regulación y uso de bases de datos en las tecnologías de la información, y el concepto de autodeterminación informativa, refiere precisamente a la protección de esa información personal sobre quién, cómo, cuándo y dónde a través de los distintos medio informáticos; asimismo, el concepto de autodeterminación informativa abarca situaciones no sólo de carácter informativo, sino los derivados de cualquier acontecimiento en el cual se ponga en riesgo tal o cual información sensible o no, íntima o no y en detrimento de su derecho, el derecho a la autodeterminación constituye un derecho fundamental, el derecho informático no.

Podemos mencionar que el concepto de autodeterminación informativa, es el fruto de una reflexión doctrinal y de las elaboraciones jurisprudenciales que se han producido en otros ordenamientos en relación con el control, por parte del sujeto afectado, sobre las informaciones que se refieren a su persona o a su familia, y se encamina fundamentalmente a dotar a las personas de cobertura jurídica frente al peligro que supone la informatización de sus datos personales.

Aun en el supuesto de que no hubiese duda alguna sobre la identidad del ámbito material tutelado por ambas categorías de derechos, siempre permanecería como dato diferencial el hecho de que ese aspecto de la intimidad relacionado con el control de la información personal plantea perfiles absolutamente nuevos con la irrupción de las nuevas tecnologías.

Se trata de dos figuras conceptualmente distintas, puede ocurrir que los problemas específicos que plantea la informática hagan conveniente organizar la defensa jurídica del ciudadano en lo que toca a sus datos personales desde una posición de independencia sistemática respecto de los otros perfiles de la intimidad.

Finalmente, podemos decir que el derecho a la autodeterminación informativa (denominación por la que me inclino) refiere la decisión autónoma del titular de

controlar la información que corre por el tráfico de la informática, esto es que, la autodeterminación informativa es el medio para garantizar la libertad informativa en los medios tecnológicos.

A continuación expondremos los principios sobre los que descansa el derecho a la protección de datos personales y sin los cuales el derecho fundamental no puede gozar de la libertad que encierra su naturaleza, ya que el cumplimiento de estos principios garantiza la utilización racional de los datos personales y permite compatibilizar el tratamiento de ellos tanto en ficheros manuales como automatizados, logrando que el desarrollo informático beneficie a las necesidades sociales con el respeto más escrupuloso a los derechos y libertades de las personas. Por ello, a través de la configuración de los principios que enseguida veremos, el legislador pretende configurar un sistema preventivo de tutela de la persona frente al tratamiento de la información que le concierne, estableciendo un adecuado equilibrio entre la sociedad de la información y el derecho a la autodeterminación informativa.

1.2. Principios generales relativos a la protección de datos

Los principios que rigen la protección de datos personales, ha emanado del Derecho Comunitario, el cual ha sido participe en la elaboración de normatividad en otros Estados-Nación, como sucede con Argentina, país que ha adoptado dichos principios a su legislación interna y que lo han considerado como su fuente inmediata, los principios generales relativos a la protección de datos personales, constituyen los pilares en los que se basa la protección de este derecho, mismos que son reconocidos internacionalmente en aquellos países en cuya legislación se protegen los datos personales.

En los epígrafes subsecuentes veremos los casos de la *Ley Argentina 25.326, de Protección de Datos de Carácter Personal*, en España la *Ley 15/99 de Protección de Datos*, en México el caso de la Ley Federal de Transparencia y Acceso

a la Información Pública Gubernamental y la reciente Ley Federal de Protección de Datos Personales en Posesión de Particulares.

En el caso de la República Argentina, los principios de la protección de datos están regulados en el segundo capítulo de de la ley 25.326, que está compuesto por diez artículos, y sigue los lineamientos de su fuente comparada inmediata, la *Ley Orgánica de Regulación del Tratamiento Automatizado de Datos* (LORTAD) española de 1992 (misma que fue remplazada en 1999, por la *Ley Orgánica de Protección de Datos de Carácter Personal*), tomando además los principios rectores de la reglamentación de los ficheros computarizados de datos personales de la ONU de 1990.[29]

Los presentes principios rectores deben ser aplicables a los ficheros de las organizaciones internacionales gubernamentales de datos personales, a reserva de las adaptaciones necesarias para tener en cuenta las posibles diferencias que puedan existir entre los ficheros con fines internos, como los relativos a la gestión del personal, y los ficheros con fines externos relativos a terceras personas relacionadas con la organización. Con base en estos principios, cada organización debe designar a la autoridad que estatutariamente es competente para velar por la correcta aplicación de estos principios rectores, debiendo preverse de manera específica una excepción a estos principios cuando el fichero tenga por finalidad proteger los derechos humanos y las libertades fundamentales de la persona de que se trate, o prestar asistencia humanitaria.

Asimismo, la legislación nacional debe contener una excepción análoga para las organizaciones internacionales gubernamentales en cuyo convenio sobre la sede no se hubiera excluido la aplicación de dicha legislación nacional, así como para las

[29] Principios relativos a las garantías mínimas que deberían preverse en la legislación nacional: principio de licitud y lealtad, principio de exactitud, principio de finalidad, principio de acceso a la persona interesada, principio de no discriminación, facultad de establecer excepciones, principio de seguridad, control y sanciones, flujo de datos a través de las fronteras.

organizaciones internacionales no gubernamentales a que sea aplicable dicha legislación.

Por su parte, el Estado mexicano ha recogido los principios rectores del tratamiento de datos personales recientemente en la *Ley Federal de Protección de Datos Personales en Posesión de Particulares*, que sigue los lineamientos fijados por la *Constitución Política de los Estados Unidos Mexicanos*, así lo establece en sus artículos 6 a 21, del Capítulo denominado "De los Principios de Protección de Datos Personales", mismos a los que deben someterse los particulares en el tratamiento de datos personales.

Siguiendo con ello los principios de la reciente adición al artículo 16 constitucional, que sientan las bases sobre las que deben permanecer la creación de leyes en materia de protección de datos personales, así se desprende de la lectura del artículo, en donde se plasman los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

A continuación abordaremos los principios que se encuentran en las legislaciones de los países objeto de estudio.

1.2.1. Seguridad de los datos

La Seguridad en materia de protección de datos, se encontraba regulada en la abrogada *Ley Orgánica que regula el Tratamiento Automatizado de Datos Personales* (en adelante *LORTAD)*, la cual en su título II, se dedicaba a los principios de la protección de datos, y en donde se prohibía registrar datos de carácter personal en ficheros automatizados, centros de tratamiento, y en general programas que no reuniesen las condiciones respecto a la integridad y seguridad de ellos.

El artículo 9 de la *Ley Orgánica Española 15/1999*, de 13 de diciembre, referente a la Protección de Datos de Carácter Personal, mantuvo el mismo texto legal contenido en la abrogada ley, por lo que de igual manera resulta ilegal el tratamiento de datos personales sin las condiciones de seguridad, estableciéndolo de la siguiente manera:

> Artículo 9.
> 1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.
> 2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
> 3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Al respecto la Sentencia 292/2000, del Tribunal Constitucional Español, de 30 de noviembre,[30] hace referencia a dicho principio al manifestar: "garantizada la seguridad de los datos, resulta legítimo el tratamiento de datos personales", lo que señalado a contrario sensu, dispone que si no se encuentra garantizada la seguridad de los datos personales, el tratamiento de esos datos en cualquiera de sus modalidades resulta ilegítimo.

Por su parte, el artículo 9 de la *Ley 25.326 Argentina*, tiene su fuente en la LORTAD española, por ello, podemos apreciar situaciones similares, en materia de seguridad de datos personales, pues en ambas legislaciones, se concreta, el sistema

[30] Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

de seguridad, entendiéndolo no como una simple obligación, sino como condición de licitud de la actividad, en los términos siguientes:

> ARTICULO 9° — (Seguridad de los datos).
>
> 1. El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.
> 2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

La garantía de seguridad que debe brindar el responsable o usuario de los datos debe ser entendida como el deber a su cargo de implementar y mantener el conjunto de medidas tecnológicas, de normas y procedimientos que aseguren la confidencialidad, integridad y disponibilidad de la información en sus diferentes estados de proceso, almacenamiento, transmisión y recuperación.[31] De manera que la seguridad no se configure sólo como un principio de la protección de datos, sino como un condicionante previo al tratamiento de los mismos.[32]

En México, la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental* dispone el principio de seguridad en el tratamiento de datos, impidiendo a personas no autorizadas el acceso a los sistemas de datos personales, en particular, y a los datos en general, para evitar el desvío de la información, malintencionadamente o no, hacia sitios no previstos, además de garantizar el tratamiento de datos en los límites permitidos por la norma y con respeto a los derechos del afectado, asegurando la confidencialidad y la integridad

[31] Carranza Torres, Luis R. *"Hábeas Data. La Protección jurídica de los datos personales"*. Alverone Ediciones, Córdova, Argentina, 1996. P.74
[32] Almuzara Almaida, Cristina, et. al. *"Estudio Práctico sobre la protección de datos de carácter personal"*. Lex Nova, 1ª, edición, España, 2005. P. 540

de los datos personales evitando su alteración, pérdida, transmisión y acceso no autorizado.

En concreto la Ley prevé en su artículo 20, fracción VI, la obligación de quienes tengan sistemas de datos personales de "adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado".

Por su parte la LFPDP, establece:

> "Artículo 19.- Todo responsable que lleve a cabo el tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.
> Los responsables no adoptarán medidas de seguridad menores a aquellas que mantengan para el manejo de su información. Asimismo se tomará en cuenta el riesgo existente, las posibles consecuencias para los titulares, la sensibilidad de los datos y el desarrollo tecnológico."

Igualmente, la Directiva Comunitaria relativa al Tratamiento de Datos de las Personas[33], señaló en su Considerando 25 que, los principios de la protección de datos, tienen su expresión en las distintas obligaciones que incumben a las personas, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos-obligaciones, en particular, entre las que se incluyen la seguridad técnica, y en el Considerando 46, manifiesta que la protección en el tratamiento de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la creación del sistema de tratamiento como en el de la aflicción de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado.

[33] Directiva Comunitaria 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 esos datos (ví: 18 de mayo de 2008) http://www.markalliance.com/index.php?parlamento/63

En consecuencia, los responsables como los encargados del tratamiento de datos relativos a persona físicas, deben poner en práctica medidas de carácter físico, técnico y organizativo adecuadas para garantizar un nivel de seguridad apropiado en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse, de lo que se trata es de diseñar la estructura organizativa que en el ámbito interno del responsable o del encargado del tratamiento debe existir para satisfacer las necesidades especiales de la protección de datos.

Otro de los principios que deben garantizarse, es el de calidad de los datos.

1.2.2. Calidad de los datos

La *Ley Orgánica 15/1999* del Derecho positivo Español, dispone el principio de calidad de los datos, que, ligado al principio de proporcionalidad de los datos, exige que los mismos sean adecuados a la finalidad que motiva su acopio.

El acopio y tratamiento de datos de carácter personal debe efectuarse desde su subordinación a los principios de calidad de los datos y de proporcionalidad que establece la Ley.

Así el artículo 4 de la *Ley Orgánica 15/1999,* del derecho español sostiene:

"Artículo 4. Calidad de los datos.

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.
3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.
4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.
   Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.
6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.
7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos."

Simultáneamente, este principio ha sido abordado por los Tribunales españoles tal como expondremos a continuación.

> 1. La Sentencia de la Sala de lo Contencioso Administrativo de la Audiencia Nacional Española, de 6 de julio de 2001, sostuvo que "La conducta de la entidad recurrente recabando o intentando recabar unos datos de carácter personal (en concreto los relativos a la cuenta bancario o VISA) para su tratamiento automatizado que resultaban completamente innecesarios e inadecuados en relación con el ámbito y finalidades legítimas para las que se hayan obtenido, debe ser constitutiva de infracción (....) Y aunque los datos no llegaron a ser incorporados a los ficheros (...), ello no implica que falte el necesario tratamiento automatizado de los mismos para que se produzca el tipo sancionador".

La sentencia precedente, señala la calidad de los datos contenida en el artículo 4º previamente transcrito, pues la entidad recurrente, violentó lo establecido en el punto 1 de dicho numeral, toda vez que se recogieron datos personales injustificadamente, sin ninguna relación en el ámbito y sin ninguna finalidad determinada; continuemos con la siguiente:

> 2. La Sentencia de la Sección Novena de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 5 de noviembre de 1998, sostiene al respecto: "Sin embargo, aunque (...) no hubo (...) una intención de dañar ni enriquecimiento injusto (...) los hechos han tenido una doble perturbación para la perjudicada: (...) imputarle una deuda inexistente (.....) lo más grave fue su inclusión en un Registro Informático de Morosos y además sin conocimiento de la perjudicada (....) y de esa inclusión indebida en el Registro de Morosos no eran responsables los que llevan el Registro sino los que suministraron el dato".

En la presente resolución, podemos ver la inclusión, del principio de la calidad de los datos, mismo que se ha agraviado, puesto que tales datos ahora fueron destinados para otro uso del cual no fueron objeto de su recogimiento, en concreto, incluir a un particular en el Registro Informático de morosos, y más aun, los mismos no responden a la situación real del afectado, según lo dispuesto por el multicitado artículo 4º, en su punto 3.

> 3. En la resolución de fecha 18 de octubre de 2000, la Sección Octava de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, manifestó: "(....) para incluir en un fichero de solvencia patrimonial el dato relativo a una deuda, ésta, además de cierta, vencida y exigible, ha de haber resultado efectivamente impagada (....) debiendo además, el acreedor (como requisito previo a la inclusión del dato en un fichero de estas características) proceder en la forma más arriba descrita y cuya finalidad no es otra que garantizar la exactitud de los datos que se pretender incluir".

En la sentencia anterior, se señala uno de los elementos del principio de calidad de los datos, nos referimos a la "exactitud" a que se refiere el artículo en comento "Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado", continuando:

> 4. La Sentencia de la Sección Octava de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 26 de mayo de 1999, declara "'Si los datos registrados se han obtenido de una fuente accesible al público (como en el caso de autos) el medio más efectivo para mantener actualizados aquellos será notificando al afectado la existencia del dato a fin de que éste (si el dato obtenido de esa fuente de acceso publico es incorrecto o la situación ha variado) pueda instar las rectificaciones pertinentes en el momento en que el dato registrado no responda a la realidad y si el afectado declina realizar las oportunas rectificaciones, entendemos, su inactividad exculpará al titular del fichero de toda responsabilidad en orden a la actualización de los datos, en la medida que esa actualización no pueda obtenerse de la misma forma en la que se obtuvo el dato." Artículo 4, punto 4.
>
> 5. Y por último, la Sentencia de la Sección Octava de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 9 de febrero de 2000, esbozaba "(...) el dato registrado (..) es transcripción del contenido en dos edictos

publicados en el BOCAM, por lo que ignoramos si son o no exactos dichos datos y, en todo caso, la inexactitud del mismo nunca sería imputable a la actora. Si (..) para los datos obtenidos de fuente accesibles al publico la LORTAD no exige la notificación del registro al afectado, difícilmente puede saber el titular del fichero si el dato obtenido de una fuente accesible al público es o no correcto y, además, en el caso de autos, dado que en el edicto no constan otros datos que el nombre y apellidos de los demandados, nunca hubiera sido posible efectuar tal notificación, ni averiguar la exactitud del dato publicado, ni de lo actuado puede afirmarse que dicho dato se refiera siquiera al denunciante, por lo que en la medida que no conste al titular del fichero la inexactitud del dato registrado, inexactitud que, reiteramos, no consta, no existe para éste la obligación legal de cancelar el dato".

Resulta obvio que ante la duda de saber si el dato recabado en archivos públicos es correcto o incorrecto, preservarse dichos datos, toda vez que su cancelación puede ser un acto de imposible reparación, ya que al erradicar los mismos del archivo, nuevamente se tendría que contar con el consentimiento del afectado para el recogimiento y tratamiento de los datos, cuestión que podría ser incierta al no poder localizarlo, ya que la Ley no obliga a notificar al titular, cuando los datos se extrajeron de fuentes públicas.

La Ley 25.326 Argentina, refiere el principio en su artículo 4º, el cual expresamente menciona el deber de los responsables de bancos de datos de recopilar y dar tratamiento a aquellos que sean veraces y actualizados, mencionando que aquellos datos que sean total o parcialmente inexactos o sean incompletos deben ser suprimidos o completados por el responsable. El principio de calidad considera una serie de obligaciones sobre los distintos aspectos del tratamiento de ellos con el fin de resguardar las condiciones propias del dato como derecho del individuo.

Uno de los principios que inspira la legislación sobre Tratamiento Automatizado de Datos de Carácter Personal es el de calidad de datos. Este principio implica, entre otras cosas, que los datos sean necesarios y pertinentes

para la finalidad para la cual hubieran sido recabados o registrados y que sean exactos y completos.[34]

Por lo tanto, si los datos han dejado de ser necesarios para los fines que fueron recabados o registrados o resultan inexactos, se debe proceder a su cancelación, sin necesidad de solicitud del afectado.

Así lo recogió en México la LFPDP de 6 de julio de 2010, que establece:

> Artículo 11.- El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.
> Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados.
> El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.

A manera de conclusión puedo decir que la calidad de datos personales consiste en una depuración y limpieza de ellos a fin de validar todos los datos que se poseen sobre las personas físicas, corregirlos, normalizarlos y en su caso cancelarlos cuando sea posible y necesario conforme a los lineamientos legales, con el objeto de ganar productividad en la finalidad para la que fueron recogidos.

[34] De la misma forma en México, la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, sostiene en su artículo 20 "Los sujetos obligados serán responsables de los datos personales y, en relación con estos deberán: II. Tratar datos personales sólo cuando estos sean *adecuados, pertinentes y no excesivos,* en relación con los propósitos para los cuales se hayan obtenido...; IV. Procurar que los datos sean *exactos* y actualizados.

1.2.3. Consentimiento

El llamado consentimiento del derecho a la autodeterminación, proviene del derecho alemán, y consiste en el derecho de los particulares a decidir cuándo y cómo permitir que sea difundida información respecto de su persona.[35]

Respecto de este principio de la protección de datos personales, el artículo 5 de la *Ley 25.326 Argentina,* sostiene lo siguiente:

> "ARTICULO 5° — (Consentimiento).
>
> 1. El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias.
>
> El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al requerido de datos, de la información descrita en el artículo 6° de la presente ley.
>
> 2. No será necesario el consentimiento cuando:
>
> a) Los datos se obtengan de fuentes de acceso público irrestricto;
>
> b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
>
> c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;
>
> d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;
>
> e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526. "

Por lo que respecta a este tópico, la jurisprudencia Argentina, se ha centrado en lo establecido en la Constitución Nacional, en su artículo 43, párrafo tercero que implica el reconocimiento del principio conforme al cual en un Estado de Derecho el ciudadano es propietario de los datos que sobre él se registren, por lo tanto, ellos

[35] Ruiz Martínez, Esteban. "Los informes comerciales y el derecho a la información". Citado por Carranza Torres, Luis R. *"Hábeas Data. La Protección jurídica de los datos personales".* Alverone Ediciones, Córdova, Argentina, 1996. P. 63

deben estar a su disposición para que sea él quien decida si los cede o en qué condiciones lo hace.[36]

Dentro del derecho español, el artículo 6º de la *LOPD*, sostiene:

"Artículo 6. Consentimiento del afectado.

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado"

De las características que conforman el consentimiento en la normatividad referida, la doctrina científica en el derecho comparado señala que debe ser: a) *libre,* (que se haya obtenido sin la intervención de vicio alguno del consentimiento en los términos regulados por la leyes, es decir, que no esté viciado); b) *específico,* (debe ser referido a una determinada operación de tratamiento y para una finalidad determinada, explícita y legítima del responsable del tratamiento); c) *informado,* (el titular conoce con anterioridad al tratamiento de sus datos la existencia del mismo y las finalidades para las que se produce); d) *inequívoco,* (no se puede deducir el consentimiento de los meros actos realizados por el afectado –el llamado

[36] Corte Suprema de Justicia de la Nación, *"Hábeas Data"*, Revista de Derecho Procesal, No. 5, Sección Jurisprudencia Temática, Argentina, agosto-septiembre de 1999, P. 348.

consentimiento presunto-, sino que es preciso que exista expresamente una acción u omisión que implique la existencia del consentimiento).[37]

En cuanto a la forma en la que se puede otorgar el consentimiento, con carácter general cabe distinguir entre consentimiento expreso y tácito, en cualquiera de ambos casos, la cuestión se centra en la prueba de la obtención del consentimiento. Es decir, tanto en el consentimiento tácito como el expreso, hay que implementar procedimientos estandarizados de recogida de dicho consentimiento para que luego se pueda probar la obtención el mismo. Dicha prueba recae en quien solicita el consentimiento para el tratamiento de datos de carácter personal, es decir, el responsable del fichero. Por tanto, deberá hacerse uso de vías que permitan acreditar que se solicitó del interesado una manifestación en contra para oponerse al tratamiento de sus datos, de manera que su omisión pueda ser entendida como consentimiento al mismo, dando un plazo prudencial para que el interesado pueda conocer que su omisión implica su aceptación.

En materia de protección de datos personales no existe otra forma de consentimiento que el modo expreso y por escrito, u otro medio que se le equipare en cuanto a la prueba del acto de acuerdo a las circunstancias, es decir, a lo particular del soporte bajo el cual se recolectan los datos, situaciones que se ven corroboradas en la jurisprudencia de mérito.

En el derecho mexicano, la Ley Federal de Transparencia y Acceso a la Información Pública, sostiene que se requiere el consentimiento expreso, por escrito o por un medio de autentificación similar, de los individuos a que haga referencia la información para poder difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información, estableciendo excepciones por razones de estadística, científicas, interés general o mandamiento judicial.

[37] Castán Tobeñas, Alonso, Alonso Martínez, C. "Protección de Datos de carácter personal. El consentimiento en entidades financieras". Madrid, ASNEF, 2002. p. 56

El consentimiento, también fue recogido por la LFPDP como principio reconocido por el artículo 6º, y regulado mediante disposición del artículo 8 y 9 (tratándose de datos sensibles) que versan:

> Artículo 8.- Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley.
>
> El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología o por signos inequívocos.
>
> Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.
>
> Los datos financieros o patrimoniales requerirán el consentimiento expreso de su titular, salvo las excepciones a que se refieren los artículos 10 y 37 de la presente Ley.
>
> El consentimiento podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos. Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.
>
> Artículo 9.- Tratándose de datos personales sensibles el responsable deberá obtener consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.
>
> ...

El artículo 10 de la Ley, menciona los casos de excepción al principio de consentimiento para el tratamiento de datos personales.

> Artículo 10.- No será necesario el consentimiento para el tratamiento de los datos personales cuando:
>
> I. Esté previsto en una Ley;
> II. Los datos figuren en fuentes de acceso público;
> III. Los datos personales se sometan a un procedimiento previo de disociación;
> IV. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;
> V. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
> VI. Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o
> VII. Se dicte resolución de autoridad competente.

El consentimiento del titular debe existir para que sea válido el acto que se vaya a realizar en la recogida y tratamiento de sus datos personales. Las legislaciones a estudio establecen una serie de limitaciones al tratamiento de los datos, mismas que son fijadas para garantizar el uso adecuado, lícito, no excesivo y con las debidas medidas de seguridad que impidan la alteración, pérdida o tratamiento no autorizado de los datos, por lo cual, la Ley entiende la necesidad manifiesta del consentimiento, con las excepciones que la propia norma fija y no sea necesario el consentimiento del titular.

1.2.4. Deber de confidencialidad

Por otro lado, como un principio de carácter general, si bien específico en relación con la normativa, el principio de confidencialidad o deber de secreto, se destaca como un deber que debe observarse por toda persona que tenga acceso a los datos, durante todo el tiempo que dure el tratamiento y aun después de que finalice el mismo, que busca garantizar que quienes traten datos de carácter personal en el desarrollo de sus funciones, los guarden y garanticen el secreto sobre los mismos.

La *Ley Orgánica de Protección de Datos Personales española 15/1999*, trata de forma individualizada este deber, en el sentido de que aquéllos que tratan de forma directa o indirecta, datos de carácter personal estén obligados a hacerlo, respetando siempre en todo momento su confidencialidad, impidiendo el acceso a dichos datos por parte de terceros, y desde luego no transmitirlos o hacerlos públicos, así lo disponen los artículos 9 y 10 de la citada ley.

Asimismo, el artículo 10 de la *Ley 25.326 Argentina*, prevé lo relativo al deber de confidencialidad, sosteniéndolo como un deber de secreto, empero, como hemos acotado en repetidas ocasiones, dicha ley, está basada en la Ley Española en materia de protección de datos, por lo que la misma guarda principios similares en esta materia, de tal suerte que tal artículo menciona:

"ARTICULO 10. —

1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.

2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública."

En dicho precepto, se señala "y las personas que intervengan en cualquier fase del tratamiento de datos personales", por lo que el legislador al hacer énfasis en dicho artículo, extendió la obligación de guardar el secreto profesional, de tal forma que ésta no afecta únicamente al responsable del fichero, sino que se extiende a todas aquellas personas que participen en el tratamiento durante el periodo en el que dichos datos se encuentren almacenados en los ficheros organizados y estructurados bajo su control. [38]

De igual manera, el Derecho positivo argentino, ha sostenido en su jurisprudencia los siguientes criterios:

"El Derecho que otorga la Carta Magna para exigir la confidencialidad de los datos no puede extenderse a todo tipo de información. El mencionado remedio constitucional sólo puede alcanzar a la llamada información sensible, esto es a aquellos datos que hagan referencia a la vida íntima de las personas, a sus ideas políticas, religiosas o gremiales". [39]

"El derecho de exigir la confidencialidad de datos no se extiende a aquella información de alcance comercial o financiero. Ello es así pues tal información (cierre de una cuenta corriente por haber producido el tercer rechazo de cheques

[38] Almuzara Almaida, Cristina. *Op. Cit*.. P. 515
[39] Corte Federal Argentina. Sentencia de la Sala IV, en autos "Farrel Desmond, Agustín c/BCRA y otros, s/amparo", 5 de septiembre de 1995, Jurisprudencia, 1995-IV-350. (ví: 20 de mayo de 2008) http://www.en.us.ar/php?option=com_conterd/12_1.htm

sin provisiones de fondos), por su carácter está destinada a divulgarse entre todas las entidades financieras, tal como lo prevé la circular OPASI 2 del BCRA". [40]

Por tanto, esta obligación afecta tanto a personas que trabajan para el responsable del fichero como a aquellas que trabajan para terceros que acceden a los datos como consecuencia de un servicio prestado al responsable.

En México, tal principio se encuentra regulado expresamente a nivel federal en la *Ley Federal de Protección de Datos Personales en Posesión de Particulares*, en el artículo 21, al señalar en similares términos lo que prevé la ley Española 15/99 y Argentina 25.326 que: *"El responsable o terceros que intervengan en cualquier fase del tratamiento de datos personales deberán guardar confidencialidad respecto de éstos, obligación que subsistirá aun después de finalizar sus relaciones con el titular o, en su caso, con el responsable";* y la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental*, lo establece en sus artículos 20, fracción VI, en relación con el 18 y 21 del propio ordenamiento[41].

Sin embargo, dentro de *los Lineamientos de Protección de Datos Personales* publicados por el IFAI en el Diario Oficial de la Federación en 30 de septiembre de 2005, se establece en las Disposiciones Generales, punto Décimo, que se deberán adoptar las medidas necesarias para garantizar... confiabilidad, confidencialidad... de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado, ello con el fin de dar reconocimiento al derecho a la vida privada, y tomando en cuenta el objetivo de la Ley de

---

[40] *Idem.*

[41] "Artículo 18. Como información confidencial se considerará: I. La entregada con tal carácter por los particulares a los sujetos obligados, de conformidad con 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...

Artículo 20. Los sujetos obligados serán responsables de los datos personales y, en relación con éstos deberán: ... VI. Adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

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 medio de autenticación similar, de los individuos a que haga referencia la información.

Transparencia y Acceso a la Información, que es el de garantizar la protección de datos personales en posesión de los sujetos obligados.

1.2.5. Transferencia internacional

La informática y la telemática han desplazado el interés desde la creación de informaciones a su transmisión. De ahí que si en cualquier época histórica se dio un intercambio de datos entre los diferentes países, en la nuestra su volumen y su importancia han adquirido, gracias a las modernas tecnologías de la información y la comunicación, dimensiones de un crecimiento tan rápido y progresivo que ha situado su reglamentación en el nudo de problemas apremiantes del Derecho internacional de nuestros días.

El problema de flujo trasnacional o internacional de datos ha suscitado un abierto conflicto de intereses entre los países productores y los países consumidores de datos informáticos. Los países tecnológicamente avanzados se hallan en condiciones de recoger informaciones, almacenarlas y distribuirlas con la utilización de la informática. Por el contrario, los países subdesarrollados sólo pueden recibir y consumir informaciones, es más, en determinados casos ni tan siquiera pueden servirse de ellas por carecer de los medios electrónicos necesarios para aprovecharlas. Esta circunstancia ha determinado que los países desarrollados mantengan una posición decidida a favor de una libertad ilimitada de intercambio de informaciones entre todos los países; mientras que los países subdesarrollados, que carecen de una tecnología informática propia, exigen que se reconozca la facultad de ejercer un control sobre los datos que puedan recogerse en su territorio.

El *Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal,* señaló con respecto a los instrumentos incorporados para el logro de sus fines que debe destacarse lo siguiente: de un lado, el reconocimiento del derecho al acceso por parte de los interesados a las informaciones que le conciernen, con la posibilidad de cancelarlas o corregirlas cuando se haya procesado indebidamente, así como de la facultad de

recurrir ante cualquier transgresión de los derechos anteriores; y, de otro, la consagración jurídica del principio de la libre circulación de datos entre los Estados miembros. Con respecto al reconocimiento del principio *free flow* debe advertirse sin embargo, que el Convenio faculta a los países signatarios para establecer excepciones a su aplicación: en relación con datos especialmente sensibles y cuando se trate de transmitir datos que, por mediación de un Estado que sea parte del Convenio, puedan tener como destino último el territorio de un Estado que no lo sea.

Se ha objetado al Convenio, precisamente, el adolecer de una cierta ambigüedad en su reglamentación del flujo transfronterizo de datos, así como el no haber establecido la correspondiente distinción en la disciplina jurídica del tratamiento de datos personales, en los sectores público y privado, y el haber omitido una específica tutela jurídica del software. Sin embargo, este texto abre una brecha importante con relación a la cooperativa internacional de flujo de datos en el acuciante sector del derecho informático referente a la protección de datos personales.

Entremos pues, a la *Ley 15/1999 española*, toda vez que la misma ha constituido base para el estudio de los principios en comento y que han sido adoptados por otros países de América, como el caso de Argentina, dicha ley, dispone en sus artículos 33 y 34, reglas que rigen las transferencias internacionales de datos, sin embargo, las mismas no pueden ser analizadas sin la *Directiva 95/46/CE* relativa a la Protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de ellos, para la Transferencia Internacional.

Entendemos por transferencia internacional de datos, toda transmisión de datos de carácter personal, independientemente de cual sea el medio y/o soporte mediante el cual se envían los datos o la forma del tratamiento, fuera del territorio español.

En los ficheros de titularidad privada, los dos casos habituales en los que se producen Transferencias Internacionales de Datos son:

a) Supuestos de Transferencia Internacional de Datos en el acceso a datos por cuenta de terceros; por ejemplo, en el caso de una página web que recoge datos de carácter personal y los almacena, con la finalidad de proporcionar a los usuarios registrados acceso a funcionalidades específicas, contenidos, áreas de descarga, etc., y que se encuentra alojadas en un Servidor/Hosting con ubicación física de la máquina fuera del territorio Español.

b) Supuestos de Transferencia Internacional de Datos por cesión o comunicación de datos; por ejemplo, el caso de una empresa que transfiere los datos de carácter personal de sus ficheros de clientes, proveedores, trabajadores, etc. a su empresa matriz con domicilio fuera de España, por motivos de centralización de información, gestión de recursos, procesos de reorganización, etc.

Y dentro de estos supuestos, además, debemos tener en cuenta para poder delimitar las obligaciones que se imponen por la ley, el país de destino de la Transferencia Internacional de Datos, a efectos de recabar o no la autorización previa del Director de la Agencia Española de Protección de Datos, a saber:

- Estados Miembros de la Unión Europea,

- Estados no comunitarios que ofrecen un nivel de protección y regulación legal similar al establecido por la *LOPD* y *la Directiva*., o

- Estados no comunitarios que no ofrecen nivel de protección y regulación legal al establecido por la *LOPD* y *la Directiva*.

Asimismo, dentro de los requisitos generales para la Transferencia Internacional de Datos tenemos los que se establecen en el artículo 33 *LOPD* y en la Instrucción 1/2000, de 1 de diciembre, que señalan:

Artículo 33. Establece que no se podrán realizar Transferencias Internacionales de Datos con destino a países que no proporcionen un nivel de protección equiparable al establecido en la *LOPD*, sin la previa autorización del Director de la Agencia de Protección de Datos.

En principio, los requisitos generales necesarios para poder realizar la Transferencia Internacional de Datos son los siguientes:

1. Cumplimiento del deber de información y de las obligaciones establecidas por la ley para la cesión de datos (previo consentimiento informado de la cesión, informar a los sujetos sobre la transferencia internacional de datos, tipología de los datos cedidos, finalidad del fichero y la identidad del destinatario) o para el acceso a datos por cuenta de terceros (contrato de acceso a datos).

2. Notificación de la Transferencia Internacional de Datos a la Agencia Española de Protección de Datos, indicando el país de destino y, en su caso, el supuesto al que se acoge de las excepciones establecidas en el artículo 34 de la LOPD para que no sea necesaria la autorización previa del Director de la Agencia Española de Protección de Datos.

Una vez notificada la Transferencia Internacional, la Agencia Española de Protección de Datos, podrá solicitar al Responsable del Fichero que aporte documentación complementaria para autorizar dicha Transferencia; principalmente, en relación con el cumplimiento del deber de información, consentimiento de los interesados, existencia de cláusulas contractuales tipo para la cesión y/o acceso por cuenta de terceros, finalidades de la transferencia, etc.

El artículo 34 establece las excepciones a los supuestos en los que no será necesaria la previa autorización del Director de la Agencia para la Transferencia Internacional de Datos, y los supuestos más habituales: consentimiento inequívoco del afectado, contratos y precontratos entre el afectado y el responsable del fichero

y transferencia con destino a Estados miembros de la UE y Estados no comunitarios que tengan nivel de protección equivalente.

Las excepciones son las siguientes:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de los tratados o convenios en los que sea parte España.

b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.

c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médico, la prestación de asistencia o tratamientos médicos o la gestión de servicios sanitarios.

d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista. Este consentimiento debe ser previo, inequívoco e informado.

f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.

g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.

h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.

i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro Público y aquella sea acorde con la finalidad del mismo.

k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

Por otro lado, tenemos los requisitos para la Transferencia Internacional de Datos con destino a Estados no comunitarios sin nivel de protección de los datos equivalente al establecido en la *LOPD* y que no se puedan acoger a las excepciones previstas en el artículo 34, las cuales son:

1. Será preceptiva la Autorización del Director de la Agencia antes de proceder a la realización de la Transferencia. Esta autorización tiene por finalidad determinar si se prestan garantías adecuadas para el tratamiento de los datos, tomando en consideración para otorgarla o denegarla los siguientes criterios:

•Naturaleza de los datos.

•Finalidad y duración del tratamiento previsto.

•Estado de origen y destino de la transferencia.

•Normas legales vigentes en el Estado destino.

•Informes de la Comisión Europea,

•Normas profesionales y medidas de seguridad en vigor en el Estado de destino.

2. Cumplimiento de la LOPD por parte del Responsable del Fichero que quiere realizar la transferencia. Esto supone:

a) Para los supuestos de cesión de datos:

•Cumplimiento del deber de información (informar a los afectados sobre la identidad del destinatario de los datos, finalidad del tratamiento que justifica la transferencia y tipología de datos cedidos).

•Aportar contrato escrito, celebrado entre transmitente y destinatario en el que consten los siguientes extremos:

-Que el transmitente ha cumplido con las normas establecidas en la *LOPD* en cuanto a la recogida, tratamiento e inscripción del fichero.

-Que el destinatario utilizará los datos exclusivamente para la finalidad que motiva la transferencia y el tratamiento de los mismos se realizará de conformidad con lo dispuesto en la *LOPD*, comprometiéndose además a no ceder los datos a terceros.

-Que el destinatario se compromete a la adopción de las medidas de seguridad establecidas en la legislación española.

-Se establecerá la responsabilidad solidaria de transmitente y destinatario frente a los afectados, AEPD y órganos jurisdiccionales cuando el incumplimiento del contrato por el destinatario suponga una infracción establecida en la *LOPD*.

-Se garantizará el ejercicio de los derechos de acceso, rectificación, cancelación y oposición por parte del afectado, quien podrá solicitar la tutela de la AEPD.

-Compromiso del destinatario de autorizar el acceso a las instalaciones donde se realice el tratamiento de los datos a la Agencia Española de Protección de Datos.

-El destinatario se obligará a que, una vez cumplida la finalidad del tratamiento, se procederá a la destrucción de los datos o, en su caso, a la devolución de los mismos al transmitente.

-Por último, se dispondrá que los afectados podrán solicitar el cumplimiento de lo dispuesto en el contrato que les sea favorable.

Por su parte, la Comisión Europea estableció, a través de la Decisión 2001/497/CE, de 15 de junio de 2001, un modelo de cláusulas contractuales tipo para este tipo de supuestos.

b) Para los supuestos de acceso a datos por cuenta de terceros:

•Aportar el contrato escrito que regula la realización del tratamiento con el contenido establecido por el art.12 *LOPD* recogiendo, además, los siguientes extremos:

-Se establecerá la responsabilidad solidaria del Responsable del Fichero y del Encargado de Tratamiento frente a los afectados, la AEPD y los órganos jurisdiccionales, cuando el incumplimiento del contrato por el Encargado del Tratamiento suponga una infracción establecida en la *LOPD*.

-Se garantizará el ejercicio de los derechos de acceso, rectificación, cancelación y oposición por parte del afectado, quien podrá solicitar la tutela de la AEPD.

-Compromiso del Encargado del Tratamiento de autorizar el acceso a las instalaciones donde se realice el tratamiento de los datos a la AEPD.

-Por último, se dispondrá que los afectados podrán solicitar el cumplimiento de lo dispuesto en el contrato que les sea favorable.

La República Argentina, comparte los criterios adoptados por la *LOPD* española, mismos que sostiene en su artículo 12, de la *Ley 25.326*, en materia de Protección de Datos Personales en los términos que se precisan:

"ARTICULO 12.- (Transferencia internacional).

1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.

2. La prohibición no regirá en los siguientes supuestos:

a) Colaboración judicial internacional;

b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inciso e) del artículo anterior;

c) Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;

d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;

e) Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

México, se encontraba limitado respecto de este principio debido a la falta de regulación sobre el particular. Actualmente con la nueva disposición de LFPDP, nuestro país cuenta con una regulación en la materia.

Así, lo prevén los artículos 36 y 37 de la citada Ley:

Artículo 36. (Obligaciones). Cuando el responsable pretenda transferir los datos personales a terceros nacionales o extranjeros distintos del encargado, deberá comunicar a éstos el aviso de privacidad y las finalidades a las que el titular sujetó su tratamiento.

El tratamiento de los datos se hará conforme a lo convenido en el aviso de privacidad, el cual contendrá una cláusula en la que se indique si el titular acepta o no la transferencia de sus datos, de igual manera, el tercero receptor, asumirá las mismas obligaciones que correspondan al responsable que transfirió los datos.

Artículo 37.- (Excepciones). Las Transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento del titular cuando se dé alguno de los siguientes supuestos:

I. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte
II. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
III. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
IV. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
V. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;
VI. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y
VII. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

El gran reto de la sociedad mexicana, reside en hacer compatible el flujo internacional de datos, que es condición necesaria para el progreso y el desarrollo económico de la sociedad civil, así como para garantizar la eficacia de los poderes públicos, con el respeto a las libertades. En las sociedades interconectadas de nuestro tiempo el flujo internacional de datos resulta, por tanto, imprescindible para asegurar el desarrollo económico del sector privado, la comercialización con otros países principalmente con la Unión Europea y colocar a México en un nivel adecuado de Protección de Datos Personales, asegurando su inclusión al mercado

internacional además, de posibilitar que los poderes públicos alcancen sus metas y cumplan sus obligaciones con eficacia.

Hasta aquí hemos visto los principios sobre los cuales descansa la Protección de Datos Personales en los países a estudio, México, España y Argentina y como se encuentra regulado en sus distintas legislaciones. A continuación, expondremos aquellos datos considerados como sensibles y que también engloban los principios que han quedado asentados.

1.3. Datos Especialmente protegidos

Dentro de este tópico, la *LOPD*, en sus artículos 7 y 8, ha previsto disposiciones destinadas al reforzamiento de las garantías de protección para determinado tipo de datos de carácter personal, mismo a los que se les ha conocido con el nombre de datos especialmente protegidos o sensibles.

Así, las categorías de datos que gozan de una protección especial son enumerados en el artículo 7 en comento, y en donde se manifiestan tres niveles de protección reforzada, a saber son los siguientes:

a. Los Datos de carácter personal relativos a la ideología, religión, creencias y afiliación sindical, para cuyo tratamiento se exige el consentimiento expreso y por escrito.
b. Los datos de carácter personal relativos al origen racial o étnico, salud y vida sexual, para cuyo tratamiento se limitan los fines y las personas habilitadas para realizarlo, además de reforzar las garantías que aguardan la prestación del consentimiento.
c. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas que únicamente pueden ser tratados por las Administraciones Públicas.

Asimismo, el Estado Argentino se ha mantenido mediante jurisprudencia, con relación a los datos especialmente protegidos de la siguiente manera: "El Hábeas Data sólo puede alcanzar a la información sensible, esto es, a aquellos datos que hagan referencia, entre otras, a la vida íntima de las personas, a sus ideales políticos, religiosos y gremiales".

Los principios rectores de la protección de datos personales, han sido recogidos en distintas legislaciones. España es referente para la adopción de estos en las legislaciones de Argentina y en México en las diversas leyes que se han suscrito, a saber: en la *Ley 25.326 de Hábeas Data* en sus artículos 2.2., 7 y 8 se estableció lo que debe entenderse por datos sensibles y la categoría de aquéllos; y en México en la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental* en su capítulo de información reservada y confidencial, artículos 13.4, 14 y 15*;* y recientemente en la *Ley Federal de Protección de Datos Personales en Posesión de Particulares*.

La LFPDP, establece en su artículo 3º. lo que debe entenderse por datos personales sensibles: "*Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual".*

Cada una de las leyes anteriores, expone los principios que deben contener las garantías mínimas en la protección y tratamiento de datos personales, mismos que quedaron expuestos anteriormente. A manera de sumario, podemos clasificarlas de la siguiente manera:

Ley Orgánica Española 15/99 de Protección de Datos Personales:

a) Calidad
b) Información
c) Consentimiento
d) Datos especialmente protegidos
e) Relativos a la salud
f) Seguridad
g) Deber de secreto
h) Comunicación de datos
i) Acceso a los datos por cuenta de terceros

Por su parte la *Ley Argentina 25. 326 de Hábeas Data*, los recoge así:

a) Licitud de Datos
b) Calidad de los datos
c) Consentimiento
d) Información
e) Categoría de los datos
f) Seguridad
g) Confidencialidad
h) Cesión y Transferencia internacional

En México, la *Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental* hace mención a los principios de manera diferente a las leyes comparadas, sin embargo, los *Lineamiento de Protección de Datos Personales*, expedidos por el IFAI, son claros al establecer los principios, clasificándolos como sigue:

a) Licitud
b) Calidad
c) Acceso y corrección
d) Información
e) Seguridad
f) Custodia y cuidado de la información
g) Consentimiento

La *Ley Federal de Protección de Datos Personales en Posesión de Particulares,* sostiene los principios en su artículo 6 y los desarrolla en los siguientes 15, clasificándolos de la siguiente manera:

a) Licitud
b) Consentimiento
c) Información
d) Calidad
e) Finalidad
f) Lealtad
g) Proporcionalidad y
h) Responsabilidad

Las anteriores clasificaciones, responden a las exigencias de los principios a nivel internacional, es decir, en una u otra medida se sustenta un ámbito de protección de la información que es recogida en las legislaciones tratadas en este capítulo, mismas que podemos resumir en los siguientes puntos:

1. La relativa a la licitud de los datos, es decir, a la erradicación de procedimientos desleales o ilícitos, ni utilizarse con fines contrarios a los propósitos para los que fueron recogidos.
2. La calidad, es decir, la obligación de verificar la exactitud y pertinencia de los datos registrados y cerciorarse de que siguen siendo lo más completos posibles a fin de evitar los errores por omisión y de que se actualicen, periódicamente o cuando se utilicen las informaciones contenidas en un expediente, mientras se estén procesando.
3. En el momento de su creación, ponerse en conocimiento de la persona interesada.
4. El derecho que tiene toda persona a saber si se está tratando información suya y a obtener las rectificaciones o supresiones adecuadas cuando los registros sean ilícitos, injustificados o inexactos.
5. No registrar datos que puedan originar una discriminación ilícita o arbitraria, en particular información sobre el origen racial o étnico, color, vida sexual, opiniones políticas, convicciones religiosas, filosóficas o de otro tipo, o sobre la participación en una asociación o la afiliación a un sindicato.
6. A establecerse excepciones cuando son necesarias para proteger la seguridad nacional o el orden público,
7. Se adoptan medidas apropiadas para proteger los registros como el acceso sin autorización.
8. Ofrecimiento de garantías en las legislaciones de los países sobre el flujo de datos a través de sus fronteras.

A manera de conclusión, podemos afirmar que la protección de datos personales tiende a garantizar el equilibrio de poderes y situaciones que es condición indispensable para el correcto funcionamiento de una comunidad democrática de ciudadanos libres e iguales.

Para su logro se precisa un adecuado ordenamiento jurídico en la materia, capaz de armonizar las exigencias de información propias del Estado y de los particulares con las garantías de los ciudadanos.

Para garantizar la protección de los datos personales, es conveniente concebirlo como un derecho fundamental autónomo, dotado de medios específicos de tutela, que consagren un derecho a la autodeterminación en el marco de los derechos de la tercera generación, puesto que en las legislaciones actuales se ha determinado el status de habeas data, concretado en las garantías de acceso y control a las informaciones procesadas en bancos de datos por parte de los titulares de ellos.

La importancia que revisten las normas de procedimiento, y entre ellas el habeas data, se halla corroborada por la difusión creciente de instituciones de protección que tienden a completar la función de garantía de los tribunales. En este sentido, debe hacerse notar el protagonismo adquirido por un Órgano de control en la defensa actual de los derechos y libertades fundamentales en la protección de datos personales, específicamente dirigidos a la protección de los ciudadanos respecto al tratamiento de datos; es decir a hacer efectivo el habeas data, sobre todo en aquellos países que apenas comienzan a ser participes en la consagración de este modelo de protección, como el caso de México.

Verificado el marco conceptual y los principios del derecho fundamental de la protección de datos personales veamos como las tecnologías de la información han impactado en el tratamiento de datos personales, sobre todo en el uso de internet.

CAPÍTULO II

TRANSMISIÓN DE DATOS PERSONALES MEDIANTE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES

2.1. Los Medios de Comunicación y su relación con las Tecnologías de Información

2.2. Desarrollo Tecnológico e Información

2.2.1. Ventajas y daños de la tecnología
2.2.2. Impacto de las nuevas tecnologías de la información

2.3. La Revolución de Internet y su Impacto en los Medios de Comunicación

2.3.1. El flujo de datos personales en Internet

2.4. La tecnología y la Protección de Datos Personales

2.5. Margen de Protección de Datos Personales y Seguridad en los sitios web

2.6. Archivos de datos personales

CAPÍTULO II

TRANSMISIÓN DE DATOS PERSONALES MEDIANTE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES

2.1. Los Medios de Comunicación y su relación con las Tecnologías de Información

La búsqueda del hombre por satisfacer cada vez mejor la necesidad de comunicación, ha impulsado la instauración en el mundo de instrumentos cada día más poderosos y veloces en el proceso comunicativo. El desarrollo de estos instrumentos han sido ciertamente un avance en las formas de comunicación del hombre y prácticamente posibles gracias a la tecnología, que a su vez constituye un instrumento cuya evolución ha determinado el avance de la humanidad, decía Fayt, "La comunicación es una dimensión raigal de la vida humana. La necesidad de los demás, como consecuencia de la propia insuficiencia, hace imperativa la alteralidad, la que sólo es posible mediante la comunicación interpersonal y social."[42]

Continuando con el autor mencionado, sostiene que la información es un sector de la comunicación social, al mencionar que la "comunicación" significa dar forma y su concepto se limitaría a la creación del mensaje. Equivaldría a la faz estática del proceso informativo. En un sentido más amplio, información sería equivalente a una comunicación con un fin predeterminado.

En este primer apartado se intentará definir la relación entre los medios de comunicación y las tecnologías de la información, para examinar posteriormente la manera en que se estructura Internet, y el flujo de datos que sobre la red de redes circula (la forma en que son recopilados, tratados y transferidos los datos personales mediante esta tecnología de la información y comunicación) y cuyos

[42] S. FAYT, Carlos. *La Omnipresencia de la Prensa. Su juicio de Realidad en la jurisprudencia Argentina y Norteamericana.* La Ley, Argentina, 1994. Pág. 25

conceptos se dan dentro de las innovaciones propias de la revolución tecnológica de estos últimos años.

Se considera como *medio de comunicación*, todo instrumento o medio que permita y facilite la comunicación entre los seres humanos.[43]

El Diccionario de la Real Academia Española, define al medio de comunicación como "*Órgano destinado a la información pública"*[44]*,* por lo que podemos decir que tradicionalmente, los medios de comunicación se refieren a la radio, la televisión, la prensa y el cine, y se consideran instrumentos para impulsar o modificar la cultura y la educación. Sin embargo, el avance de la técnica moderna ha permitido que los medios de comunicación evolucionen, se perfeccione y se multipliquen: el fax, la computadora y el internet.

Por su parte, las T*ecnologías de la información y la comunicación* (en adelante TIC) son un conjunto de servicios, redes, software y dispositivos que tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno, y que se integran a un sistema de información interconectado y complementario.

Las TIC se conciben como el universo de dos conjuntos, representados por las tradicionales *Tecnologías de la Comunicación* (TC) -constituidas principalmente por la radio, la televisión y la telefonía convencional- y por las *Tecnologías de la información* (TI) caracterizadas por la digitalización de las tecnologías de registros de contenidos (informática, de las comunicaciones, telemática[45] y de las interfaces[46])".

---

[43]Vi en http://www.scribd.com/doc/305468/Definiciones-de-Medios-de-Comunicacion-Social-MCS. en 5 de marzo de 2009.

[44] Diccionario de la Real Academia de la lengua Española. 22ª edición, 2001.

[45] Área de conocimiento que forma parte de la informática, y que engloba a todos los tratamientos que se realicen sobre la información de manera automática y la comunicación es un intercambio de información.

[46] Metafóricamente se entiende la Interfaz como una conversación entre el usuario y la tarjeta madre (o entre el usuario y el diseñador de la misma). En sentido amplio, puede definirse interfaz como el conjunto de comandos y/o métodos que permiten la intercomunicación del programa con

En todo caso, lo que encontramos es que las tecnologías modernizan el proceso, pero mantienen el producto. Éste es el gran principio de las nuevas tecnologías, entender que sólo son piezas para aligerar un procedimiento, para obtener el mismo resultado con mayores facilidades, tal vez con menor esfuerzo humano. El término "Tecnología" por sí mismo es genérico, responde a todo tipo de actividad, es un vocablo que adquiere sentido real cuando se acompaña de un término complementario que se refiera con precisión, a la actividad a la cual se aplica el conocimiento científico. En este caso, la tecnología que se aplica para facilitar y mejorar el proceso de información y comunicación humana es entonces la que se conoce como Tecnología de Información y Comunicación (TIC).

No obstante, la rapidez y constancia de los cambios en el mundo de hoy, es lo que da forma a la definición de Tecnologías de Información, porque es bien cierto que el término, aunque puede ser aplicable a otros modos remotos de comunicación, es prácticamente moderno y es reconocido a partir de la revolución que se observa en el mundo actual, caracterizada por la informática, la computación y el Internet. Es decir, de Tecnologías de Información y Comunicación se habla a partir del instante en que la sociedad mundial comenzó a experimentar cada vez más rápidos y continuos procesos de cambio; cambios sustentados en un constante progreso científico-tecnológico.

En tal sentido, Canga Larequi[47], define la tecnología de información y comunicación como un estudio sistematizado del conjunto de procedimientos que están al servicio de la información y la comunicación.

Bajo esta perspectiva, la concepción moderna de las tecnologías de información y comunicación comprende entonces aplicaciones, sistemas, herramientas, técnicas y metodologías asociadas a la digitalización de señales analógicas, sonidos, texto e imágenes, manejables en tiempo real. Se relaciona con

---

cualquier otro programa o entre partes del propio programa o elemento interno o externo.

[47] CANGA LAREQUI, Jesús. *La Prensa y las Nuevas Tecnologías. Manual de la Redacción Electrónica*. Ediciones Deusto S.A. Madrid, España. 1988.

equipos de computación, software, telecomunicaciones, redes y bases de datos. Las Tecnologías de Información y Comunicación se refieren a todos los instrumentos, procesos y soportes que están destinados a optimizar la comunicación humana.

2.2. Desarrollo Tecnológico e Información

El desarrollo de las comunicaciones es un producto de la Revolución tecnológica, y con ello el advenimiento de la era digital, en el que el valor más importante es la información, que afecta a los modos y hábitos de vida de los seres humanos.

Los avances tecnológicos, la potencialidad de almacenamiento y el uso de la información alcanzado en la actualidad, han hecho aporte para que la información no quede estancada sólo en el ordenador o en un disco compacto, sino que puede viajar a través del ciberespacio[48] para ser alcanzada por todo aquel que tenga acceso a un ordenador. Pierini, Lorences y Tornabene, sostienen que gracias al avance tecnológico en el desarrollo de las comunicaciones, se ha producido una verdadera globalización de la información, ya que muy poco de lo que se encuentra almacenado puede quedar oculto. Por lo tanto, el efecto es devastador: la información no sólo puede ser acumulada y rescatada por quien la acumuló, sino que puede viajar y llegar prácticamente al mundo entero y casi instantáneamente [49] (aquí radica la gravidez del flujo de datos por Internet).

En la feria realizada en 1993 en el predio de Frankfurt, Alemania –cuenta Fayt-,[50] hizo sensación el libro electrónico que sustituye el papel por la pantalla de la computadora y que contiene, en un disco compacto, la información de los textos e imágenes para su uso en la computadora personal. El "electronic book", es

[48] El ciberespacio o ciberinfinito es una realidad virtual que se encuentra dentro de los ordenadores y redes del mundo. El Diccionario de la Real Academia Española, lo define como "Ámbito artificial creado por medios informáticos".
[49] PIERINI, et.al. *Hábeas Data. Derecho a la Intimidad.* Editorial Universidad, Argentina, 2002. Pág. 118
[50] S. FAYT, Carlos. *La Omnipresencia de la Prensa. Su juicio de Realidad en la jurisprudencia Argentina y Norteamericana. Ob. Cit.* Pág. 32

producido en más de 2825 compañías, con títulos que abarcan cantidad de información de interés general, ocio, recreación, artes, ciencias sociales, ciencias naturales, etc., es cuestión de tiempo su incorporación al mercado mundial.[51]

También comenta –el mismo autor-, existen dos experiencias en el mundo sobre la aparición del diario electrónico. En Adepa, de mayo de 1994, No. 127, se informa que "José Claudio Escribano, que visitó Estados Unidos y Canadá, luego de asistir a la reunión Hemisférica de libertad de prensa en México, y a la Asamblea de la SIP en Guatemala, echó algo de luz sobre esta temática a partir de la experiencia vivida durante su visita efectuada a distintas empresas periodísticas de aquellos países", según Escribano, existen dos casos notorios en el Hemisferio Norte, son las de los Diarios: San José Mercury News de California, Estados Unidos; y London Free Press de Toronto, Canadá.

El primero de ellos estableció una empresa llamada Mercury Center que tiene el objetivo de proyectar el Diario electrónico a la casa o familia de lectores, ante el interés de éstos de seguir la evolución de una información en el transcurso del día. Dicha empresa ofrece un servicio de información adicional que transmite vía telefónica a una PC establecida en el hogar u oficina, y cuyo costo es de 4.95 dls. las 5 horas de lectura. A través de un ícono clave que se publica al final de cada noticia en la edición matutina del Diario, el lector puede acceder luego con su PC a una ampliación o actualización de dicha información y hasta consultar el archivo diario. Puede también crear un pizarrón virtual para dejar mensajes a los editores o redactores.

En cuanto al caso de London Free Press, dijo –el autor-, que esta experiencia es aún más insólita: se trata de un replanteo total de la empresa periodística en la que no hay redacciones, ni secciones ni reporteros. Existe un editor-coordinador general, que depende directamente del director de la empresa, y que opera a modo

[51] Revista alemana Deutschland, No. 19 10/93. Ed. Societäs Verlang y la Oficina de Prensa e Información del Gobierno Federal, Boon. Pág 43, *Idem*.

de empresa comprando noticias a otras compañías, de acuerdo al interés y calidad de las mismas.

La informática, los medios electrónicos y las telecomunicaciones se perfeccionan merced a los avances de la electrónica y la digitalización que proporciona tratamiento numérico a los datos que transportan las redes, a los que algunos autores han denominado "autopistas de la comunicación". Las nuevas tecnologías de la información se vislumbran a un futuro cotidiano en la vida social, integrándose al ejercicio en todas las actividades, que incluso practican en lugares propios, reservados o privados. Las nuevas tecnologías de la información se proponen invadir el domicilio, convirtiéndolo en una especie de terminal global de información y comunicación.

En él se podrán consumir a través de terminales, programas que contienen toda clase de informaciones generales o especializadas, de todo tipo, espectáculos, servicios bancarios, datos científicos, todo tipo de productos corrientes, es decir, nuestra vida cotidiana estaría signada por la omnipresencia cada vez mayor de la técnica en nuestra casa, decía Fayt,[52] nuestra privacidad estará colonizada por la información electrónica, y nosotros añadiríamos que también nuestros datos personales.

2.2.1. Ventajas y daños de la tecnología

Hoy en día, la tecnología impacta directamente en las actividades cotidianas del ser humano, en ella se concentra la mayor cantidad de tareas individuales, sociales, laborales, comerciales, etc., ofreciendo beneficios sustanciales en el aprovechamiento de los recursos materiales, así como ventajas en los trabajos, entre ellas, podemos enlistar las siguientes[53]:

[52] *Ibidem*. Pág. 34
[53] Enunciativa no así limitativa.

a) Ahorro de tiempo,
b) Almacenamiento de datos y archivos,
c) Apertura global,
d) Condiciones de trabajo,
e) Desarrollo en la economía,
f) Competitividad,
g) Rapidez,
h) Conocimiento mundial, entre muchas otras.

Sin embargo, también nos encontramos en el lado opuesto del desarrollo tecnológico, aquello que no causa ventaja, empero, sí produce un daño; nos encontramos en una etapa revolucionaria de la tecnología en la información, pues podemos decir que no toda la informática y sus consecuencias, implica una mejoría para la humanidad. La rapidez, economía y concentración de actividades que pueda realizar una maquina y un programa implican también desocupación y marginalidad para quienes están alejados de la posibilidad de capacitarse en ello, convirtiéndolo en una desigualdad que bien podría decirse racial o cultural.

Aclaremos una cuestión, los avances tecnológicos, vislumbran cambios positivos hacia el futuro, empero, para los que manejan el mercado y la economía mundial, que se preocupan por estudiar y avanzar en su ciencia, el avance es positivo, pues los aplican a sus fines, pero en otros casos, para las personas, dicho avance es de alguna manera negativo desde el punto de vista humano, llegando incluso a pensarse que pudiere existir algún tipo de discriminación tecnológica para aquéllos que no tienen acceso a una red, a un ordenador, o a algún sistema informático, y en ocasiones distorsionando las relaciones humanas.

> Decía Paula Sibilia, "Sin embargo, pese al veloz crecimiento de estas prácticas y a la euforia que suele acompañar todas estas novedades, siempre espoleadas por el alegre entusiasmo mediático, hay datos que conspiran contra la estimativa más optimistas sobre la "inclusión digital" o "el acceso universal". Hoy, por ejemplo, poco menos de 200 millones de habitantes en el planeta "...tiene acceso a Internet...", "... los números sugieren que las brechas entre las regiones más ricas y más pobres del mundo no están

disminuyendo..., al contrario..., esas desigualdades parecen aumentar..."[54]

La autora agudiza la poca referencia que se hace con relación a las poblaciones mundiales con bajo nivel de infraestructura, países subdesarrollados que se encuentra incluso bajo el concepto de pueblos, poblaciones o naciones marginadas, a lo que Sibilia denomina *tecno-apartheid*.[55]

Por ello, insistimos que la información y la tecnología, hoy en día son poder, constituyen un arma en el sentido amplio de la palabra. Con ello no se pretende se elimine el conocimiento técnico o de sabiduría sobre los avances tecnológicos sino que se adopte una acepción de conocimientos profundos en la medida en que no se dé una intromisión en la esfera de la vida privada de las personas o se discrimine a ciertos sectores sociales, tomando como fin la no manipulación del hombre de manera indiscriminada.

2.2.2. Impacto de las nuevas tecnologías de la información

Siendo los medios de comunicación un apéndice de las Tecnologías de Información y Comunicación, ciertamente resultan afectados a partir de los cambios constantes y emergentes que se suceden con relación a ellas. Inclusive desde la informática, la computación, y con la instauración de Internet, son diversos los aportes que se han hecho a los medios de comunicación, no sólo en cuanto al mejoramiento y optimización de sus particulares procesos de producción, sino en los modos de transmisión de sus mensajes, en la forma como se relacionan con el público, y por supuesto, por tratarse también de organizaciones humanas en el flujo de datos personales por las carreteras de la información.

---

[54] Sibilia, Paula. *La intimidad como espectáculo*. Fondo de Cultura Económica, Argentina, 2008. Pág. 28-29

[55] "Intenta nominar esta nueva cartografía de la Tierra como un archipiélago de ciudades o regiones muy ricas, con fuerte desarrollo tecnológico y financiero, en medio del océano de una población mundial cada vez más pobre" *Ídem*.

El impacto que la revolución tecnológica causa en las personas al poner el flujo de datos a través tecnologías, es hoy ya bastante evidente. Con las Tecnologías de Información la sociedad mundial experimenta una revolución comercial y económica, porque traen consigo una infraestructura global, accesible y universal, el Internet. Esta infraestructura global representa un aporte significativo en los procesos de producción, gestión y gerencia dentro de las organizaciones, se ha convertido en una revolución de la información logrando cambios inclusive en las formas de comunicación social, pero también un fuerte medio para la recopilación y transferencia de los datos personales.

Así decimos que, las tecnologías de información y comunicación, que van en constante progreso, han significado la evolución misma de los medios de comunicación. Pero hay más, la era de la computación, la informática e Internet, abre a los medios un sinfín de nuevas oportunidades de acción y nuevos mercados, al considerar la recopilación masiva de datos personales, su transferencia electrónica y venta de bases de datos entre otros.

En síntesis, las tecnologías de la información han generado transformaciones positivas en los medios tradicionales, empero en otros como Internet, ha llegado a constituir un problema de índole social la violación a un derecho fundamental, la autodeterminación informativa, por no generarse las debidas medidas de seguridad, a partir de una adecuada y completa legislación. Pero examinemos a continuación, de qué manera se desarrolla Internet, y cuál ha sido su impacto en la sociedad.

2.3. La Revolución de Internet y su Impacto en los Medios de Comunicación

La gran revolución de la inteligencia, hoy en día no es considerada física, sino virtual. Esa invención de inteligencia, es lo que hoy conocemos como la World Wide Web, la WWW[56] o simplemente la Web, pero esta telaraña global, tiene su desprendimiento de la tecnología de la información, que se ha globalizado en el mundo moderno: el Internet.

Las tecnologías de la información y comunicaciones, han dispuesto de todos los mecanismos para instaurar un sistema eficiente que permita la distribución de la información en menor tiempo, a un costo inmejorable y prácticamente en cualquier lugar del mundo, estas TIC's, han adoptado para su sistema de reproducción la llamada red de redes, Internet, definida por Vernor Vinge escritor de ciencia ficción en 1996, como "aplicación ubicua de la ley, que los sistemas de distribución de grano fino, hacían posible mediante la utilización de chips de ordenador, unidos por la Red a todas y cada una de las partes de la vida social...".[57]

Pero podemos preguntarnos ¿qué es el Internet? En 1996, se escribió un artículo que formaría parte de un libro que jamás salió publicado, sin embargo, el autor muestra de manera coloquial lo que se conoce como "la Red", de la siguiente manera:

> "Internet es un conjunto de redes, redes de ordenadores y equipos físicamente unidos mediante cables que conectan puntos de todo el mundo. Estos cables se presentan en muchas formas: desde cables de red local (varias máquinas conectadas en una oficina o campus) a cables telefónicos

[56] Por sus siglas en inglés que significan "telaraña global", y puede definirse básicamente en tres cosas: hipertexto, que es un sistema de enlaces que permite saltar de unos lugares a otros; multimedia, que hace referencia al tipo de contenidos que puede manejar (texto, gráficos, vídeo, sonido y otros) e Internet, las base sobre las que se transmite la información.

[57] VINGE, Vernor, Citado por LESSIG, Lawrence. *El Código y otras leyes del ciberespacio*. Traducción de Ernesto Alberola, Taurus, España, 2001. Pág. 9

> convencionales, digitales y canales de fibra óptica que forman las "carreteras" principales, ...basta saber que cualquier cosa a la que se pueda acceder a través de algún tipo de "conexión," como un ordenador personal, una base de datos, un servicio electrónico de pago, etc., pueden ser, y de hecho forman, parte de Internet...".[58]

Podemos darnos una idea de lo que es considerado el Internet y la manera en que se encuentra distribuido como un conjunto descentralizado de redes de comunicación interconectadas, empero, con esto podemos continuar nuestra exposición, ya que no corresponde al presente tema desarrollar las aplicaciones de la denominada Red de redes, sino sólo el complemento de lo que en ella pueda acontecer.

Internet se ha convertido en el nuevo canal de comunicación, si desprendemos a Internet de su concepto, como una interconexión de redes informáticas que permite una comunicación directa a las computadoras que se encuentran conectadas, ya sean redes locales conectadas entre sí a través de un ordenador o por vía satelital, por lo que se trata de la mayor red de conexión de ordenadores que se conoce en el mundo y que permite una comunicación (envío y recepción de información) rápida, sin límites de tiempo ni espacio; y tomando en consideración que se trata de un instrumento que permite el envío y recepción de información, podría decirse con cierta ligereza que la Web no es más que un nuevo medio de comunicación y que su capacidad de conectar a tantos seres humanos a la vez la convierte en un medio de comunicación de masas, debido al alto impacto que ha tenido.

---

[58] IBAÑEZ, Álvaro. *El libro de internet. Una visita guiada al mundo digital.* 1996. http://web.archive.org/web/19990427222839/bbs.seker.es/~alvy/que_es_internet.html

Ramón Daniel Pizarro[59], apunta que desde el punto de vista de quien emite la información, la tecnología posibilitó notables progresos para la captación, almacenamiento, conservación y distribución de informaciones. Y, especialmente, para las metodologías de trabajo. Los ordenadores electrónicos, con su fantástica capacidad para procesar informaciones alfanuméricas, memorizar asombrosas cantidades de datos, recibir y transmitir información, han tenido participación fundamental en este proceso, alcanzando niveles notables de eficiencia y sofisticación, que permiten, junto con otros elementos tecnológicos, canalizar la información al consumidor con dinamismo y celeridad. La televisión, las redes de TV vía cable, las transmisiones satelitales, el correo electrónico, el disco óptico, la fibra óptica, el fax, las terminales multifuncionales, la informática y las 'autopistas de la comunicación' son los principales protagonistas del fenómeno informativo".

Internet destaca particularmente porque se trata de un instrumento que facilita a las personas el rápido acceso a cantidades infinitas de información, a un costo relativamente bajo, sobre cualquier índole y proveniente de cualquier rincón del mundo, ya que suministra una gran cantidad de datos (incluyendo personales), permitiendo la libre circulación de estos, pareciere que ahora toda la información que deseemos está a nuestro alcance por tener como protagonista a Internet a la libre disposición de todo individuo.

Son precisamente las características de este sistema actual de información los que hacen de esta etapa histórica una verdadera revolución, que ha impactado directamente en los medios de comunicación, cada vez son más las personas que utilizan el Internet para comunicarse y para obtener información (datos personales), tan sólo en México a nivel Nacional, se incrementó el uso de Internet de 7,097,172 en 2001 a 27,206,174 en 2009, es decir de un 8.0% de la población a 28.3% en 8 años (compras, transacciones, búsquedas, consultas, etc.).[60]

---

[59] *Responsabilidad civil de los medios masivos de comunicación*. 2ª edición, colección Responsabilidad civil vol. 8. Ed. Hammurabi S. de R.L. Argentina, 1999. Pág.63

[60] INEGI. Encuesta Nacional sobre disponibilidad y uso de las Tecnologías de la información en los hogares.

La denominada revolución tecnológica y de información que tiene en Internet a su mayor representante, ofrece por supuesto nuevas formas de acción y mercado, teniendo al menos dos grandes oportunidades con Internet: pueden aprovechar la Red para la interacción con nuevos mercados y para expandir sus formas de comunicación con la audiencia o, ir más allá, incorporarse al "ciberespacio" con un sitio propio, con características adaptadas al nuevo entorno comunicativo que le permitan imponerse como un nuevo medio en la Red, cualquiera que sea el campo de acción, constituye un claro proceso de tratamiento de datos personales, precisamente por ser el objetivo de las empresas y medios de comunicación el llegar a la mayor cantidad de individuos posibles, permitiéndose con ello el flujo de datos, muchas veces sin consentimiento del titular.

2.3.1. El flujo de datos personales en Internet

Según el Diccionario de la Real Academia Española, la palabra "dato" proviene del latín *datum*, que significa antecedente necesario para llegar al conocimiento exacto de una cosa o para deducir las consecuencias legítimas de un hecho.[61]

El "dato" ha sido considerado como elemento de primordial importancia táctica y estratégicamente. Othon Sidou, autor brasileño, define al dato como "la representación convencional de hechos, conceptos e instrucciones de forma apropiada para la comunicación y procesamiento por medios automáticos"[62], el obtener un dato, el poseerlo, el conocerlo, puede constituir una fuente poderosa para conocer acerca de lo que se quiere y lo que se pretende, el dato ayuda a descifrar y a prever futuras acciones en cualquier ámbito, como consecuencia de ello, la transmisión de datos o flujo de ellos es altamente beneficioso, práctico e incluso lucrativo para algunos, sin embargo, para los titulares de los datos pueden

---

www.inegi.org.mx/est/contenidos/español/rutinas/ept.asp?t=tinf204&s=est&c=5931

[61] *Diccionario de la Real Academia Española*. Ob. Cit.

[62] SIDOU, Othon. J.M.. *Las nuevas fronteras del derecho procesal constitucional brasileño: mandamientos de ejecución y hábeas data, 1992.* Pág. 1016

ser estas actividades perjudiciales; podemos encontrar gran diversidad de ellos, desde recetarios de cocina, recopilaciones, bibliotecas, inventarios, hasta datos personales que únicamente conciernen a la esfera de la vida privada, y que aun así pueden ser conocidos por terceros.

El ser humano desde que nace, se encuentra sometido al registro de sus datos, es decir, desde el instante mismo en que es nacido, comienza la existencia de un dato el cual puede generar conocimiento e información.

El nombre de la persona es un dato personal que puede reflejar el origen étnico, racial, cultural, costumbres, etc., durante el desarrollo de la vida de la persona, va generando cantidad de datos que pueden ser susceptibles de actividad cronológica, las cuales comienzan a plasmarse en archivos o registros públicos, bancarios, empresariales, laborales, genéticos, sanitarios, y datos conocidos como sensibles, etc., datos a los cuales el ser humano en algún momento pierde el control total de ellos, y esos datos conducen a un propósito. Sostiene el jurista argentino Roberto Cesario[63] que, vinculando todos los datos es posible la obtención de la información.

En un fallo del Tribunal Constitucional Alemán de fecha 15 de diciembre de 1983, se afirma que en la elaboración automatizada de los datos, un dato considerado en sí mismo sin importancia puede adquirir un nuevo valor, y por lo tanto, ya no puede decirse que existan datos carentes de importancia, y así son las cosas si tomamos en cuenta que un dato por sí mismo puede revelar distintas situaciones e ideologías, enfermedades, padecimientos, nivel cultural, social, económico, como en el caso del propio nombre y más aun cuando se traten datos de los denominados sensibles, la lista de datos es tan amplísima que podemos decir que una base de datos posee entre 150 y 200 datos de cada individuo.[64]

---

[63] CESARIO, Roberto. *Hábeas Data. Ley 25.326. Doctrina, jurisprudencia y Legislación.* Ed. Universidad, Buenos Aires, 2001. Pág. 23

[64] Dávara y Asociados. *Conferencia sostenida en la IV Semana de Transparencia y Acceso a la información Pública*. Instituto Federal de Acceso a la Información, México, 2005.

El dato, desde el punto de vista jurídico, es considerado como un elemento de gran valor económico y jurídico propio, el cual fue nombrado por una doctrina francesa en la época de los 80's como bien jurídico informático.

Los datos elaborados constituyen un bien jurídico y económico valioso, cabe extremar los recaudos para protegerlos adecuadamente, brindándoles toda la seguridad posible.

Algunos autores, como Roberto Cesario[65], clasifican a los datos de la siguiente manera, los cuales pueden ser datos que fluyan por Internet:

1. Registros Personales: Civil, laboral, académico, bancario.
2. Registros comerciales: Societarios, comerciantes.
3. Registros impositivos: Actividades y bienes de las personas individuales, colectivas o patrimonio de los individuos.
4. Registros de propiedad: Muebles, inmuebles, Registrales, intelectuales.
5. Registros políticos: Padrones electorales, asociaciones políticas.
6. Registros sanitarios:, Antecedentes médicos, fichas médicas, historial clínico.

Cantidad de datos personales como estos y muchos más, pueden circular por la Web, siempre que se tenga la disponibilidad de un procesador para acceder; y más aun, existen los denominados *spyware*,[66] que se introducen en el procesador personal para acceder a nuestra información, así como la actividad que tenemos en nuestro procesador, y esto incluye los de las instituciones gubernamentales, empresas, pc's individuales, etc., además de que a través de Internet, tenemos la capacidad de acceder a una infinidad de información que es constantemente agregada por el propio titular de los datos que se almacenan en páginas con

[65] CESARIO, Roberto. *Hábeas Data. Ley 25.326. Doctrina, jurisprudencia y Legislación.* Ob. Cit.
[66] Programa espía, es un software, que se instala furtivamente en una computadora para recopilar información sobre las actividades realizadas en ella. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en organismos oficiales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante. *Programa espía.* Wikipedia. La Enciclopedia libre. http://es.wikipedia.org/wiki/Programa_esp%C3%ADa

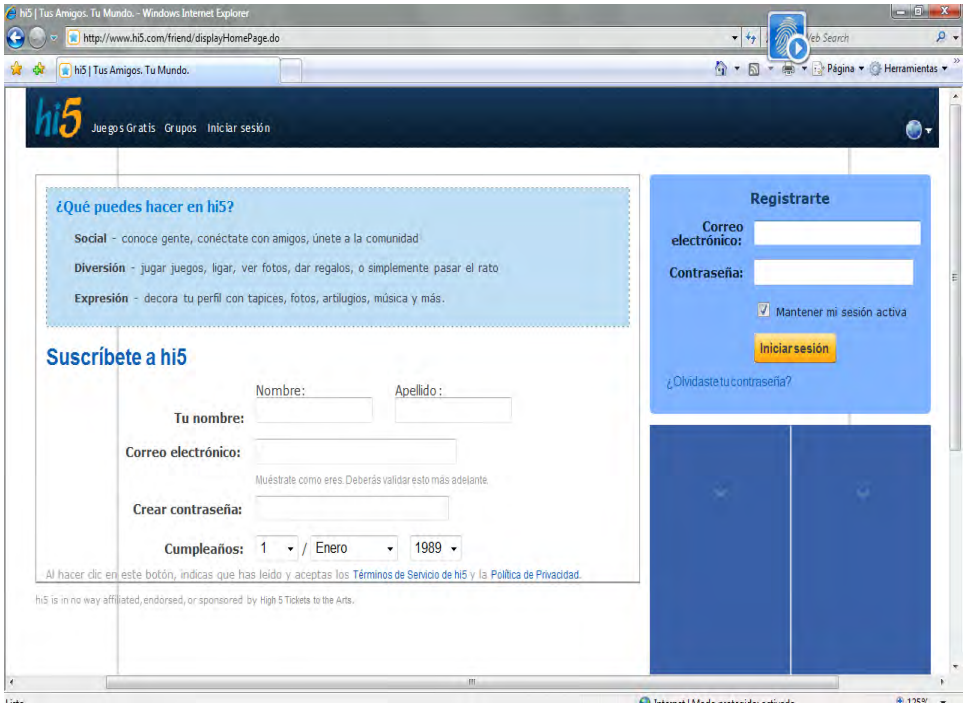
disponibilidad de usuarios, como los de fácil acceso, facebook, hi5, my space, orkut, blogs, así como los canales de comunicación chats,[67] ello bastando con que el usuario tenga una cuenta de correo electrónico y puede acceder a ellos de una forma fácil, copiar y circular datos personales por toda la red, fotografías, preferencias, árbol genealógico, etc.

Infinidad de información que podamos imaginar, la encontramos distribuida en la red, en otros casos no es necesario la cuenta de correo, ya que existen algunas páginas en las que los propios usuarios de Internet, descargan sus videos, fotos, su vida privada, su vida íntima, a fin de que los demás usuarios puedan acceder a ella de manera sencilla y rápida, sin correo, sin ningún otro requisito que una PC, el caso concreto de www.youtube.com, en donde las personas dejan huella de sus preferencias, gustos y aficiones, circunstancias a las que Paula Sibilia denominó la exposición de su vida "éxtima"[68], como contraposición a la vida íntima, argumentando, que la idea de intimidad ahora es pública, por el inconmensurable uso de las tecnología y el Internet y sus espacios para la publicidad de los datos personales, los siguientes cuadros son un ejemplo:

[67] Las Redes Sociales se han convertido en un asentamiento de datos personales. El ingreso a ellas genera información sobre la persona y esta se queda expuesta a la vinculación de su identidad con el tipo de consumo habitual, exponiéndose a que sus datos personales puedan ser incluidos en una lista de distribución o directorio que posteriormente son tratados con fines ilícitos o de lucro.
[68] SIBILIA, Paula. *La intimidad como espectáculo.* Ob. Cit. Pág. 16

[69]

Cuadro 1.



CUADRO 2.

[69] https://www.orkut.com

Mediante estas páginas web, los usuarios concentran todo tipo de información, desde la más simple hasta la más importante de sus vida, convirtiendo su vida privada en captación de las miradas ajenas, por lo que a partir del momento en que sube información a la web, se encuentra revelando datos concernientes de su situación global (económica, social, cultural, salud, gustos, profesión, religión, idiomas, familia, gustos, gastos, lugares que frecuenta, disturbios, alegrías, tristezas, etc.) cualquier cantidad de información que uno requiera, se encuentra disponible en la Red.

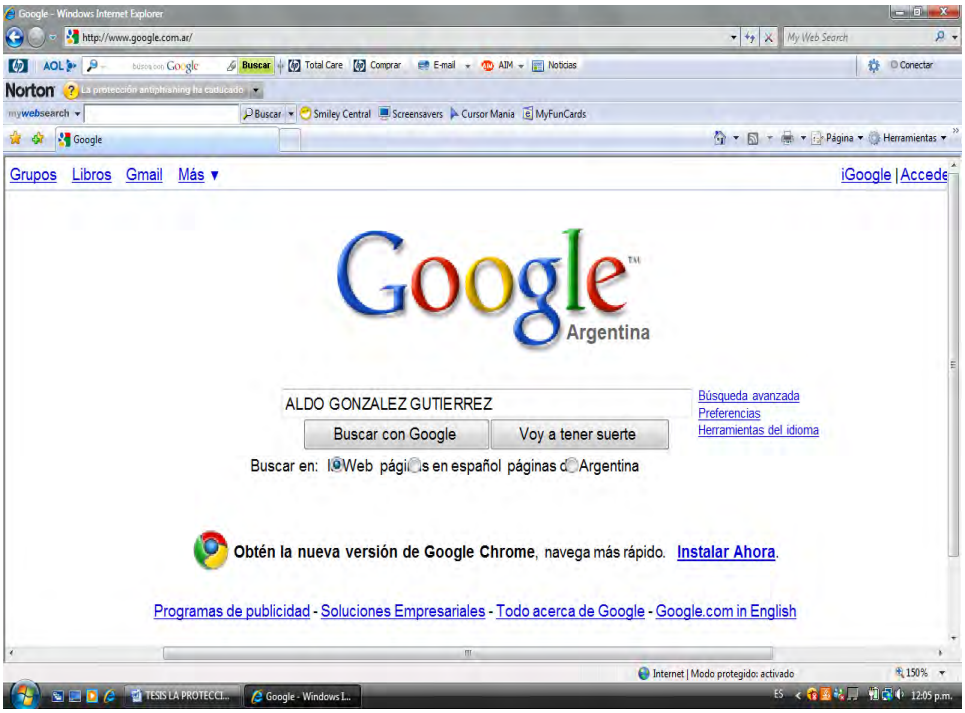
La protección de los datos personales en el ámbito de las comunicaciones en red, constituye el desafío más evidente de la sociedad tecnológica en la degradación del mundo informático por actividades delictivas o ilícitas, así como efectos de publicidad y ventas al público que no las solicitó, panorama al que deben obedecer las normatividades.

Por ello, acertadamente, la autora en comento sostenía que las páginas web y las redes sociales se han convertido en diarios que han dejado de ser íntimos para conocimiento del espectador que se encuentra a la caza de los datos personales que pudieren desprenderse de la gran cantidad de información que diariamente se sube a la red. Considerándolo como diario éxtimo[70], como denominación que se le dio a la paradoja de esta novedad, que consiste en exponer la propia intimidad en Internet.

Día a día, el hombre se ve enfrentado a la revelación de sus datos personales, llenando planillas, formularios, solicitudes, y después recibe una gran cantidad de informes publicitarios o marketing, sus datos circulan por todo el mundo de la información, convirtiendo en evidente el tráfico de circulación de los datos personales.

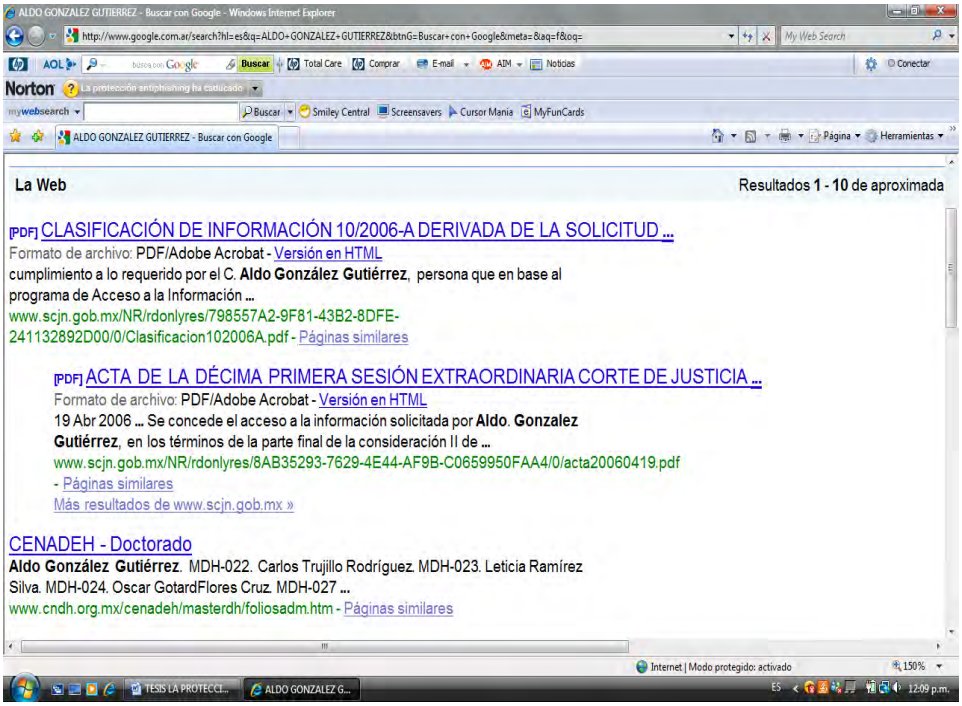
[70] SIBILIA, Paula. *La intimidad como espectáculo.* Ob. Cit. Pág. 16

Hoy en día, prácticamente cualquiera que tenga un ordenador personal podrá darse cuenta que acceder a información de cualquier índole, ya no constituye una tarea difícil, el sólo hecho de ingresar a páginas como Google, nos da un amplio panorama de datos que pueden aparecer en la Red, revelando con ello información que pudiere representar riesgo para el particular que tiene sus datos asentados en los archivos de las páginas web, como lo podemos observar en los siguientes cuadros[71]:



Cuadro 3.

[71] www.google.com.ar. Desde cualquier parte del mundo puede ser consultada esta información.



Cuadro 4.

La recopilación de datos y su tratamiento automatizado dan lugar a la aparición de los llamados banco de datos que Roberto Cesario lo llama *data bank*.[72]

El tratamiento de dicha información, constituye el objeto de estudio de la informática, respecto a este tema, Pierini, Lorences y Tornabene, sostienen que "... Por información entendemos resumen de datos (data); la informática cubrirá, entonces, los distintos sistemas de información y la forma como ésta se podrá elaborar, transmitir y compilar... Debido a los actuales ordenadores o computadoras, la informática ha alcanzado un gran desarrollo, fundamentalmente por la gran capacidad de almacenamiento y la rapidez de acceso a los datos acumulados. Si a esto se le suma el avance tecnológico en materia de comunicaciones, se obtiene el resultado actual, que es que la información acumulada y dispersa por distintos puntos del planeta pueda ser accesible a través

[72] Conjunto organizado de bases de datos junto con el soporte físico y el soporte lógico para su explotación, tal como los programas de almacenamiento y actualización y los programas de gestión, administración y aplicación. Conjunto no redundante de datos asignados e interrelacionados de acuerdo con ciertos atributos comunes en función de los posibles requerimientos de distinta aplicación" *Ob. Cit. Hábeas Data. Ley 25.326.* Pág. 27

de las grandes redes informáticas, como por ejemplo, Internet…"[73]

Estas constituyen las bases de datos, programas destinados a almacenar información de diversa índole en soportes magnéticos, electrónicos u ópticos, contenidos en una computadora (hardware), y cuyo acceso puede realizarse a través de una simple búsqueda coherente.

El Derecho Argentino definió en el Decreto No. 165/94, B. O. de fecha 8 de febrero de 1994, punto 3, inciso b), a la base de datos: "…Se entenderá por obras de base de datos, incluidas en la categoría de obras literarias, a las producciones constituidas por un conjunto organizado de datos interrelacionados, compilado con miras a su almacenamiento, procesamiento y recuperación mediante técnicas y sistemas informáticos."

Como consecuencia de todo lo anterior, se forman bases de datos de carácter público y privado. Se consideran las de carácter público aquellos que se encuentren en registros públicos y que provienen del Estado nacional, estatal o municipal, además de aquellas que el propio particular pone a disposición del escarnio público por la circunstancia de contener información a la que se puede acceder al público o de pertenecer a todos los ciudadanos, en el caso del Estado, o por el hecho de que el particular pretenda que esos datos deban ser conocidos; por oposición encontramos los registros privados, los cuales se encuentran en manos de entes particulares y a cuyo acceso sólo está en poder de unos cuantos.

En México, tenemos el claro ejemplo de una gran base de datos de carácter público, las listas del padrón electoral del Instituto Federal Electoral, que corresponden a millones de votantes, entre los que se encuentran, nombres, domicilios, teléfonos, empleos, entre decenas de datos correlativos a las personas, y cuya base de datos fue vendida a una empresa norteamericana en el año 2003, burlándose todas las medidas de seguridad del organismo público.

[73] *Hábeas Data. Derecho a la intimidad. Ob. Cit.* Pág. 111

Del lado de las bases de datos privadas, continuando con el ejemplo mexicano, tenemos a la gran empresa Telmex, cuya base de datos constituye una de la más grandes de carácter privado, tenemos otras como Telcel, Iusacell, Movistar, e incluso en los sistemas bancarios, sin dejar de mencionar al Buró de Crédito, quien conserva en su poder gran información sobre el comportamiento crediticio de las personas en el país.

En el sistema argentino, se dice que en todos los casos, el legislador ha buscado la preservación del secreto, así como asegurar que sus fuentes se encuentren disponibles sólo para aquellos que tengan interés legítimo en consultarlas. En un banco de datos público, hay que acreditar el interés legitimo, todos tienen regulación específica, existe una relación de control o de tutela según como se encuentre organizado cada banco de datos, existe la responsabilidad extracontractual objetiva del Estado, de quien se presume que tiene solvencia para cumplir. Los registros privados en cambio, ahora cuentan con una regulación específica, la Ley 25.326 de Hábeas Data y su Reglamento 1558/01.

Dentro del sistema mexicano, la protección de los bancos de datos públicos a nivel federal, se encuentra regulada en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, estableciendo que cualquier persona es libre para accesar a su información privada sin necesidad de acreditar legitimación alguna o interés, así como los derechos de rectificación, cancelación y oposición; y recientemente la Ley Federal de Protección de Datos Personales en Posesión de Particulares los tutela, dejando al Instituto Federal de Acceso a la Información la tarea de protegerlos, misma ley que entró en vigencia el 6 de julio de 2010 como respuesta a lo dispuesto por el artículo 16 de la Constitución Política.

Por lo anterior, es que algunos países, el caso de México por ejemplo, al no contar con una regulación específica en materia de protección de datos personales en Internet, resulta ser un país más vulnerable al flujo de datos por este medio de comunicación, toda vez que caen las barreras que limitan; hoy la comunicación

puede conocerse prácticamente al instante en todo el mundo, un simple click hace propagar la noticia por diferentes partes, y con ello el flujo de datos incluso transfronteras.

Con la aparición de la telemática, toda la información que antes sólo podía recuperarse del propio ordenador que la contenía directamente viajaba por todo el ciberespacio y puede ser recuperada, consultada e impresa en cualquier parte del mundo, con un ordenador disponible.

Así la transmisión de datos es el "movimiento de información codificado, de un punto a uno o más, mediante señales eléctricas, ópticas, electroópticas o electromagnéticas, dando la vuelta al mundo a bordo de la superautopista informática... La verdadera trascendencia de estos conceptos es lo que convierte a internet es la mayor base mundial de la información."[74]

El ser humano ha sido objeto constante de anotaciones referidas a sus datos personales. Actas de nacimiento, registros de bautismo, confirmaciones, comuniones, vacunas, ingreso a escuelas, pago de cuotas, compra de artículos, trámites administrativos y/o judiciales, matriculaciones, afiliaciones a obras sociales, sociedades, partidos políticos, tarjetas de crédito, cuentas bancarias, consumo en restaurantes, y aun después de fallecido, figuras los datos en juicios sucesorios, y todo esto, hoy en día constituye una multiplicidad de registros y de las huellas de que aquel individuo ha realizado tantas actividades a lo largo de su vida, datos que pasan a formar parte de los bancos de datos electrónicos.

Nos percatamos que un manejo constante de la tecnología y medios, con internet a la cabeza, exige a las compañías un manejo cuidadoso en los datos personales. El comercio electrónico, es hoy en día el tema y no es para menos, cada minuto se pueden agregar 2000 páginas a Internet y se envían diariamente, millones de correos electrónicos o e-mail *(electronic mail)* como se le conoce, y en

[74] Pierini, Lorences y Tornabene. *Op. Cit.*

cuyos mensajes se encuentran inmersos, cantidad de datos personales, que fluyen por las carreteras de la Red de manera indiscriminada, dándose un intercambio de información entre los usuarios o entre personas que se encuentren a la caza de los datos que fluyen, pagando en cada caso estratosféricas cantidades por el contenido de los correos, o archivos de datos personales,[75] sin embargo, autores argentinos reconocidos sostienen el contrapeso que puede ejercerse por el particular afectado a través del hábeas data, quien hace frente al poder informático.[76]

2.4. La tecnología y la protección de datos personales

A comienzos de los años 70's, era apreciable que el aparato administrativo estatal obtendría un esencial instrumento de poder: la tecnología, y con ello al acceso a la información. Científicos, políticos entre otros, discutían acerca de si la omisión del Estado a los principios jurídicos que permitían restringir su poder a favor de los ciudadanos debería ser extendida.

Con el desarrollo de la tecnología y de la información surge una nueva forma jurídica, no como invención, sino como un avance hacia la consolidación, ventilación e interpretación de los Derechos del hombre, contra la constante amenaza del Estado, y en algunos países, de los particulares.

Al principio, se pensó que los derechos fundamentales eran derechos de defensa frente al funcionamiento interventor del Estado, "esta idea se alimentaba de la presunción fundada de que se debía observar con cuidado al Estado, así como también a las largas experiencias con las actividades de observación estatal, todo lo

[75] "Resulta sumamente significativa en este sentido la decisión de Microsoft de cerrar sus salas gratuitas de chat en todo el mundo, con el mantenimiento de los canales de pago en Estados Unidos, Japón y Canadá bajo el argumento de luchar contra la creciente difusión de contenidos pornográficos, spam (publicidad comercial no solicitada) detectada en estos espacios online de mensajes instantáneos". Ballesteros Moffa, Luis Angel. *La Privacidad Electrónica. Internet en el centro de protección.* Valencia, 2005. Página 139

[76] DALLA VÍA, Alberto y Marcela Basterra. *Hábeas Data y otras garantías constitucionales.* Némesis, Argentina, 1999. Pág. 115

cual demostraba que el Estado no puede desarrollarse según sus propias leyes, que se le debe encadenar a los derechos humanos y civiles."[77]

El desarrollo hacia un derecho a la protección de datos constituyó una herramienta contra el Estado, avance que debía necesariamente producirse ante el desarrollo tecnológico. Ya lo expresaba Orwell en su libro en 1984, "El gran hermano" *(Big Brother)*, se había establecido en el corazón del concepto de privacidad. En esas épocas, el concepto de autodeterminación informativa, se estableció como un derecho de defensa contra el hombre informativo, y el domino informativo del Estado moderno cobró vida.

Lo que aun no podía preverse era el desarrollo del procesamiento de datos realizado en forma privada, el cual, como lo sabemos hoy, puede conducir a amenazas contra los derechos humanos que los pueden esperar de un dominio informativo ilimitado en manos del Estado.

Este ambiente global de la información y la tecnología ha puesto en entredicho el concepto tradicional de intimidad para dar paso a nuevos matices conceptuales -como por ejemplo, la privacidad como un derecho con proyección social y no como un grado cero de sensibilidad-, a nuevas perspectivas de comunicación entre personas y países, generando con ello nuevos retos para el derecho a la protección de datos, el cual se debate hoy en día entre sus ligámenes a los viejos sistemas de control y la necesidad de utilizar nuevas herramientas tecnológicas para garantizar el derecho fundamental de los ciudadanos a decidir quién, cuándo, dónde y bajo qué circunstancias toma contacto con sus datos.

Es así posible encontrar actualmente trabajos como el de Schmitt Glaeser, quien sostenía que una protección de la esfera privada, es esencialmente una protección de la información[78]. Este tipo de propuestas ofrecen un amplio elenco

[77]HASSEMER, Winfreied y Alfredo, Chirino Sánchez. *El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales.* Editorial del Puerto, Argentina, 1997. Pág. 30
[78] Citado Por RUIZ MIGUEL, Carlos. *En torno a la protección de los datos personales automatizados.*

de posibilidades para articular la tutela de la privacidad bajo el entramado básico de la facultad de ciudadanos de controlar el uso de las informaciones que los puedan afectar. La definición de esta tendencia de concebir a la *privacy* como una posibilidad de control de información se encuentra ya en el libro de Alan Westin, *Privacy and Freedom*, quien a finales de la década de los 60's planteó el derecho del ciudadano a controlar las informaciones por sí mismo, *"a right to control information oneself"*. Esta tendencia es seguida por quienes subrayan la necesidad de que los ciudadanos controlen la información que les concierne ya no como un mero hecho de defensa frente a las intromisiones de otros, sino ahora frente a los riesgos tecnológicos, como un derecho activo de control sobre el flujo de informaciones que circulan sobre todos nosotros.

No se trata de limitar el tratamiento electrónico de los datos que es, en esencia, y esto como una verificación de los posibles desarrollos futuros, una condición para el progreso del Estado, sino más bien de luchar porque dicho tratamiento se realice de una manera democrática, afianzando los derechos y garantías del ciudadano y promoviendo la participación social de todos. Salta a la vista que un acceso a las informaciones públicas permitirá no sólo mayor transparencia en el funcionamiento de las instituciones, sino también una mayor posibilidad de que los ciudadanos tengan acceso a mejores condiciones para su desarrollo individual y para el ejercicio de sus derechos políticos.

Pero también hay que ser conscientes de que eso no justifica que por alcanzar la transparencia de la sociedad, los ciudadanos pierdan la posibilidad de preservar su personalidad del acceso extralimitado y objetivamente del Estado o de los particulares. Este dilema enfrenta a las sociedades modernas ante una complicadísima y difícil ponderación de intereses, donde entran en juego no sólo las necesidades de información de la sociedad y la nueva configuración de las relaciones económicas entre los países, sino que habrá de considerarse igualmente el interés del ser humano, no sólo a gozar de mayor información en todos los

---

Revista de Estudios Político (Nueva Época), No. 84, abril-junio, 1994. Pág. 242.

ámbitos del conocimiento y de la cultura, sino también a la necesidad de tutelar a la persona frente al uso desmedido de sus datos personales.

El nuevo papel de la privacidad, así planteado, rompe los viejos estancos en que se desarrollaba la escisión entre lo público y lo privado, entre lo personal y lo colectivo, entre lo íntimo y lo general, para abrir la puerta a la discusión sobre los espacios sociales donde se produce la interacción entre los ciudadanos para el alcance de objetivos comunes, haciendo ejercicio de nuevos matices de la libertad, potenciados por nuevas formas de comunicación.

En 1968, el Consejo de Europa, realizó un estudio a fin de poder determinar si los Estados miembros contaban con la debida protección de la privacidad con relación a los avances tecnológicos y científicos. Es preciso advertir que el tratamiento automatizado de datos personales se ha convertido en un arma estratégica de manipulación de conductas individuales, y la aplicación de avanzados métodos telemáticos a la información de carácter personal ha dejado de ser la excepción para convertirse en una rutina diaria, es por ello que frente al tratamiento automatizado de esos datos, fue creada la Convención para la Protección de los Individuos con relación al Procesamiento Automatizado de Datos Personales, conocida como la Convención de Estrasburgo y suscrita por 21 Estados europeos.

Lo importante a destacar del presente Convenio, es el derecho que tiene el individuo de acceso a sus datos que deben ser proporcionado sin restricciones y con una periodicidad razonable, confirmándole la existencia o inexistencia del tratamiento de datos que le conciernen, que se informe por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen sus datos, además de la comunicación, en forma inteligible, de los datos objeto de los tratamientos, y de toda la información disponible sobre el origen de ellos, así como el conocimiento

del tratamiento automatizados de los datos referidos al titular, sobre todo en los casos de decisiones automatizadas.

Esto bien, se refiere al derecho que tiene toda persona a no verse sometida a una decisión jurídica que les afecte significativamente y basada únicamente en un tratamiento automatizado de datos destinado a evaluar aspectos de su personalidad, y por otro lado, la Convención comprende el derecho de exigir la rectificación, supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la Directiva, en particular a causa del carácter incompleto o inexacto de los datos.

2.5. Margen de Protección de Datos Personales y Seguridad en los sitios Web

Guardar los datos personales en un mundo con millones de testigos potenciales como Internet es difícil, y la probabilidad de que alguien identifique los datos, las conversaciones, los correos, etc., es mayor conforme lo hace la distancia que las separa, por la globalidad de la red, nada es secreto, todo puede ser interceptado, leído, conocido, y el valor de esos datos son utilizados para cantidad de actividades comerciales, en el mejor de los casos, porque en otros puede ponerse en riesgo la propia vida cuando los niveles de seguridad no son los adecuados.

Uno de los aspectos más importantes sobre el particular, es distinguir dónde se encuentra la línea que divide a la privacidad de aquello que puede afectar los intereses del individuo, lesionándolo, puesto que en todo sistema, nos encontramos frente a riesgos, unos más potenciales que otros, y ante ello, debemos encontrar métodos de salvaguarda de la integridad física, moral, psicológica, emocional, etc.

De ello, el ser humano busca procedimientos de adecuación a la necesidad de protección de sus intereses, resultado del anhelo de seguridad que busca. Podemos referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el

área o campo al que haga referencia. La seguridad puede referirse a un estado de ánimo, una sensación, una cualidad intangible, pero también puede entenderse como un objetivo y un fin que el hombre aspira constantemente como una necesidad primaria.

Hablamos de aquellas circunstancias en las que la vida privada se ve envuelta en las actividades de comunicación y en las tecnologías de la información, en donde opera la inseguridad del usuario de servicios, cuando sus datos personales se encuentran en constante flujo de información.

En los negocios, la información que se proporciona en tarjetas de crédito, correos electrónicos e incluso llamadas telefónicas acaba siendo enrutada a través de Internet y la necesidad de seguridad es obvia.

Hoy en día, es difícil tratar a los datos personales en secrecía, pues los modernos medios de comunicación y las TIC's han centrado toda su atención en irrumpir al máximo la categoría que la privacidad da a nuestra vida, lo que antes podría ser considerado como derecho del disfrute a la privacidad, hoy en día la podemos definir como derecho de defensa, una exigencia mayor frente al flujo de información en intromisiones a la misma.

Es de esa manera como Adelina Loianno[79] identifica principalmente dos fuentes de intromisión a la privacidad,:

a) Los bancos informáticos de datos personales. En donde zonas que debieran ser estrictamente de intimidad de las personas se pueden hacer del conocimiento público, y
b) Los medios de prensa, desde la perspectiva de la ofensiva de los medios masivos de comunicación.

La autora sostiene dos maneras de quebrantar la vida privada, en los supuestos de consideración en que se desenvuelve la actividad privada o

[79] GOZAINI, Osvaldo Alfredo. (Coordinador). *La Defensa de la intimidad y los datos personales a través del Hábeas Data. Ley 25.326.* Ediar, Argentina, 2001. Págs. 21-22.

gubernamental, para ello, el derecho juega un papel importante de protección y seguridad en la defensa del individuo con su respectiva reglamentación, y es justamente al individuo al que la ley debe regular en el uso y tratamiento de los datos personales, de la privacidad.

Con la transnacionalización de la actividad tecnológica y el proceso de globalización, aparece en la Argentina una ley de protección al marco de la privacidad en materia de datos personales y más interesante aun el hábeas data, como remedio que el derecho brinda al individuo para defender su privacidad e intimidad, especificando los límites que la sociedad debe imponer, ello en pro y en beneficio de la dignidad personal; el artículo 9 de la Ley 25.326 de Protección de Datos personales, hace alusión a la seguridad de los mismos.

El Estado Argentino, dentro de su respectiva normatividad, ha reglamentado una institución base para otorgar seguridad y protección de los datos personales, nos referimos a la Dirección Nacional de Datos Personales, en donde si nos adentramos al sitio del organismo, encontraremos las actividades encaminadas a corresponder a la demanda social en materia de protección y seguridad a la privacidad.

La Seguridad en Internet no debe ser sólo una preocupación del usuario, sino de todas las empresas que participan de la Red social. Toda persona tiene derecho a la privacidad y cuando ésta accede a Internet la necesidad de privacidad aumenta. La privacidad no es sólo confidencialidad, también incluye el anonimato. Lo que leemos, las páginas que visitamos, las compras, la gente con la que nos comunicamos, todo ello representa información, que es "personal".

Es por eso que deben de adoptarse medidas que den seguridad a las personas sobre las actividades que realicen en la Red. Ahora bien, existen diversas formas en que puede generarse una intromisión a los datos personales, poniéndolos en riesgo

y clasificándolos de la siguiente manera[80]:

- **Interrupción**: un recurso del sistema se destruye o no llega a estar disponible o se inutiliza. Ésta es una agresión de disponibilidad. Ejemplos de esto son la destrucción de un elemento hardware (un disco duro), la ruptura de una línea de comunicación o deshabilitar el sistema de gestión de ficheros.
- **Intercepción:** un ente no autorizado consigue acceder a un recurso. Ésta es una agresión a la confidencialidad. El ente no autorizado puede ser una persona, un programa o un computador. Ejemplos de agresiones a la confidencialidad son las intervenciones de las líneas para capturar datos y la copia ilícita de ficheros o programas.
- **Modificación:** un ente no autorizado no solamente gana acceso sino que también deteriora el recurso. Ésta es una agresión a la integridad. Algunos ejemplos son los cambios de valores en un fichero de datos, alterando un programa para que funcione de una forma diferente, y modificando el contenido de los mensajes que se transmiten en una red.
- **Fabricación:** una parte no autorizada inserta objetos falsos en el sistema. Esta es una agresión a la autenticidad. Un ejemplo sería la incorporación de registros a un fichero.

En cualquiera de los precedentes se ponen en riesgo los datos personales, para ello, se propone implementar la seguridad en la red puede darse a través de ciertos pasos que a continuación se mencionan[81]:

- **Gestión de claves** (incluyendo negociación de claves y su almacenamiento): Antes de que el tráfico sea enviado/recibido, cada router/cortafuegos/servidor (elemento activo de la red) debe ser capaz de verificar la identidad de su interlocutor.

- **Confidencialidad**: La información debe ser manipulada de tal forma que ningún atacante pueda leerla. Este servicio es generalmente prestado gracias al cifrado de la información mediante claves conocidas sólo por los interlocutores.

- **Imposibilidad de repudio**: Ésta es una forma de garantizar que el emisor de un mensaje no podrá posteriormente negar haberlo enviado, mientras que el receptor no podrá negar haberlo recibido.

[80] http://es.wikipedia.org/wiki/Seguridad_en_Internet/
[81] Idem

- **Integridad**: La autenticación valida la integridad del flujo de información garantizando que no ha sido modificado en el tránsito emisor-receptor.

- **Autenticación**: Confirma el origen/destino de la información - corrobora que los interlocutores son quienes dicen ser.

- **Autorización**: La autorización se da normalmente en un contexto de autenticación previa. Se trata un mecanismo que permite que el usuario pueda acceder a servicios o realizar distintas actividades conforme a su identidad.

Estas formas elevan la calidad de resguardo de la información, evitando en un porcentaje mayor la intromisión, generando con ello mayor seguridad al usuario, tratándose de los sistemas de información en Red.

Una especie de encriptación de datos que, únicamente el usuario conozca y quienes, él mismo decida que deben conocer sus datos, para ello, también las empresas, deben garantizar un estado de seguridad a través de sus políticas de privacidad, generando en el usuario mayor conforte en la utilización de servicios de Red, Internet, tarjetas de crédito, telefonía celular, etc.

La adopción de medidas de seguridad, es presupuesto indispensable para que la tutela legal sea altamente efectiva, para evitar en la medida de lo posible que otros sujetos no autorizados, pudieren apropiarse del contenido para la aplicación de fines ilícitos, ello de conformidad con lo que establece el Convenio 108 del Consejo de Europa, en su artículo 7, al disponer que los Estados miembros deberán adoptar medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Alejandra Gils Carbó,[82] sostiene que la seguridad informática debe consistir en medidas técnicas y de organización. Por un lado, el responsable de la base de datos debe seleccionar, adquirir e instalar los equipos y dispositivos adecuados para proveer la seguridad física y lógica de los archivos luego de haber identificado los riesgos. Aquéllos deben ser aptos para evitar tanto la pérdida y la destrucción material, ya sea por causas naturales o por virus, como los accesos no autorizados.

Las medidas de seguridad para los ficheros automatizados que contengan datos personales, supone una revisión enorme que refleja el peso que este derecho ha ido adquiriendo con el tiempo. El responsable del fichero o tratamiento debe elaborar el documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información. Las medidas concretas que el responsable se obliga a cumplir dependen fundamentalmente de la naturaleza de los datos: medidas de nivel básico, nivel medio y nivel alto.

a. **Medidas de nivel básico:** se aplican a cualquier fichero o tratamiento de datos de carácter personal.
b. **Medidas de nivel medio:** estas medidas se aplican cuando los datos personales abarcan información sobre infracciones administrativas o penales, servicios de información sobre solvencia patrimonial y crédito, datos de gestión tributaria, servicios financieros, de la Seguridad Social y datos que permiten la elaboración de un perfil de la personalidad del sujeto.
c. **Medidas de nivel alto:** se aplican fundamentalmente a los datos especialmente protegidos. (ideología, afiliación sindical, religión, creencias, salud, origen racial o vida sexual), a los datos con fines policiales recogidos sin consentimiento de las personas afectadas y los datos sobre violencia de género.

Según el nivel de seguridad aplicable a los datos, se deben definir medidas de seguridad concretas, desde cosas básicas como un registro de incidencias y asegurar la correcta identificación y autenticación de los usuarios que accedan a los

[82] *Régimen Legal de las Bases de Datos y Hábeas Data.* La Ley, Argentina, 2001. Pág. 98

datos personales; medidas de nivel medio como auditorias y control de acceso físico; hasta medidas de nivel alto como el cifrado de las comunicaciones o un registro de acceso detallado que debe guardar cómo mínimo la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

Sin embargo, la seguridad, también puede ser constituida por el propio usuario de la Red en internet, colocación de antivirus a PC, el cuidado en páginas que visita, datos que proporciona, operaciones realizadas, y desde luego en las páginas de redes sociales, dar la información menor posible, puesto que la tarea de seguridad es una labor conjunta de quienes tienen acceso a los sistemas y de las empresas que manejan las bases de datos de los usuarios, toda vez que la seguridad no es sólo una cuestión de carácter técnico, empero, el responsable del archivo o base de datos debe estructurar una organización de recursos humanos que preserve el correcto funcionamiento del sistema.

La Dirección Nacional de Protección de Datos Personales en el Estado Argentino, dictó una serie de recomendaciones, destinadas a ampliar el margen de seguridad en los sitios web, sobre todo en el aspecto de redes sociales, dentro del ámbito de la "informática preventiva",[83] mismos que podemos identificar en el siguiente cuadro:

[83] Dirección Nacional de Protección de Datos Personales. http://www.jus.gov.ar/dnpdpnew/

"Consejos básicos para el uso de las redes sociales con Protección de Datos Personales" Facebook, HI5, y otros...

Que hacer

- ***Usar***
  si para su participación en REDES SOCIALES, fuera necesario revelar su identidad haga saber sólo los datos indispensables para su identificación, como ser su nombre completo, pero sin indicar su dirección, teléfono, o cualquier otro dato personal. Un email exclusivo y distinto del habitual para las redes sociales, y un seudónimo. En caso que ya se esté registrado, darse de baja y volver a hacerlo siguiendo este sistema.
- ***Privacidad***
  Ajuste sus opciones de privacidad para mantener su información fuera del dominio público.
- ***Crear***
  Los padres pueden crear sus propias cuentas y "añadir" a sus hijos como contactos para monitorear sus actividades en línea.
- ***Cuidado***
  Tenga cuidado con correos electrónicos que dicen provenir de su sitio de contactos sociales. No entregue información personal en respuesta a un correo electrónico.
- ***Revisar***
  Para evitar fraudes, revise la dirección de URL en la parte superior de la pantalla antes de ingresar su nombre de usuario y clave en un sitio de contactos sociales – existen sitios impostores cuyo propósito es conseguir esta información, por lo que debe asegurarse de estar donde cree que está.
- ***Reportar***
  Si se encuentra con algo sospechoso, repórtelo al sitio, o a una autoridad.

Que no hacer

- ***No poner fotos de otros*** *sin su consentimiento, sobretodo de menores de edad. Intentar evitar colgar fotos privadas incluso de uno mismo.*
- ***No suministrar datos personales*** *como dirección, teléfono ni la ubicación (donde se encuentra).*
- ***No admitir a desconocidos*** *dentro de la red.*
- ***No permitir la recepción automática*** *de comentarios de cualquier persona.*
- ***No responder a comentarios o e-mails*** *mal intencionados o de personas desconocidas que hacen preguntas personales.*

Asistimos y somos participes del fruto de la evolución constante en donde la tecnología cumple un rol, destacando que debe ser congruente con los valores preestablecidos, pero que también nos lleva a la reflexión de tener que estar alerta jurídicamente, dado los desórdenes que en algunos sentidos acompañan al progreso.

En nuestro cotidiano vivir enfrentamos situaciones debido al avance tecnológico que posibilita que el hombre pueda tener acceso a información de manera inmediata de otra persona, que hasta el pasado reciente y en el presente esto no ocurría, permitiéndose de ésta manera la apropiación de datos que, no siempre son contenidos por quien le pertenecen, lo que en ocasiones, puede traer con ello daños irreparables.

El uso de las redes sociales, facilitan las relaciones humanas y los accesos de comunicación, sin embargo, cuando la privacidad se ve quebrantada surgen medidas de seguridad que el usuario del servicio y los proveedores del mismo deben adoptar para incrementar el nivel de protección a la privacidad, alertándolos sobre los riesgos potenciales en aquellos sitios en los que se genera información sobre la persona y ésta queda expuesta a que se vincule su identidad con el tipo de bienes o servicios adquiridos. Un nivel alto de seguridad tecnológica, humana y racional, generará un fuerte contrapeso para el quebranto a la privacidad del individuo.

2.6. Archivos de datos personales

Uno de los problemas a los que nos enfrentamos al consultar la Ley 25.326 de Hábeas Data, es la definición de archivo de datos personales, porque la ley los enuncia de manera indistinta a los archivos, registros, bases o banco de datos, siendo un poco escueta al respecto, esto es así, puesto que la ley no se ocupó de definir o diferenciar este concepto, tratándolo incluso como sinónimos que se caracterizan únicamente por la gran colección de información que poseen de datos

personales, el artículo 2º de la ley en comento, señala: *"Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso."*

Ahora bien, de lo anterior podemos definir al Archivo como una unidad de datos o información almacenada en algún medio, y según la definición anterior, puede ser electrónico o no.

Alfredo Gozaini nos dice que en el lenguaje informático, archivar es registrar un conjunto de información que tiene similar estructura. El archivo puede ser lógico o estar referido a un sistema de ingreso y búsqueda; o ser físico y permanecer en un lugar establecido. [84] Esto es que, el archivo corresponde a un sistema de almacenamiento de información que puede descargarse desde un punto electrónico con una función de búsqueda de lo que se pretende consultar, por un lado, y por el otro, un soporte físico que no requiere de una estructura de movilidad toda vez que es estático.

Por su parte, Puccinelli,[85] nos refiere a la sentencia emitida por la Corte Constitucional de Colombia, en donde se considera que el archivo no es la simple recopilación o colección de documentos. El archivo es un conjunto orgánico de documentos, unidos por un vínculo originario o de procedencia, que sirven para recuperar con agilidad y en tiempo oportuno toda la información almacenada por una oficina o institución en el curso de su actividad.

Sin embargo, para Marcela Basterra[86], la definición que otorga la ley 25.326, en su artículo 2º, no puede considerarse reducida a registros donde se almacenen

---

[84] *Derecho Procesal Constitucional. Hábeas Data. Protección de datos personales. Ley 25.326 y reglamentación (decreto 1558/20001). Ob. Cit.* Pág. 41

[85] PUCCINELLI, Oscar. *Protección de Datos de Carácter Personal.* Astrea, Argentina, 2004. Pág. 172

[86] *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados. Derecho Constitucional Provincial. Iberoamérica y México. Ob.Cit*. Págs. 360-361

informaciones escritas o informatizadas, dado que también debe comprender a aquellos que lo hagan con imágenes, sonidos, o cualquier otra forma creada o a crearse de codificación de información para su comunicación. No sólo la naturaleza de los datos archivados merece atención, sino también los soportes donde se efectúe su almacenamiento, es decir, la modalidad de registración. No obstante, la definición resulta clara en cuanto resalta la indiferencia de que el procesamiento o tratamiento de los datos sea o no electrónico.

Lo cierto es que, de las definiciones propuestas por los autores es, que los archivos, bases o bancos, poseen información que puede resultar de carácter confidencial, son verdaderos padrones de datos personales, que requieren de un nivel de resguardo estructural según el tipo de archivo que sea éste, público o privado, y en el que se puede tener registros particularizados, o bien datos destinados a dar informes sobre determinados aspectos de la vida social, por lo que se constituyen en campos de almacenamiento con una finalidad específica.

Los archivos de datos personales, poseen información que puede ser en algunos casos del conocimiento general cuando consten en archivos públicos y estén destinados a dar información, pero en otros casos, esos archivos serán privados, y por consecuencia el tratamiento que se dé a los datos que almacena serán de carácter confidencial.

En la República Argentina, se cuenta con un organismo público encargado de llevar el registro de los archivos o bases de datos que se manejen en el ámbito de la vida privada y pública, a fin de regular la actividad desarrollada por los sectores sociales que manejan información, y con el objeto de garantizar el control del uso de los datos personales, nos referimos a la Dirección Nacional de Protección de Datos Personales, quien tiene bajo su encargo una Registro Nacional de Bases de Datos a fin de dar cumplimiento a lo dispuesto por el artículo 3º de la Ley 25.326 de hábeas data.

De tal suerte que en el manejo de los archivos de datos personales, se deberán observar los principios para el tratamiento de los mismos, licitud, seguridad, consentimiento, calidad de los datos, y con las obligaciones que la ley impone para el tratamiento de los mismos a los usuarios y a los responsables de esos archivos, de conformidad con lo dispuesto por los artículos 21, 22, 23, 24, 25, 26, 27 y 28 de la multicitada Ley.

En este capítulo constatamos la forma en que los medios de comunicación y las tecnologías de la información se han apoderado de la sociedad en todo el mundo y cómo cada día las actividades cotidianas requieren de los medios tecnológicos para realizarse; el Internet en su máxima expresión se sitúa en todos los rincones del mundo lo que supone ventajas para la ejecución de nuestras labores, empero también ciertos daños que produce el depender de las denominadas TIC´s.

Pese a ello, la revolución de Internet ha impactado en todos los sectores sociales que, poco a poco los tradicionales medios de comunicación han sido desplazados por este fenómeno informático, lo que ha llevado al flujo indiscriminado de datos personales que son transmitidos, tratados, enajenados, y explotados muchas veces con fines ilícitos y lucrativos; este último tópico supone las ventajas para las empresas que se dedican a comercializar sus productos a cualquier precio, adquiriendo las listas de distribución o directorios que componen los perfiles de los individuos que han dejado sus datos personales bajo el disfraz de registros en páginas web al ser visitadas, compras, transacciones, solicitudes, pagos, etc., circunstancias que permiten la intromisión de las denominadas cookies que almacenan la información a modo de pequeños archivos de los distintos comportamientos y datos de los usuarios durante las sesiones de navegación, con el fin de que en ulteriores visitas, esa información pueda ser recuperada para fines publicitarios no solicitados (el caso del *spam).*

Lo anterior exige la adopción por parte de los usuarios y/o empresas a implementar medidas de seguridad que restrinjan el uso indiscriminado de la información que es constantemente recogida en el uso de esta tecnología.

Son diversos los mecanismos que sitúan los datos personales en constante peligro, pero también las medidas para reducirlo. Hasta aquí hemos visto la problemática que se da en el tratamiento de datos personales en las tecnologías de la información, así como el flujo de ellos por Internet. Simultáneamente a esta situación resulta de especial interés para el objeto de nuestro estudio examinar el marco normativo que envuelve el derecho a la autodeterminación informativa y la manera en que ha sido regulado en los países a estudio, México, España y Argentina, repasando la legislación que ha servido de referente para estas tres naciones, su régimen legal y cuál será el futuro de este derecho conforme a las disposiciones normativas en el plano del derecho internacional.

CAPÍTULO III

MARCO NORMATIVO DE LA PROTECCIÓN DE DATOS PERSONALES: MÉXICO, ESPAÑA Y ARGENTINA

3.1. Legislación aplicable en México.

- 3.1.1. Constitución Política de los Estados Unidos Mexicanos
- 3.1.2. Legislación Federal
- 3.1.3. Legislación Estatal
- 3.1.4. Normatividad conexa
- 3.1.5. Ley Federal de Protección de Datos Personales en Posesión de los Particulares

3.2. Legislación aplicable en España.

- 3.2.1. Constitución Española
- 3.2.2. Ley 15/1999 de Protección de Datos Personales
- 3.2.3. Legislación Estatal en España por sectores de actividad
  - 3.2.3.1. Administración Pública
  - 3.2.3.2. Civil, mercantil y consumidores
  - 3.2.3.3. Firma y DNI electrónicos
  - 3.2.3.4. Fuerzas y cuerpos de seguridad
  - 3.2.3.5. Sanidad, salud y Reproducción asistida
  - 3.2.3.6. Seguros
  - 3.2.3.7. Telecomunicaciones y sociedad de la información

3.3. Régimen Legal de la Protección de datos personales en Argentina.

- 3.3.1. Constitución Argentina
- 3.3.2. Ley 25.326 de Protección de los datos personales y su Decreto Reglamentario 1558/2001
- 3.3.3. El Hábeas Data y los derechos tutelados

3.4. Presente y Futuro en la Protección de datos personales en el plano del Derecho Internacional: México, España y Argentina.

3.5. La integración de normas internacionales a los ordenamientos internos de Protección de Datos personales.

CAPÍTULO III

MARCO NORMATIVO DE LA PROTECCIÓN DE DATOS PERSONALES: MÉXICO, ESPAÑA Y ARGENTINA

3.1. Legislación aplicable en México

Desde el año 2000, se presentaron diversas iniciativas de Ley sobre Protección de Datos Personales a nivel federal, cuyo objetivo consistía en garantizar la protección de dichos datos que se encontraren contenidos en documentos, archivos, registros, bancos de datos, o bien, en otros medios tecnológicos de procesamiento de datos, sean de carácter público o privado, con el fin de proteger los derechos de la persona, iniciativas que no causaron estado parlamentario.

A partir del mes de octubre de 2008, volvieron a someterse iniciativas de Ley de Protección de Datos Personales en Posesión de Particulares,[87] las cuales sirvieron de referente para la Ley de 6 de julio de 2010; ello no obstó para que anteriormente se hubiese legislado en entidades federativas, municipios e incluso se concretaran las reformas a los artículos 6º y 16º constitucionales publicadas en el Diario Oficial de la Federación el pasado 20 de julio de 2007 y 1 de junio de 2009, respectivamente, las cuales son el resultado de uno de los procesos más esperados de los últimos años en nuestro país, referente al tema.

3.1.1. Constitución Política de los Estados Unidos Mexicanos

El 20 de julio de 2007, se publico en el Diario Oficial de la Federación, la reforma al artículo 6º constitucional que adiciona un segundo párrafo con siete

[87]Iniciativa del Diputado Miguel Barbosa Huerta, Iniciativa del Diputado Jesús Martínez Álvarez del Grupo Parlamentario de Convergencia, Iniciativa del Diputado David Hernández Pérez del Grupo Parlamentario del PRD, Iniciativa de la Diputada Sheyla Fabiola Aragón Cortés del Grupo Parlamentario del PAN, Iniciativa del Diputado Gustavo Parra Noriega, Iniciativa del Diputado Adolfo Mota Hernández.

fracciones, que constituyen el contenido mínimo del derecho de acceso a la información pública, el cual quedó de la siguiente manera:

> "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:
>
> 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 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."[88]

La propuesta de esta reforma, se inscribió plenamente dentro de la Agenda democrática del país por tratarse de un derecho fundamental, y con el fin de proteger un bien jurídico en sí mismo que es el derecho a saber y a acceder a la información por parte de los ciudadanos.

En este contexto, se consideró importante por un lado, el derecho a informar y emitir mensajes y por el otro, el derecho a ser informado, y cuya fundamentación fueron los antecedentes de la reforma política de 1977 sobre este derecho, y con la interpretación realizada por la Suprema Corte de Justicia de la Nación con motivo

[88] Constitución Política de los Estados Unidos Mexicanos, Porrúa, 2009.

de la investigación en relación con la matanza de Aguas Blancas, Guerrero y en donde fijó la postura de que las autoridades públicas no pueden asumir conductas faltas de ética, al entregar a la comunidad información manipulada, incompleta, condicionada a intereses o grupos o personas, que les vede la posibilidad de conocer la verdad para poder participar libremente en la formación de la voluntad general, puesto que se incurriría en una violación grave a las garantías individuales.[89]

Asimismo la reforma basada en diversos antecedentes,[90] propone el fortalecimiento del derecho a la información veraz y oportuna, garantizando los principios de máxima publicidad y gratuidad, así como facilitar al máximo las solicitudes de acceso a la información sin condiciones, poniendo a disposición del público todas las modalidades para tramitarlas, incluyendo las herramientas electrónicas, creando instancias, autónomas e imparciales para generar una cultura de transparencia, además de las sanciones para los funcionarios que nieguen la información injustificadamente, empero, todo ello garantizando y asegurando la protección de los datos personales.

[89] Semanario Judicial de la Federación y su Gaceta, Novena Época, Pleno, Tomo III, junio de 1996, tesis P. LXXXIX/96, p.513

[90] Declaración de Guadalajara, dentro del Foro Nacional de Transparencia Local, en la que se propone una reforma constitucional que incorpore al texto fundamental el derecho de acceso a la información pública y los requisitos mínimos a cumplir en y por toda la República, 22 de noviembre de 2005; XXVII Reunión ordinaria de la Conferencia Nacional de Gobernación (CONAGO), marzo de 2006; Iniciativa de Chihuahua en el marco del Segundo Congreso de Transparencia Local 10 de noviembre de 2006; Acuerdo de la Junta de Coordinación Política de la Cámara de Diputados, para el fortalecimiento del derecho fundamental de acceso a la información y la transparencia 16 de noviembre de 2006; Aprobación del Pleno de la Cámara de Diputados de la Propuesta de la Junta de Coordinación Política sobre la necesidad de la reforma al artículo 6º de la Constitución, en atención al problema de la heterogeneidad en las leyes de transparencia en México, 28 de noviembre de 2006; Presentación de la Iniciativa de Chihuahua en la Cámara de Diputados, 13 de diciembre de 2006; Reunión de trabajo con el Presidente de la Comisión de Puntos Constitucionales de la Cámara de Diputados, se reconoce la Iniciativa de Chihuahua, 13 de diciembre de 2006; Presentación de la Iniciativa en el Pleno de la Cámara de Diputados y envío a la Comisión de Puntos Constitucionales para su dictamen, 19 de diciembre de 2006; Iniciativa en la Comisión de Puntos Constitucionales. Dictamen en Proceso, 21 de diciembre de 2006; Reunión de la Comisión de Puntos Constitucionales, 7 de febrero de 2007; Proyecto de Decreto que adiciona un Segundo Párrafo con VII fracciones al artículo sexto de la Constitución Política de los estados Unidos Mexicanos; Decreto, 20 de julio de 2007.

De igual manera, el artículo 16 de la Constitución Política fue reformado y adicionado con un segundo párrafo el 1 de junio de 2009, en el cual se reconoce por vez primera el derecho fundamental a la Protección de Datos Personales, conocido como Hábeas Data (sobre los llamados derechos ARCO: acceso, rectificación, cancelación y oposición), quedando como sigue:

"Artículo 16. ...

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.

…."

Esta reforma, tuvo sus orígenes en las iniciativas que el 5 de abril de 2006, el entonces Senador Antonio García Torres (PRI) presentó para adicionar al artículo 16 constitucional, la cual fue dictaminada y aprobada en el Senado el 18 de abril del mismo año, y el 19 de abril de 2006 la minuta fue recibida en la Cámara de Diputados, aprobándose el dictamen respectivo el 20 de septiembre de 2007, el 25 de septiembre del mismo año, la minuta fue turnada a las comisiones respectivas en la Cámara de Senadores. Antes de ser aprobada la minuta presentó dos modificaciones, por lo que se llevó a cabo una reunión de trabajo de la Comisión de Puntos Constitucionales del Senado de la República, en la que al analizarla se estuvo de acuerdo en las modificaciones propuestas.

El 21 de abril de 2009 se declaró la aprobación del decreto al contar con la aprobación de 18 Congresos de los Estados (Aguascalientes, Baja California, Coahuila, Colima, Chiapas, Chihuahua, Durango, Guanajuato, Michoacán, Morelos, Nuevo León, Oaxaca, Sinaloa, Tabasco, Tamaulipas, Tlaxcala, Yucatán y Zacatecas), para finalmente publicarse el 1 de junio de 2009 en el Diario Oficial de la Federación.

La reforma supone el reconocimiento de un nuevo derecho fundamental, independiente de cualquier otro, visto al máximo nivel, la protección de datos personales y el derecho que tiene el individuo de acceder, rectificar, cancelar y oponerse al tratamiento de ellos a nivel federal.

El Dictamen de las Comisiones Unidas de Puntos Constitucionales y Estudios Legislativos del Senado de la República, en su sesión de fecha 5 de noviembre de 2009, sostuvo que con esta reforma se asegura el derecho a la protección de datos personales a nivel nacional, extendiendo su aplicación a todos los niveles y sectores en dos ámbitos:

a) Los datos personales en posesión de los entes públicos.
b) Los datos persones en poder del sector privado.

El mismo artículo establece los supuestos de excepción a este derecho los que deberán preverse en una ley y estar sustentados en razones de seguridad nacional, orden y salud públicos así como para proteger los derechos de terceros.

Con el nuevo texto constitucional se reconoce la necesidad que existe de incluir entre los derechos fundamentales, el de la protección de datos personales, con el objetivo de conferir al gobernado un poder de disposición y control sobre los datos personales que le conciernan

La reforma establecida, pretende consolidar el derecho de protección a la persona en relación con el uso que se dé a su información personal, tanto por entes públicos como privados, es decir, desarrollando su ámbito de aplicación a todos los niveles y sectores.

3.1.2. Legislación Federal

Es importante destacar que hasta julio de 2010, no existía una regulación homogénea en materia de protección de datos personales en posesión de particulares a nivel federal, en consecuencia encontrábamos dispersión de este derecho en distintas normas que de una u otra forma aportaron un conocimiento inocuo del mismo, por ello la promulgación de la LFPDP en julio de 2010, unificó criterios de salvaguarda a tal derecho, reconocido en otros Estados.

Dentro de la legislación federal, se hace mención en cierta medida a la protección, situación en las que apreciaremos la tutela del derecho a la vida privada, sin que ello signifique que tal tutela se encontraba plena, empero de alguna manera se manifestaba, ello tomando en consideración que son incompletas en materia de protección de datos personales, como lo podré evidenciar a continuación, lo vemos en los términos que se mencionan en los ordenamientos siguientes:

a) Código Civil Federal[91]

El artículo 1916 de dicho Código, prevé al daño moral, señalando que por daño moral se entiende *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.*

…

Estarán sujetos a la reparación del daño moral de acuerdo a lo establecido por este ordenamiento y, por lo tanto, las conductas descritas se considerarán como hechos ilícitos:

…

[91] Código Civil Federal, Ediciones ISEF, 2008.

IV. Al que ofenda el honor, ataque la vida privada o la imagen propia de una persona.

b) Código Federal de Procedimientos Civiles[92]

En el presente ordenamiento, se prevé, una disposición que regula la vida privada, en los siguientes términos:

> *"Artículo 90. Los terceros están obligados en todo tiempo, a prestar auxilio a los tribunales en las averiguaciones de la verdad. Deben, sin demora, exhibir documentos y cosas que tengan en su poder, cuando para ello fueren requeridos."*

Aquí vemos que a toda persona que requiera la autoridad jurisdiccional, está obligada a exhibir todo tipo de información, incluyendo datos personales, cuando así se le ordene.

c) Código Penal Federal [93]

Dentro del presente ordenamiento jurídico federal, se prevé el capítulo denominado "Delitos en materia de Vías de Comunicación y Violación de la Correspondencia" la cual destina diversos numerales, encaminados a la protección de la vida privada, a saber:

> *Artículo 167. Se impondrá de uno a cinco años de prisión y de cien a diez días multa:*
>
> *…*
>
> *VI. Al que dolosamente o con fines de lucro, interrumpa o interfiera las comunicaciones, alámbricas, inalámbricas o de fibra óptica, sean*

[92] Código de Procedimientos Civiles, Ediciones ISEF, 2008.
[93] Código Penal Federal, Ediciones ISEF, 2008

telegráficas, telefónicas o satelitales, por medio de las cuales se transfieren señales de audio, de video o de datos.

Por otra parte, vemos en cuanto a la violación de la correspondencia el siguiente:

Artículo 173. Se aplicarán de tres a ciento ochenta jornadas de trabajo a favor de la comunidad:

4. *Al que abra indebidamente una comunicación escrita que no esté dirigida a él.*
5. *Al que indebidamente intercepte una comunicación escrita que no esté dirigida a él, aunque la conserve cerrada y no se imponga de su contenido*

Igualmente, con la reforma de 1999, se crea un nuevo capítulo denominado "Revelación de secretos y acceso ilícito a sistemas y equipos de informática", además del segundo capítulo llamado "Acceso ilícito a sistemas y equipos de computo", así encontramos en el artículo 211 bis 1, lo siguiente:

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

Esta norma constituye un avance en materia de delitos informáticos, aunque no del todo plena, sin embargo, se va llevando a cabo una estructuración, en materia de protección de información, archivos, y desde luego, datos personales.

d) Código Federal de Procedimientos Penales[94]

Por su parte el presente Código señala con relación al tópico que nos interesa, una clara protección a la vida privada del acusado, en los términos siguientes:

> *Artículo 192. No se obligará a declarar al tutor, curador, pupilo o cónyuge del acusado, ni a sus parientes por consanguinidad o afinidad en la línea recta ascendente o descendente, sin limitación de grados, y en la colateral hasta el tercero inclusive, ni a los que estén ligados con el acusado por amor, respeto o gratitud. Si estas personas tuvieran voluntad de declarar, se les recibirá su declaración y se hará constar esta circunstancia.*

e) Código Fiscal de la Federación

Por lo que respecta esta norma federal, encontramos lo que se denomina el secreto fiscal, el cual es considerado como una obligación a cargo de la persona, entidad, autoridad, etc., de guardar información personal y patrimonial que alguien le haya proporcionado, ya sea por alguna actividad mercantil, o porque alguna autoridad se la haya remitido, dicho secreto se encuentra regulado en el artículo 69, y se prevé de la siguiente manera:

> *Artículo 69. El personal oficial que intervenga en los diversos trámites relativos a la aplicación de las disposiciones tributarias estará obligado a guardar absoluta reserva en lo concerniente a las declaraciones y datos suministrados por los contribuyentes o por terceros con ellos relacionados, así como los obtenidos en el ejercicio de las facultades de comprobación.*
>
> *...*

[94] Código de Procedimientos Penales, Ediciones ISEF, 2008

f) Código Federal de Instituciones y Procedimientos Electorales[95]

El presente Código prevé de manera categórica la confidencialidad de los datos personales, que se encuentren en el Registro Federal de Electores, en contraposición al derecho a la información en los términos siguientes:

Artículo 135.

...

6. *Los documentos, datos e informes que los ciudadanos proporcionen al Registro Federal de Electores, en cumplimiento de las obligaciones que les impone la Constitución y este Código, serán estrictamente confidenciales y no podrán comunicarse o darse a conocer, salvo cuando se trate de juicios, recursos o procedimientos en que el Instituto Federal Electoral fuese parte, para cumplir con las obligaciones previstas por este Código en materia electoral y por la Ley General de Población en lo referente al Registro Nacional Ciudadano o por mandato del juez competente.*

Por otro lado, el artículo 155 del propio ordenamiento, prevé en listas nominales el nombre de los electores, mismos datos, que aunque no lo menciona el artículo, deberán quedar resguardados.

Artículo 155. Las listas nominales de electores son las relaciones elaboradas por la Dirección Ejecutiva del Registro Federal de Electores que contienen el nombre de las personas incluidas en el Padrón Electoral, agrupadas por distrito y sección, a quienes se ha expedido y entregado su Credencial para Votar.

Artículo 156.

...

[95] Código Federal de Instituciones y Procedimientos Electorales, IFE, 2006.

4. *Las listas nominales de electores que se entreguen a los partidos políticos serán para su uso exclusivo y no podrán destinarse a finalidad u objeto distinto al de revisión del Padrón Electoral. Cuando un partido político no desee conservarlas, deberá reintegrarlas al Instituto Federal Electoral.*

Asimismo, el voto de los mexicanos en el extranjero también crea listas nominales garantizándose su confidencialidad, en los términos previstos en el artículo 280:

...

3. *En todo caso, el personal del Instituto y los partidos políticos están obligados a salvaguardar la* ***confidencialidad de los datos personales*** *contenidos en las listas nominales de electores residentes en el extranjero. La Junta General Ejecutiva dictará los acuerdos e instrumentará las medidas necesarias para tal efecto.*

g) Ley Federal de Protección al Consumidor

La reforma de la Ley Federal de Protección al Consumidor, de 4 de febrero de 2004, consignó dos principios fundamentales en materia de protección contra la publicidad, y el conocido spam; en segundo lugar determinó la protección de los consumidores en las operaciones en las que se utilicen medios electrónicos o cualquier otra tecnología, y la adecuada utilización de los datos. En la presente ley, se resguardan de modo alguno los datos personales, en las transacciones comerciales, restringiendo de igual manera el empleo de información sobre los consumidores con fines de marketing.

Veamos de qué manera se da esta regulación:

Artículo 16. Los proveedores y empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios están obligados a informar gratuitamente a cualquier persona que lo solicite si mantienen información acerca de ella. De existir dicha información, deberán ponerla a su disposición si ella misma o su representante lo solicita, e informar acerca de qué información han compartido con terceros y la identidad de esos terceros, así como las recomendaciones que hayan efectuado. La respuesta a cada solicitud deberá darse dentro de los treinta días siguientes a su presentación. En caso de existir alguna ambigüedad o inexactitud en la información de un consumidor, éste se la deberá hacer notar al proveedor o a la empresa, quien deberá efectuar dentro de un plazo de treinta días contados a partir de la fecha en que se le haya hecho la solicitud, las correcciones que fundadamente indique el consumidor, e informar las correcciones a los terceros a quienes les haya entregado dicha información.

Para los efectos de esta ley, se entiende por fines mercadotécnicos o publicitarios el ofrecimiento y promoción de bienes, productos o servicios a consumidores.

Artículo 17. En la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor, de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la Procuraduría.

El consumidor podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de

trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad. Asimismo, el consumidor podrá exigir en todo momento a proveedores y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial.

Disposición, la anterior, que manifiesta la protección en contra de los correos no deseados con fines de publicidad o marketing.

Artículo 18bis. Queda prohibido a los proveedores y a las empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios y a sus clientes, utilizar la información relativa a los consumidores con fines diferentes a los mercadotécnicos o publicitarios, así como enviar publicidad a los consumidores que expresamente les hubieren manifestado su voluntad de no recibirla o que estén inscritos en el registro a que se refiere el artículo anterior. Los proveedores que sean objeto de publicidad son corresponsables del manejo de la información de consumidores cuando dicha publicidad la envíen a través de terceros.

Nuevamente, encontramos el derecho a protección del consumidor de no recibir publicidad no deseada, constituyendo una prohibición expresa a los proveedores.

Por su parte, el artículo 76 bis, de la citada ley, señala en su fracción I, que *el proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente.*

La fracción II del citado artículo impone la obligación a los proveedores de medidas que garanticen la seguridad y confidencialidad de la información que los consumidores les proporcionen: *el proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos.*

La Ley Federal de Protección al Consumidor, constituyó un avance notable en el derecho a la protección de datos personales en materia de publicidad, ya que sin haber estado regulado constitucionalmente, ya se acercaba a los denominados derechos ARCO, y a los principios que rigen en la materia, así se desprende de los artículos antes invocados. Esta legislación federal fue un acierto, que muchos de las Leyes (en su mayoría) no preveía, sin embargo, constituye un antecedente importante sobre la regulación de ellos ya que, aun con la LFPDP, no se prevé la protección de datos tratándose de publicidad y marketing, sino que se delega esta función en materia comercial para su correspondiente regulación a un organismo Administrativo (Secretaria de Economía).

h) Ley Federal de Telecomunicaciones[96]

Este ordenamiento regula la confidencialidad que debe existir en la transmisión de la información que se realice mediante los servicios de red y del espectro radio eléctrico. Veamos de qué manera lo hace:

Artículo 49. La información que se transmita a través de las redes y servicios de telecomunicaciones será confidencial, salvo aquella que, por su propia naturaleza sea pública, o cuando medie orden de autoridad competente.

[96] Ídem.

En abril de 2010, se presentó una Iniciativa de ley, por el Diputado Javier Corrales, en la cual como parte del proceso de reforma democrática del Estado se propuso la creación de una nueva Ley Federal de Telecomunicaciones y de Contenidos Audiovisuales que regule el uso, aprovechamiento y explotación del espectro radioeléctrico, las redes de telecomunicaciones, así como la prestación de servicios de telecomunicaciones y los contenidos audiovisuales, manteniendo en este sentido como uno de los ejes fundamentales de la iniciativa el garantizar que en la prestación de los servicios de telecomunicaciones, se respeten los derechos de los usuarios, en particular la protección de los datos personales; asimismo mantener la reserva y protección de las bases de datos personales, mismas que no podrán ser usadas con fines diferentes a los señalados en las leyes, dando conexidad con el principio de calidad de los datos.

i) Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental[97]

Esta ley, constituye el primer intento en materia federal, de una protección de datos personales, sin que llegue a regularlo de manera exhaustiva, y tan sólo es enunciativa de los conceptos y principios que rigen a los datos personales, derivados del derecho a la información pública.

El artículo 3º, define el concepto de datos personales:

Para los efectos de esta Ley se entenderá por:

III. Datos Personales. 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

[97] Ídem.

religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad.

Cabe aclarar que esta ley regula la protección de datos siempre y cuando se encuentren en poder de un organismo gubernamental, no así de particulares, puesto que la citada ley sólo obliga a los sujetos de gobierno; por su parte, el artículo 18 señala lo que se considera como información confidencial, el artículo 20, prevé la obligación de incorporar medidas de seguridad y el 21, impone la obligación del responsable de no difundir o comercializar los datos personales.

Artículo 18. Como información confidencial se considerará:

I. La entregada con tal carácter por los particulares a los sujetos obligados, de conformidad con 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…

Artículo 20. Los sujetos obligados serán responsables de los datos personales y, en relación con éstos deberán:

…

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

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 medio de autenticación similar, del os individuos a que haga referencia la información.

En dicha norma, se establece en el artículo 24 que cualquier persona puede solicitar ante las Unidades de Enlace de las dependencias, información sobre sus datos personales, y el artículo 25, invoca que cualquier persona podrá solicitar por sí o por medio de su representante legal, a través de las Unidades de Enlace de las dependencias y entidades, la modificación de sus datos personales en el sistema de que se trate.

Asimismo, el Instituto Federal de Acceso a la Información Pública Gubernamental, ha elaborado una serie de lineamientos, con el fin de establecer particularidades a observar por parte de los órganos gubernamentales en la recepción, procesamiento, trámites, resolución, notificaciones, etc., con relación al manejo de los datos personales,[98] a saber son:

- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares.
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental que formulen los particulares, así como en su resolución y notificación, y la entrega de la información en su caso, con exclusión de las solicitudes de acceso a datos personales y su corrección.
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos.
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal para notificar al Instituto el listado de sus sistemas de datos personales.
- Lineamientos de protección de datos personales

j) Ley General de Salud[99]

En esta Ley, el artículo 77 bis, se establece el trato de confidencialidad a favor del beneficiario del Sistema de Protección Social, con ello se protegen los denominados datos sensibles.

---

[98] Instituto Federal de Acceso a la Información Pública Gubernamental. *Lineamientos. IFAI, México, 2003.*
[99] Ídem.

Artículo 77. Los beneficiarios del Sistema de Protección Social en Salud tendrán además de los derechos establecidos en el artículo anterior, los siguientes:

…

X. Ser tratado con confidencialidad.

Con relación a esta normativa, de igual manera, la NOM 168-SSA1-1998, establece los criterios científicos, tecnológicos y administrativos obligatorios en la elaboración, integración, uso y archivo del expediente clínico:

5. En todos los establecimientos para la atención médica, la información contenida en el expediente clínico será manejada con discreción y confidencialidad, atendiendo a los principios científicos y éticos que orientan la práctica médica y sólo podrá ser dada a conocer a terceros mediante orden de autoridad competente, o a CONAMED, para arbitraje médico.

k) Ley General de Población[100]

La Ley General de Población, establece en su artículo 98, la obligación de los mexicanos de inscribirse en el Registro Nacional de Población, a fin de obtener la Cédula de Identidad Ciudadana.

Al ser parte de este registro, se nos asigna una Clave Única de Registro de Población (CURP), misma que constituye un número único de identificación, que permite, por sus solas características, identificar a la persona de que se trata, junto sus datos de carácter personal.

[100] Ídem.

Podemos concluir que la heterogeneidad de las legislaciones que se han situado a nivel federal y a nivel municipal en casi toda la República Mexicana, se constituyeron –por así decirlo-, por falta de una guía de jerarquización para la construcción del Derecho a la Protección de Datos Personales, situación que hacía sumamente complicada la defensa de este derecho de tercera generación, empero con la aparición de la LFPDP, evolucionaron los criterios y argumentos, disminuyendo una dificultad tan grande, la pluralidad legislativa.

El problema de la dispersión legislativa sobre la materia ocasiona una disparidad de interpretaciones que no adminiculan criterios base para comenzar a consolidar el derecho fundamental a la protección de datos personales, las normas federales expuestas toman consideraciones relativas a la privacidad de las personas, no así concretamente en la protección de datos, salvo algunas legislaciones (Código Electoral, Ley Federal de Acceso y Transparencia a la Información Pública Gubernamental, Ley Federal de Protección al Consumidor).

Esto ocasiona distintas acepciones del derecho que se estudia, lo cual no permite una evolución de los argumentos, y ocasiona que la legislación pueda ser deficiente o insuficiente en su conteniendo para salvaguardar el derecho que se busca proteger, pues no se prevén todos los supuestos de lesión.

Todo ello ocasiona que no pueda mostrarse un proceso de aplicación que se halle articulado, el propio ordenamiento jurídico heterogéneo implica diversas exigencias lógicas y jurídicas de aplicación, que establecen que esa aplicación no se produce en el mundo como un hecho aislado pese a que los ordenamientos jurídicos no homogenicen con otros. Ello motiva que al analizar la norma aisladamente, en su aplicación se comprenda una dificultad de la autoridad para destinarla, trayendo por consiguiente problemas del ordenamiento en su sistema, siendo totalmente limitantes en relación con su contenido que en ocasiones puede ser incoherente con otros, sin que guarden relación entre sí y no se satisfaga de

principio de compatibilidad,[101] con que deben cumplir las normas que conforman el sistema jurídico. Esto último, constituye una salvaguarda de la unidad y coherencia de la norma y en consecuencia de los principios instrumentales del derecho: el orden y la seguridad.

Lo anterior implica que pudieren encontrarse una de las dificultades particulares en la existencia de las normas (contradicciones o antinomias), rompiendo con el marco jurídico, el establecimiento y orden que supone el derecho debe aportar y con ello evitar que el sistema jurídico sea incompleto o insuficiente por tener lagunas y se deje de cumplir con la característica de la plenitud del ordenamiento jurídico, la unidad y la coherencia.

La exposición precedente nos permitirá desarrollar la normatividad en materia federal, que en algunos casos envuelve el derecho de protección de datos personales, en otros atendiéndolo como derecho a la privacidad, y en otras más, con la postura de confidencialidad de datos, sin embargo, la legislación en materia federal, no es la única que pretende hacer alusión en la materia, también encontramos leyes estatales que, poco a poco, se fueron consolidando en este tópico, como lo veremos en el siguiente tema.

3.1.3. Legislación Estatal

El derecho a la protección de los datos personales, ha sido una regulación de carácter sectorial, es decir, su adaptación en los sistemas jurídicos en las distintas regulaciones federativas no es creciente a la par.

Hoy en día, tan sólo cuatro Estados de la República Mexicana, el Distrito Federal, Colima, Guanajuato y Oaxaca cuentan con una Ley Estadual de Protección de Datos Personales teniendo como sujetos obligados a los organismos públicos (excepto Colima que regulaba también a los entes particulares, misma que deberá

[101] Alvárez Ledesma, Mario I. *Introducción al Derecho.* Mc Graw-Hill, 2004, Pág. 259

ser modificada según artículo quinto transitorio de la LFPDP), sin dejar de soslayar que las demás entidades federativas regulan la protección de datos y/o la información confidencial, dentro de sus respectivas leyes de Acceso a la Información Pública.

Respecto de las leyes que regulan el tratamiento de datos personales, de manera autónoma, encontramos las siguientes:

- **Ley de Protección de Datos Personales del Estado de Colima**[102]
- **Ley de Protección de Datos Personales para el Distrito Federal**
- **Ley de Protección de Datos Personales para el estado y los Municipios de Guanajuato**
- **Ley de Protección de Datos Personales del Estado de Oaxaca**

*****

- **Ley de Protección de Datos Personales del Estado de Colima**

Esta ley, se constituyó como primera en la materia a nivel estatal, y considera entre sus numerales lo siguiente:

> *Artículo 1. 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.*
>
> *Artículo 2. 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* (éste artículo deberá ser modificado, en términos del quinto

[102] Deberá ser reformada en términos del artículo quinto transitorio de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares. *"En cumplimiento a lo dispuesto por el artículo tercero transitorio del Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, publicado en el Diario Oficial de la Federación el 30 de abril de 2009, las disposiciones locales en materia de protección de datos personales en posesión de los particulares se abrogan, y se derogan las demás disposiciones que se apongan a la presente Ley".*

transitorio de la LFPDP de 6 de julio de 2010).

- **Ley de Protección de Datos Personales para el Distrito Federal**

El 3 de octubre de 2008, se público en la Gaceta Oficial del Distrito Federal la Ley de Protección de Datos Personales para el Distrito Federal, como una respuesta a la exigencia social en la defensa de los datos personales, ley que tiene por objeto lo siguiente:

Artículo 1. La presente Ley es de orden público e interés general y tiene por objeto establecer los principios, derechos, obligaciones y procedimientos que regulan la protección y tratamiento de los datos personales en posesión de los entes públicos.

- **Ley de Protección de Datos Personales para el estado y los Municipios de Guanajuato**

Por su parte la legislación de Guanajuato señala en su artículo 1:

Artículo 1. La presente ley es de orden público e interés general y tiene por objeto garantizar la protección de los datos personales en poder de los sujetos obligados a que se refiere este ordenamiento.

- **Ley de Protección de Datos Personales del Estado de Oaxaca**

El 23 de agosto de 2008 se publicó la presente ley, cuyo artículo 1º prevé que es de orden público e interés social y cuyo objeto es:

I. Garantizar la protección de datos personales en poder de los sujetos obligados a que se refiere el ordenamiento.
II. Regular el registro, almacenamiento, distribución, transmisión, modificación, eliminación, duración, y en general, el tratamiento de

los datos personales asentados en archivos, registros bases de datos u otros medios similares en soporte manual o automatizado y a toda modalidad de uso posterior de estos datos por el sector público.

Podemos observar, sin lugar a dudas, que en las legislaciones anteriormente señaladas, se coincide plenamente en la importancia de la protección de datos personales, todo ello, derivado de la necesidad de brindar al ciudadano una protección adecuada contra el posible mal uso de la información que le concierne.

Las presentes legislaciones, son el resultado de un minucioso análisis del derecho, previsto por nuestra Constitución Federal, de todas ellas se han realizado profusos pronunciamientos de la sociedad, ya sea sobre sus respectivos contenidos y alcances, o bien incluso sobre sus limitaciones, pero en todas ellos apreciamos que la coincidencia resulta unánime, la protección del derecho fundamental.

3.1.4. Normatividad conexa

Los Gobiernos Municipales, no han sido ajenos a la normatividad en esta materia, han logrado implementar Reglamentos[103], los cuales garantizan el derecho a la información, a la par que la protección de datos de carácter personal, así tenemos los siguientes:

b) Coahuila de Zaragoza

a. Torreón
    i. Reglamento de Transparencia y Acceso a la Información Pública del Municipio de Torreón *(Capítulo IV Protección de Datos Personales)*
b. Piedras Negras
    i. Reglamento de Transparencia y Acceso a la Información del Municipio de Piedras Negras *(Capítulo IV Protección de Datos Personales)*
c. Ramos Arizpe
    i. Reglamento de Transparencia y Derecho a la Información

[103] Legislación consultada en el sitio http://www.ifai.org.mx/Vinculacion/legisMunicipal

del Municipio de Ramos Arizpe *(Capítulo IV Protección de Datos Personales)*

c) Estado de México

a. Metepec

   i. Reglamento de Transparencia y Acceso a la Información Pública del Gobierno Municipal de Metepec *(Capítulo IV Protección de Datos Personales)*

b. Tlalnepantla de Baz

   i. Reglamento Municipal de Transparencia y Acceso a la Información Pública de Tlalnepantla de Baz *(Capítulo III Protección de Datos Personales)*

d) Jalisco

a. Guadalajara

   i. Reglamento de Transparencia y Acceso a la Información Pública del Municipio de Guadalajara *(Capítulo IV, Información Pública de Acceso Limitado, Sección Segunda Derechos de Hábeas Datas)*

b. Zapotlán el Grande

   i. Reglamento de Transparencia y Derecho a la Información del Municipio de Zapotlán el Grande (Capítulo IV. Protección de Datos Personales)

e) Nuevo León

a. Monterrey

   i. Reglamento de Derecho de Acceso a la Información Pública del Municipio de Monterrey *(Capítulo IV Protección de Datos Personales)*

b. San Pedro Garza García

   i. Reglamento de Acceso a la Información Pública Gubernamental del Municipio de San Pedro Garza *(Capítulo V Protección de Datos Personales)*

f) Guanajuato

a. Celaya

   i. Reglamento de la Unidad de Acceso a la Información Pública del Municipio de Celaya *(Capítulo VII. Del Procedimiento de Acceso a la Información Pública y datos Personales)*

b. San Felipe

    i. Reglamento de Acceso a la Información Pública del Municipio de San Felipe *(Capítulo VIII. Del Procedimiento para la corrección de datos)*

c. San Miguel de Allende

    i. Reglamento de Transparencia y Acceso a la Información Pública del Municipio de Allende *(Capítulo IV Protección de Datos Personales)*

d. Victoria

    i. Reglamento de Acceso a la Información Pública para el Municipio de Victoria *(Capítulo VII del Procedimiento para la corrección de Datos)*

g) Sinaloa

a. Cosalá

    i. Reglamento de la Ley de Acceso a la Información Pública del Estado de Sinaloa para el Municipio de Cosalá *(Capítulo VI. Del Ejercicio del Derecho de Hábeas Data)*

b. Culiacán

    i. Reglamento de la Coordinación de Enlace de Acceso a la Información Pública del Municipio de Culiacán *(Capítulo VIII. Del Ejercicio del Derecho de Hábeas Data)*

c. Rosario

    i. Reglamento de la Ley de Acceso a la Información Pública del Estado de Sinaloa para el Municipio de Rosario *(Capítulo VI. Del Ejercicio del Derecho de Hábeas Data)*

d. Escuinapa

    i. Reglamento de la Ley de Acceso a la Información Pública del Estado de Sinaloa para el Municipio de Escuinapa *(Capítulo VI. Del Ejercicio del Derecho de Hábeas Data)*

e. Mazatlán

    i. Reglamento de la Ley de Acceso a la Información Pública del Estado de Sinaloa para el Municipio de Mazatlán *(Capítulo VI. Del Ejercicio del Derecho de Hábeas Data)*

f. Mocorito

    i. Reglamento de la Ley de Acceso a la Información Pública del Estado de Sinaloa para el Municipio de Mocosito *(Capítulo VI. Del Ejercicio del Derecho de Hábeas Data)*

h) Durango

a. Durango

i. Reglamento de Transparencia y Acceso a la Información Pública para el Municipio de Durango *(Capítulo IV. De la clasificación de la Información Pública Municipal. Sección III. Información reservada. IV Información sensible. V. Información confidencial).*

b. Gómez Palacio

i. Reglamento de Acceso a la Información Pública del Municipio de Gómez Palacio Durango *(Capítulo II. De la información clasificada como reservada, confidencial y sensible).*

3.1.5. Ley Federal de Protección de Datos Personales en Posesión de los Particulares

El 5 de julio de 2010, se publicó en el Diario Oficial de la Federación el Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y se reformaron los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Título Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

Con ello se desarrolla en nuestro país un nuevo modelo de protección de este derecho humano de tercera generación, consolidándose todas y cada una de las iniciativas propuestas por los distintos grupos parlamentarios,[104] y dejando atrás el modelo híbrido de protección de datos personales en México.

[104] Gaceta Parlamentaria, año IV, número 832, viernes 7 de septiembre de 2001. PRESENTADA POR EL DIPUTADO MIGUEL BARBOSA HUERTA, DEL GRUPO PARLAMENTARIO DEL PARTIDO DE LA REVOLUCION DEMOCRATICA, EN LA SESION DEL JUEVES 6 DE SEPTIEMBRE DE 2001. Gaceta Parlamentaria, Cámara de Diputados, número 1895-I, jueves 1 de diciembre de 2005. INICIATIVA DE LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES, POR EL DIPUTADO JESÚS MARTÍNEZ ÁLVAREZ, DEL GRUPO PARLAMENTARIO DE CONVERGENCIA.
Gaceta del Senado, No. 164, Tercer Año de ejercicio, segundo periodo ordinario, Miércoles 5 de abril de 2006. INICIATIVA DEL SENADOR ANTONIO GARCÍA TORRES, DEL GRUPO PARLAMENTARIO DEL PARTIDO REVOLUCIONARIO INSTITUCIONAL, LA QUE CONTIENE PROYECTO DE DECRETO QUE REFORMA EL ARTÍCULO 16 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS.
Gaceta Parlamentaria, Cámara de Diputados, número 1953-I, jueves 23 de febrero de 2006. INICIATIVA DE LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES, A CARGO DEL DIPUTADO DAVID

Los miembros de la Comisión Dictaminadora en el Congreso, coincidieron en el surgimiento de un nuevo derecho fundamental a la protección de datos personales, amén de que la Constitución Política de los Estados Unidos Mexicanos, lo había reconocido con la reforma del 1 de junio de 2009 en el artículo 16, y tomando en consideración las exigencias internacionales sobre estándares de protección sobre datos personales y su tratamiento, mismo que fue debate de la Cumbre Mundial de la Sociedad de la Información en el que se hace un llamamiento a todas las partes a fin de garantizar los datos personales mediante la *adopción de una legislación,* la aplicación de marcos de colaboración, mejores prácticas y medidas tecnológicas y de autorregulación por parte de las empresas y usuarios.

Atendiendo a los reclamos de los instrumentos internacionales sobre la materia, se tomó en consideración lo establecido por el artículo 12 de la *Declaración Universal de los Derechos del Hombre*; en el mismo sentido lo dispuesto por el artículo 8 del *Convenio para la Protección de los Derechos y Libertades Fundamentales*; el artículo 17 del *Pacto Internacional de Derechos Civiles y Políticos;* y en el mismo tenor también se adhirió a la *Convención Americana sobre Derechos Humanos* en su artículo 11 apartado 2; el *Convenio 108 del Consejo de Europa para la Protección de la Personas con respecto al Tratamiento Automatizado de Datos de carácter Personal,* la *Directiva 95/46 de la Comunidad Europea sobre Protección de Personas Físicas en lo que respecta al Tratamiento de Datos de Carácter Personal y Libre Circulación de éstos* y la *Carta de Derechos Fundamentales de la Unión Europea*, no fueron la excepción.[105]

HERNÁNDEZ PÉREZ, DEL GRUPO PARLAMENTARIO DEL PRI.
Gaceta Parlamentaria, Cámara de Diputados, número 1972-I, miércoles 22 de marzo de 2006. INICIATIVA DE LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES, A CARGO DE LA DIPUTADA SHEYLA FABIOLA ARAGÓN CORTÉS, DEL GRUPO PARLAMENTARIO DEL PAN.

[105] Artículo 12. Ninguna persona podrá ser objeto de injerencias en su vida privada y familiar, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación, gozando del derecho a la protección de la ley contra tales injerencias y ataques.
Artículo 8. Toda persona tiene derecho al respeto de su vida privada y familiar de su domicilio y correspondencia.

Las leyes de otros países sirvieron de igual manera para reforzar la sanción de la Ley de Protección de Datos Personales en México, por ejemplo: Alemania, Francia, España, Argentina, Paraguay.

Entre las razones de creación de la ley, cabe destacar la necesidad de unificar la tutela de un derecho fundamental en todo el país en cuanto derechos, principio y procedimientos de protección, evitando con ello una dispersión legislativa al expedirse tantas leyes como entidades federativas en la República Mexicana haya, y como una segunda exposición el comercio internacional que exige a nuestro país el contar con una legislación uniforme en sus relaciones internacionales, con el fin de ampliar el comercio con bloques económicos de la importancia de la Unión Europea.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares, consta de 69 artículos, divididos en XI Capítulos y 8 Transitorios, mismos que pueden ser observados en el ANEXO I.

3.2. Legislación aplicable en España

La regulación normativa en la comunidad española es basta sobre el tema, diversas normas han sido sancionadas a nivel estatal para proteger este derecho, y a nivel federal la Ley 15/99 que regula el Tratamiento de Datos Personales ha sido referente para otras legislaciones en América (Argentina y México), el objeto de esta ley, es garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Artículo 17. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
Artículo 11. 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.

El Derecho Fundamental protegido por esta Ley es de los llamados de tercera generación y se encuentra recogido en el Art. 18.4 de la Constitución Española, como lo mencionaré a continuación.

3.2.1. Constitución Española

El artículo 18.4 de la Constitución, establece que la Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Esta protección se cumple en el ámbito de la automatización de la información sobre los datos personales y familiares, ante la preocupación de un posible abuso en la utilización de las nuevas tecnologías, lo que da lugar a plantearse qué posibilidades de protección tiene una persona frente a la utilización de sus datos personales y cuáles son los límites de esta protección.

La Constitución Española establece un derecho de protección frente al uso de la informática constituyendo un derecho fundamental especialmente protegido respecto al tratamiento informático de datos de carácter personal, tomando en cuenta el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter Personal, celebrado en Estrasburgo, el 28 de enero de 1981, y ratificado por España el 27 de enero de 1984 (BOE de 15 de noviembre de 1985), y la doctrina del Tribunal Constitucional conforme a los principios de los Tratados Internacionales ratificados por España, así como el artículo 12 de la Declaración Universal de derechos Humanos y el artículo 8 del convenio Europeo de 1995.

3.2.2. Ley 15/1999 de Protección de Datos Personales

El objeto de la LOPD es garantizar y proteger, las libertades públicas y los derechos fundamentales de las personas físicas, con respecto al tratamiento automatizado de sus datos personales.

Las ideas centrales de la LOPD 15/99 se encuentran recogidas en los siguientes puntos:

- **(Principio) Calidad de los datos (art.4 LOP):** Los datos deben adecuarse a la finalidad para los que fueron conseguidos, ser exactos, no mantenerse más allá de su uso normal y ser recogidos de forma lícita. La exactitud de los datos no se extiende a los cambios que no pudieron ser conocidos por el responsable del fichero, por ejemplo cambio de dirección, pero si deberán ser corregidos una vez notificado por el titular.
- **(Acceso) Derecho de información (art.5 LOP):** Cuando se recaben datos de un interesado, este deberá saber de la existencia del fichero, de su finalidad y de los destinatarios. De la obligatoriedad o no de facilitarlos, así como de su derecho de acceso, rectificación, cancelación y oposición. Por último deberá conocer la identidad y dirección del responsable del tratamiento o de su representante.

  Cuando los datos sean recabados de terceros, el responsable tendrá tres meses para informar al interesado. Si proceden de fuentes públicas, se deberá entonces informar del origen de los mismos y del responsable del fichero.
- **(Principio) Consentimiento inequívoco del afectado (art. 6 LOPD):** Las exclusiones vienen tasadas en el art 6.2, indicando que no será necesario, cuando se recojan los datos para funciones propias de las administraciones públicas, cuando se refieran a las partes de un contrato o precontrato, de una relación laboral o administrativa y sean necesarias para su mantenimiento y cumplimiento. Esto no impide que el consentimiento sea revocado por su titular.
- **(Datos Sensibles) Datos especialmente protegidos (art. 7 LOP):** Es preciso el consentimiento expreso y por escrito para recabar los datos relativos ideología, afiliación política y sindical, religión, salud, vida sexual y origen racial, salvo que se trate de un partido político, sindicato, asociación o fundación, o en el caso de la salud sea para prestar asistencia sanitaria.

- **(Principio) Seguridad de los datos (art. 9 LOPD):** El responsable del fichero y en su caso el encargado del tratamiento adoptarán las medidas físicas y tecnológicas apropiadas (o reglamentariamente establecidas) para garantizar la seguridad de los mismos en función de su importancia y sensibilidad.
- **(Principio) Obligación de secreto (art.10 LOPD):** El responsable del fichero y cualquier persona que tenga acceso a su tratamiento tienen una obligación de secreto profesional con respecto a los datos.
- **(Transferencia de Datos) Comunicación de los datos a terceros (art.11 LOPD):** Solo podrán cederse datos en cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento informado del interesado. Las principales excepciones son cuando se trate de cesión de datos públicos o ligados a una relación contractual, entre administraciones públicas y afines.

  La cesión entre empresas de un mismo grupo, se consideran cesión a terceros y por tanto sujetas a las normas de la LOPD.
- **Cesión de datos para la prestación de un servicio (art. 12 LOP):** No se considera cesión de datos, cuando mediante contrato, el responsable del tratamiento de datos los cede a un encargado para la realización de un servicio. En el contrato se deberá especificar, la finalidad del servicio, prohibición de cederlo a terceros, obligación de cumplir con las instrucciones del responsable, las medidas de seguridad a adoptar y la obligación de devolver o destruir los datos y soportes.
- **(Derechos de los Interesados) (art.13 a 19 LOPD):**
    - **Derecho de impugnación de valoraciones:** De especial relevancia para las operaciones de aceptación o denegación de créditos, el titular podrá obtener información sobre los criterios de valoración y el programa utilizado en el tratamiento de datos realizado para adoptar la decisión e impugnar los actos administrativos o decisiones privadas que se basen en una valoración de sus datos privados.
    - **Derecho de consulta al Registro General de Protección de Datos.**
    - **Derecho de acceso:** Cualquier titular tiene derecho de forma gratuita a acceder a sus datos.
    - **Derecho de rectificación y cancelación:** En caso de ejercitarse el derecho de rectificación, este deberá ejecutarse en 10 días. En caso de cancelación, los datos quedarán bloqueados de forma que no puedan ser usados, durante el tiempo mínimo que las legislaciones específicas así lo indiquen, 15 años para datos de clientes, 6 años para datos de proveedores y suministradores y 5 años para datos de empleados.

- **Derecho de oposición:** Es un derecho que asiste a cualquier titular salvo que alguna ley establezca lo contrario.

- **Inscripción de los ficheros:** Todo fichero conteniendo datos de personas físicas, organizado de forma lógica, ya sea en soporte informático o en papel, así como sus modificaciones y supresiones deben ser inscritos en el Registro General de Protección de Datos. Con ello se persigue un conocimiento público de los mismos, facilitar los derechos de los titulares y ejercitar la labor supervisora de la APD.
- **Infracciones y sanciones de ficheros de titularidad privada (art. 44 y 45 LOP)**

3.2.3. Legislación Estatal en España por sectores de actividad[106]

3.2.3.1. Administración Pública

- **Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.**

La presente ley tiene como fundamento el reconocimiento general del derecho de acceder electrónicamente a las Administraciones Públicas, empero la progresiva utilización de medios electrónicos suscita la cuestión de la privacidad de los datos que se facilitan en relación con un expediente concreto pero que, archivados de forma electrónica como consecuencia de su propio modo de transmisión, hacen emerger el problema de su uso no en el mismo expediente en el que es evidente, desde luego, pero, sí la eventualidad de su uso por otros servicios o dependencias de la Administración o de cualquier Administración o en otro expediente. Las normas de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal sirven de base para establecer previsiones que garanticen la utilización de los datos obtenidos de las comunicaciones electrónicas para el fin preciso para el que han sido remitidos a la Administración.

[106] Legislación consultada en el sitio https://www.agpd.es/portalweb/canaldocumentacion/legislacion/index-ides-idphp.php

- **Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado (Disposición Adicional 10).**

Esta ley únicamente remite a la organización estructura y funcionamiento de las Instituciones Públicas de la Administración General, entre ellas la Agencia de Protección de Datos, rigiéndose por su regulación específica y supletoriamente por ésta pero sin hacer más pronunciamiento al respecto.

La Agencia de Protección de Datos, es un organismo público con personalidad jurídica propia y con facultades públicas y privadas, actúa con independencia de las administraciones públicas en el ejercicio de sus funciones, así lo establece la disposición adicional Décima de esta Ley.

"Disposición Adicional Décima. Régimen Jurídico de determinados organismo públicos.

1. *... La Agencia de Protección de Datos,..." El Gobierno y la Administración General del Estado ejercerán respecto de tales organismos las facultades que la normativa de cada una de ellas les asigne, en su caso, con estricto respeto a su correspondiente ámbito de autonomía.*

   Por lo tanto, su régimen legal queda excluido de la Ley de Organización y Funcionamiento de la Administración General del Estado; su competencia, según lo dispuesto por la Ley 30/1992 del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, su régimen patrimonial y contratación son de derecho privado; sus funcionarios y personal son contratados según la naturaleza de las funciones; el presupuesto está integrado con independencia en los presupuestos generales del Estado.

Entre sus funciones se encuentran aquéllas que la Agencia ha clasificado de la siguiente manera:

1. General
Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

2. En relación con los afectados
Atender a sus peticiones y reclamaciones.
Información de los derechos reconocidos en la Ley.
Promover campañas de difusión a través de los medios.

3. En relación con quienes tratan datos
Emitir autorizaciones previstas en la Ley.
Requerir medidas de corrección.
Ordenar, en caso de ilegalidad, el cese en el tratamiento y la cancelación de los datos.
Ejercer la potestad sancionadora.
Recabar ayuda e información que precise.
Autorizar las transferencias internacionales de datos.

4. En la elaboración de normas
Informar los Proyectos de normas de desarrollo de la LOPD.
Informar los Proyectos de normas que incidan en materias de protección de datos.
Dictar Instrucciones y recomendaciones de adecuación de los tratamientos a la LOPD.
Dictar recomendaciones en materia de seguridad y control de acceso a los ficheros.

5. En materia de telecomunicaciones
Tutelar los derechos y garantías de los abonados y usuarios en el ámbito de las comunicaciones electrónicas, incluyendo el envío de comunicaciones comerciales no solicitadas realizadas a través de correo electrónico o medios de comunicación electrónica equivalente

6. Otras funciones
Velar por la publicidad en los tratamientos, publicando anualmente una lista de los mismos (CD).
Cooperación Internacional.
Representación de España en los foros internacionales en la materia.
Control y observancia de lo dispuesto en la Ley reguladora de la Función Estadística Pública.
Elaboración de una Memoria Anual, presentada por conducto del Ministro de Justicia a las Cortes.

Regulándose según lo establecido por la Ley 15/99 de Protección de Datos Personales en su título VI, artículos 35 y siguientes.

- **Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.**

El objeto de esta ley es establecer y regular las bases del régimen jurídico, el procedimiento administrativo común y el sistema de responsabilidad de las Administraciones, siendo aplicable a todas ellas, situaciones que deberán quedar ajustadas a los principios que establece la Ley Orgánica de 15/1999 de Protección de Datos de Carácter Personal.

- **Ley 12/1989, de 9 de mayo de la Función Estadística Pública.**

Es objeto de la presente Ley la regulación de la función estadística para fines estatales, al amparo de lo dispuesto en el artículo 149.1.31 de la Constitución Española. Asimismo, regula la planificación y elaboración de estadísticas para fines estatales desarrolladas por la Administración del Estado y las entidades de ella dependientes; la organización de sus servicios estadísticos y sus relaciones en materia estadística con las Comunidades Autónomas y las Corporaciones Locales, así como con la Comunidad Europea y Organismos Internacionales, con base en los principios de protección de datos personales y el secreto estadístico, en los términos que fija la ley.

3.2.3.2. Civil, mercantil y consumidores

- **Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.**

Los objetivos de la Ley se concretan en tres puntos básicos:

1. Establecer, sobre bases firmes y directas, los procedimientos eficaces para la defensa de los consumidores y usuarios.

2. Disponer del marco legal adecuado para favorecer un desarrollo óptimo del movimiento asociativo en este campo.

3. Declarar los principios, criterios, obligaciones y derechos que configuran la defensa de los consumidores y usuarios y que, en el ámbito de sus competencias, habrán de ser tenidos en cuenta por los poderes públicos en las actuaciones y desarrollos normativos futuros en el marco de la doctrina sentada por el Tribunal Constitucional y en base a los principios de protección de datos personales para los consumidores.

3.2.3.3. Fuerzas y cuerpos de seguridad

- **Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.**

El articulado de la presente Ley comienza determinando lo que constituye su objetivo fundamental, que no es otro que la creación de una base de datos en la que, de manera única, se integren los ficheros de las Fuerzas y Cuerpos de Seguridad del Estado en los que se almacenan los datos identificativos obtenidos a partir de los análisis de ADN que se hayan realizado en el marco de una investigación criminal, o en los procedimientos de identificación de cadáveres o de averiguación de personas desaparecidas. En relación con su integración orgánica, la base de datos policiales sobre identificadores obtenidos a partir del ADN dependerá del Ministerio del Interior.

3.2.3.4. Sanidad, salud y Reproducción asistida

- **Ley 45/2003, de 21 de noviembre, por la que se modifica la Ley 35/1988, de 22 de noviembre, sobre Técnicas de Reproducción Asistida.**

Dentro de esta legislación, se desprende, la situación de revelar datos biológicos en el momento y en la forma que se determine, los centros deberán poner a disposición el Centro Nacional los preembriones cuyas estructuras biológicas vayan a ser utilizadas con fines de investigación. Junto con los preembriones, los centros deberán facilitar todos los datos biológicos necesarios para determinar la trazabilidad y el tipaje de las células que se obtengan, de tal forma que no sea desvelada la identidad de sus progenitores.

3.2.3.5. Seguros

- **Ley 50/1980, de 8 de octubre, de Contrato de Seguro.**

En esta normatividad, el objeto de la misma es el contratar un seguro por medio del cual el asegurador se obliga, mediante el cobro de una prima y para el caso de que se produzca el evento cuyo riesgo es objeto de cobertura, a indemnizar, dentro de los límites pactados, el daño producido al asegurado o a satisfacer un capital, una renta u otras prestaciones convenidas, y el seguro se obliga a resguardar todos los datos proporcionados que el asegurado le remitió para la póliza.

3.2.3.6. Telecomunicaciones y sociedad de la información

- **Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.**

La presente Ley tiene como objeto la incorporación al ordenamiento jurídico español de la Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). Asimismo, incorpora parcialmente la Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores, al regular, de conformidad con lo establecido en ella, una acción de cesación contra las conductas que contravengan lo dispuesto en esta Ley. Lo que la Directiva 2000/31/CE denomina «sociedad de la información» viene determinado por la extraordinaria expansión de las redes de telecomunicaciones y, en especial, de Internet como vehículo de transmisión e intercambio de todo tipo de información. Su incorporación a la vida económica y social ofrece innumerables ventajas, como la mejora de la eficiencia empresarial, el incremento de las posibilidades de elección de los usuarios y la aparición de nuevas fuentes de empleo.

Pero la implantación de Internet y las nuevas tecnologías tropieza con algunas incertidumbres jurídicas, que es preciso aclarar con el establecimiento de un marco jurídico adecuado, que genere en todos los actores intervinientes la confianza necesaria para el empleo de este nuevo medio. Eso es lo que pretende esta Ley, que parte de la aplicación a las actividades realizadas por medios electrónicos de las normas tanto generales como especiales que las regulan, ocupándose tan sólo de aquellos aspectos que, ya sea por su novedad o por las peculiaridades que implica su ejercicio por vía electrónica, no están cubiertos por dicha regulación.

Como conclusión podemos mencionar que desde la perspectiva legal, el punto de partida en España de la protección de datos personales lo marca el artículo 18.4 de su Constitución, el cual establece que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos». Partiendo de este precepto, nos encontramos frente a distintos bloques normativos que se aplican de forma más o menos inmediata como los que han quedado precisados anteriormente, y desde luego en su reglamentación específica, la Ley Orgánica 15/1999 de Protección de Datos, constituye un referente legislativo en la materia para las entidades de aquél país comunitario, y que se ve desarrollada en las normativas internas de cada comunidad española, el régimen español sobre este derecho de tercera generación, constituye uno de los pilares fundamentales sobre los que descansan otras legislaciones no solo nacionales sino de carácter internacional.

3.3. Régimen Legal de la Protección de datos personales en Argentina

El régimen legal de protección de datos personales en el Estado Argentino, encontró su institucionalización en el año 2000, tras algunos años de intento que resultaron fallidos desde la reforma constitucional de 1994, pese a los inconvenientes que surgieron para la creación de una ley que protegiera la garantía

consagrada en el artículo 43 de la Constitución, por fin se logró bajo el resguardo de la Ley 25.326 de Hábeas Data.

3.3.1. Constitución Argentina

En 1994, la República Argentina tuvo una de las mayores reformas a su Constitución Nacional, como respuesta a las exigencias sociales, las cuales ya demandaban cambios trascendentes en aquella región del sur de América.

Dentro de los grandes cambios estructurales que se adoptaron en aquel año, fue la incorporación de un derecho fundamental que asegurara protección a los datos personales de un individuo dentro del país Argentino, es por ello que se consagró el artículo 43, en un apartado que se denominó "Nuevos Derechos y Garantías"; bajo una redacción no muy precisa, se sostiene la llamada garantía del hábeas data, es por vez primera que se reconoce este derecho derivado de la aludida reforma, para quedar en su párrafo tercero de la siguiente manera:

"Artículo 43.

...

Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos..."[107]

Este artículo garantista, además del hábeas data, prevé otros derechos como la acción de amparo y el hábeas corpus, sin embargo, conjuntamente con ello el Constituyente se encargó de edificar el sistema de protección de los derechos fundamentales a través de este precepto constitucional, asegurando el derecho de

[107] *Constitución de la Nación Argentina y Tratados Internacionales con jerarquía constitucional.* Ed. Estudio, Argentina, 2008.

toda persona a proteger sus datos personales, cómo, cuándo, dónde y quién cuenta con los datos de uno, para qué fueron recopilados, de qué manera y en su caso rectificar, suprimir, etc., un derecho al que la doctrina alemana llamó "autodeterminación informativa".

La institucionalización de un derecho conocido como de tercera generación, se encontraba plasmado ya en la Carta Magna del pueblo Argentino, ahora resta saber la manera en que ese derecho es garantizado.

3.3.2. Ley 25.326 de Protección de los datos personales y su Decreto Reglamentario 1558/2001[108]

La Constitución Argentina refirió el derecho de Protección de datos personales en su artículo 43, en el año 1994, tal como lo hemos mencionado, no fue sino hasta el 2000, en que se reglamenta el derecho en una norma federal que describe su alcance y el procedimiento de defensa al mismo. La ley 25.326 Argentina, fue sancionada el 4 de octubre de 2000, y promulgada en dos partes que salieron publicadas en el B.O. el 30 de octubre y el 2 de noviembre del mismo año, tras haber sido una iniciativa que partió del Senado de la Nación, y principalmente recogiendo el proyecto del Senador Menem[109].

El 3 de diciembre de 2001, hay cumplimiento a lo establecido por el artículo 45 de la citada ley, en el que se le daba al Ejecutivo Nacional un plazo de 180 días a partir de la promulgación de la ley, para reglamentarla y establecer el organismo de control sobre el particular. A pesar de haberse dictado fuera del plazo, mediante Decreto 1558/01, se crea la Dirección Nacional de Protección de Datos Personales, un Decreto reglamentario que vino a cubrir en cierta medida las lagunas que el legislador no había cubierto y por Decreto 1892/02, se designó y puso en funciones al titular del órgano de control.

[108] Véase Anexo I de la Ley 25.326 y Decreto 1558/01, en cuadro comparativo.
[109] PUCCINELLI, Oscar R. *Protección de Datos de Carácter Personal. Ob. Cit.* Pág. 45

La Ley 25.326 de Protección de los Datos Personales, quedó estructurada en siete capítulos:

I. Disposiciones Generales,
II. Principios Generales relativos a la protección de datos,
III. Derechos de los Titulares de datos,
IV. Usuarios y responsables de archivos, registros y bancos de datos,
V. Control,
VI. Sanciones, y
VII. Acción de Protección de los datos personales.

En general se reglamenta la acción prevista por el artículo 43 de la Constitución Argentina, a la cual se le rotuló indistintamente con el nombre de "Protección de Datos Personales" o "hábeas data".

La disposición del artículo 44 sostiene que la ley es de aplicación en toda la República Argentina intimando a las provincias a adherir sus normas a las de la Ley 25.326. Según la disposición del precepto en cita se exceptúa de aplicación general en los casos siguientes:

- El Órgano de Control;
- Inscripción del Código de Conducta;
- Sanciones administrativas;
- La obligación de Inscripción en los Registros de los Archivos Existentes al momento de la Sanción de la Ley y
- La Acción de Protección de Datos Personales

Quedando para las Entidades Federadas la regulación de los aspectos no abarcados por la norma federal, pero siempre respetando los principios de autonomía provincial según lo dispuesto por el artículo 5 de la Constitución Nacional Argentina.

Algunos autores han criticado la Ley, entre ellos Alejandra M. Gils Carbó[110] quien sostuvo que la Ley contiene algunas deficiencias como las siguientes:

- No prevé un recurso judicial directo contra las decisiones del Órgano de Control;
- No establece en el Capítulo de Sanciones normas específicas sobre responsabilidad civil por violación de los derechos de los registrados.

Cabe destacar que la garantía establecida por el artículo 43 de la Constitución Argentina, incorporó la acción de Hábeas Data como un subtipo de amparo, y en palabras de Puccinelli[111] se remarca que con la aparición de la Ley General de Protección de Datos Personales no se acaba la labor, pues, además de su reglamentación por vía de decreto y de las disposiciones de la Dirección General de Protección de Datos Personales, esta debe complementarse con otras Leyes sectoriales tanto en el plano Federal, como en el de las Provincias.

El Decreto reglamentario 1558/01, fue promulgado vencido largamente el plazo que le atribuyó el artículo 45 de la Ley 25.326, en ejercicio de lo dispuesto por el artículo 99, inciso 2 de la Constitución Nacional Argentina.

El Decreto consta de cuatro artículos, en los que se aprueba la reglamentación de la multicitada ley, que se conforma como Anexo del documento; se establece el término de 180 días como plazo previsto para lo dispuesto por el artículo 46 de la ley (inscripción, registro y bancos de datos existentes antes de la sanción de la misma, conforme a lo dispuesto por el artículo 21); asimismo, se exhorta a las provincias y a la Ciudad Autónoma de Buenos Aires a adherir sus normas a la observación de la Ley 25.326, en los términos previstos por el artículo 5 de la Constitución, como lo mencionamos anteriormente; y finalmente, se ordena la comunicación y publicación del Decreto.

---

[110] *Régimen Legal de las Bases de Datos y Hábeas Data. Ob. Cit.* Pág. 47 y sigs.
[111] *Protección de Datos de carácter personal. Ob. Cit.* Pág. 51

Por lo que hace al anexo respectivo, es preciso mencionar que la reglamentación, manifiesta en su artículo 1 qué tipos de datos quedan comprendidos por la Ley 25.326, " quedan comprendidos en el concepto de archivos, registros, bases o bancos de datos privados destinados a dar informes, aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito", y por último, el anexo consta de siete capítulos, donde reproduce el sistema adoptado por la ley e indica los artículos que reglamenta (17) y los que deja sin reglamentar (29).

3.3.3. El Hábeas Data y los derechos tutelados

Partiendo de la constatación de que el Hábeas Data es una garantía de tercera generación, en tanto que protege algunos derechos que han evolucionado, corresponde definirlos como aquéllos que intrínsecamente son, a la vez individuales y colectivos, por ejemplo el derecho a la paz, a un ambiente saludable, derecho al acceso, a la rectificación, a la verdad, etc. Ante la revolución informática han aparecido los derechos humanos de la libertad informática, derecho de tercera generación protegido por garantías de tercera generación: el hábeas data.

El término Hábeas Data, fue acuñado para designar lo que se conoce en término castellano como traer o presentar el dato, como una especie de analogía del Hábeas Corpus (traer o presentar el cuerpo).

La historia del hábeas data en cada región del mundo se ha intensificado desde distinta perspectiva, ya sea en la Constitución Nacional o en algunos casos a través de regulación en leyes federales, como en el caso Argentino.

Sin embargo, en otras regiones del mundo, el término "hábeas data", no alude específicamente al nombre como tal, aunque su norma suprema lo suponga,

como el caso mexicano -con la reforma al artículo 6 y 16 constitucional, para este caso específico, el sistema mexicano cuenta con la acción de amparo como medio de control constitucional y como defensa a los derechos establecidos en la parte dogmática de la Constitución desde la perspectiva del derecho a la información pública y a la seguridad jurídica, empero el artículo 6º, incorpora una fracción, haciendo alusión a la defensa derivada de leyes secundarias (fracción II), antes de ejercitar la acción de amparo, caso contrario, en algunas reglamentación municipales del propio país, se considera al hábeas data como tal y como medio de defensa ante las violaciones a los datos personales; también tenemos, el caso de la Constitución brasileña, que adoptó desde 1988 al hábeas data como un medio de control constitucional.

Marcela Basterra[112], nos dice que la garantía de hábeas data prescrita por el constituyente tiene una finalidad inmediata y otra mediata. En relación a la primera, se encuentra comprendida en la posibilidad que tienen las personas de tomar conocimiento de los datos a ella referidos y de su finalidad y, en lo que respecta a la segunda, si dichos datos resultan falsos o discriminatorios se puede exigir la supresión, rectificación, confidencialidad o actualización de los mismos.

En este sentido, para la autora, el Habeas Data, puede tener varias subdivisiones:

a) Hábeas Data informativo. El cual se relaciona con el conocimiento e información de los datos que existan respecto de cada persona. Es aquél que permite cumplir con los fines inmediatos, el que a su vez que subclasifica en:
    i. Hábeas Data exhibitorio: que nos permite conocer qué datos se poseen acerca de mi persona.

[112] BASTERRA, Marcela. *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados. Derecho Constitucional Provincial. Iberoamérica y México.* IIJUNAM-Ediar, Argentina, 2008. Pág. 81

ii. Hábeas Data finalista. Nos permite saber cuál va a ser la finalidad que se les dará a nuestros datos personales.
iii. Hábeas Data autoral. Permite conocer quién recopiló esos datos.

b) Hábeas Data cancelatorio. Para la supresión de datos, para evitar que sean usados con fines discriminatorios o en forma abusiva, referido a los datos conocidos como sensibles. Sobre este esquema tenemos la siguiente clasificación:

i. Hábeas Data aditivo: por medio de esta acción se puede solicitar que se agregue un dato que no está en el registro o banco ante el que iniciamos la misma, es considerado como aquél que puede actualizar un dato antiguo o agregar uno omisivo.
ii. Hábeas data rectificador. se interpone cuando se ha considerado que un dato es falso, solicitando se cambie por uno cierto.
iii. Hábeas Data reservador. Un dato es verdadero, pero no hay obstáculo alguno para la conservación, en tal sentido la autoridad que intervenga podrá ordenar la confidencialidad de los datos.

En consecuencia, podemos definir al habeas data como el derecho que tiene cualquier persona, para informase acerca de la existencia de sus datos personales, en poder de quién se encuentran, cuál es la finalidad de su recopilación y quién los recopiló, y una vez conocido estos términos, solicitar se agregue algún dato que no conste en los archivos, registros o bancos de datos y que sea considerado para actualizar, rectificar o suprimir el dato erróneo, así como pedir la confidencialidad de los datos sensibles.

Considerando el objeto del hábeas data, y por cuestiones que han sido tratadas, podemos desprender tanto por la doctrina como por la legislación nacional e internacional, sin perjuicio de que el mismo pueda ser conexo con otros:

a) El derecho a la autodeterminación informativa.

Para Gozaini, encontrar el derecho tutelado específicamente, es tarea sencilla, cuando el análisis se circunscribe a las posibilidades de acción que tiene un individuo frente a quien se aplica en su provecho los datos que a aquél le conciernen. [113] Si tomamos esta idea, entonces bastaría con tener el más básico de los derechos que es el de acceso a los datos personales, para saber cuál será la acción procesal que ejercitaremos y con ello estar en posibilidad de conocer o identificar el derecho tutelado.

3.4. Presente y Futuro en la Protección de datos personales en el plano del Derecho Internacional: México, España y Argentina

A lo largo de estas páginas hemos abordado las diversas normas que integran los sistemas de protección de datos personales en los países motivo de la presente investigación, el caso mexicano, quien a partir del año 2003, dio a conocer la llamada Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, que entre otros objetivos, buscaba consolidar el derecho de acceso a la información pública, teniendo como sujetos obligados a las propias instituciones gubernamentales, pero sobre todo protegen los datos personales de los individuos en lo que se relacionara con datos de carácter confidencial y desde luego los datos sensibles, ya que según la legislación, es posible solicitar información pública, empero los sujetos obligados tienen el deber de disociar los datos de la persona con lo que se pide, o en su defecto solicitar su consentimiento para darlos a conocer, cuando la información solicitada sea factible proporcionarse,

[113] GOZAINI, Osvaldo Alfredo. *Derecho Procesal Constitucional. Hábeas Data. Protección de datos personales. Ley 25.326 y reglamentación (decreto 1558/20001).* Rubinzal Culzoni, 2002.

so pena de responsabilidad y cuyo objetivo es precisamente evitar circunstancias de imposible reparación con el conocimiento de algún dato.

Hoy en día la mayoría de los Estados del territorio nacional cuentan con una legislación en materia de transparencia y acceso a la información pública, de las que se deriva en algunas la protección de datos personales, en poder de entes públicos, y adoptando el modelo de hábeas data para su resguardo legal, aun así, estas legislaciones estaduales y municipales no son lo suficientemente garantistas para evitar la circulación de datos personales en poder de los particulares.

Con la entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, se dio un cambio significativo en la materia, lo que constituyó un primer momento para la protección de datos personales, empero únicamente en posesión de entes públicos, pese a ello, se motivó la creación de la tan esperada Ley Federal de Protección de Datos Personales en Posesión de Particulares que fue aprobada promulgada el pasado mes de julio de 2010, con fundamento en lo dispuesto por el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos en materia de protección de datos.

La protección de datos personales en México, hoy constituye una realidad, aprobada en el Congreso retomada de los proyectos de Ley que fueron presentados a partir de 2001; no obstante, la Ley cuenta con algunas omisiones en materia, pues no prevé el ejercicio de los derechos ARCO en la publicidad, sino que da una remisión a otros sectores de la Administración (Secretaría de Economía), por lo que se continúa con el problema (menor, pero se continúa) de la dispersión legislativa sobre la protección de datos personales en la publicidad, pues no se permite la unificación de criterios para proteger plenamente los derechos descritos; la actual Ley de Protección de Datos Personales contempla el uso de los datos en posesión de particulares, sin embargo en otras actividades tiene que remitir a otros sectores como lo veremos en el capítulo V.

Por otra parte, la citada ley no avista la creación de un Registro Nacional de Bases de Datos, lo que hoy ocasiona que sea difícil llevar un control de los archivos y las bases de datos, no obstante, sabemos de antemano que los cambios y las nuevas tecnologías de la información, requieren cada día de un nivel de protección más amplio que genere seguridad y resguardo en ellos, por lo que estamos conscientes y seguros que México tendrá que adaptarse a las necesidades que demanda la sociedad, extendiendo el nivel de protección de datos y complementándolo con los Lineamientos que al efecto expida la autoridad reguladora (Instituto Federal de Acceso a la Información y Protección de Datos Personales).

Igualmente, deberán hacerse las reformas, adiciones y/o modificaciones necesarias a efecto de dotar a esta nueva Ley de instrumentos que le permitan reconocer un pleno ejercicio de los derechos ARCO, y creando los sistemas de seguridad correspondientes, así como incrementar el resguardo de los mismos en todas las facetas de su tratamiento en soportes físicos y automatizados, así como la participación de los diversos sectores sociales y políticos para el fortalecimiento de un sistema de seguridad en la materia, a saber:

A) Requerimientos sociales:
    a. Seguridad en líneas
    b. Acción de padres, profesores, consumidores, usuarios de internet y correos electrónicos.
B) Mejores prácticas:
    a. Capacitación a usuarios
    b. Gobierno de Tecnologías de la Información
    c. Políticas de seguridad corporativa
C) Acciones política y legislativas:
    a. Iniciativas de ley
    b. Colaboración y creación de leyes internacionales
    c. Leyes contra delitos cibernéticos

Con ello el futuro del sistema podrá consolidar a la norma de protección de datos personales en poder de entes públicos y particulares (recientemente creada), y cuyos factores de atribución, creen nuevas fronteras del derecho y permitan a

México colocarse a la vanguardia de los países que cuentan con un alto nivel de resguardo para estar en posibilidad de sustentar acuerdos comerciales con bloques económicos alrededor del mundo, permitiendo flujos de inversión extranjero al brindar certeza en los intercambios comerciales transfronterizos, pero sobre todo para proteger lo constitucionalmente amparado "los datos personales".

En la República Argentina la regulación ha sido prolija al respecto, pues la adecuación con la norma federal 25.326 de hábeas data, del año 2000, maneja uno de los sistemas en materia de protección de datos personales modelo para otros países de América, cuestión que puede constituirse como referente en México para acrecentar el nivel de resguardo.

Ello es así, ya que la Constitución Argentina con la reforma de 1994, dispuso en el artículo 43, un subtipo de amparo como protección de datos personales para los individuos, reglamentando además por Decreto 1558/01, las lagunas que el legislador dejó en la citada ley, y estableciendo niveles de protección altos, incluso con la creación de un órgano de control como la Dirección Nacional de Protección de Datos Personales, el modelo Argentino de hábeas data, mantiene serias expectativas de control sobre los archivos, registros y bancos de datos, en poder de entes públicos y particulares, normando la responsabilidad administrativa y penal sobre las que pudieren incurrir los usuarios y/o responsables de los ficheros.

La citada legislación, invoca a las leyes provinciales a generar normas conforme a la legislación federal siempre dentro del marco de su autonomía, según lo dispone el artículo 5º de la Constitución Nacional Argentina.

Con este modelo de protección, la Nación Argentina aun no tiene todo el trabajo resuelto, sino que debe continuar en una labor constante para reforzar el sistema que ha creado.

El futuro de la protección de datos en el Estado Argentino es prometedor, pues sus proyectos sobre políticas digitales, agenda digital en donde asociaciones, universidades, expertos en tecnología, sector privado, etc., sean partícipes de un nuevo modelo de invención proteccionistas dentro de un nuevo gobierno digital, en donde se manejen bases de datos y condiciones de información: recibida, accedida, ampliada, corregida, gestiones de derechos de los titulares de los datos y control de calidad, con estas políticas, el gobierno Argentino pretende obtener resultados que le permitan actualizar información, incorporar novedades, depurar errores y disminuir los casos confusos (homonimia, similitudes).

Pero aun el futuro de la protección de datos personales en la Argentina no queda ahí, el 14 de mayo de 2009, se llevó a cabo el Sexto Seminario Nacional Internacional de Protección de Datos Personales en la República Argentina,[114] entre lo más destacable, se encontraba una normativa para la región del MERCOSUR, sobre buenas prácticas en la Protección de Datos Personales.

Con ello se pretende promover políticas y estrategias comunes referentes a la sociedad de la información, en cooperación conjunta con la Comunidad Europea, cuyo costo comprende la creación de una plataforma, que sostuviera un sistema transnacional, que permitiera a los países integrantes, entre otras cosas un mercado libre, oportunidades comerciales, apertura a las Pymes, bajo una logística de distribución de productos, la creación de un marco regulatorio a nivel regional para el usuario, recolecta de información, páginas web comerciales dentro de la región, recepción de productos, etc., pero todo ello bajo el esquema de una Protección de Datos Personales.

Como vemos el futuro de la Nación Argentina en la materia es prometedor, pero sumamente laborable y complicado, pues tendrá que evaluar, organizar pero

[114] Ponencia a cargo de SORIANO, José, Coordinador en la Argentina del MERCOSUR Digital Union Europea Mercosur. *Sexto Seminario Nacional e Internacional de Protección de Datos Personales. Éxitos e Innovaciones hacia el bicentenario de la República Argentina.* Buenos Aires, Argentina, 14 de mayo de 2009.

sobre todo llevar a cabo las expectativas que ellos mismos se proponen.

Y por último el caso de España, como lo hemos acotado, en la región española, rige actualmente la Ley Orgánica 15/99 de Protección de Datos de carácter personal de 13 de diciembre que vino a derogar la conocida LORTAD, esta nueva legislación hizo posible la creación de la Agencia Española de Protección de Datos Personales, que se constituye como un referente a nivel internacional, lo que impone una serie de obligaciones para los particulares que posean ficheros con datos personales.

Conjuntamente el Real Decreto 1720/2007 de 21 de diciembre por el que se aprueba el Reglamento de la Ley Orgánica de Protección de Datos establece la obligación de las empresas de tomar las medidas de seguridad para garantizar la protección de los datos, afectando a sistemas informáticos, archivos de soportes de almacenamiento personal, procedimientos operativos, etc.

La antigua LORTAD, hoy derogada por la Ley 15/99, es menos amplia que esta última, ya que sólo era aplicable a los ficheros automatizados, en cambio la LOPD incluye también desde su ámbito de aplicación los no automatizados (artículo 3 c). Esto es que la LORTAD 15/92 pretendía limitar el uso a la informática y otros medios de tratamiento automatizado, en aras de la protección del derecho al honor, la intimidad y la propia imagen, siendo de aplicación la norma respecto de los ficheros automatizados o bases de datos tratadas por medios informáticos, dejando fuera los ficheros en cualquier otro medio o soporte de tratamiento.

Como novedad principal, la LOPD 15/99 introduce en su ámbito de aplicación los ficheros no automatizados o ficheros en papel, centrando toda su protección en el tratamiento de datos personales sea cual fuere el soporte o medio de su tratamiento.

El sistema español es sumamente avanzado sobre el tema y lo que podríamos decir al respecto es que la experiencia española es basta, y dentro de sus acciones a futuro el Estado español, aparte de considerar el establecimiento de mejores prácticas y dedicarse a la recopilación de experiencias en otros países subdesarrollados en la materia, consciente de su sistema a nivel internacional, se comprometió a la cooperación con América Latina y la contribución a la implantación en países como México a la creación de un marco jurídico que garantice un nivel de protección de datos adecuado en los mismos, como eje de la acción internacional.

En el siguiente capítulo veremos de qué manera la publicidad se introduce en los medios de comunicación, y cómo puede ser violatorio el tratamiento de los datos personales mediante la publicidad y el marketing, así como las circunstancias en las que pueden ser tratados los datos personales y su resguardo.

CAPÍTULO IV

LA PROTECCIÓN DE DATOS PERSONALES EN LA PUBLICIDAD Y EL MARKETING

4.1. La influencia de la publicidad y el marketing en la sociedad

- 4.1.1. Publicidad. Definición
- 4.1.2. Marketing. Definición

4.2. La publicidad y los medios de comunicación

- 4.2.1. Internet
- 4.2.2. Correo electrónico
- 4.2.3. Teléfono

4.3. La protección de datos personales en la sociedad informatizada

- 4.3.1. Alcance de la informática y sus repercusiones en el disfrute de los derechos fundamentales

4.4. Aspectos relevantes del Binomio protección de datos personales y publicidad y marketing

- 4.4.1. Casos en los que se pueden tratar datos con fines de publicidad
- 4.4.2. Derecho de acceso del titular de los datos
- 4.4.3. Retiro, bloqueo o cancelación del nombre de los bancos de datos con fines de publicidad
- 4.4.4. Problemas de la recopilación y tratamiento de datos con fines de publicidad sin consentimiento del titular
- 4.4.5. Necesidad de inscripción en un Registro de los responsables o usuarios de archivo, registros, bancos o bases de datos con fines de publicidad.
- 4.4.6. Garantía de Confidencialidad y Seguridad de los ficheros automatizados

CAPÍTULO IV

LA PROTECCIÓN DE DATOS PERSONALES EN LA PUBLICIDAD Y EL MARKETING

4.1. La influencia de la publicidad y el marketing en la sociedad

En una obra clásica, citada por Maximiliano Márquez Alarralde, cuenta la anécdota de Rudyar Kipling, quien se encontraba de vacaciones, cuando recibió un paquete de revistas remitidas por un amigo, quien para economizar gastos, había arrancado todas las páginas de publicidad. Al agradecer a su amigo el envío, Kipling le expresó su decepción, porque él mismo hubiera podido escribir todas las historias de aquéllas revistas o reconstruido sus textos, mientras que los anuncios mutilados lo privaban de la verdadera información –quizá pensó añadir comunicación, es decir, el verdadero interés humano y motivacional de toda publicidad-.[115]

Hoy en día, la comunicación es un agente vital en la cotidianeidad del ser humano y la publicidad y el marketing, se han convertido en lo usual, decía Teodoro Levitt "en todo el mundo, el tipo de comunicación que cada vez abunda más es la comercial, no la información acerca de los acontecimientos que ocurren",[116] cualquiera que sea el lugar en el que habitamos, el entorno, el territorio, las comunicaciones del comercio, se tornan cada vez más pronunciadas hacia cualquier sector poblacional y en todas partes tienen el mismo propósito: persuadir a alguien a entregar su dinero a cambio de mercancías, bienes o servicios.

Un paisaje florido, montañas, veredas y llanuras, una pintura surrealista, unos jardines colgantes, colores, aromas, sabores, edecanes, premios, concursos, descuentos, oportunidades, viajes, etc., son sólo algunas de las estrategias para

[115] MÁRQUEZ ALURRALDE, Maximiliano. *Régimen Jurídico de las Comunicaciones.* Depalma. Buenos Aires, Argentina, 1986. Pág. 1

[116] La legitimidad moral del materialismo. Disertación pronunciada en el XIV Congreso Mundial de Publicidad, Buenos Aires, Argentina, 19 mayo de 1976. http://blogs.clarin.com/oscarschiavetta/2008/3/27/curriculum

atraer clientes, la publicidad y el marketing se encuentra hoy en día fuertemente influenciando las decisiones en una sociedad.

Si bien, podemos decir que el objeto de la publicidad, es extender el reconocimiento del mercado hacia la sociedad, además de un producto cultural, porque es el resultado adecuado para la difusión de las ideas de una sociedad de consumismo que da a conocer los hechos y actividades de un sector poblacional, económico o social.

4.1.1. Publicidad. Definición

De acuerdo al Diccionario de la Lengua Española,[117] se le da el término de publicidad a la divulgación de noticias o anuncios de carácter comercial para atraer a posibles compradores, espectadores, usuarios, etc.

También es conocida como toda forma de comunicación realizada por una persona física o jurídica, pública o privada, en el ejercicio de una actividad comercial, industrial, artesanal o profesional, con el fin de promover de forma directa o indirecta la contratación de bienes, servicios, derechos y obligaciones.[118]

El Convenio Europeo sobre Televisión Transfronteriza de Estrasburgo de 5 de mayo de 1989, designó a la publicidad como *todo anuncio público realizado con el fin de estimular la venta, la compra o el arrendamiento de un producto o de un servicio,, de promover una causa o una idea, o de producir cualquier otro efecto deseado por el anunciante, por el cual se cede un tiempo de transmisión al anunciante mediante remuneración o cualquier contrapartida similar.*

La publicidad es una técnica de comunicación a las masas, que tiene por objeto dar a conocer o difundir al público los bienes y servicios a través de los distintos

[117] *Op. Cit. Diccionario de la Lengua Española*
[118] LANDERIA Prado, Renato Alberto, et. Al. *Colección de Derecho de las Nuevas Tecnologías. Diccionario Jurídico de los Medios de Comunicación.* Reus, España, 2006.

medios de comunicación a fin de que el público consumidor realice una acción de compra, estos medios de comunicación pueden consistir en la Televisión, Radio, Cine, Revistas, Prensa e Internet, así como también a través de las acciones de Marketing Directo, Relaciones Públicas, Patrocinio, Promociones, Punto de Venta.

La Suprema Corte de Justicia de la Nación, se pronunció en enero de 2005 sobre la publicidad comercial, señalando que puede constituir una aportación de debate ciudadano sobre los asuntos públicos y puede ayudar a difundir ideas públicas, empero cuando esa publicidad propone a sus receptores una transacción comercial, su producción puede ser regulada ampliamente que si fuera mera libertad de expresión y por lo tanto puede someterse a los limites de veracidad y claridad exigibles.[119]

La jurisprudencia norteamericana ha señalado a la publicidad comercial bajo el manto de la libertad de expresión, con el nombre de "expresión comercial",[120] amparada por el derecho norteamericano, porque el libre flujo de información comercial es indispensable para que los individuos puedan tomar sus decisiones económicas y formarse opiniones acerca del mercado, sin embargo, posiciones encontradas en la doctrina anglosajona[121], nos dicen que la publicidad comercial no afecta a la toma de decisiones públicas ni hace referencia a ideas, que los anunciantes conocen muy bien su producto, por lo que se les puede exigir más que al resto de las personas que se expresan.

---

[119] *LIBERTAD DE EXPRESIÓN E IMPRENTA, LAS LIMITACIONES ESTABLECIDAS POR EL LEGISLADOR RELACIONADAS CON LA VERACIDAD Y CLARIDAD DE LA PUBLICIDAD COMERCIAL SON CONSTITUCIONALES CUANDO INCIDAN EN SU DIMENSIÓN PURAMENTE INFORMATIVA.* Novena Época, Primera Sala, SJF y su Gaceta, XXI, enero 2005, página 421, tesis 1ª CLXV/2004, Tesis Aislada, materia Constitucional.

[120] *Libertad de Expresión y Publicidad Comercial en los Estados Unidos de América: Una aproximación a la reciente jurisprudencia del Tribunal Supremo.* Jordi Freixes Montes. Comunicación y Pluralismo. Actas del Congreso Internacional. España, 1994.

[121] Frente a esta jurisprudencia y para suprimir y limitar la protección de la publicidad se pronunció el entonces Presidente del Tribunal Supremo William Hubbs Rehnquist. *Chief Justice of the United States.* 1994.

Sobre esta tutela de la publicidad comercial frente a la libertad de expresión el Tribunal Europeo de Derechos Humanos se ha pronunciado, diciendo que: no por tener efecto publicitario, una información se convierte en publicidad comercial, y por lo tanto en el momento de resolver un conflicto, debiera hacerse a favor de la inclusión de la publicidad comercial entre las conductas protegidas por la libertad de expresión.

La publicidad comercial libre, como ejercicio de la libertad de expresión pretende facilitar la existencia de un flujo adecuado de información y transmitir la opinión y que las autoridades, aunque pueden regular este privilegio en aras del interés público, no pueden, sin embargo, proscribir indebidamente el ejercicio de aquel, ya que como quedó señalado, es una conducta protegida por la libertad de expresión, lo que finalmente viene a considerar y resolverse a través de un ejercicio de ponderación ante su contrastación con otro derecho.

4.1.2. Marketing. Definición

El marketing o mercadotecnia es español, es el conjunto de principios y prácticas que buscan el aumento del comercio, especialmente de la demanda.[122]

El Diccionario Jurídico de los Medios de Comunicación, menciona que el marketing constituye *el conjunto de principios y prácticas que buscan el aumento del comercio, especialmente de la demanda, y estudio de los procedimientos y recursos tendientes a este fin.*[123]

El marketing involucra, como su nombre lo indica en español, técnicas, estrategias de mercado, de ventas, estudio de mercado, posicionamiento de mercado, posibles clientes, etc., a diferencia de la publicidad que constituye sólo una herramienta de la mercadotecnia.

[122] *Ob. Cit. Diccionario de la Lengua Española.*
[123] *Ob. Cit. Colección de Derecho de las Nuevas Tecnologías. Diccionario Jurídico de los Medios de Comunicación.*

El marketing utiliza las técnicas de la publicidad de respuesta directa y la imagen, de ahí que se le denomine marketing directo, constituyéndose así como un ejemplo de comunicaciones integradas, porque focalizan no sólo en la comunicación al consumidor, sino también a la imagen que se le vende al mismo.

En tanto va dirigido a la persona indicada, el marketing directo cambia el monólogo de la publicidad masiva por el diálogo. Llamando a cada cliente por su nombre y apellido.[124] Por eso, es un medio certero, muy efectivo y que permite a la vez una gran creatividad. Se usa no sólo para productos relativamente masivos, sino también para obtener resultados a corto y mediano plazo.

La base de datos es la llave del negocio, las alternativas son multiplicar esa base de datos. Lo que para algunos es considerado valioso por ser dato personal, para otros es considerado negocio. Esto se traduce en una serie de ventajas para el vendedor, por ejemplo, la personalización, la cobertura geográfica, y desde luego el desarrollo de una base de datos para la empresa de los clientes, este último tópico lo tocaremos en capítulos posteriores, cuando hablemos del binomio protección de datos personales y marketing, ya que el objeto del presente trabajo no es realizar un estudio exhaustivo de la publicidad y el marketing, sino de su posible inclusión en el derecho a la protección de datos personales.

4.2. La publicidad y los medios de comunicación

La planeación estratégica de la publicidad y las promociones deben estar integradas, decía John Philip Jones,[125] y las promociones deben comunicar los mismos valores tanto como sea posible. Esto significa que las promociones no deben ser utilizadas sólo para generar ventas, sino también para construir la concesión de la marca, lo que acontece en la mayoría de los casos de páginas

[124] El caso de telemarketing, en donde por vía telefónica se realizan mensajes publicitarios, ya sea desde la empresa o también el propio usuario lo realiza, con los números conocidos 0800.
[125] PHILIP JONES, John. *Cuando la publicidad si funciona. Nuevas pruebas de que anunciar dispara sus ventas.* Grupo Editorial Norma, Traducción de Manuel Lorenzo Villegas, Colombia, 1997. Pág. 203-205.

publicitarias, no se requiere la compra de los servicios o consumos, sino el espacio para publicitar u ofertar su marca.

Un aspecto importante que debe resaltarse es que la publicidad va encaminada en relación a los números de consumidores de información. Ello determinó una mutación, no sólo cuantitativa de los potenciales consumidores de informaciones, sino también de orden cualitativo. La proliferación de consumidores pertenecientes a distintas clases sociales, con diferentes inquietudes, expectativas y necesidades, marcó un hito en la historia de los medios de comunicación.

Dentro del ámbito publicitario, existen diversos tipos de publicidad, la institucional, la filantrópica, de producto, etc., y se utilizan de igual manera distintos medios para comunicar o dar a conocer lo que publicitarán, así tenemos, la publicidad gráfica, en diarios, revistas, las establecidos en la vía pública, los cuales tienen un impacto visual, poca información y mucha capacidad de llegada.

Decía la Profesora en Letras de la Universidad de Buenos Aires Mónica Ana Silberman, todo mensaje debe capitalizarse partiendo de la premisa de que su contenido se debe codificar en 3 segundos. De ahí la importancia de la síntesis a través de un título claro y breve, y de una imagen que esté anclada en el mismo. [126]

Hemos visto como aspecto tradicional, grandes carteleras en edificios, azoteas, posters, panels, en baldíos, pasos peatonales, taxis, en plazas, parques, calles, esquinas, bancos, pisos, escaleras, que publicitan lo mismo que el aparato radiofónico, la televisión, el cine publicitario, actualmente estos medios de comunicación, han sido rebasados por las Nuevas Tecnologías de la Información, al adentrarse a Internet, el correo electrónico, el teléfono, elementos de tecnología que han sido y son en la actualidad fuentes de publicidad como lo veremos más adelante.

[126] SILVERMAN, Mónica Ana. *Comunica Comunicador. Desafíos y tendencias e la publicidad en el fin de siglo.* Ed. Belgrano, 1996, Pág. 74

La inclusión de la publicidad en las páginas de los periódicos y ulteriormente de los diferentes medios de difusión de noticias e informaciones ha sido el gran factor determinante para el proceso de transformaciones de éstos. El producto de los anuncios publicitarios está en relación directa con el número de personas que consumen la publicación. A mayor cantidad de receptores, mayor atractivo para quien desee publicar sus productos o servicios, y en consecuencia, mejores niveles de rentabilidad para el medio a través del cual dicha actividad se realiza. A la luz de esta realidad cambia la ponderación de los esquemas de costos de los periódicos y de los modernos medios masivos de comunicación.

En los años 60's, la publicidad estaba en su apogeo y la comunicación masiva era el imperativo de los tiempos en los que todos compraban de todo. En los años 70's, la crisis de valores hizo que la publicidad se empezara a cuestionar mientras aparecían otros segmentos y consumidores. En los años 80's, la gente comenzó a comprar lo que le gustaba, se volvió más selectivo. Entonces surgió el marketing de muchos. En los años 90's, con la recesión mundial, la generación "X" y la generación digital, comprar sólo lo más competente, son más exigentes en el consumo y más tradicionales en los valores.

Se enfatiza la integración de medios: lo clásico con lo alternativo, lo masivo con las nuevas formas de la comunicación publicitaria. El telemarketing, complementado al marketing directo; el sponsoring,[127] apoyando a la imagen empresaria y en publicidad filantrópica sumando puntos justo con las acciones promocionales.

Hoy en día la publicidad y el marketing abren nuevas perspectivas, no sólo para ventas, sino para un estilo de vida.

[127] Constituye una forma de comunicación que permite ligar directamente una marca o una sociedad con un acontecimiento atractivo para un público determinado.

En los siguientes tópicos examinaremos específicamente a tres medios de comunicación masivos que constituyen una realidad de nuestro tiempo debido a que existe una vinculación directa hacia la persona, y en donde sí, se realizan ventas directas, además de haber una mayor cantidad de agresiones por estos medios de comunicación.

Se escogieron únicamente Internet, correo electrónico y el teléfono, puesto que en estos medios de comunicación se da de forma más concreta y específica la violación de datos personales; la publicidad va con especificidad dirigida al individuo en la que previamente le han sido recopilados y tratados sus datos, haciendo un estudio del comportamiento de la persona y obteniendo su perfil de consumo, es por ello que la mayor demanda de información desde las diversas perspectivas se ha dado con el perfeccionamiento de las tecnologías informáticas.

En concreto la libertad informática constituye uno de los más claros exponentes de la realidad de nuestros tiempos, porque la información es trato de la sociedad de la información o también denominada sociedad de red, como un modelo de organización industrial, cultural y social caracterizado por el acercamiento de las personas a la información a través de las nuevas TIC´s.

En concreto, si se toma en consideración que el derecho fundamental indicado implica la tutela de los “datos personales de las personas físicas” y no de las morales, colectivas o jurídicas privadas, se justifica porque el derecho a la protección de los datos personales se refiere únicamente al individuo por estar encausado el respeto de un derecho personalísimo, esto es porque no se actualiza una igualdad jurídica entre las personas físicas y las morales o colectivas porque ambas están en situaciones de derecho dispares al publicitarles por los medios tradicionales de comunicación o por las tecnologías de la información, ya que la protección de datos personales, entre ellos el del patrimonio y su confidencialidad, es propia y exclusiva de la cual goza el individuo, entendido como la persona humana.

4.2.1. Internet

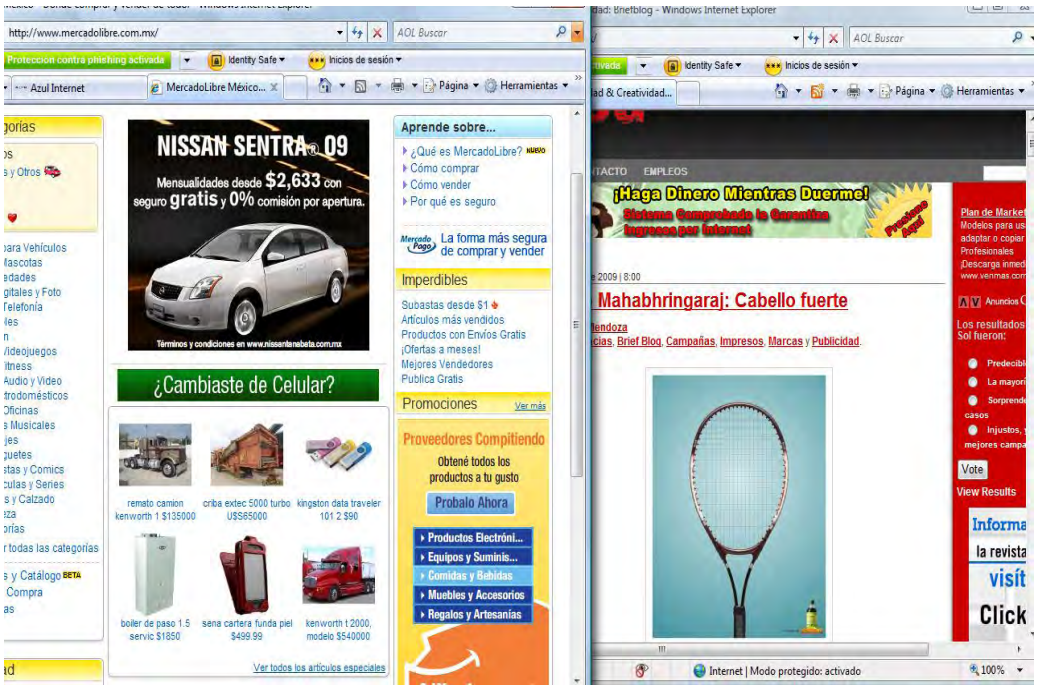
La publicidad en Internet es sin duda una de las herramientas que más ha crecido en los últimos años, su uso en América Latina es menor al comparado con países de alto desarrollo económico y tecnológico como Estados Unidos, Canadá, Inglaterra o Alemania. Abrir una cuenta en las páginas web es muy fácil y con la modalidad de pago por click, los anunciantes tendrán más oportunidades de recibir más visitas a sus páginas

En capítulos anteriores, establecimos que Internet se ha convertido en el nuevo canal de comunicación, como una interconexión de redes informáticas que permite una comunicación directa a las computadoras que se encuentran conectadas, ya sean redes locales conectadas entre sí a través de un ordenador o por vía satelital, por lo que se trata de la mayor red de conexión de ordenadores que se conoce en el mundo y que permite una comunicación (envío y recepción de información) rápida, sin límites de tiempo ni espacio.

Por ser Internet una vía de comunicación directa y prácticamente sin límites de territorio, la capacidad de creación se ve prácticamente capturada por los brazos del mercado, su potencia de invención para llegar al público consumidor se ha convertido en una fuente de lujo del capitalismo.

Hoy en día, Internet, se ha convertido en una sociedad informática de control, apoyado en las tecnologías electrónicas y digitales, una organización basada en el capitalismo más desarrollado, donde el marketing y la publicidad imperan hacia el consumo exacerbado de los bienes y servicios.

Vemos en Internet, gran cantidad de sitios web en los que con sólo ingresar a uno de ellos se bombardea nuestro monitor con gran cantidad de promociones:



A través de internet, se puede mantener información que se almacena en el disco duro del visitante de una página web a través de su navegador. Esta información puede ser luego recuperada por el servidor en posteriores visitas, a esto se le denomina *cookies* o "galletitas". De esta manera, las cookies permiten llevar el control de usuarios: nombre de usuario y contraseña, para que no tenga que estar introduciéndolas para cada página del servidor, así como conseguir información sobre los hábitos de navegación del usuario, e intentos de *spyware*[128], por parte de agencias de publicidad y otros, lo que ocasiona invariablemente problemas de privacidad.

Otra de las cuestiones que trae aparejada Internet, son los denominados *spam,* que consisten en correos electrónicos no solicitados o no deseados que se envían a múltiples usuarios con el propósito de hacer promociones comerciales,

[128] Se le denomina spyware a un programa espía y consiste en un software dentro de la categoría, que se instala furtivamente en una computadora para recopilar información sobre las actividades realizadas en ella. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas.

publicidad, ofertas por asistencia financiera o para tentar al usuario a visitar cierta página web. Los que envían spam construyen sus listas utilizando varias fuentes. Algunos utilizan programas que recogen direcciones de e-mail, otros recogen direcciones de otras listas de suscriptores, también pueden ser recogidos desde directorios de email on-line. Inclusive desde una sesión de chat. La lista de mailing spam también puede ser comprada a un vendedor legítimo al cual nosotros mismos le proporcionamos nuestra dirección de e-mail al comprar algún servicio o al registrarnos en alguna encuesta.

Estos ejemplos, ilustran la forma en que opera el mercado cultural contemporáneo. Hace algunos años, la empresa que administra el sitio web *My Space*, anunció el lanzamiento de su nuevo servicio de publicidad, para cuya implementación no sólo recurre a los datos personales que componen los perfiles de sus usuarios, sino también a eventuales informaciones rastreadas en sus blogs, gustos y hábitos de consumo, clasificando a sus usuarios en diferentes categorías según sus gustos sobre los autos, modas, finanzas, música, con el fin de que cada uno de ellos recibiera publicidad acorde con sus potenciales como consumidor.

En la actualidad, las empresas disponen aun más que, de simples datos demográficos sustraídos de formularios de inscripción o encuestas, el internet se ha convertido en una sociedad de información donde todos los consumidores somos presa de las estrategias de publicidad y marketing que rodea al sistema capitalista, siendo ello un ataque constante al derecho a la protección de datos personales.

4.2.2. Correo electrónico

El correo electrónico, es un sistema de comunicación que nació en 1971, época en que se utilizó la red Arpa net, la antecesora de Internet. En la actualidad ha variado mucho este antiguo esquema. Aunque su principal característica es su sencillez. Al enviar un correo, éste se almacena en un servidor y con la ventaja de

que puede utilizarse en cualquier computadora personal del mundo sabiendo los datos del usuario en cuestión.

Una cuenta de correo electrónico es un servicio online que consiste en un espacio para la recepción, envío y almacenamiento de mensajes de correo electrónico en internet, se asocia a un único usuario, el cual puede acceder a su cuenta a través de un nombre de usuario y contraseña, constituyendo así, un sistema de mensajería informática que permite el intercambio instantáneo de mensajes textuales y gráficos.

Las cuentas de e-mail suelen ser servicios que ofrecen empresas de forma gratuita como Yahoo, Hotmail, Google. Es decir que las comunicaciones electrónicas — que son el objeto protegido en la figura— se encuentran guardados, alojados, archivados, etc. en una cuenta de correo. De ahí que para violentar la intimidad del usuario, previamente debe tenerse acceso a la cuenta de e-mail. Recién una vez allí, el agresor podrá abrir, acceder, apoderarse, suprimir, desviar, interceptar o captar una comunicación electrónica, se puede señalar que, el mismo permite el envío de mensajes de remitentes a destinatarios, desde y hacia una casilla de correo, de unos y de otros, entrelazándose el sistema por un número indefinido de servidores — son computadoras de mayor capacidad— de propiedad de diferentes empresas, que se interconectan entre sí.

Así los avances tecnológicos que en los últimos tiempos se han producido en el ámbito de las telecomunicaciones, especialmente en conexión con el uso de la informática, hacen necesario un nuevo entendimiento del concepto de comunicación y del objeto de protección del Derecho fundamental, que extienda la protección a esos nuevos ámbitos.

En la actualidad, la irrupción masiva de la utilización de las nuevas tecnologías en materia de comunicación y transferencias de datos, mensajes e información que ha hecho que en la práctica millones de intercambios se realicen diariamente a

través de Internet, sustituyendo y ampliando los usos que antes tenía el intercambio de correo tradicional en virtud de su inmediatez y facilidad de utilización, lo cual indudablemente ha importado grandes beneficios para nuestra sociedad, sin perjuicio que paralelamente a dichos beneficios, muchos usuarios del servicio experimentan perjuicios tales como la posibilidad de violación del contenido de su correo electrónico y el denominado spam o correo comercial indiscriminado, que agresivamente es utilizado para ofrecer bienes y servicios no requeridos por el usuario de la red, y hasta la transferencia de programas dañinos.

El sistema jurídico mexicano, ha señalado que el consumidor podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su *dirección electrónica*, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad, exigiendo en todo momento a proveedores y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial.

La regulación específica en el ámbito de los servicios de la sociedad de la información relativa al *spam,* en España lo ha contemplado la Ley de Sociedades de la Información y Comercio Electrónico de 11 de julio de 2002.

Con esta regulación del correo electrónico comercial, incluidos otros medios equivalentes de publicidad electrónica, el Estado español se coloca en los altos estándares de protección, atento a las Directivas de la Comunidad Europea, en donde se extiende una regulación de las comunicaciones promocionales no solicitadas al correo electrónico, es decir, su remisión se encuentra condicionada al previo consentimiento expreso del destinatario.

4.2.3. Teléfono

El teléfono es considerado un medio de comunicación para enviar y recibir señales acústicas a distancia, esta tecnología de la información, ha permitido que las grandes empresas contemplen a la gran cantidad de usuarios que cuentan con este servicio para realizar el denominado telemarketing, utilizando para ello bancos de datos que previamente han sido elaborados, comprados o clasificados mediante la información de su historial de compras, encuestas, participación en sorteos o concursos, solicitudes de empleo (algunas de ellas sacadas de Internet) o como lo mencionamos, los nombres también pueden ser comprados de la base de datos de otra empresa u obtenidos de alguna guía telefónica u otra lista pública o privada.

El proceso de clasificación sirve para encontrar aquellos clientes potenciales con mayores probabilidades de comprar los productos o servicios que la empresa en cuestión ofrece, lo que violenta con ello el derecho a la protección de datos personales, pues ellos son distribuidos sin ninguna limitante entre los vendedores, publicistas, etc., generando en el cliente un riesgo potencial porque nunca sabemos en manos de quiénes pueden caer nuestros datos.

A través del teléfono, se realiza el telemarketing (técnica de mercado por teléfono) es una forma de marketing directo en la que un asesor de la empresa vendedora o promotora utiliza el teléfono para contactar con los posibles clientes y comercializar los productos y servicios.

Antes se estilaba que los operadores telefónicos eran vendedores que ofrecían productos y servicios sin importarles las necesidades de los consumidores sino solamente su beneficio económico y al azar, hoy por hoy, el operador telefónico ya no se considera un vendedor sino un asesor dependiendo el rubro que esté trabajando (comercial, financiero, publicitario, etc), y el que previamente ha tenido contacto con el historial de consumo del cliente. Comercializando productos o servicios en alternativas económicas. Para ello la empresa tuvo la ventaja de contar

con la fuerza de la información personal del cliente potencial para incrementar sus ventas, tomando como gancho o señuelo la necesidad del cliente derivada de las necesidades de compra que previamente haya efectuado.

El telemarketing para la empresa es un alto beneficio que se traduce en mejoras económicas, después de realizar un estudio potencial del cliente, sin embargo, se trata de una práctica con falta de ética al realizar muchas compañías llamadas telefónicas no deseadas y por utilizar técnicas de venta agresiva, pero sobre todo porque nuestros datos personales siguen circulando a diestra y siniestra, por lo que es necesario que esas prácticas sean objeto de control legislativo relacionados con la protección del consumidor.

En México, el Derecho del Consumidor ha establecido que los proveedores y empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios están obligados a informar gratuitamente a cualquier persona que lo solicite si mantienen información acerca de ella. De existir dicha información, tienen obligación de ponerla a su disposición o de su representante si lo solicita, e informar acerca de qué información han compartido con terceros y la identidad de esos terceros, así como las recomendaciones que hayan efectuado.

A pesar de que existen varios métodos para que las personas eviten las llamadas de telemarketing. Por ejemplo, utilizando el identificador de llamadas, una persona puede identificar al interlocutor antes de descolgar y tomar la decisión de no responder al teléfono, donde el usuario tiene derecho a que sus datos no sean transmitidos por doquier sin su autorización, de ahí la necesidad de regular estas acciones.

4.4. La protección de datos personales en la sociedad informatizada

En capítulos anteriores, señalamos que la protección de datos personales constituye la facultad jurídica del individuo de controlar y disponer de sus datos sean íntimos o no e impone la obligación a terceros de omitir o realizar actos que importen peligro al titular de aquellos frente al tratamiento automatizado o manual y que identifiquen o permitan la identificación de la persona, exigiendo la actuación del Estado para obtener la tutela constitucional de ellos.

Ahora bien, el tratamiento de datos personales en una sociedad informatizada es aquella donde hay creación, distribución y manipulación de información que forma parte de las actividades culturales y económicas dentro de los avances tecnológicos, los cuales derivaron en una nueva forma de interacción que se caracteriza por la relación en una denominada sociedad de la información, misma que se da mediante teléfonos, internet, televisión y satélites, todo lo que antes se hacía aisladamente, se conjunta para llegar a una forma de comunicación tecnológica.

Las actividades cotidianas como usar la tarjeta de crédito, ingresar a un sitio web, generan registros de datos sobre los consumidores, los cuales serán procesados para fines de control, publicidad y mercado. Este avance tecnológico en los últimos años y el aumento previsto en el número de usuarios, junto con el aumento de volumen de transacciones comerciales, constituyen la característica más destacada de la sociedad informatizada.

La capacidad de obtener información se ha visto potenciada de manera exponencial con la automatización de instrumentos para la captación de datos y del procedimiento por el cual se almacenan y procesan, que ahora se realiza en forma directa en el ordenador, es decir, en el mismo instante en que se generan los datos, ya están siendo almacenados para su posterior tratamiento, con lo cual la capacidad de recoger información se vuelve ilimitada.

Actualmente el mercado mundial del comercio electrónico está creciendo con gran rapidez, millones de personas están conectadas a internet en todo el mundo, por lo que ha sido necesario que se vayan adecuando propuestas, encaminadas a establecer un marco jurídico coherente para el desarrollo de los negocios electrónicos, en el cual se tenga que generar seguridad y confianza a los usuarios de los servicios y de transacciones *online*, a través de una firma electrónica, la cual es utilizada ya en muchos países y cuyo propósito es facilitar la manifestación de voluntad por vía electrónica en redes abiertas, eliminando las diferencias del reconocimiento legal de la firma.

El tema de la validez de la firma electrónica debe mantenerse íntimamente vinculado al tema de la contratación electrónica, que es la que ha generado la necesidad de aquélla y del reconocimiento de su fuerza ejecutiva y probatoria, para que los servicios de la sociedad informatizada, entendiendo por tales, los proporcionados de forma remunerada, a distancia, por vía electrónica y en respuesta a la petición individual del cliente, abarcando con ello los servicios de periódicos, financieros, profesionales, hobby, y en general cualquier tipo de servicio en línea, nos otorguen exactitud de quién o quiénes tienen poder de nuestros datos personales para hacer publicidad y comercializar.

Todo lo anterior, se manifiesta ante el uso indiscriminado de los datos personales para fines ilícitos, por lo que existe una gran desprotección del individuo ante la posibilidad de ser objeto de decisiones adoptadas con base en el tratamiento de sus datos personales en esta sociedad informatizada, que en ocasiones pueden ser falsos, no estar actualizados o discriminatorios, desnaturalizándose el fin para el que fueron recogidos.

Es por ello que las redes de Internet revisten cada vez mayor importancia para la comunidad mundial, ofreciendo nuevas posibilidades empresariales y creando herramientas que mejoran la productividad para crear nuevas formas de llegar al público consumidor, sin embargo, también se deben adoptar mecanismos

de control como lo mantiene la Directiva 95/46 sobre protección de las personas físicas en lo que respecta al tratamiento de datos personales y la libre circulación de éstos en el sector de las telecomunicaciones, por lo cual los proveedores únicamente pueden recabar datos personales directamente del titular de los mismos, los cuales no podrán obtenerse o tratarse con fines distintos sin el consentimiento de su titular, ya que también, el usuario se pudiere encontrar en una situación de desventaja.

4.4.1. Alcance de la informática y sus repercusiones en el disfrute de los derechos fundamentales

La palabra informática, fue acuñada en 1962 por el Ingeniero Philippe Dreyfrus, como una conjunción de las palabras información automática. La informática constituye las técnicas, maquinaria y procesos para apoyar de manera ágil y eficaz la comunicación del hombre, empero podemos decir que es la disciplina que se encarga del estudio de los ordenadores (computadoras), para almacenar, procesar y transmitir información en datos de manera digital.

De ahí podemos ver su utilización al servicio del Derecho; sin duda es que desde éste ángulo se llega a la conclusión que nos encontramos frente a la informática jurídica que es de manejo cotidiano en los distintos estudios y que permite a los profesionales del derecho poder contar de manera inmediata con doctrina y jurisprudencia conforme el caso que les ocupe.

Cuando la informática se analiza como objeto del derecho, el ángulo de la temática cambia porque nos encontramos frente al llamado "derecho informático", ámbito en el que debe de tenerse en cuenta la libertad de información, el índice de criminalidad, el derecho a protección de datos personales, el derecho a la intimidad, a la privacidad, etc.

La realidad así planteada, nos lleva inmediatamente a conectarnos con la problemática jurídica, que debe tener en cuenta un sinnúmero de situaciones que devienen de un mismo origen con connotaciones y consecuencias diferentes, en donde están en juego los derechos fundamentales.

El propósito es impedir que el uso de la informática pueda lesionar en su contenido los derechos fundamentales (honor, intimidad, etc.,) como consecuencia de una información inexacta, incompleta, no actualizada, falaz o derivada del uso del delito.

La cesión masiva de información a través de la informática vulnera el derecho a la autodeterminación informativa, toda vez que la recopilación, tratamiento, y transferencia de los datos personales, son usados de manera desmedida. Sin duda alguna, la información generalizada y abierta produce el progreso de la ciencia y la tecnología, pero al mismo tiempo abre un frágil espacio que pretende superar los ámbitos privados de la confidencialidad.

La mayoría de las personas que usan el internet, no saben que mientras navegan, están siendo vigiladas por todos aquellos sitios que visitan, creándose así el perfil del individuo y violentando sus derechos. Los datos personales son objeto de tratamiento con diversas finalidades y sin nuestro consentimiento a través del uso de las redes. El flujo de datos y de información es hoy en día la base de productividad del capital, sin que nosotros tengamos conocimiento de quién o quiénes están detrás de ese tratamiento.

Como respuesta a ello, la República Argentina, cuenta con un organismo de Protección de Datos Personales que constituyó el primer escalón en la protección de este derecho ante las denuncias y los reclamos de quienes hubieran sufrido algún perjuicio o menoscabo. Una segunda protección, lo constituye la justicia, los jueces están interpretando el derecho a la protección de los datos personales de manera dinámica y creativa a través de sus fallos que reiteran el contenido del artículo 19 de la Constitución.

Es por ello, que la protección de datos pueden conducir tanto a nivel estatal como a nivel privado a mejorar el tratamiento de la información más sensible, e internacionalmente a cumplir con estándares que ayuden al comercio y a los servicios internacionales a posicionarse de modo más competitivo, alejando a la informática de ser considerada como un mal y sacando el mayor provecho de esta tecnología.

En México, el artículo 42 de la LFPDP, sostiene que en lo referente a las bases de datos de comercio, la regulación que emita la Secretaría, únicamente será aplicable a aquellas bases de datos automatizadas o que formen parte de un proceso de automatización; cuestión que es complementada con lo dispuesto por el artículo 43 párrafo 8, en la que atribuyen a la Secretaría de Economía, diseñar e instrumentar políticas y coordinar la elaboración de estudios para la modernización y operación eficiente del comercio electrónico, así como para promover el desarrollo de la economía digital y las tecnologías de la información en materia de protección de datos personales

4.5. Aspectos relevantes del Binomio protección de datos personales y publicidad y marketing

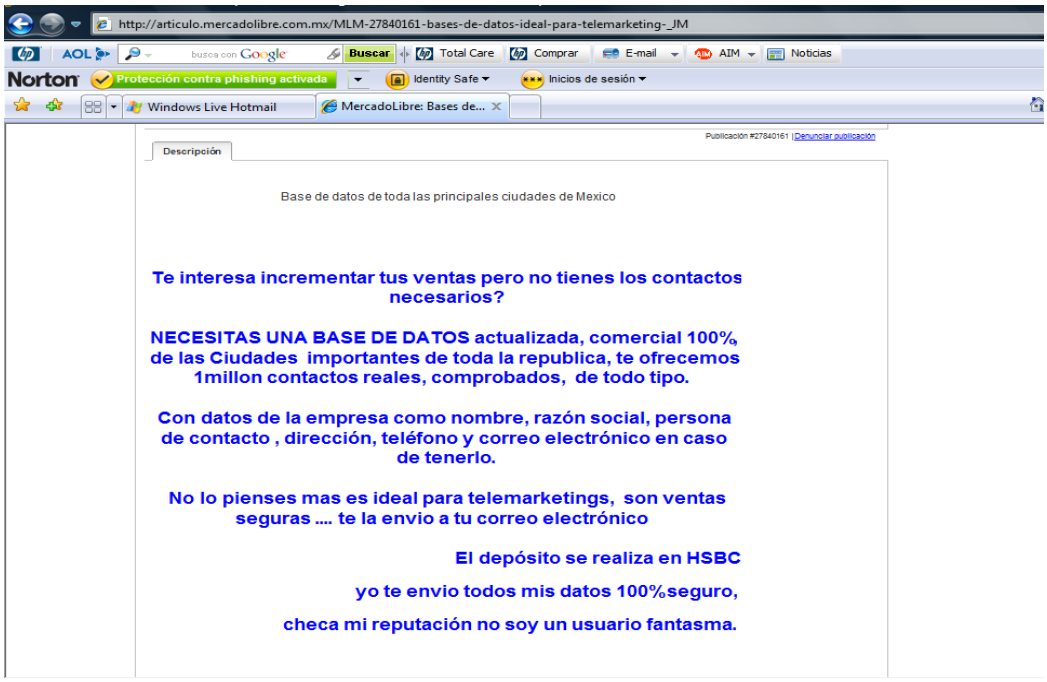
A lo largo del presente trabajo hemos referido lo que implica el derecho de protección de datos personales y su vulneración por diversos medios de comunicación, es momento de revisar la regulación específica de este derecho en el caso concreto de la publicidad y el marketing en Argentina y México.

Para el marketing, las bases de datos se transforman en una herramienta privilegiada, elaborándose perfiles de posibles clientes. Al respecto, algunas legislaciones regulan esta actividad meramente comercial que, para lograr un mejor posicionamiento en el mercado mediante la búsqueda de consumidores potenciales para productos o servicios específicos, recopilan datos, como los hábitos de consumo, y cuyo fin es el de establecer perfiles que puedan coincidir con tales

pretensiones comerciales, lucrando en muchas ocasiones con las bases de datos y poniéndose a la venta incluso por Internet, como lo vemos en los siguientes cuadros.

CUADRO 1

CUADRO 2



Toda vez que Argentina, posee una regulación especializada, la abordaré primero, para después verificar las deficiencias de la regulación en México.

La ley 25.326 de la República Argentina sostiene en el artículo 27: *Archivos, registros o bancos con fines de publicidad. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando estos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.*

En alcance al citado numeral, el Decreto Reglamentario 1558/01, sostuvo que podrán recopilarse, tratarse y cederse datos con fines de publicidad sin consentimiento de su titular, cuando estén destinados a la formación de perfiles determinados que categoricen preferencias y comportamientos similares de las personas, siempre que los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos genéricos.

En dicha normativa, se manifiesta que las particularidades de los archivos de datos con fines de publicidad son referidas a los temas del consentimiento para la obtención y uso de información personal para determinar perfiles o establecer hábitos de consumo, el derecho de acceso gratuito permanente, y la calidad de los datos que se pueden trabajar en marketing.

Para Osvaldo Gozaini,[129] la formación de perfiles determinados suponen generalizar los gustos, las preferencias y conductas de las personas, de modo tal que, a partir de la clasificación y orden que se practica, se pueden conocer las preferencias o gustos de la misma, logrando de esa manera dirigir con alguna precisión, en forma directa o indirecta, ofertas, promociones o ventas a través de

[129] GOZAINI, Osvaldo Alfredo. *Derecho Procesal Constitucional. Hábeas Data. Protección de datos personales. Ley 25.326 y reglamentación (decreto 1558/20001).* P. 328.

cualquier medio. Asimismo, el citado autor refiere que los hábitos de consumo constituyen información personal; tienen carácter individual y requieren de mayores seguridades para la formación de archivos específico.

Este régimen especial, adoptado por la Ley de Hábeas Data 25.326, legitima esta clase de actividad para fines comerciales que supone la recopilación de datos relativos al interés de consumir determinados productos o servicios y hábitos de consumo, sin embargo a estas prácticas publicitarias deben sumarse el resto de los articulados de la ley para preservar el goce de los derechos del titular de los datos, a saber: información al titular, licitud, calidad y sujeción a la finalidad de su registración, seguridad, confidencialidad y transferencia internacional, lo que obliga a los oferentes a advertir al titular del dato sobre qué datos van a ser registrados o ingresados en una base de datos, para marketing, así como cumplir los extremos del artículo 6º de la Ley:

b) Deber de información,
c) Objeto y destinatarios,
d) Datos del archivo,
e) Información adicional,
f) Consecuencias de proporcionar datos, negativa a hacerlo o inexactitud de los mismos,
g) Ejercicio de los derechos de acceso, rectificación y supresión de datos.

La sujeción a la finalidad del registro, se manifiesta en la pertinencia de los datos que pueden ser recogidos, es decir, estrictamente necesarios para tratar su perfil o hábito de consumo, empero se debe tener cuidado cuando se trate de datos sensibles, pues cuando estos puedan ser tratados, el responsable del archivo o registro deben asignar prioridad a la prohibición de tratamiento, por encima del interés lucrativo, excepto cuando el titular preste su consentimiento expreso y previamente haya sido informado de las consecuencias de facilitar esos datos, y su derecho a oponerse; en segundo lugar, la finalidad, es decir, que las listas de

consumidores sean utilizadas para el propósito por el que fueron recopilados y por último, el responsable de la base de datos debe adoptar medidas para protegerlos de acceso no autorizados, adoptando medidas de seguridad y preservando su confidencialidad.

En el caso de los archivos de datos con fines de publicidad, las particularidades del caso, son referidas a los temas del consentimiento para el tratamiento de los datos personales, el derecho de acceso y la calidad de ellos que pueden ser trabajados en marketing.

En el sistema mexicano, la *Ley Federal de Protección al Consumidor* asegura los datos personales y nos dice que los proveedores y empresas que utilicen información sobre consumidores con fines de mercadotecnia o publicidad, están obligados a informar gratuitamente a cualquier persona que lo solicite si mantienen información acerca de ella y para los casos en que exista tal información, deben ponerla a disposición del interesado, e informar acerca de qué información han compartido con terceros y la identidad de esos terceros, así como las recomendaciones que hayan efectuado. La ley entiende por mercadotecnia y publicidad el ofrecimiento y promoción de bienes, productos o servicios a consumidores.

Según el Derecho del Consumidor, en la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor, de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la Procuraduría, esto se da con el fin de identificar a las empresas que cuentan con archivos de datos personales, y a los cuales el consumidor tiene el derecho de exigir directamente no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad, así como que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial, pero

quedando prohibido a las empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios y a sus clientes, utilizar la información relativa a los consumidores con fines diferentes a los mercadotécnicos o publicitarios, así como enviar publicidad a los consumidores que expresamente les hubieren manifestado su voluntad de no recibirla o aquéllos que se encuentren inscritos en el registro que se lleva ante la Procuraduría Federal del Consumidor.

Por último la el derecho mexicano señala que el proveedor que utilice la información del consumidor, deberá hacerlo en forma confidencial, y no podrá difundirla o transmitirla a terceros, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente.

La legislación mexicana de protección al consumidor, sigue el mismo parámetro que la *"Ley de Hábeas Data"* en el sentido de la necesidad de consentimiento del titular para el tratamiento y cesión de sus datos personales tratándose de marketing y publicidad, con la diferenciación de que no establece de manera específica el consentimiento aun cuando los datos se encuentren disociados, pues la norma mexicana hace hincapié a todos los casos.

Uno de los principales problemas a los que se enfrenta México, es el tratamiento y recaudación de datos de carácter personal, pero sobre todo el abuso hacia los consumidores sobre publicidad engañosa por parte de los proveedores que intenten vender sus productos, haciendo creer al consumidor la adquisición de un beneficio específico; por tanto la PROFECO ha puesto en marcha en coordinación con otras autoridades (según el producto que se oferte y la autoridad reguladora) un monitoreo especial en prensa, radio, televisión e internet, con la finalidad de detectar publicidad engañosa o abusiva que induce al consumidor al error o confusión, habilitando con ello un correo especial para reportar cualquier anomalía (publicidad@profeco.org.mx).

Ante ese escenario, la PROFECO, ejerció las facultades conferidas por la ley para requerir la comprobación de frases publicitarias y ordenar la suspensión de

mensajes engañosos, instando a los consumidores a no proporcionar información personal por Internet, ya que esto aumenta el riesgo de robo de datos personales, esto ha constituido un avance en la materia con fines de publicidad, la actividad no es ilícita, siempre y cuando el titular de los datos otorgue su consentimiento y se encuentre informado, sin embargo, la Ley Federal de Protección de Datos Personales en Posesión de Particulares es omisa sobre el particular, por lo que esta actividad regulatoria en materia de publicidad se encuentra en poder de la Procuraduría Federal de Protección al Consumidor, no así al IFAI como nuevo organismo de protección de datos personales.

Sin embargo, la LFPDP, deja abierta la posibilidad de distribución de competencias y atribuciones en materia de comercio a la Secretaría de Economía, en los siguientes términos:

> Artículo 43. La Secretaría tiene las siguientes atribuciones
>
> I. Difundir el conocimiento respecto a la protección de datos personales en el ámbito comercial;
> II. Fomentar las buenas prácticas comerciales en materia de protección de datos personales;
> III. Emitir los lineamientos correspondientes para el contenido y alcances de los avisos de privacidad en coadyuvancia con el Instituto, a que se refiere la presente Ley;
> ...
> ...
> VI. Llevar a cabo los registros de consumidores en materia de datos personales y verificar su funcionamiento;
> VII. Celebrar convenios con cámaras de comercio, asociaciones y organismos empresariales en lo general, en materia de protección de datos personales;
> VIII. Diseñar e instrumentar políticas y coordinar la elaboración de estudios para la modernización y operación eficiente del comercio electrónico, así como para promover el desarrollo de la economía digital y las tecnologías de la información en materia de protección de datos personales;
> IX. Acudir a foros comerciales nacionales e internacionales en materia de protección de datos personales, o en aquellos eventos de naturaleza comercial, y
> ...

Lo anterior permite a la Secretaría emitir la regulación correspondiente para las mejores prácticas comerciales respecto a la protección de datos personales, como autoridad reguladora en este ámbito, pero sin precisar aun las circunstancias sobre el manejo de datos con fines publicitarios.

La actividad del marketing es lícita, siempre y cuando los datos personales sean utilizados con el fin legítimo para el que fueron recopilados, y se preserve el derecho del titular de no participar en esa actividad, advirtiéndose además previamente que los datos que proporcionarán serán ingresados en una base de datos para marketing y serán cedidos a terceros, pues en tal caso no hay lesión a los bienes jurídicos de los consumidores y se favorece el desarrollo de las prácticas publicitarias vinculadas con la libertad de comerciar y ejercer la libre competencia, cuya prohibición podría además colocar en una situación de desventaja para nuestra inserción en el mercado internacional.[130]

El que los consumidores sean advertidos con toda oportunidad de proporcionar sus datos, de que éstos van a ser ingresados en una base de datos para marketing, constituye un requisito esencial para el respeto a sus derechos personalísimos. Que la ley autorice a las empresas a utilizar datos personales con fines lucrativos, es un aspecto de libertad que merece ser respetado; si ello se realiza con deslealtad y ocasiona molestias en la vida privada, esto es deshonesto e ilegal.[131]

Veamos a continuación cuáles son los casos en que pueden tratarse datos con fines publicitarios y como ha sido regulado en Argentina y México.

4.5.1. Casos en los que se pueden tratar datos con fines de publicidad

De conformidad a la Ley 25.326 en su artículo 27, apartado 1, se pueden tratar datos con fines de publicidad, y dispone que son archivos con fines de publicidad los que persigan:

[130] GILS CARBÓ, Alejandra. *Régimen legal de las bases de datos y Hábeas Data.* La Ley, Argentina, 2001, P. 154
[131] *Ídem.*

a) Recopilar domicilios.

b) Repartir documentos.

c) La publicidad o venta directa, y otras actividades análogas.

Con relación al inciso a), Osvaldo Gozaini,[132] mencionaba que la recopilación del domicilio, no tiene como finalidad la identificación de la persona, sino el de generar un marco de referencia que identifique una zona donde se pueda llevar a cabo un emprendimiento particular. El domicilio es un dato de carácter público y disponible, de modo tal que no encuentra limitaciones para su aplicación y uso en una base de datos con fines de publicidad.

Respecto al inciso b), los registros que van destinados al reparto de documentos, adicionan al domicilio datos reveladores de una preferencia a habitualidades del consumidor, Gozaini,[133] refiere el ejemplo de la suscripción de revistas que llegan a domicilio.

Puccinelli,[134] hace una crítica relacionada con el último de los incisos, toda vez que considera que la publicidad y la venta directa que refiere el inciso c), no pueden considerarse como sinónimos como lo pretende hacer ver la norma, porque la publicidad va en abstracto, es decir, va dirigida a un público indeterminado, a través de la radio, televisión, gráficos, viales, o por otros medios de comunicación, como los correos postales o por internet, sin que el nombre del destinatario sea específico, en cambio en la venta directa, la actividad va dirigida a la persona determinada, siendo específico sobre el individuo al que se va a ofrecer el bien o servicio, por ejemplo por telemarketing en que el asesor tiene contacto directo con el cliente-consumidor, por lo que la disyunción "o" no es correcta debido a que puede generar confusión en dos cosas que son totalmente diferentes.

---

[132] GOZAINI, Osvaldo Alfredo. *Derecho Procesal Constitucional. Hábeas Data. Protección de datos personales. Ley 25.326 y reglamentación (decreto 1558/20001).* P. 325

[133] *Ídem.*

[134] *Ob. Cit. Protección de Datos de Carácter Personal.* P. 400

Afirmación que comparto, es necesario que se haga la distinción de estas dos actividades, ya que el poder separarlas permitiría obtener una mejor regulación pues se puede especificar la actividad en concreto tanto en Argentina como en México, en la publicidad, el público es abstracto mientras que en la venta directa, si tiene trato inmediato con el consumidor.

Como todo archivo de datos personales en poder de proveedores y empresas, éstas tienen la obligación de cumplir con los principios que marca la ley de la materia, es decir, la recolección de los datos no podrá ejercerse de manera alguna a través de medios ilícitos, por lo cual el portador de los archivos de datos deberá hacer del conocimiento al afectado sobre la recolección de sus datos personales, así como el tratamiento para el cual serán recabados.

Ello también implica desde luego que el proveedor o la empresa que tenga en su poder archivos de datos personales tenga la obligación de mantener la información almacenada bajo un alto nivel de seguridad y confidencialidad, sobre todo cuando se traten de datos sensibles (aquéllos que puedan constituir los hábitos de consumo).

Por ende, cuando el proveedor o la empresa solicite a las personas la proporción de sus datos cuyos fines sean promocionales debe advertírseles de manera precisa el destino y tratamiento que se les va a dar y quiénes serán los posibles destinatarios, sin que estos datos puedan ser recogidos por medios ilícitos o engañosos. Bajo este concepto, el titular tiene el derecho de negarse a que sus datos sean tratados con los fines para los que fueron recabados, y en especial a que sean cedidos a terceros o no, esto con el objetivo de que el interesado o titular de los datos pueda ejercer su derecho de acceso.

En todos los casos, es necesaria la identificación del responsable del fichero a fin de tener la precisión y seguridad de que sus datos están en poder de una persona jurídica determinada,

Ahora bien, la ley, sostiene que hay pertinencia de los datos que pueden ser recogidos, es decir, los que sean estrictamente necesarios para tratar un perfil o hábito de consumo, sin embargo, es considerado un poco riesgoso, toda vez que puede existir información que revelen directa o indirectamente datos sensibles, esto es que, mediante la adquisición de determinados productos, es factible determinar o evidenciar datos sobre la conducta del individuo, en cuanto su aspecto sexual, ideológico, patológico, religión, etc.

En todo momento resulta necesario que las empresas se sometan al régimen sobre el cual radica la autorización del uso de datos no disponibles, respecto de los cuales en algunos casos se exime del consentimiento y en otros se autoriza la elaboración de perfiles,[135] que categoricen preferencias y comportamientos similares de las personas; para ello, la propia ley garantiza el derecho de acceso del titular de los datos sin limitaciones con el fin de bloquear o retirar los mismos, así como su eliminación total o parcial, y la exclusión inmediata de los registros.

Por último, sólo nos resta mencionar que aquellas bases de datos que sirven para proveer informes a terceros con fines publicitarios deben inscribirse en el Registro de Archivos de Datos Personales, según lo dispuesto por el artículo 21 de la ley 25.326, organismo dependiente de la Dirección Nacional de Protección de Datos Personales en la Argentina.

En México, la Ley Federal de Protección al Consumidor, establece en el artículo 51 la venta a domicilio, mediata o indirecta, lo que obliga al proveedor la identificación por escrito de la operación y los datos del mismo: nombre y domicilio del proveedor e identificación de las operaciones y de los bienes y servicios de que se trate.

[135] "La formación de perfiles determinados suponen generalizar los gustos, las preferencias y conductas de las personas, de modo tal que, a partir de la clasificación y orden que se práctica, se pueden conocer las preferencias o gustos de la misma, logrando de esa manera dirigir con alguna precisión, en forma directa o indirecta, ofertas, promociones o ventas a través de cualquier medio". GOZAINI, Alfredo. *Ob. CIt.* 328

Las operaciones entre proveedores y consumidores son lícitas siempre y cuando exista el consentimiento del titular del dato y se respeten los principios de confidencialidad de la información empero deberá abstenerse el proveedor de utilizar información engañosa y no sea clara y suficiente por los servicios ofrecidos por él, sin embargo, ni en la Ley Federal de Protección al Consumidor ni en la Ley Federal de Protección de Datos Personales, se enuncia de manera concreta en qué casos pueden tratarse datos con fines de publicidad, lo que deja sólo a interpretación de su articulado.

Así lo desprendemos del artículo 2 de la LFPDP al establecer:

> "Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado **que lleven a cabo el tratamiento de datos personales**, **con excepción de**:
> I. Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y
> II. **Las personas que lleven a cabo la recolección y almacenamiento de datos personales**, **que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial."**

A contrario sensu la fracción II, nos menciona que *son sujetos de esta ley los que lleven a cabo la recolección y almacenamiento de datos personales, que no sean para uso exclusivamente personal, y que tengan fines de divulgación o utilización comercial.*

Lo mismo ocurre con la Sección II del Capítulo VI, de la referida Ley que delega a la Secretaría de Economía, el establecimiento de una regulación en materia comercial en lo que refiere a la protección de datos personales, disponiendo en su artículo 41:

> "La Secretaría (Secretaría de Economía), para efectos de esta Ley, tendrá como función difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial en territorio mexicano; promoverá las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía digital, y el desarrollo económico nacional en su conjunto".

El artículo 42 dispone:

"En lo referente a las bases de datos de comercio, la regulación que emita la Secretaría, únicamente será aplicable a aquellas bases de datos automatizadas o que formen parte de un proceso de automatización.

Y el artículo 43 sostiene:

"La Secretaría tiene las siguientes atribuciones:

I. Difundir el conocimiento respecto a la protección de datos personales en el ámbito comercial;
II. Fomentar las buenas prácticas comerciales en materia de protección de datos personales;
III. Emitir los lineamientos correspondientes para el contenido y alcances de los avisos de privacidad en coadyuvancia con el Instituto, a que se refiere la presente Ley;
IV. Emitir, en el ámbito de su competencia, las disposiciones administrativas de carácter general a que se refiere el artículo 40, en coadyuvancia con el Instituto;
V. Fijar los parámetros necesarios para el correcto desarrollo de los mecanismos y medidas de autorregulación a que se refiere el artículo 44 de la presente Ley, incluido la promoción de Normas Mexicanas o Normas Oficiales Mexicanas, en coadyuvancia con el Instituto;
VI. Llevar a cabo los registros de consumidores en materia de datos personales y verificar su funcionamiento;
VII. Celebrar convenios con cámaras de comercio, asociaciones y organismos empresariales en lo general, en materia de protección de datos personales;
VIII. Diseñar e instrumentar políticas y coordinar la elaboración de estudios para la modernización y operación eficiente del comercio electrónico, así como para promover el desarrollo de la economía digital y las tecnologías de la información en materia de protección de datos personales;
IX. Acudir a foros comerciales nacionales e internacionales en materia de protección de datos personales, o en aquellos eventos de naturaleza comercial, y
X. Apoyar la realización de eventos, que contribuyan a la difusión de la protección de los datos personales.

Como podemos ver, la LFPDP establece ciertos parámetros en materia de comercio y datos personales, pero señalando a la Secretaría de Economía como autoridad reguladora en ámbitos comerciales, sin embargo, la legislación es omisa en señalar en qué momentos se pueden tratar datos con fines de publicidad, pero atribuye a la autoridad reguladora el fijar parámetros y lineamientos necesarios para el desarrollo de las actividades comerciales y buenas prácticas en materia de protección de datos personales.

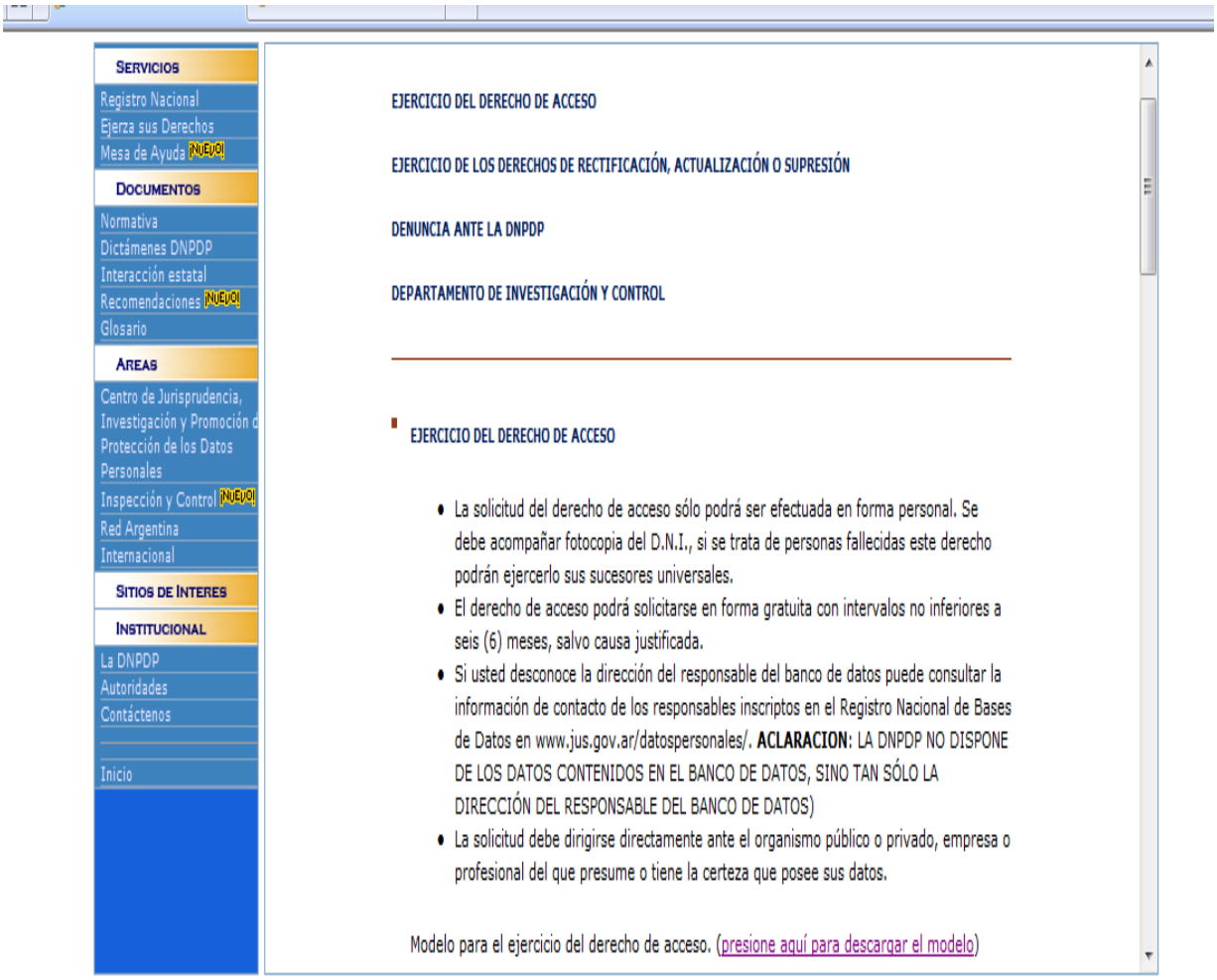
4.5.2. Derecho de acceso del titular de los datos

La Ley 25.326 de Hábeas Data, destina un capítulo especial sobre los derechos de los titulares de los datos, que en palabras de Oscar Puccinelli,[136] se proyectan en una serie de potestades que son reconocidas a toda persona que desee conocer la existencia y características de registro de datos de carácter personal, verificar el contenido de ellos y, en su caso, operar sobre sus datos y los sistemas de información.

El artículo 14 de la ley en comento sostiene que "*El titular de los datos, previa acreditación de su identidad, tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes. 2. El responsable o usuario debe proporcionar la información solicitada dentro de los diez días corridos de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido, o si evacuado el informe, éste se estimara insuficiente, quedará expedita la acción de protección de los datos personales o de hábeas data prevista por la ley. 3. El derecho de acceso a que se refiere este artículo sólo puede ser ejercido en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legitimo al efecto. 4. El ejercicio del derecho al cual se refiere este artículo en el caso de datos de personas fallecidas le corresponderá a sus sucesores universales.*"

La Dirección Nacional de Protección de Datos Personales en la Argentina, reconoce este derecho en su sitio web, incluyendo los formularios de petición de acceso a los archivos de datos personales en poder de particulares o archivos públicos, como se señala a continuación:

[136] *Ob. Cit. Protección de Datos de Carácter Personal.* Pág. 263



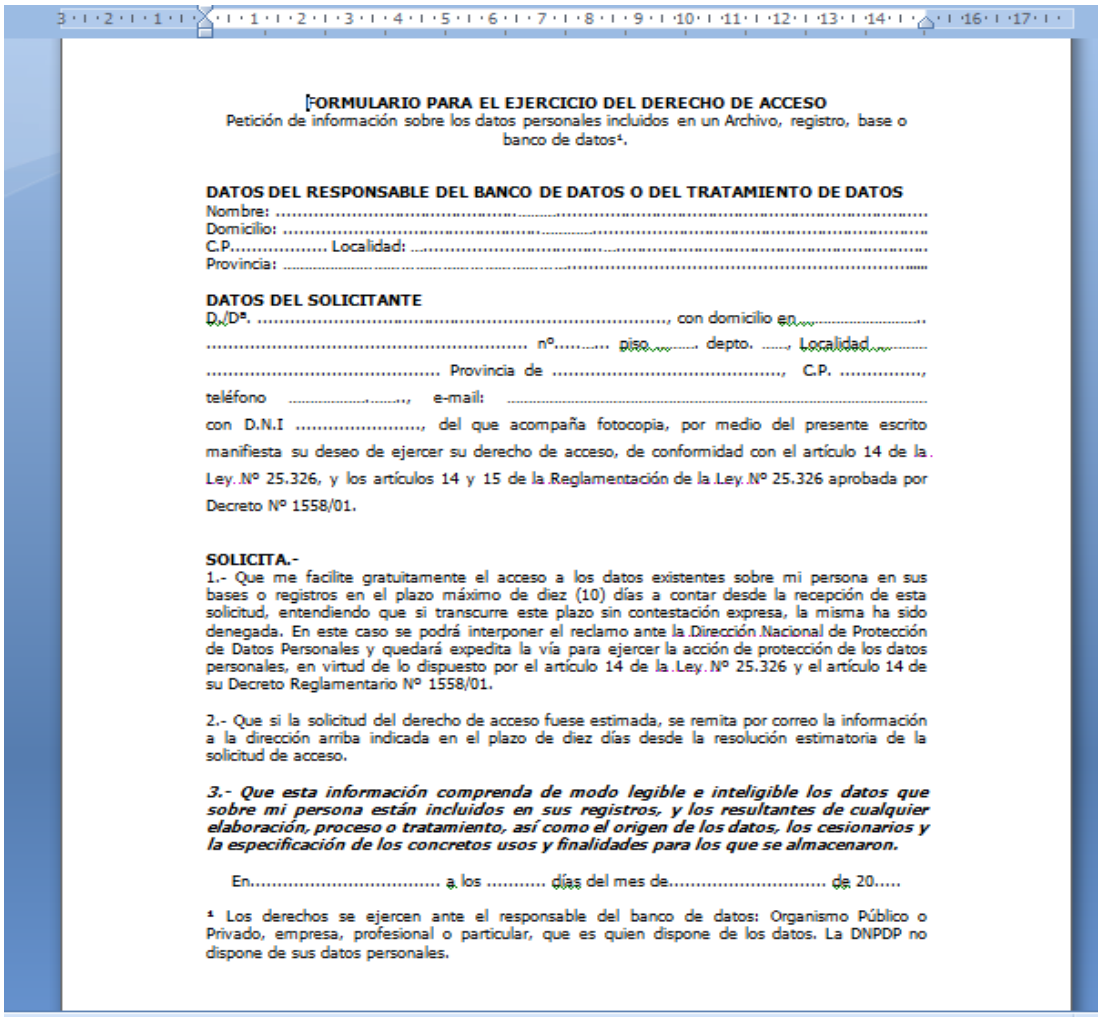
137

Aquí la Dirección Nacional brinda asesoría a las personas que se encuentren interesadas en solicitar a un organismo público o privado el acceso a sus datos personales, antes de ejercer la vía jurisdiccional o el hábeas data.

El siguiente cuadro, muestra el modelo de formulario que debe ser llenado, y el cual será entregado en el organismo correspondiente para intimarlo, para ejercitar el derecho referido, según lo dispone el artículo 14.2 de la Ley 25.326, esta carta documento, es importante que en términos del artículo citado se intime al responsable del archivo de datos, toda vez que ante la omisión de hacerlo y en su

[137] http://www.jus.gov.ar/dnpdpnew/

defecto se promueva el amparo, el juez puede rechazar, o en su defecto si el juez da curso y el emplazado rinde el informe respectivo de manera oportuna y satisfactoria, se evidenciaría que el actor no tenía motivos para promover un trámite judicial, y en consecuencia se le hará la imputación de costas al accionante.



FORMULARIO PARA EL EJERCICIO DEL DERECHO DE ACCESO
Petición de información sobre los datos personales incluidos en un Archivo, registro, base o banco de datos[1].

DATOS DEL RESPONSABLE DEL BANCO DE DATOS O DEL TRATAMIENTO DE DATOS
Nombre: .....
Domicilio: .....
C.P..... Localidad: .....
Provincia: .....

DATOS DEL SOLICITANTE
D./Dª. ....., con domicilio en .....
..... nº..... piso..... depto. ....., Localidad .....
..... Provincia de ....., C.P. .....,
teléfono ....., e-mail: .....
con D.N.I ....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con el artículo 14 de la Ley Nº 25.326, y los artículos 14 y 15 de la Reglamentación de la Ley Nº 25.326 aprobada por Decreto Nº 1558/01.

SOLICITA.-
1.- Que me facilite gratuitamente el acceso a los datos existentes sobre mi persona en sus bases o registros en el plazo máximo de diez (10) días a contar desde la recepción de esta solicitud, entendiendo que si transcurre este plazo sin contestación expresa, la misma ha sido denegada. En este caso se podrá interponer el reclamo ante la Dirección Nacional de Protección de Datos Personales y quedará expedita la vía para ejercer la acción de protección de los datos personales, en virtud de lo dispuesto por el artículo 14 de la Ley Nº 25.326 y el artículo 14 de su Decreto Reglamentario Nº 1558/01.

2.- Que si la solicitud del derecho de acceso fuese estimada, se remita por correo la información a la dirección arriba indicada en el plazo de diez días desde la resolución estimatoria de la solicitud de acceso.

3.- Que esta información comprenda de modo legible e inteligible los datos que sobre mi persona están incluidos en sus registros, y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

En..... a los ..... días del mes de..... de 20.....

[1] Los derechos se ejercen ante el responsable del banco de datos: Organismo Público o Privado, empresa, profesional o particular, que es quien dispone de los datos. La DNPDP no dispone de sus datos personales.

138

El derecho de acceso, el cual ha sido acuñado bajo el conocido nombre de la propia ley "Hábeas Data", es la forma más pura de lo que la sentencia del Tribunal Alemán denominó en diciembre de 1983 como "autodeterminación informativa", y en la cual, el individuo solicita el acceso a una base de datos que contenga

138 *Ídem.*

información acerca de aquélla, ya sea en registros públicos o registros privados, de manera extrajudicial o de manera judicial y en algunos países como en México, de manera administrativa cuyo derecho lo confiere el artículo 16 constitucional y recientemente la Ley Federal de Protección de Datos Personales, principio que previo a la vigencia de esta nueva legislación, lo acuñaba la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y leyes conexas sobre la materia de carácter estadual e incluso municipal.

El objeto de este derecho es el conocimiento de los datos personales de una persona identificada o identificable, de modo claro, completo y exacto, de tal suerte que el afectado se encuentre en posibilidad de conocer el tratamiento que se le ha efectuado a sus datos personales, si estos son ciertos, o requieren de alguna modificación, supresión o bloqueo, por ser datos erróneos, imprecisos o falsos.

El procedimiento comienza con la solicitud que realiza el titular de los datos al responsable de un archivo de carácter público o privado destinados a dar informes, previa acreditación de la identidad y también el apoderado o representante legal, ampliando la norma la legitimación de quien los solicita, ya que según el artículo 43 de la Constitución Argentina, es un derecho personalísimo que sólo habilita para promover la acción de hábeas data a la persona cuyos datos sean objeto de tratamiento, derecho que puede hacerse incluso verbalmente, porque la norma no prohíbe ni indica nada.

El responsable tiene el término de diez días para producir un informe, cuyo contenido debe ser claro y preciso, y en su caso acompañarse alguna explicación que facilite la comprensión, conteniendo la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales, empero, bajo ningún aspecto deben proporcionarse datos de tercero aun cuando estuvieren vinculados al solicitante.

Es importante señalar que el solicitante del derecho de acceso tiene el beneficio de gratuidad, siempre y cuando este derecho no lo realice en un intervalo menor a 6 meses, esto con el fin de no generar sobrecarga de peticiones, toda vez que se generarían gastos. Asimismo, la entrega de la información, puede ser según a elección del titular de los datos, por un medio electrónico, copias, telefónico, etc., y siempre que la reproducción de la información pudiere tener un costo se le hará saber al titular de manera justificada a fin de hacer el recaudo que corresponda.

Ahora bien, como todo derecho establecido en las Constituciones es absoluto, el derecho de acceso del titular de los datos, tiene excepciones para la oposición de la entrega de dicha información, como puede ser por razones de interés público vinculadas a la defensa nacional y a la seguridad pública; la protección de intereses de terceros aun cuando se encuentren vinculados con el solicitante o bien la existencia de actuaciones judiciales o administrativas que se encuentren en curso.

A las excepciones mencionadas, la Directiva 95/46 de la Unión Europea agregó la posibilidad de limitar el alcance de los derechos y obligaciones allí reconocidos ante *"un interés económico y financiero importante de un estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales"* e incluye como causal de excepción al derecho de acceso la protección del interesado",[139] sin embargo, la negativa debe ser totalmente fundada. Por otro lado, la negativa de acceso a los datos personales asentados en registros de Estado, fundada en razones de seguridad pública o defensa nacional, puede ser revisable en el fuero jurisdiccional, por encontrarse en juego el ejercicio de un derecho personalísimo y reconocido constitucionalmente.

Por lo que respecta al derecho de acceso a los datos con fines de publicidad, según lo dispuesto por el artículo 27, rige el mismo sistema, que ha quedado expuesto, con la diferencia de que este numeral no establece limitación alguna

[139] GILS CARBÓ, Alejandra, *Régimen Legal de la Base de Datos y Hábeas Data. Ob. Cit.* Pág. 172

respecto del lapso para ejercerlo según lo que dispone el artículo 14.3, que indica que el derecho sólo puede ser ejercido a intervalos no menores a seis meses, la justificación, según Puccinelli, es que el ablandamiento de la previsión general mencionada se debe a que por un lado, constituye una excepción a la prohibición de establecer perfiles, contenidas en el artículo 20, y además a que si bien este tipo de registros cumple un rol social, tiene menor trascendencia colectiva, y persiguen fines primordialmente individuales.

En México, el derecho de acceso se encuentra regulado por tres diversas leyes: La Ley Federal de Transparencia a la Información Pública Gubernamental, la Ley Federal de Protección al Consumidor y recientemente la Ley Federal de Protección de Datos Personales en Posesión de Particulares, cada una de ellas en lo dispuesto sobre la actividad que regula, es así que las disposiciones normativas en México señalan lo siguiente:

> La **LFTAIP** dispone en su **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. 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."

Es importante referir que el derecho de acceso a la información se da en el tratamiento de datos personales con referencia al artículo 1 de la citada ley, cuya finalidad es la de 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.

> De igual manera, la **LFPC** establece en el **artículo 16.** "Los proveedores y empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios están obligados a informar gratuitamente a cualquier persona que lo solicite si mantienen información acerca de ella. De existir dicha información, deberán ponerla a su disposición si ella misma o su representante lo solicita, e informar acerca de qué información han

> compartido con terceros y la identidad de esos terceros, así como las recomendaciones que hayan efectuado. La respuesta a cada solicitud deberá darse dentro de los treinta días siguientes a su presentación. En caso de existir alguna ambigüedad o inexactitud en la información de un consumidor, éste se la deberá hacer notar al proveedor o a la empresa, quien deberá efectuar dentro de un plazo de treinta días contados a partir de la fecha en que se le haya hecho la solicitud, las correcciones que fundadamente indique el consumidor, e informar las correcciones a los terceros a quienes les haya entregado dicha información".

Este derecho de acceso se da en el marco de lo dispuesto por la propia ley del Consumidor al promover y proteger los derechos y cultura del consumidor y procurar la equidad, certeza, seguridad jurídica en las relaciones entre proveedores y consumidores.

> Y finalmente, la **LFPDP**, que prevé en su **artículo 23.**"Los titulares tienen derecho a acceder a sus datos personales que obren en poder del responsable, así como conocer el Aviso de Privacidad al que está sujeto el tratamiento"-

Esta legislación reciente, tiene por objeto la protección de los datos personales en posesión de particulares, con la finalidad de regular su tratamiento legitimo, controlado e informado a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa.

Como podemos ver el derecho de acceso de los titulares en México, tiene un mismo objetivo que es el de acceder a la información que se tiene sobre su persona, sin embargo, cada una regula lo relativo a la actividad para la que fue creada, lo que podría concentrarnos nuevamente ante una dispersión legislativa sobre un mismo derecho, que si bien, no es dable del todo afirmar sobre una deficiencia completa, tampoco constituye un acierto el no poder aun unificar los derechos que implica la protección de datos personales y tratándose aun con fines publicitarios en lo que respecta al tratamiento de ellos, lo que a juicio propio pudiere homogeneizarse como lo prevé la Ley Argentina 25.326, que recoge los tres aspectos de protección de datos personales:

> **Ley 25.326 Artículo 1, (Objeto)**
>
> La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las

mismas se registre, de conformidad a lo establecido en el art. 43 Ver Texto , párr. 3 de la Constitución Nacional.

Artículo 27, (Archivos, registros o bancos de datos con fines de publicidad).

1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.
2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.
3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo.

México ha dado un paso grandísimo sobre la materia al haberla contemplado con la reforma del artículo 16 constitucional y al haberse creado la LFPDP, pero queda mucho por hacer, todavía nos encontramos ante la implementación de los denominados derechos ARCO y ante la creación del Reglamento de la Ley, Lineamientos y Parámetros que según una solicitud de acceso presentada por el suscrito a la Dirección de Clasificación de Datos Personales en el IFAI, el titular de los datos podrá ejercitarlos hasta enero de 2012, como periodo de implementación de la Ley y en febrero del mismo año presentar su queja ante el IFAI, por vulneración de los derechos ARCO.[140]

4.5.3. Retiro, bloqueo o cancelación del nombre de los bancos de datos con fines de publicidad

La Constitución Argentina, reconoció el derecho de rectificar, suprimir, actualizar o dar confidencialidad a los datos propios en caso de falsedad o discriminación, circunstancias que fueron recogidas en la sanción de la Ley 25.326 de Hábeas Data, como derecho de los titulares de los datos que consten en archivos públicos o privados facultando a retirar o bloquear el nombre de la persona cuando

[140] Solicitud de Acceso a la Información de fecha 17 de agosto de 2010, presentada por Aldo González Gutiérrez a la Directora de Clasificación y Datos Personales del Instituto Federal de Acceso a la Información, referente a la estructura interna del IFAI para atender sus nuevas obligaciones derivadas de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, así como la posición del IFAI respecto de la Ley y sus nuevas atribuciones. No omitiendo establecer que estas consideraciones no prejuzgan sobre las determinaciones que en su caso el Pleno pudiere adoptar posteriormente.

se sienta perturbado por la recopilación de su domicilio en un banco de datos destinado al reparto de documento; o cuando sus datos se apliquen para marketing o publicidad.

Este derecho es correlativo al deber de información que tienen los bancos de datos publicitarios, tal como lo afirma la reglamentación al disponer que en toda comunicación que se realice se deberá indicar en forma expresa y destacada la posibilidad del titular del dato de solicitar el retiro o bloqueo, total o parcial, de su nombre de la base de datos. La legislación regula el caso especial de bloqueo de los datos con fines de publicidad, que es conocido como "op out".

El artículo 27.3, sostiene que "*El titular podrá en cualquier momento solicitar el retiro o el bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo"* (con fines de publicidad).

Asimismo, el Decreto reglamentario 1558/01, mantuvo la misma expectativa al señalar que toda comunicación con fines de publicidad por correo, teléfono, correo electrónico, internet u otro medio a distancia se deberá indicar en forma expresa y destacada, la posibilidad del titular del dato de solicitar el retiro o bloqueo, total o parcial, de su nombre de la base de datos. A pedido del interesado, se deberá informar el nombre del responsable o usuario del banco de datos que proveyó la información.

Es interesante este aspecto, ya que si vemos, la ley exclusivamente menciona que el titular de los datos puede solicitar el retiro o bloqueo de su "nombre", más no de toda la información que se haya generado con motivo de esta persona, es decir, el nombre de la persona desaparece pero la demás información continúa latente, una especie de disociación del dato, lo que permite ver que el derecho de retiro o bloqueo no implica la oposición al tratamiento de la baja de todos los datos, los cuales pueden seguir siendo tratados.

Decía Puccinelli: si sólo se bloquea el nombre, no se impide enviar las comunicaciones al residente en determinado domicilio postal o virtual, número de teléfono, etc., ya que el uso masivo de los medios electrónicos para enviar correspondencia virtual provoca lo que hoy se conoce como spam, y por eso varios países ya intentan regularlo de alguna manera, como lo hizo Estados Unidos como la ley anti-spam, aprobada a fines de 2003, cuando el 70% de los correos electrónicos recibidos por los estadounidenses encuadraba en la categoría de correo no deseado o basura (junk mail), y en ese país se generaba el 80% del spam de todo el mundo.[141]

Al respecto, Osvaldo Gozaini, sostiene la propuesta de un mecanismo de articulación y complemento con las agrupaciones de cada sector, con el fin que sean éstas quienes promuevan un sistema de retiro o bloqueo a favor del titular de los datos, dicho mecanismo, deberá seguir un programa de acción cumpliendo ciertas etapas como las siguientes:

a) Definir cuál es el sector (marketing, bancos, etc.) y la entidad que los representa (sea por disposición legal o convencional).
b) Establecer en cada uno un código de ética para las conductas del sector.
c) Designar representantes para que, junto con la autoridad de aplicación de la ley 25.326, implementen (en el término de 90 días siguientes a la publicación de la ley) los requisitos y procedimientos que faciliten el cumplimiento del derecho de bloqueo.

Podemos destacar que el titular de los datos puede ejercer los derechos de retiro o bloqueo, entendiendo en principio que se hace en forma escrita, sin embargo, ello no es obstáculo para utilizar cualquier otro medio que le haga saber al proveedor o empresa el retiro de su nombre, por ejemplo un spam o correo no

[141] PUCCINELLI, Oscar, *Protección de Datos de Carácter Personal. Ob. Cit.* P. 406

deseado, y puede solicitarse por este mismo medio que se realice el bloqueo correspondiente.

La ley no fija un plazo específico para que el responsable o usuario del banco de datos con fines de publicidad cumpla con el retiro o bloqueo solicitado, según corresponda, para Marcela Basterra,[142] debe aplicarse el plazo de cinco días previsto en el artículo 16 inciso 2, en tanto se refiere al derecho de rectificación, actualización o supresión.

La ley faculta a las empresas a llevar actividades de publicidad y marketing, siempre y cuando los titulares de esos datos, hagan valer los derechos que le confiere la Ley de Protección de Datos Personales, e incluso el derecho de no ser molestado con ofertas publicitarias indeseables salvo que haya mediado consentimiento del afectado o por lo contrario la negativa a que dicha información sea tratada con esos fines y por consecuencia se solicite el retiro o bloqueo de los mismos.

Por último, la Dirección Nacional de Protección de Datos Personales en Argentina, estableció que la opción para el ejercicio del derecho de retiro o bloqueo contemplado en el artículo 27, inciso 3, de la Ley Nº 25.326, deberá aparecer en toda comunicación que se efectúe con fines publicitarios, junto con el mecanismo previsto para su ejercicio, regulando el tratamiento de datos personales correspondiente a los archivos y bancos de datos con fines de publicidad, y que el titular del dato tienen el derecho de solicitar el retiro o bloqueo de su nombre de los bancos de datos, derecho que se le conoce como *opt out*, y que alude a la opción de ser excluido de una lista de distribución que en la normativa se denomina como derecho de retiro o bloqueo.

[142] *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados. Derecho Constitucional Provincial. Iberoamérica y México Ob. Cit.* Pp. 492-493

Es por ello que, a fines de permitir un mejor ejercicio de los derechos del titular de los datos en las actividades de publicidad directa, resultó conveniente instrumentar mecanismos que permitieran identificar con facilidad las comunicaciones no requeridas y cuando éstas se efectúen sin solicitud previa del titular del dato, las mismas deberán hacer saber en forma expresa y clara que se trata de una publicidad, debiendo el banco proporcionar algún mecanismo para que el titular del dato receptor de la comunicación publicitaria directa no requerida pueda hacer valer su derecho a ser bloqueado o eliminado del listado correspondiente y no recibir más información publicitaria del banco de datos emisor.

La Dirección Nacional de Protección de Datos Personales dictó una medida en uso de sus facultades en las que se dispone:

> Artículo 1º — En las comunicaciones con fines de publicidad directa, el banco de datos emisor debe incorporar un aviso que informe al titular del dato sobre los derechos de retiro o bloqueo total o parcial, de su nombre de la base de datos, el mecanismo que se ha previsto para su ejercicio, con más la transcripción del artículo 27, inciso 3, de la Ley Nº 25.326 y el párrafo tercero del artículo 27 del Anexo I del Decreto Nº 1558/01.
>
> Art. 2º — Cuando se efectúen envíos de comunicaciones de publicidad directa no requeridas o consentidas previamente por el titular del dato personal, deberá advertirse en forma destacada que se trata de una publicidad. En caso de realizarse dicha comunicación a través de un correo electrónico deberá insertarse en su encabezado el término único "publicidad".
>
> Art. 3º — En las comunicaciones a que aluden los artículos precedentes, el banco de datos emisor deberá verificar que los mecanismos previstos para el ejercicio del derecho de retiro o bloqueo cuentan con suficiente capacidad operativa para responder al eventual ejercicio de tal derecho por parte de los titulares de los datos.

En el sistema mexicano, la Procuraduría del Consumidor cumple con un fin parecido al incorporarse en los artículos 16, 17, 18, 18 bis y 76 bis, de la LFPC, sin embargo, no contempla como tal el derecho de cancelación de datos personales, solamente establece que cuando el titular de los datos no consienta el envío de información publicitaria a su domicilio, casilla de correo, teléfono o cualquier otro medio, a fin de evitar esto, se crea según lo dispuesto por el artículo 18 un registro público de consumidores que no deseen que su información sea utilizada para fines

mercadotécnicos o publicitarios, además de que los consumidores podrán comunicar por escrito o por correo electrónico a la Procuraduría su solicitud de inscripción en dicho registro, el cual será gratuito, la diferencia entre estos dos sistemas es que en el sistema Argentino existe el retiro o bloqueo del nombre, mientras que en el derecho mexicano en materia de publicidad y marketing, el titular puede exigir únicamente al proveedor o a la empresa que tenga sus datos personales, que los mismos no tengan tratamiento ni cesión, so pena de sanción administrativa por parte de la Procuraduría Federal de Protección al Consumidor (PROFECO).

Hasta hace poco más de un año, la Constitución Política de los Estados Unidos Mexicanos, reformó su artículo 16, reconociendo los derechos ARCO, de entre los cuales se establece el derecho del titular de cancelar sus datos personales, misma situación que recogió la LFPDP, en sus artículos 25 y 26, sin que refiera específicamente a aspectos publicitarios, pues las actividades de comercio aun se encuentran pendientes derivado de las regulaciones y parámetros que la Secretaría de Economía debe implementar para reglamentar la actividad en materia de comercio y protección de datos personales, los artículos en comento quedaron de la siguiente manera:

> Artículo 25.- El titular tendrá en todo momento el derecho a cancelar sus datos personales.
> La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. El responsable podrá conservarlos exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia.
>
> Una vez cancelado el dato se dará aviso a su titular.
> Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá hacer de su conocimiento dicha solicitud de rectificación o cancelación, para que proceda a efectuarla también
>
> Artículo 26.- El responsable no estará obligado a cancelar los datos personales cuando:
> I. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;
> II. Deban ser tratados por disposición legal;
> III. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas;
> IV. Sean necesarios para proteger los intereses jurídicamente tutelados del titular;

V. Sean necesarios para realizar una acción en función del interés público;
VI. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular, y
VII. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto

4.5.4. Problemas de la recopilación y tratamiento de datos con fines de publicidad sin consentimiento del titular

El consentimiento en la recopilación y tratamiento de los datos con fines de publicidad, sólo sigue la suerte del principio establecido por el artículo 5 de la Ley 25.326., en algunos casos, y consiste en el derecho de los particulares a decidir cuándo y cómo permitir que sea difundida información respecto de su persona.

Dice la ley que el tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso e informado, el que deberá constar por escrito, o por otro medio que permita se le equipare, de acuerdo a las circunstancias, no obstante, veremos que en ocasiones no se requiere del consentimiento de la persona para recopilar y tratar esos datos con fines publicitarios, como el caso del artículo 27 de la citada ley y su Decreto reglamentario 1558/01.

Para explicar este tópico del consentimiento de la recopilación y el tratamiento en la publicidad, tomemos un ejemplo que el Dr. Gozaini[143] nos muestra: El asunto fue expuesto en el debate parlamentario con el ejemplo de la compra de zapatillas y la autorización siguiente del comprador para ser incorporado en un banco de datos; el problema se plantea porque de acuerdo con la sistemática general de la normativa, cada vez que ese banco de datos se venda habría que pedir el consentimiento del titular de la información. Eso significaría poner en situación de falta de competitividad a las empresas argentinas respecto de las chilenas, uruguayas o paraguayas, que cuentan con un sistema más abierto.

[143] GOZAINI, Osvaldo. *Derecho Procesal Constitucional. Hábeas Data. Protección de datos personales. Ley 25.326 y reglamentación (decreto 1558/20001). Ob. Cit.* Pp. 329-330

No se suprime el requisito del consentimiento -se alegaba-, pero se establecía que cuando la persona prestaba el consentimiento original también consentía que los datos fueran cedidos. No era exigido un consentimiento posterior, pero quedaba establecido que la persona consiente la cesión cuando permite que la información a ella referida sea incluida en un banco de datos.

Para el citado autor, los archivos sobre marketing trabajan con datos personales habitualmente logrados de fuentes accesibles al público, en cuyo supuesto no sería necesario tener expresamente autorizado por el afectado el uso de los mismos, esto derivado de que se pueden recopilar, tratar y ceder datos con fines de publicidad, sin consentimiento del titular, cuando estén destinados a la formación de perfiles determinados que categoricen preferencias y comportamientos similares de las personas.

Caso contrario cuando el comportamiento de alguien en específico se le pueda reconocer y precisar, en este caso, si se requerirá el consentimiento del titular de los datos.

El tema va referido a los perfiles determinados y a los hábitos de consumo, en los cuales, como vimos en capítulos anteriores, la recolección y tratamiento de datos con fines publicitarios siempre y cuando sean disociados del individuo, esto es que el perfil determinado pertenezca a un grupo y no a un individuo en específico, en estos casos no se requerirá del consentimiento del titular, empero tratándose de los hábitos de consumo, que como habíamos visto, pueden revelar afecciones, sexualidad, enfermedades, y en general, cualquier dato que pudiere considerarse como sensible, debe existir el consentimiento del titular de esos datos.

Así lo ratificó el Decreto reglamentario 1558/01, al establecer que podrán recopilarse, tratarse y cederse datos con fines de publicidad sin consentimiento de su titular, cuando estén destinados a la formación de perfiles determinados, que categoricen preferencias y comportamientos similares de las personas, siempre que

los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos genéricos, con más los datos individuales estrictamente necesarios para formular la oferta a los destinatarios.

En México, el derecho de oposición reconocido por el artículo 16 de la Constitución y lo señalado por el artículo 29 de la LFPDP, que refiere a la facultad del titular del dato para oponerse al tratamiento de ellos, cuando considere que se violenta este derecho, sin embargo nuestra legislación no es específica en lo que refiere a la recopilación y tratamiento con fines publicitarios y de mercado, lo que delega a la LFPC en su artículo 16 para oponerse al tratamiento, con implementación aun de las actividades comerciales a regular por parte de la Secretaría de Economía en términos de lo dispuesto por los artículos 41, 42 y 43 de la LFPDP, esto coloca en cierta desventaja a México en comparación con las legislaciones internacionales en materia de protección de datos personales en la publicidad y el marketing.

4.5.5. Necesidad de inscripción en un Registro de los responsables o usuarios de archivo, registros, bancos o bases de datos con fines de publicidad.

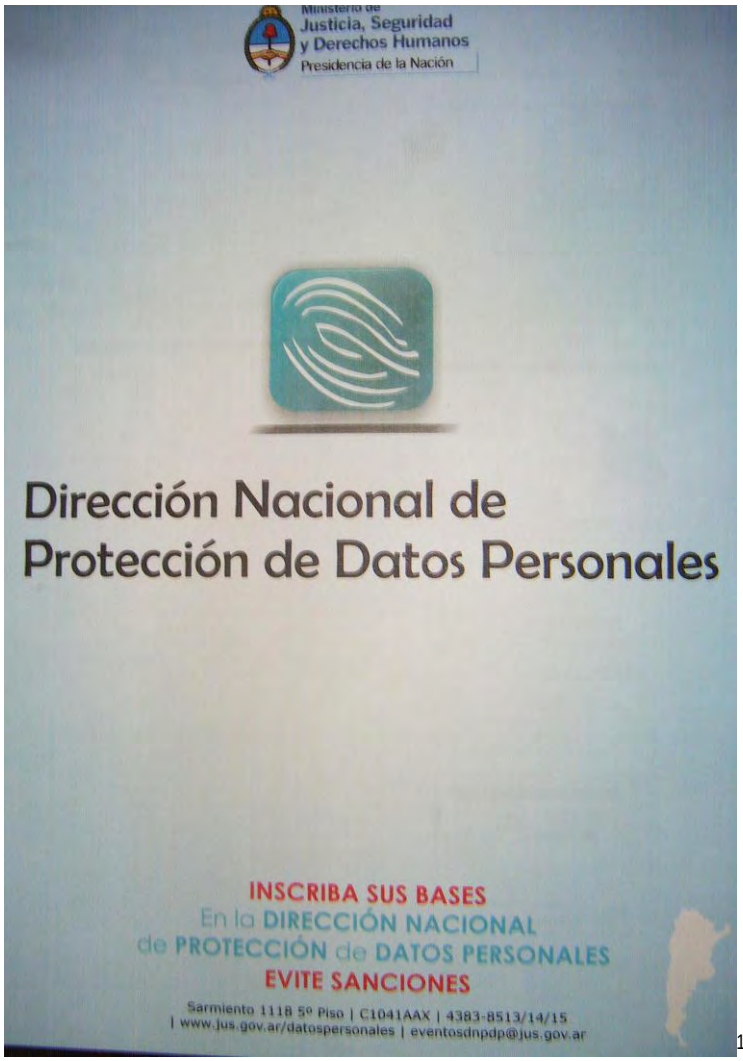
Diversas legislaciones sobre protección de datos personales, han llegado a coincidir en establecer un control de todos los archivos y bases de datos públicos y privados que excedan el uso personal, a través de la exigencia de su inscripción en un registro que se ha habilitado por la autoridad de control.

Este registro sirve para supervisar que los registros adecuen su funcionamiento a las disposiciones legales, a fin de que no se violenten los principios que la legislación en materia de protección de datos sustenta.

El artículo 21 de la Ley 25.326, sostiene el deber de registro de archivos, bases de datos o bancos tanto públicos como privados destinados a proporcionar informes, mismos que deberán inscribirse en el Registro que habilite el organismo

de control, en el caso de la Nación Argentina la Dirección Nacional de Datos Personales, es quien orienta al responsable de los ficheros para la inscripción de los archivos, bancos o bases de datos.

El propio artículo dispone los requisitos que deben de comprenderse para poder hacer el registro respectivo. Los siguientes cuadros nos muestran de manera ejemplificativa la manera en que la Dirección Nacional de Protección de Datos Personales ha implementado este servicio:



[144]

[144] Dirección Nacional de Protección de Datos Personales, Sarmiento 1118, 3er piso, Capital Federal, Argentina, 2009.

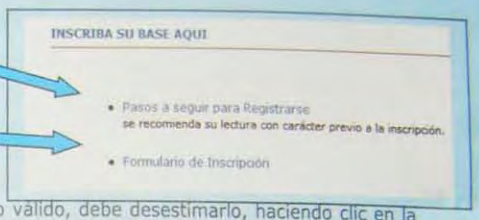
¡ IMPORTANTE !

La inscripción en el Registro NO implica revelar el contenido de las bases de datos registradas.
Implica tan solo una descripción de la estructura de las bases de datos.

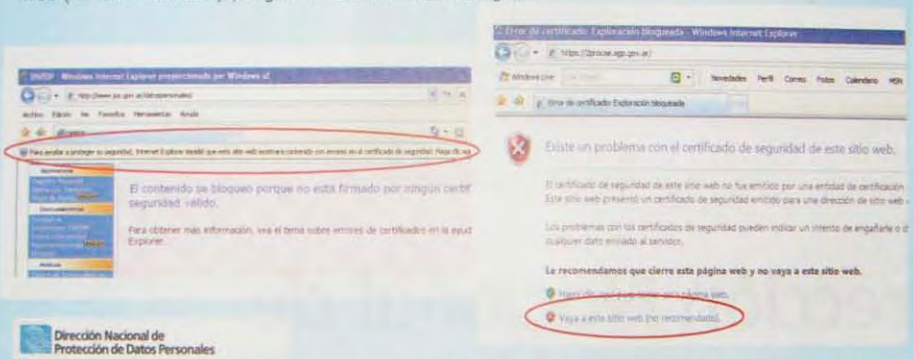
PROCEDIMIENTO DE INSCRIPCIÓN ANTE EL REGISTRO NACIONAL DE BASES DE DATOS

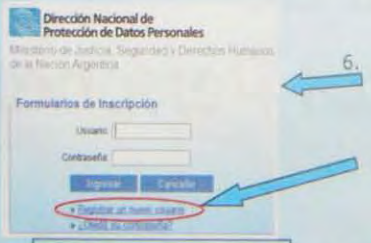
1. Ingresar a: www.jus.gov.ar/datospersonales/
2. Hacer clic sobre el siguiente botón:

3. Previo a la carga del formulario deberá seguir las instrucciones y sugerencias del enlace "Pasos a seguir para registrarse".
4. Seguir el enlace "Formulario de Inscripción"



5. Si recibe un mensaje de certificado de seguridad no válido, debe desestimarlo, haciendo clic en la barra amarilla debajo de las barras de herramientas, o haciendo clic en la frase "Vaya a este sitios web (no recomendado)", según la versión de su navegador.

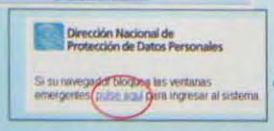




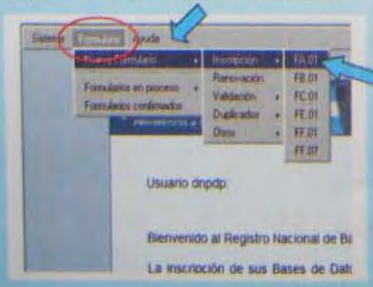
6. Se abrirá una nueva ventana con la pantalla para ingresar al sistema con nombre de usuario y contraseña.

   La primera vez que ingrese al sistema deberá inscribirse como Usuario ingresando en "Registrar un nuevo usuario", completando los datos allí solicitados y pulsando "Aceptar".

   En caso que su navegador bloquee las ventanas emergentes, debe presionar sobre las palabras "pulse aquí" para ingresar al sistema.



7. Una vez ingresado al sistema, aparecerá una pantalla de Bienvenida que contiene en su parte superior una barra de herramientas.



8. Se debe hacer clic en "Formulario"; → "Nuevo Formulario"; → "Inscripción", para acceder al formulario FA.01 (GENERAL). En el caso de asociaciones sin fines de lucro está previsto un formulario específico, el FF.01 o FF.07 (en "Pasos a seguir para registrarse" encontrará las precisiones sobre cuál completar).

La Dirección Nacional de Protección de Datos Personales, ha adoptado procedimientos de inscripción ante el Registro Nacional de Bases de Datos, según lo dispuesto por el artículo 21 de la ley 25.326; para el registro de las bases de datos, el responsable de los archivos, bases o bancos, tiene la obligación de comprender como mínimo los requisitos que señala el propio artículo en sus ocho incisos.

El artículo 21, establece el principio de registro obligatorio más que una necesidad, de los ficheros públicos y privados destinados a proporcionar informes, cuyo único fin es el de ejercer un control sobre las inscripciones masivas.

Para Marcela Basterra, la exigencia de la registración de una serie de informaciones brinda operatividad y eficacia a otras disposiciones de la ley como los derechos de información y acceso consagrados en los artículos 13 y 14 de la Ley de Protección de Datos Personales[145], además de constituirse como una medida de transparencia y seguridad de las personas.

Ahora bien, si alguno de ellos no acepta los términos de la vinculación al sector, o no se adhiere a ningún código de conducta –dice Gozaini-[146], *deberán inscribirse en el registro como si se tratara de un archivo de los previstos en el artículo 21 de la ley 25.326.*

Sin embargo, el incumplimiento de inscribirse en el Registro que al efecto se habilite, dará lugar a los variados tipos de sanciones administrativas previstas en la ley según lo dispuesto por el artículo 29, a saber, apercibimiento, suspensión, multa clausura y cancelación según sea el caso concreto.

---

[145] *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados Derecho Constitucional Provincial, Iberoamérica y México, Ob. Cit.* P. 457

[146] *Derecho Procesal Constitucional. Hábeas Data. Protección de datos personales. Ley 25.326 y reglamentación (decreto 1558/20001). Ob. Cit.* Pp. 335

De igual manera, no sólo los responsables de los archivos habrán de registrar sus bases de datos, sino también los usuarios de los mismos (cuando escapen de lo dispuesto por el artículo 21 de la Ley 25.326 y el artículo 2, tercer párrafo de la LFPDP), esto es que ningún usuario de datos personales podrá poseer datos de naturaleza distinta a los declarados en el registros, so pena de sanción.

Lo anterior en concordancia con la finalidad que tiene la garantía de habeas data, y que es la posibilidad que tienen las personas de saber y tener conocimiento de los datos que tienen acerca de ella, el tratamiento y la finalidad que se les dé, sin olvidar que los mismos pudieren ser motivo de alguna supresión, rectificación, o bloqueo, por información discriminatoria, falsa, o errónea y a fin de que puedan ser actualizados según corresponda.

La LFPDP recientemente entrada en vigor el 6 de julio de 2010, no establece la necesidad de inscripción de los registros de bases de datos en posesión de particulares, únicamente les establece una serie de obligaciones, sobre información, confidencialidad, transferencia de datos y medidas de seguridad a adoptar sobre el tratamiento de aquéllos, pero sin obligar a ninguno a inscribir sus bases de datos.

La Dirección de Clasificación y Datos Personales del IFAI, recientemente dio respuesta a una solicitud presentada por el suscrito en la que se señaló lo siguiente[147]:

> *"…**b) Con relación a tu consulta sobre si existe un estudio de la Ley que exprese las criticas, aciertos, ventajas y desventajas,** me permito informarte que hasta el momento de la elaboración de la presente respuesta no tenemos conocimiento de que exista algún estudio elaborado sobre el particular.*

[147] *Loc. Cit.* P. 224

Sin embargo y a efecto de que cuentes con mayores elementos, a continuación se describen las ventajas y beneficios de contar con una ley de esta naturaleza para México, así como del modelo o sistema de protección de datos personales que adoptó el legislador federal y que se refleja en la Ley:

…

- *Retoma elementos del Marco de Privacidad APEC que la hacen muy flexible al no imponer cargas excesivas e innecesarias de cumplimiento, a saber:*
    - ***No se requiere un registro de las bases de datos en posesión de los particulares…***

Como vemos la nueva LFPDP no impone la obligación a las empresas de inscribir sus bases de datos, cuyos archivos de datos personales tengan en tratamiento lo cual a mi juicio es grave, porque no permite controlar el tratamiento de datos por parte de las autoridades regulatorias.

La LFPDP, constituye una norma de carácter público, y entre sus funciones está la de regular la actividad de las bases de datos que registran información personales y cuyo objetivo es garantizar a las personas el control del uso de sus datos personales, por lo que considero que la información debe ser lícita de acuerdo a los principios expuestos en la Ley, y el inscribirlas debidamente en un asentamiento de archivos, ayudará a controlar aun más el tratamiento de datos personales.

En consecuencia, considero que toda base de datos pública y privada destinada a proporcionar informes, debe inscribirse en un Registro que al efecto se habilite por parte de la autoridad de control, en este caso al IFAI como autoridad reguladora, ello atendiendo a los conceptos fundamentales de la Ley sobre la cesión y transferencia de datos.

Todo banco de datos destinados a proveer informes y que permita obtener información sobre las personas, sean trasmitidos o no a terceros, debe encontrarse

registrado, debido al alto riesgo que pudiere causarse al titular del dato, más aun tratándose de bancos de datos sensibles, y ello también porque constituye el derecho de controlar la información personal por parte del titular, mismo que debe ser respetado como tal, cuestión que no recoge la multicitada legislación mexicana, por lo que a mi parecer la regulación de la protección de datos personales o autodeterminación informativa presenta serias deficiencias, pues no se permite interpretar de manera unánime y favorable el ejercicio de controlar la información personal, que corresponde como lo establecimos en el primer capítulo una de las condiciones del derecho de protección de datos personales.

Podemos ver que la LFPDP, es omisa al establecer la creación de un archivo que registre los bancos de datos que traten datos personales en posesión de particulares, la nueva ley no establece un capítulo respectivo sobre los usuarios y responsables de archivos, registros y bancos de datos.

Actualmente no se ha expedido el Reglamento de la Ley, dándole el término de 1 año al Ejecutivo a partir de la entrada en vigencia de la ley para la expedición del mismo, por lo que durante el año 2011, aun no tendremos oportunidad de ejercitar nuestros derechos ARCO, además de que la Dirección de Clasificación de Datos Personales del IFAI, no considera necesaria la creación de un registro como lo mencioné anteriormente.

A mi juicio debe contarse con un Registro de bases de datos, pues ello permite una sinergia por parte de la autoridad de control y el usuario sobre el tratamiento de sus datos personales y corroborar si ellos son tratados según la finalidad para la que fueron recopilados, pues ese es un derecho del titular que debe ser resguardado por todos los medios, pese a que no se constituye como un derecho, la creación de un archivo de bases de datos, éste implementa y complementa el derecho fundamental plenamente reconocido.

4.5.6. Garantía de Confidencialidad y Seguridad de los ficheros automatizados

El avance de las tecnologías de la información ha conducido a la creación de modernas y novedosas bases de datos de diversa índole, financieras, de consumo, publicitarias, etc., con apoyo de ello, los datos personales van siendo recolectados y procesados por medios electrónicos, pero también pueden ser manuales, ya sea en fichas, en hojas clínicas, en documentos, en expedientes, etc. Todo ello motivó que el legislador incrementara en algunos países la protección de esos datos personales, basados en principios para su recolección, tratamiento, seguridad, confidencialidad e incluso cesión.

El manejo de los datos personales es una constante de los sectores públicos y privados, en atención a los miles de usuarios que día a día se registran sin tener conocimiento de que sus datos están siendo recolectados para fines diversos; las modernas formas de adquirir bases de datos va en aumento, hoy en día el documento ya no es sólo la forma de recopilación de ellos.

Hace unos días, el gobierno mexicano anunció la creación de la "Cédula de Identidad Ciudadana", un documento que contará con plena identidad biométrica de cada mexicano, que consiste en la verificación de la identidad de una persona con base en las características de su cuerpo o de su comportamiento, para lo cual se utilizan, por ejemplo, la mano, el iris, la voz o el reconocimiento facial.

El nuevo documento, asegura el gobierno mexicano, será garantía de identidad legal jurídica y seguridad para cada ciudadano del país, por lo que los archivos de datos personales van en aumento, no sólo el nombre, el domicilio, raza, religión, estado de salud, hábitos de consumo, sino también las características biométricas, ello constituye recolección de datos con fines estadísticos, científicos, pero en algunos casos pudieren llegar a tener fines publicitarios, que de a poco van siendo almacenados en ficheros o archivos de uso interno, personal o doméstico.

Ante ello, la adopción de sistemas de seguridad es considerada por la ley un presupuesto indispensable para que la tutela legal sea efectiva, por lo que la recolección de estos datos personales deberán estar en resguardo y sobre condiciones técnicas de seguridad.

Gils Carbó sostiene que, la seguridad debe consistir en medidas técnicas y de organización. Por un lado, el responsable de la base de datos debe seleccionar, adquirir e instalar los equipos y dispositivos adecuados para proveer a la seguridad física y lógica de los archivos luego de haber identificado los riesgos. Aquéllos deben ser aptos para evitar tanto la pérdida y la destrucción material, por causas materiales, causas naturales o por virus, como los accesos no autorizados.[148]

El principio de seguridad de los datos personales, es recogido en el artículo 9 de la Ley 25.326 de Hábeas Data, el cual señala que "el responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado, y queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad".

El principio de seguridad que debe brindar el responsable o usuario de los datos debe entenderse como la obligación de mantener las medidas tecnológicas, de normas y procedimientos que aseguren la "confidencialidad", integridad y disponibilidad de la información, almacenamiento, tratamiento, transmisión, es por ello que consideramos que el principio de seguridad no es una base que debe configurarse cuando exista el dato en sí mismo, sino como un principio que condicione el tratamiento previo de ellos.

[148] *Régimen Legal de las Bases de Datos y Hábeas Data.* La Ley, *Ob. Cit.,* 2001. P. 98

El sistema jurídico mexicano ha adoptado en la *LFTAIP,* el principio de seguridad en el tratamiento de datos, impidiendo a las personas no autorizadas el acceso a los sistemas de datos personales, para evitar el desvío de la información, malintencionadamente o no hacia sitios no previstos, además de garantizar el tratamiento de ellos dentro de los límites que la norma le permite, asegurando la "confidencialidad" y la integridad, tratamiento, cesión, etc.; este precepto ha sido alcanzado por la LFPDP, que dispone de la seguridad de los datos personales en su artículo 19.

Asimismo, la confidencialidad, es un principio que va de la mano con la seguridad de los datos, el artículo 10 de la ley Argentina de Hábeas Data, dice *que el responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos…",* se releva al responsable de la obligación anterior por resolución judicial, por razones de seguridad pública, la defensa nacional o la salud pública.

El artículo citado, hace alusión al secreto en relación a las bases de datos personales que conjuntamente con el principio de seguridad, configuran una defensa de los archivos automatizados de datos personales.

Para Gils Carbó[149] la norma no protege sólo los datos privados sino todos los que hayan sido objeto de tratamiento, en la inteligencia de que también los datos que son íntimos, si son combinados con otros y sometidos a técnicas de prospección, pueden servir para proporcionar un perfil del individuo. Sin perjuicio de ello, podrá valorarse la naturaleza de los datos para exigir un mayor rigor y duración en el cumplimiento del deber de secreto.

De lo que se trata bajo el principio de confidencialidad de los datos en ficheros es que, toda persona que tenga acceso a los datos, durante todo el tiempo

[149] *Ibídem.* P. 103-104

que dure el tratamiento y aun después de que finalice el mismo, que busca garantizar que quienes traten datos de carácter personales en el desarrollo de sus funciones, los guarden y garanticen el secreto sobre los mismos.

El sistema jurídico mexicano actualmente encuentra regulado principio de confidencialidad en la LFPDP en su artículo 21, reconocido por el artículo 16 de la CPEUM, principio que la LFTAIP, lo señala a interpretación en su artículo 20, fracción VI, en relación con el 18 y 21 del propio ordenamiento, supuestos que no establecen de forma clara el deber de confidencialidad o secreto, que se destaca como algo que debe ser observado por toda persona que tenga acceso a los datos, durante todo el tiempo que dure el tratamiento y aun después de que finalice el mismo.

No obstante el Instituto Federal de Acceso a la Información, hizo una remisión a los Lineamientos publicados en el Diario Oficial de la Federación el 30 de septiembre de 2005, en los que se establece que se deberán adoptar las medidas necesarias para garantizar... confiabilidad, confidencialidad... de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado, ello con el fin de dar reconocimiento al derecho a la vida privada, y tomando en cuenta el objetivo de la LFTAIP, que es el de garantizar la protección de datos personales en posesión de los sujetos obligados (Poderes de la Unión, Órganos Constitucionales Autónomos y cualquier otra entidad federal).

Los aspectos publicitarios han determinado una cultura impositiva en la que las actividades cotidianas no pueden desarrollarse sin la inclusión de la comercialización en diversos sectores poblacionales, utilizando para ello los datos personales que los usuarios y/o consumidores[150] dejan por su andar en el uso de las tecnologías.

---

[150] *Ley Federal De Protección al Consumidor.* Artículo 2, frac. I. "El *Consumidor* es la persona física o moral que adquiere, realiza o disfruta como destinatario final bienes, productos o servicios.

Las TIC's han desplazado a los tradicionales medios de comunicación, tomando las herramientas de mayor rentabilidad a fin de llegar a más sectores sociales. El internet, el correo electrónico, el teléfono, se han constituido en nuevos receptores de publicidad, toda vez que gracias a ellos, se cubre una mayor cantidad de personas en el menor tiempo posible, dejando en segundo plano, los carteles, los posters, anuncios, etc.

Ello ha implicado que para la distribución de ventas, tenga que allegarse de elementos necesarios para construir la plataforma sobre las cuales se dejará expandir el marketing y la publicidad, lo que se traduce también en tratamiento de datos personales. A la par deben ponderar los derechos del titular de los datos a fin de no transgredir el disfrute del derecho fundamental que se pretende proteger, respetando en todo tiempo el acceso, rectificación, cancelación u oposición de aquéllos.

La publicidad se ha adentrado en los medios de comunicación de manera rápida, sobre todo por el uso indiscriminado de las tecnologías de la información y las comunicaciones, el Internet, el correo electrónico y el teléfono se han constituido como piezas fundamentales en donde se tratan de manera oficiosa los datos personales que diariamente son transportados por el ciberespacio, la mayoría de las veces sin consentimiento del titular.

Agregado a ello, los problemas en materia legislativa no son menores, pues en el caso de sistema mexicano, las normas establecidas no contemplan de manera

---

Se entiende también por consumidor a la persona física o moral que adquiera, almacene, utilice o consuma bienes o servicios con objeto de integrarlos en procesos de producción, transformación, comercialización o prestación de servicios a terceros…". "También se define como aquél que consume o compra productos para el consumo. Es por tanto el actor final de diversas transacciones productivas". *Wikipedia. La Enciclopedia Libre.* http://es.wikipedia.org/wiki/Wikipedia:Consultas.- El *Usuario* es la persona que utiliza o trabaja con algún objeto o que es destinataria de algún servicio público, privado, empresarial o profesional. *Ídem.*

"categórica" la recogida y tratamiento de datos de carácter personal en posesión de particulares; incluso para ciertas actividades tienen que remitir a otras legislaciones, como acontece en la propia LFPDP recientemente creada, ya que la misma es omisa en el tratamiento de datos con fines publicitarios, más aun delega las funciones de regulación comercial a otro sector de la economía (Secretaría de Economía) cuestión que se encuentra pendiente, teniendo que recurrir a otras fuentes federales de regulación del sector publicitario hacia el consumidor, la propia LFPC no prevé todos los principios a los que deben encontrarse sujetas las empresas en el tratamiento de datos con fines de publicidad, no obstante, es la única que regula este ámbito (aunque incompleta).

Lo anterior, también conduce a los problemas del abuso por parte de los proveedores hacia el consumidor en la publicidad engañosa, que intentan vender productos haciendo creer que se obtendrá algún beneficio, ya que esto desde luego genera la recopilación de información cuando los usuarios la introducen en internet, aumentando el riesgo de que sus datos sean robados y tratados con fines no sólo publicitarios sino ilícitos.

Otro de los problemas a los que se enfrenta nuestra nueva legislación es la poca regulación sobre el tratamiento automatizado de datos personales; la información que circula por las comunicaciones electrónicas, debe responder a las medidas de seguridad que al respecto tenga que establecer la autoridad de control, para evitar problemas que se generen con el uso del internet, la recepción de correos electrónicos no deseados *–spam, cookies-,* y en general las actividades de recopilación ilícita de datos personales dentro de las modernas tecnologías de la información, por lo que las autoridades (IFAI y Secretaría de Economía), tendrán la obligación de crear altos estándares de protección a fin de complementar las deficiencias que la LFPDP ha tenido en la materia, ya sea en la expedición del Reglamento, o creando los Lineamientos para la aplicación de las normas de la autodeterminación informativa, acuerdos generales, programas, parámetros, criterios, recomendaciones, políticas, buenas prácticas y en general todas aquellas

disposiciones administrativas según las competencias y atribuciones que se le han conferido al Instituto y a la Autoridad reguladora con la nueva legislación, acorde con los principios establecidos en los artículos 41, 42 y 43 de la citada ley, actuando el IFAI como coadyuvante para la mejora regulatoria, tanto del sector público como privado en términos de lo dispuesto por el artículo 39 de la Ley.

Por último, la omisión de la Ley respecto a la creación de un Registro de bases de datos, constituye también otra deficiencia que debiere tomarse en cuenta para las empresas en el tratamiento de datos en materia de publicidad, ya que con esto se da un control más amplio sobre lo que se maneja, cómo y dónde se están tratando datos personales y ver si los responsables de los ficheros cumplen o no con los principios de la autodeterminación informativa, por lo que también consideró pertinente la creación de alguno.

En el siguiente capítulo examinaremos al IFAI como autoridad garante del derecho fundamental de la autodeterminación informativa, las tareas que le han sido conferidas por la nueva Ley, y después si las atribuciones encomendadas responden a las exigencias de protección que marcan los de transgresión de datos personales; y por último, expondremos cuál es el papel del IFAI ante la omisión de la Ley sobre el binomio protección de datos personales y publicidad.

CAPÍTULO V

EL IFAI COMO INSTITUCIÓN GARANTE DEL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES

CAPÍTULO V

EL IFAI COMO INSTITUCIÓN GARANTE DEL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES: AVANCE O RETROCESO

5.1. El IFAI. Instituto Federal de Acceso a la Información y Protección de Datos Personales en México: Funciones

En el capítulo IV, se evidenciaron las deficiencias normativas en materia de Protección de Datos Personales en la publicidad y el marketing, y la forma en que México lo ha abordado, así como algunas de las nuevas atribuciones que esta legislación otorga a un organismo de la Administración Pública como el IFAI y la Secretaría de Economía como autoridad reguladora en materia de actividades comerciales.

Es momento de verificar las facultades que tiene este organismo público, y si responde a las exigencias demandadas, así como si debe establecerse un poder de control de todos los archivos y bases de datos privados habilitando para ello una autoridad que supervise adecuadamente el funcionamiento de las disposiciones legales que quedaron sancionadas en la materia y que permitan al ciudadano gozar libremente del derecho reconocido por los instrumentos internacionales. La protección de datos personales como derecho fundamental debe ser plenamente reconocido y respetado en cada una de sus modalidades, lo que incluye su recogida y tratamiento ya sea en soporte documental o informático.

Algunos países ya gozan de esta autoridad de control como lo hemos venido mencionando a lo largo del presente trabajo: en Argentina la Dirección General de Protección de Datos Personales realiza esa labor; en Europa, concretamente, España ha consolidado la Agencia de Protección de Datos Personales, lo que motivó a nuestro país a no constituirse ajeno a las actuales circunstancias de estos organismos garantes del derecho de tercera generación, otorgándose esta tarea al

Instituto Federal de Acceso a la Información y Protección de Datos Personales como lo señaló la reforma que entró en vigor el pasado 6 de julio de 2010.

Las deficiencias que aun presenta la legislación mexicana, deben ser subsanadas a través de la homogeneidad normativa, la heterogeneidad o dispersión legislativa debe dejar de ser un obstáculo para la observancia del derecho reconocido en la Constitución Mexicana en su artículo 6º y recientemente en el artículo 16º, ello permitirá que el IFAI aseguré confianza y determinación en el uso de las atribuciones que el Estado le confiere y que garantice el respeto a los datos personales, pero que al mismo tiempo elabore y ejecute planes, programas y políticas relacionadas con la defensa de este derecho fundamental.

Dicho órgano de control en el ámbito nacional, debe servir para la efectiva tutela de los datos personales, pero sobre todo que tenga a su cargo un Registro de las Bases de Datos, a fin de conocer y controlar esas bases, que asesore y asista a los titulares de datos personales recibiendo las denuncias y reclamos efectuados contra los responsables de los registros, archivos, bancos o bases de datos por violar los derechos de acceso, rectificación, cancelación y oposición en el tratamiento de los datos en la sociedad informatizada y con el uso de las tecnologías de la información.

Cada vez son más las actividades que requieren del tratamiento de datos personales, por ello, su protección es una condición importante para el adecuado desarrollo de los proyectos.

A continuación examinaremos si el IFAI, cumple con las exigencias[151] que durante 9 años han venido demandándose por la sociedad civil y política, plasmada en todas las iniciativas de ley sobre protección de datos personales.

[151] Funciones exigidas por la sociedad civil y los grupos parlamentarios, según propuestas presentadas, las que pueden resumirse de la siguiente forma: a) Informar sobre el contenido del derecho a la autodeterminación informativa; b) Tutelar al ciudadano en el ejercicio de los derechos que corresponden al contenido de la autodeterminación informativa (ARCO), así como el tratamiento de sus datos personales; c) Garantizar el respeto a los datos personales, investigando a los responsables o encargados de ficheros, y entablar procedimientos para la tutela del derecho; d) Control de las bases de datos en poder de particulares.

5.1.1. Naturaleza Jurídica del IFAI

Para señalar las tareas que la reforma reciente otorga al IFAI, su nueva denominación,[152] deficiencias y aciertos, es conveniente exponer los antecedentes de creación del organismo de protección de datos personales en el sistema jurídico mexicano.

En febrero de 2001, el senador Antonio García Torres, presentó ante la Comisión Permanente del Congreso General, un Proyecto de Ley Federal de Protección de Datos Personales.[153] En dicho proyecto, se propone la creación de un Instituto Federal de Protección de Datos Personales, como organismo público cuyo objeto consistiría en controlar a los responsables de los archivos, registros, bases o bancos de datos personales y la protección de éstos, con facultades de fiscalización y facultado para imponer sanciones administrativas.

La iniciativa de la Ley Federal de Protección de Datos Personales fue dictaminada y aprobada en la Cámara de Senadores el 30 de abril de 2002, y fue turnada a la Cámara de Diputados el mismo día. Cabe mencionar que su articulado sufrió modificaciones, en varios aspectos: supresión de las personas morales como titulares de datos personales, y la supresión del Instituto Federal de Protección de Datos Personales, haciendo remisión al IFAI, considerándose inconveniente que se crearan dos organismos públicos en un mismo momento (El IFAI y el Instituto Federal de Protección de Datos Personales) y sólo se aprobó crear al IFAI bajo la

[152] *Diario Oficial de la Federación*. Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de entes Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Titulo Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. 5 de julio de 2010. Artículo 3.- Para los efectos de esta Ley se entenderá por: …; VII. Instituto: El Instituto Federal de Acceso a la Información y Protección de Datos Personales, establecido en el artículo 33 de esta Ley.

[153] Gaceta Parlamentaria, Cámara de Diputados, número 1904, miércoles 14 de diciembre de 2005. DICTAMEN DE LA COMISIÓN DE GOBERNACIÓN, EN SENTIDO NEGATIVO, DE LA MINUTA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES. *http://gaceta.diputados.gob.mx/Gaceta/59/2005/dic/20051214-VIII.html*

naturaleza jurídica con la que actualmente cuenta el Instituto Federal de Acceso a la Información.

Cabe mencionar que en el proceso legislativo de la Ley Federal de Protección de Datos Personales y de la Ley Federal de Acceso a la Información Pública Gubernamental en la Cámara de Senadores, existió el compromiso de aprobar ambas leyes hasta llegar a su envío al Ejecutivo Federal; sin embargo, no fue así con relación a la Ley Federal de Protección de Datos Personales.

El 6 de septiembre de 2001, fue presentado otro Proyecto de Ley, por el Diputado Miguel Barbosa Huerta, mismo que fue rechazado el 30 de abril de 2004.[154]

En dicho Proyecto, se propone la creación del Registro Nacional de Protección de Datos Personales, sin embargo, este organismo, no tendría personalidad jurídica propia, pues se constituiría como un unte integrado al Instituto Nacional de Estadística, Geografía e Informática, con funciones limitadas de presupuesto y aplicación de sanciones, ya que la acción de habeas data, se encontraría destinada al Juez de lo Civil del orden común con base en el procedimiento ordinario establecido en el Código Civil local.

Un tercer intento de proyecto, es propuesto el 1 de diciembre de 2005,[155] por el Diputado Jesús Martínez Álvarez del Partido Convergencia, en él se dispone la creación de un Instituto Federal de Protección de Datos Personales, sin embargo, el proyecto no es claro al establecer sobre la cuestión estructural y financiera del Instituto, haciendo alusión solamente a que el órgano de control, será el que disponga la Ley Federal de Acceso a la Información Pública Gubernamental,

[154] Gaceta Parlamentaria, año IV, número 832, viernes 7 de septiembre de 2001. PRESENTADA POR EL DIPUTADO MIGUEL BARBOSA HUERTA, DEL GRUPO PARLAMENTARIO DEL PARTIDO DE LA REVOLUCION DEMOCRATICA, EN LA SESION DEL JUEVES 6 DE SEPTIEMBRE DE 2001. *http://gaceta.diputados.gob.mx/Gaceta/58/2001/sep/20010907.html#Ini20010907Barbosa*

[155] Gaceta Parlamentaria, Cámara de Diputados, número 1895-I, jueves 1 de diciembre de 2005. INICIATIVA DE LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES, POR EL DIPUTADO JESÚS MARTÍNEZ ÁLVAREZ, DEL GRUPO PARLAMENTARIO DE CONVERGENCIA. *http://gaceta.diputados.gob.mx/Gaceta/59/2005/dic/20051201-I.html*

pudiéndose entender que será un órgano dependiente del Instituto Federal de Acceso a la Información.

Sin embargo, más adelante se menciona que el Instituto, para efecto de sus resoluciones, no estará subordinado a autoridad alguna, adoptará sus decisiones con plena independencia y contará con los recursos humanos y materiales necesarios para el desempeño de sus funciones, en este último sentido, se entendería al Instituto con cierta autonomía.

El 2 de febrero de 2006, nuevamente el Senador García Torres presenta un Proyecto de Ley Federal de Protección de Datos Personales.[156] Es importante mencionar que se trata del mismo proyecto presentado anteriormente con algunas modificaciones, sin embargo, en este proyecto, se prevé la creación de un organismo de control con las facultades previstas en el primer proyecto.

De igual manera el 23 de febrero[157] y 22 de marzo[158] de ese mismo año, fueron presentadas otras dos iniciativas de Ley Federal de Protección de Datos Personales, la primera, por el Diputado David Hernández Pérez del Partido Revolucionario Institucional y la segunda por la Diputada Sheyla Fabiola Aragón Cortés del Partido Acción Nacional.

En la primera de ellas, no se establece la creación de organismo alguno, más aun, en su artículo 33, se dispone que las funciones de vigilancia e interpretación

---

[156] Gaceta del Senado, No. 164, Tercer Año de ejercicio, segundo periodo ordinario, Miércoles 5 de abril de 2006. INICIATIVA DEL SENADOR ANTONIO GARCÍA TORRES, DEL GRUPO PARLAMENTARIO DEL PARTIDO REVOLUCIONARIO INSTITUCIONAL, LA QUE CONTIENE PROYECTO DE DECRETO QUE REFORMA EL ARTÍCULO 16 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. *http://senado.senado.gob.mx/gace2.php?sesion=2006/04/05/1&documento=9*

[157] Gaceta Parlamentaria, Cámara de Diputados, número 1953-I, jueves 23 de febrero de 2006. INICIATIVA DE LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES, A CARGO DEL DIPUTADO DAVID HERNÁNDEZ PÉREZ, DEL GRUPO PARLAMENTARIO DEL PRI.
http://gaceta.diputados.gob.mx/Gaceta/59/2006/feb/20060223-I.html#Iniciativas

[158] Gaceta Parlamentaria, Cámara de Diputados, número 1972-I, miércoles 22 de marzo de 2006. INICIATIVA DE LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES, A CARGO DE LA DIPUTADA SHEYLA FABIOLA ARAGÓN CORTÉS, DEL GRUPO PARLAMENTARIO DEL PAN. *http://gaceta.diputados.gob.mx/Gaceta/59/2006/mar/20060322-I.html#Iniciativas*

estarán a cargo de Instituto Federal de Acceso a la información Pública, es decir se dota al Instituto con mayores facultades.

En el segundo de los proyectos, se menciona que si bien puede opinarse que el Instituto Federal de Acceso a la Información Pública es por definición un organismo rector de relaciones entre el sector público y los particulares, y no de relaciones que se establecen entre particulares, existen consideraciones de carácter presupuestaria e incluso del derecho administrativo que bien permiten evaluar la conveniencia de que sea el propio IFAI, y no un nuevo instituto, quien tenga a su cargo la función de ejecución de las disposiciones propuestas en esta iniciativa.

El 7 de octubre de 2008, el Diputado Federal Luis Gustavo Parra Noriega de la Sexagésima Legislatura del H. Congreso de la Unión, sometió a consideración una iniciativa con proyecto de decreto por el que se crea la Ley de Protección de Datos Personales en Posesión de Particulares, en tal documento se crea una Comisión Nacional de Protección de Datos Personales como la autoridad administrativa independiente encargada entre otros asuntos, del cumplimiento de la legislación, de conocer y resolver los procedimientos administrativos interpuestos por los particulares, así como para resolver los recursos de revisión interpuestos en contra de sus resoluciones, con la naturaleza jurídica de un organismo descentralizado de la Administración Pública Federal, no sectorizado, dotado de personalidad jurídica y patrimonio propio; contando con plena autonomía técnica y de gestión, así como para dictar sus resoluciones, y se propone la creación de una Contraloría como órgano de control interno.

Finalmente el 12 de abril de 2010, es dictaminada con proyecto de aprobación la Ley Federal de Protección de Datos Personales en Posesión de Particulares, misma que entró en vigor el pasado 6 de julio de 2010, la cual armoniza las propuestas presentadas por las fracciones parlamentarias sobre la

materia, adiciona algunas, pero es omisa en otras.[159]

La Ley contempla la circunstancia de no crear un Instituto de Protección de Datos Personales que proponen las iniciativas *"sino de dotar con amplias facultades a un organismo ya existente*", el IFAI, para ello, se propone de igual manera la reforma a los artículos 3, fracciones II y VII, y 33, así como la denominación del capítulo II del Título Segundo de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, para convertirlo en el Instituto Federal de Acceso a la Información Pública y Datos Personales.

Examinemos, cuáles fueron las atribuciones que se le dieron a este órgano, pronunciándome desde este momento sobre el acuerdo -ad cautelam- que tengo con los aciertos que la LFPFP prevé en cuestión de facultades, empero, cuestiono la institución en la que recayeron, por los argumentos que precisaré a continuación.

El IFAI, es el encargado de velar por la protección y observancia del derecho fundamental a la autodeterminación informativa (así lo establece el artículo 1º de la propia Ley). Por medio de procedimientos ágiles se le permite recibir las reclamaciones de los afectados por la violación del derecho, y debe tomarse en cuenta que la tutela no se dará por recomendaciones únicamente, sino que con base en las facultades que la legislación de la materia le prevé, pueda sancionar a quienes lo violenten.

Igualmente, se facultó al Instituto para la promoción, estudio y divulgación de este derecho humano, debido a la incipiente cultura de este derecho.

[159] A) Es omisa al tutelar al ciudadano ante el tratamiento de datos personales con fines de publicidad. No se establece de manera específica su regulación, se faculta a la Secretaría de Economía para difundir el conocimiento y regulación en torno a los datos personales entre la iniciativa privada nacional e internacional con actividad comercial. Se está en espera de Lineamientos de la autoridad. B) No prevé un control sobre el Registro Nacional de Bases de Datos de los Particulares, como consecuencia es omisa al considerar la creación de dicho Registro, por considerarlo una carga excesiva e innecesaria.

Considerando las facultades previstas por la LFPDP, realizamos el siguiente cuadro comparativo señalando las tareas que a juicio del suscrito debe de cumplir la Autoridad, y si las establecidas en la Ley, cumplen con estándares internacionales:

FUNCIONES CONSIDERADAS	FUNCIONES SEGÚN LA LEY DE PROTECCIÓN DE DATOS PERSONALES	CUMPLE CON ESTÁNDARES DE LEGISLACIONES INTERNACIONALES
INFORMAR sobre el contenido, los principios y las garantías del derecho fundamental a la protección de datos regulado en la ley.	**Artículo 38.** El Instituto..., tendrá por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana...	✓
AYUDAR al ciudadano a ejercitar sus derechos y a los responsables y encargados de tratamientos a cumplir las obligaciones que establece la legislación de la materia.	**Artículo 38.** El Instituto..., tendrá por objeto..., promover su ejercicio... **Artículo 39.** El Instituto tiene las siguientes atribuciones: ... Proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en la presente Ley...	✓
TUTELAR al ciudadano en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición cuando no han sido adecuadamente atendidos por los responsables de los ficheros.	**Artículo 39.** El Instituto tiene las siguientes atribuciones: ... Conocer y resolver los procedimientos de protección de derechos. **Artículo 45.** ... La solicitud de protección de datos deberá presentarse ante el Instituto dentro de los quince días siguientes a la fecha en que se comunique la respuesta al titular por parte del responsable...	✓
TUTELAR al ciudadano ante el tratamiento de datos personales con fines de publicidad	**Omisión Legislativa**. No se establece de manera específica esta regulatoria. Se faculta a la Secretaría de Economía para difundir el conocimiento y regulación en torno a los datos personales entre la iniciativa privada nacional e internacional con actividad comercial. Se está en espera de Lineamientos por la autoridad.	✗

GARANTIZAR el derecho a la protección de datos investigando aquellas actuaciones de los responsables o encargados de ficheros que puedan ser contrarias a los principios y garantías contenidos en la ley e imponer en su caso la sanción que corresponda.	**Artículo 38.** El Instituto..., tendrá por objeto..., vigilar por la debida observancia de las disposiciones previstas en la presente Ley; en particular aquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados... **Artículo 39**. El Instituto tiene las siguientes atribuciones: Vigilar y verificar el cumplimiento de las disposiciones contenidas en esta Ley; ...Imponer las sanciones según corresponda. **Artículo 59.** El Instituto verificará el cumplimiento de la presente Ley y de la normatividad que ésta derive... **Artículos 61 y 62.** Del procedimiento de imposición de sanciones	✓
INVESTIGAR sobre temas relacionados en protección de datos personales.	**Artículo 39.** El Instituto tiene las siguientes atribuciones: ... Elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamiento ya existentes; Desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales en Posesión de los Particulares y brindar capacitación a los sujetos obligados...	✓
FORMULAR procedimientos no legislados para la operatividad de su estructura y funcionamiento, etc.	**Artículo 39.** El Instituto tiene las siguientes atribuciones: Emitir los criterios y recomendaciones, de conformidad con las disposiciones aplicables de esta Ley, para efectos de su funcionamiento y operación; Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable.	✓
COOPERACIÓN nacional e internacional	**Artículo 39.** El Instituto tiene las siguientes atribuciones: ... Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales a efecto de coadyuvar en materia de protección de datos personales. ... Acudir a foros internacionales en el ámbito de la presente Ley...	✓

CONTROL sobre un Registro Nacional que contenga las bases de datos de los particulares con actividad de tratamiento de datos personales	**Omisión Legislativa.** La Ley no prevé la creación de un Registro Nacional de Bases de Datos en Posesión de Particulares, por considerarlo una carga excesiva e innecesaria.	x

Con base en lo anterior, y tomando en consideración los aciertos de la ley (sin dejar de soslayar las insuficiencias) al garantizar por vez primera los denominados derechos ARCO, tutelar el derecho a la autodeterminación informativa , las atribuciones que la LFPDP previó para la defensa del derecho, los procedimientos ágiles, las sanciones a los infractores de la Ley, etc., no debo omitir señalar a mi consideración, que "no" debió de ser el IFAI, en quien recayeran todas estas facultades, ya que no se garantiza la independencia e imparcialidad de su actuación.

A mayor abundamiento, la creación de un Instituto de Protección de Datos Personales, tiene que ser con plena independencia, autonomía y absoluta transparencia, porque sólo así se contribuye a la creación de mejores prácticas, para complementar las deficiencias que pudiere tener un organismo ya existente, o frenar en el sentido de contrapesos, sobre el excesivo poder que se genera por la colosal cantidad de información que manejan (ahora también privada), aunado a las nuevas atribuciones que se le dan, empero ahora, con un absoluto control, no sólo a los entes públicos, sino a los particulares, y más aun, la obligatoriedad que se le dan a sus resoluciones so pena de infracción o peor aún, la consignación de los hechos al Ministerio Público.

Me pregunto ¿en qué sentido podemos generar una cultura democrática a partir del ejercicio real de un derecho fundamental, si desde origen el sistema se encuentra viciado, derivado del Leviatán que el sistema jurídico mexicano ha creado? Y facultándolo no sólo para conocer los actos públicos, sino privados, bajo

un poder descomunal que le fue conferido legalmente, ello sin contar la atribución de imponer sanciones.

Aclaro, en este último tópico, sí es a mi parecer un acierto legislativo, pues obliga a los responsables de ficheros a tratar los datos según los Lineamientos de la Ley, bajo pena administrativa e incluso penal, pero insisto, no debió ser el IFAI en quien recayera esta facultad, pues se dotó de más poder a un organismo ya existente; por el contrario, debió de haberse creado otro Instituto a fin de no centralizar toda la información en un solo ente.

Empero, la naturaleza jurídica del Instituto, quedó establecida en la reforma del artículo 33 de la LFTAIPG de la siguiente manera:

> Artículo 33.- El Instituto es un órgano de la Administración Pública Federal, con autonomía operativa, presupuestaria y de decisión, encargado de promover y difundir el ejercicio del derecho a la información; resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de las dependencias y entidades.

"Con lo anterior tenemos que la naturaleza jurídica del IFAI es la de un organismo descentralizado, no sectorizado, de la Administración Pública Federal, por lo que entra en la estructura de Poder Ejecutivo Federal. Derivado de su inserción dentro del Ejecutivo, es que no cuenta con facultades de fiscalización del Poder Legislativo ni el judicial ni de los organismo autónomos constitucionales".[160]

Cabe finalmente mencionar los periodos de implementación de la Ley de acuerdo a los Artículos Transitorios se manifiestan de la siguiente manera:

---

[160] GÓMEZ GALLARDO, Perla. *IFAI: Avances y Retrocesos. Análisis jurídico de sus resoluciones.* Universidad de Guadalajara, Editorial e, México, 2007. Pág. 28

6 de julio de 2010

- La Ley entra en vigor.

Julio de 2011

- El Ejecutivo Federal deberá expedir su Reglamento.[161]
- Las empresas designarán a una persona o departamento de datos personales para atender las solicitudes de derechos ARCO.
- Las empresas deberán expedir los avisos de privacidad.

Enero de 2012

- Toda persona podrá ejerce sus derechos ARCO ante los responsables designados por las empresas.

Febrero de 2012

- Toda persona podrá interponer su queja ante el IFAI, en caso de que considere que cualquiera de sus derechos ARCO ejercido ha sido vulnerado por el responsable de que se trate.

[161] En comunicados de prensa IFAI/019/11 e IFAI /020/11, de 16 y 20 de febrero de 2011, el IFAI sostuvo que "El documento será expedido en julio próximo por el Ejecutivo Federal, una vez que haya sido sometido a una amplia consulta pública" y "será el resultado de un proceso abierto en el que serán incorporadas opiniones e inquietudes de la sociedad…, así como una amplia consulta entre autoridades, empresarios y público en general…, antes de ser publicado el 5 de julio próximo, el Reglamento será sometido a una serie de consultas con las dependencias reguladoras, con las cámaras industriales y la Consejería Jurídica de la Presidencia de la República, para que después la Comisión de Mejora Regulatoria (COFEMER) suba el documento a su página de Internet y lo someta a consulta pública".

5.1.2. Estructura orgánica y financiera

Conforme a las atribuciones que la LFPDP concede al Ejecutivo (Transitorio Segundo), se encuentra la implementación del Reglamento de la Ley dentro del término de 1 año a partir de la entrada en vigor de la norma (6 de julio de 2010), en el que deberá de especificarse la estructura orgánica del Instituto, a fin de ejecutar sus nuevas obligaciones, actualmente el IFAI, se encuentra en un proceso de análisis y valoración de las unidades administrativas de nueva creación así como el número necesario de recursos humanos, materiales y financieros para velar por el respeto del derecho de protección de datos personales en posesión de los particulares.

Sin embargo, para ello, deberán de tomarse en cuenta los siguientes aspectos para la estructura organizacional:

a) La Especialización del Trabajo que se sustente en el hecho de que en lugar de que un individuo realice todo el trabajo, este se divide en cierto número de pasos y cada individuo realiza uno de ellos.

b) Departamentalización, una vez divididos los puestos por medio de la especialización del trabajo, se necesita agruparlos a fin de que se puedan coordinar las tareas comunes.

La calidad de la estructura dependerá mucho de la calidad de la Especialización con la que cuenten los sujetos que se desarrollen en el área y de la consecuente delegación de funciones y autoridad para el desarrollo eficiente de las mismas, implicando la coordinación entre las unidades que se definan en la Institución.

Por lo que respecta al financiamiento de los recursos presupuestales del IFAI, los mismos serán recaudados en concepto de tasas por los servicios que

preste de acuerdo a lo dispuesto por los artículos 35 y 55 de la LFPDP[162], así como por las infracciones que imponga a quienes resulten responsables por tratamiento ilícito de datos personales en términos del artículo 64 de la Ley; y las asignaciones presupuestales que se incluyan en la Ley Federal de Presupuesto y Responsabilidad Hacendaria según lo dispone la propia Ley para el ejercicio Fiscal anual, toda vez que no debe limitarse por ley, la protección y satisfacción de nuevos derechos y necesidades por parte del Estado, que van surgiendo por virtud del natural dinamismo social y tecnológico

Por otro lado, de acuerdo a cifras oficiales publicadas en el Diario Oficial de la Federación el 07 de diciembre de 2010[163], éste Instituto recibirá durante el 2011 la cantidad total de $180 millones de pesos para la creación de plazas; dicho presupuesto podrá ser utilizado de acuerdo a lo que se indica en el Décimo Primer Transitorio del Presupuesto de Egresos de la Federación para el ejercicio fiscal 2011, mismo que a la letra indica:

> "DÉCIMO PRIMERO. Las erogaciones previstas en el presente Decreto, incluyen los recursos para el Instituto Federal de Acceso a la Información y Protección de Datos, conforme a lo previsto en el Anexo 26. Los recursos autorizados al Instituto en este Presupuesto no podrán ser traspasados.

---

[162] Artículo 35.- La entrega de los datos personales será gratuita, debiendo cubrir el titular únicamente los gastos justificados de envío o con el costo de reproducción en copias u otros formatos. Dicho derecho se ejercerá por el titular en forma gratuita, previa acreditación de su identidad ante el responsable. No obstante, si la misma persona reitera su solicitud en un periodo menor a doce meses, los costos no serán mayores a tres días de Salario Mínimo General Vigente en el Distrito Federal, a menos que existan modificaciones sustanciales al aviso de privacidad que motiven nuevas consultas. El titular podrá presentar una solicitud de protección de datos por la respuesta recibida o falta de respuesta del responsable, de conformidad con lo establecido en el siguiente Capítulo.
Artículo 55.- Interpuesta la solicitud de protección de datos ante la falta de respuesta a una solicitud en ejercicio de los derechos de acceso, rectificación, cancelación u oposición por parte del responsable, el Instituto dará vista al citado responsable para que, en un plazo no mayor a diez días, acredite haber respondido en tiempo y forma la solicitud, o bien dé respuesta a la misma. En caso de que la respuesta atienda a lo solicitado, la solicitud de protección de datos se considerará improcedente y el Instituto deberá sobreseerlo. En el segundo caso, el Instituto emitirá su resolución con base en el contenido de la solicitud original y la respuesta del responsable que alude el párrafo anterior. Si la resolución del Instituto a que se refiere el párrafo anterior determina la procedencia de la solicitud, el responsable procederá a su cumplimiento, sin costo alguno para el titular, debiendo cubrir el responsable todos los costos generados por la reproducción correspondiente
Artículo 64.- Derivado de las infracciones a la presente Ley...

[163] *Diario Oficial de la Federación de 7 de diciembre de 2010.* http://dof.gob.mx/nota_detalle.php?codigo=5169843&fecha=07/12/2010

Se autoriza al instituto señalado a crear las plazas necesarias para dar cumplimiento a las nuevas atribuciones que le fueron conferidas por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares."

5.1.3. Competencia

El Instituto ha sido facultado de acuerdo a la existencia de la Ley Federal de Protección de Datos Personales, teniendo competencia para realizar determinados actos por el ordenamiento jurídico, quedando expresadas en el artículo 38 y 39 del capítulo VI. de la citada ley.

El estatus del IFAI como un órgano competencialmente superior, en virtud de formarse como un órgano federal, estará encargado de lo siguiente:

Artículo 38.- El Instituto, para efectos de esta Ley, tendrá por objeto difundir el conocimiento del derecho a la protección de datos personales en la sociedad mexicana, promover su ejercicio y vigilar por la debida observancia de las disposiciones previstas en la presente Ley y que deriven de la misma; en particularaquellas relacionadas con el cumplimiento de obligaciones por parte de los sujetos regulados por este ordenamiento.

Artículo 39.- El Instituto tiene las siguientes atribuciones:
I. Vigilar y verificar el cumplimiento de las disposiciones contenidas en esta Ley, en el ámbito de su competencia, con las excepciones previstas por la legislación;
II. Interpretar en el ámbito administrativo la presente Ley;
III. Proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en la presente Ley;
IV. Emitir los criterios y recomendaciones, de conformidad con las disposiciones aplicables de esta Ley, para efectos de su funcionamiento y operación;
V. Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información, en atención a la naturaleza de los datos; las finalidades del tratamiento, y las capacidades técnicas y económicas del responsable;
VI. Conocer y resolver los procedimientos de protección de derechos y de verificación señalados en esta Ley e imponer las sanciones según corresponda;
VII. Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos;
VIII. Rendir al Congreso de la Unión un informe anual de sus actividades;
IX. Acudir a foros internacionales en el ámbito de la presente Ley;
X. Elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes;
XI. Desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales en Posesión de los Particulares y brindar capacitación a los sujetos obligados, y
XII. Las demás que le confieran esta Ley y demás ordenamientos aplicables.

En síntesis, podemos clasificar las facultades del Instituto:

Facultades de carácter informativas:

- Proporcionar apoyo técnico a los responsables que los soliciten para el cumplimiento de las obligaciones establecidas en la Ley.
- Rendir al Congreso de la Unión un informe anual de sus actividades.
- Desarrollar, fomentar y difundir análisis, estudios e investigaciones en materia de protección de datos personales en posesión de los particulares.

Facultades de carácter normativas:

- Interpretar en el ámbito administrativo la ley.
- Emitir criterios y recomendaciones para garantizar el pleno derecho a la protección de datos personales.
- Divulgar estándares y mejores prácticas internacionales en materia de seguridad de la información.

Facultades en materia de verificación:

- Vigilar y verificar el cumplimiento de la ley.

Facultades de carácter resolutorias:

- Conocer y resolver los procedimientos de protección de derechos, verificación e imposición de sanciones.

Facultades en materia preventiva:

- Elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes.

Facultades en materia de cooperación nacional e internacional:

- Acudir a foros internacionales en la materia.
- Cooperar con otras autoridades de supervisión y organismos nacionales e internacionales, a efecto de coadyuvar en materia de protección de datos personales.

Facultades sancionadoras:

- Llevar a cabo el procedimiento de imposición de sanciones

5.1.3.1. El IFAI como autoridad reguladora en el tratamiento de Datos Personales con fines de Publicidad.

En capítulos anteriores, abordamos el caso del sistema mexicano sobre el tratamiento de datos personales con fines publicitarios estableciendo que la Ley Federal de Protección al Consumidor es quien asegura los datos personales en México sobre este tópico específico, aplicando la regulación sobre proveedores y empresas que utilicen información de consumidores con fines de mercadotecnia o publicidad, por lo que están obligados a informar gratuitamente a cualquier persona que lo solicite si mantienen información acerca de ella, es decir, se contempla el derecho de acceso, debiendo ponerla a disposición del interesado así como qué tipo de información han compartido con terceros y la identidad de esos terceros.

Conforme a lo dispuesto por el artículo 16 de la LFPC, en la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor, de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la Procuraduría, con el fin de identificar a las empresas que cuentan con archivos de datos personales, y a los cuales el consumidor tiene el derecho de exigir directamente no ser molestado y que no le envíen publicidad.

El titular del derecho a que su información no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial, pero quedando prohibido a las empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios y a sus clientes, utilizar la

información relativa a los consumidores con fines diferentes a los mercadotécnicos o publicitarios, así como enviar publicidad a los consumidores que expresamente les hubieren manifestado su voluntad de no recibirla o aquéllos que se encuentren inscritos en el registro que se lleva ante la Procuraduría Federal del Consumidor.

La legislación mexicana de protección al consumidor, prevé la necesidad de consentimiento del titular para el tratamiento y cesión de sus datos personales tratándose de marketing y publicidad.

Ahora bien, uno de los principales problemas a los que se enfrenta México, es el tratamiento y recaudación de datos de carácter personal que hasta julio de 2010 no había sido regulado, por ello, las empresas podían tratar los datos personales sin miramientos, y con los fines que ellos consideraran, pero sobre todo el abuso hacia los consumidores sobre publicidad engañosa por parte de los proveedores quienes intentan vender sus productos, lo que se aconsejó a los consumidores no proporcionar información personal por Internet, ya que esto aumenta el riesgo de robo de datos personales, lo que constituyó un avance en la materia con fines de publicidad.

Con la aprobación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares el 6 de julio de 2010, se pensó que este tema sería abordado sistemáticamente sin embargo, tristemente vemos que no fue así, peor aún, se delegan funciones de carácter comercial a otras entidades de la Administración Pública para el resguardo de los datos personales, que si bien, todos los organismos deben de adoptar lineamientos de protección de datos, también lo es que no puede dejarse a todas y cada una de las autoridades la regulación sobre una materia, ya que la citada ley debe establecer los mecanismos base para la formulación de leyes secundarias, cuestión que no desarrolla en específico la norma.

Veamos de qué manera lo regulada la LFPC, cuyo organismo garante es la Procuraduría Federal del Consumidor en materia de publicidad en contraste con la LFPDP, la cual es omisa sobre el tratamiento de datos con fines de publicidad, y por lo tanto, no establece atribuciones al respecto para el IFAI como nuevo órgano de protección de datos personales, sino que las delega.

LEY FEDERAL DE PROTECCIÓN AL CONSUMIDOR	LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES
a)Regulación en materia de publicidad **ARTICULO 1.-** La presente ley es de orden público e interés social y de observancia en toda la República. Sus disposiciones son irrenunciables y contra su observancia no podrán alegarse costumbres, usos, prácticas, convenios o estipulaciones en contrario. El objeto de esta ley es promover y proteger los derechos y cultura del consumidor y procurar la equidad, certeza y seguridad jurídica en las relaciones entre proveedores y consumidores. Son principios básicos en las relaciones de consumo: VI. El otorgamiento de información y de facilidades a los consumidores para la defensa de sus derechos; VII. La protección contra la publicidad engañosa y abusiva, métodos comerciales coercitivos y desleales, así como contra prácticas y cláusulas abusivas o impuestas en el abastecimiento de productos y servicios. VIII. La real y efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios convencionales, electrónicos, ópticos o de cualquier otra tecnología y **la adecuada utilización de los datos aportados**, y IX. El respeto a los derechos y obligaciones derivados de las relaciones de consumo y las medidas que garanticen su efectividad y cumplimiento.	**a) Omisión de regulación en materia de publicidad** **Artículo 2.-** Son sujetos regulados por esta Ley, los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de: ... Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y **sin fines de divulgación o utilización comercial**.
b)Implementación de los derechos **ARTICULO 16.-** Los proveedores y empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios están obligados a informar gratuitamente a cualquier persona que lo solicite si mantienen información acerca de ella **(Derecho de Acceso)**. De existir dicha información, deberán ponerla a su disposición si ella misma o su representante lo solicita, e informar acerca de qué información han compartido con terceros y la identidad de esos terceros, así como las recomendaciones que hayan efectuado. La respuesta a cada solicitud deberá darse dentro de los treinta días siguientes a su presentación. En caso de existir alguna ambigüedad o inexactitud en la información de un consumidor, éste se la	**b) Delegación de funciones en aspectos comerciales** **Artículo 40.** La presente Ley constituirá el marco normativo que las dependencias deberán observar, en el ámbito de sus propias atribuciones, para la emisión de la regulación que corresponda, con la coadyuvancia del instituto. *Lo anterior permite suponer una regulación para el sector comercial y las prácticas que se desenvuelvan sobre la actividad económica, de entre las que se incluye la publicidad y el*

deberá hacer notar al proveedor o a la empresa, quien deberá efectuar dentro de un plazo de treinta días contados a partir de la fecha en que se le haya hecho la solicitud, las correcciones que fundadamente indique el consumidor, e informar las correcciones a los terceros a quienes les haya entregado dicha información **(Derecho de rectificación)**.
Para los efectos de esta ley, se entiende por fines mercadotécnicos o publicitarios el ofrecimiento y promoción de bienes, productos o servicios a consumidores.

ARTICULO 17.- En la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor; de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la Procuraduría.
El consumidor podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad. Asimismo, el consumidor podrá exigir en todo momento a proveedores y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial **(derecho de oposición)**.

ARTICULO 18.- La Procuraduría podrá llevar, en su caso, un registro público de consumidores que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios. Los consumidores podrán comunicar por escrito o por correo electrónico a la Procuraduría su solicitud de inscripción en dicho registro, el cual será gratuito.

ARTÍCULO 18 BIS.- Queda prohibido a los proveedores y a las empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios y a sus clientes, utilizar la información relativa a los consumidores con fines diferentes a los mercadotécnicos o publicitarios, así como enviar publicidad a los consumidores que expresamente les hubieren manifestado su voluntad de no recibirla o que estén inscritos en el registro a que se refiere el artículo anterior. Los proveedores que sean objeto de publicidad son corresponsables del manejo de la información de consumidores cuando dicha publicidad la envíen a través de terceros **(finalidad de los datos).**

marketing para ampliar las ventas hacia los consumidores, así lo vemos en los siguientes artículos:

Artículo 41.- La Secretaría (*Secretaría de Economía*), para efectos de esta Ley, tendrá como función **difundir el conocimiento de las obligaciones en torno a la protección de datos personales entre la iniciativa privada nacional e internacional con actividad comercial** en territorio mexicano, **promoverá las mejores prácticas comerciales en torno a la protección de los datos personales como insumo de la economía** digital, y el desarrollo económico nacional en su conjunto.

Artículo 42. – En lo referente a las bases de datos de comercio, la regulación que emita la Secretaría, únicamente será aplicable a aquellas bases de datos automatizadas o que formen parte de un proceso de automatización.

Artículo 43.- La Secretaría tiene las siguientes atribuciones:
I. Difundir el conocimiento respecto a la protección de datos personales en el ámbito comercial;
II. Fomentar las buenas prácticas comerciales en materia de protección de datos personales.
III. Emitir los lineamientos correspondientes para el contenido y alcances de los avisos de privacidad en coadyuvancia con el Instituto, a que se refiere esta Ley;
…
VI. Llevar a cabo los registros de consumidores en materia de datos personales y verificar su funcionamiento;
VII. Celebrar convenios con cámaras de comercio, asociaciones y organismos empresariales en lo general, en materia de protección de datos personales;
VIII. Diseñar e instrumentar políticas y coordinar la elaboración de estudios para la modernización y operación eficiente del comercio electrónico, así como para promover el desarrollo de la economía digital y las tecnologías de las información en materia de protección de datos personales;

Con este esquema, podemos ver la escaza regulación que se dio en materia de publicidad, bajo el argumento de la adopción de un modelo regulatorio como el de Canadá, a través del cual cada autoridad emite regulación secundaria derivada de la Ley, en el ámbito de sus atribuciones, y por otra parte, existe una instancia u

órgano garante frente al titular de los datos que resuelve sus quejas denominadas solicitudes de protección de datos personales, ya que -según las exposición de motivos de la Ley-, dada la especialización en temas como comercio, comunicaciones y transportes o salud, correspondería a las Secretarías de Estado del ramo específico, el emitir lineamientos, recomendaciones y criterios que permitan la adecuada observancia de los principios y derechos que rigen en materia de protección de datos.

En el sentido precedente, se destaca que es la Secretaría de Economía la que gozará de estas nuevas atribuciones, porque en materia comercial es donde se da el mayor flujo de información, repercutiendo directamente en el mejoramiento de la economía nacional al crear fuentes de empleo e impulsar la venta de bienes y servicios tanto a nivel nacional como internacional.

La anterior situación, en primera instancia pareciere la idónea, ya que cada autoridad regularía sobre la materia de su actividad, empero llegamos nuevamente al hecho de contar con disposiciones diversas sobre un mismo tema, que generarán en un futuro los problemas de leyes y/o reglamentos contrapuestas, antinomias, etc., ello por no adoptar criterios de unificación base para todos los órganos y entes, y sobre todo en materia de publicidad.

Un derecho debe ser plenamente reconocido, empero si no se tiene la fuerza y el empuje para hacerlo valer mediante las acciones que garanticen la tutela del derecho, no sirve de nada, por lo que analizadas las competencias del Instituto, a continuación exponemos la manera de ejercitar este derecho de tercera generación.

5.1.3.2. Acción de protección de datos personales

El 1 de Junio de 2009, se público un Decreto en el Diario Oficial de la Federación por el que se adiciona un segundo párrafo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, ello dio pauta para reconocer por primera vez en México el derecho a la protección de datos como una garantía individual, mejor conocido como Habeas Data, que refiere al derecho de todo ciudadano a la protección de su datos personales y a solicitar que sus datos e información sean actualizados, modificados, cancelados o suprimidos, en caso de que la información acerca de su persona vulnere ese derecho.

Esta nueva disposición constitucional junto con la reforma a la fracción XXIX-O al artículo 73 constitucional constituyó un fundamento para la creación de una Ley sobre Protección de Datos en Posesión de los Particulares.

El Habeas Data se constituye como una acción constitucional que se ejerce mediante una petición formal del interesado al IFAI, en términos del artículo 35, párrafo tercero y 45 de la LFPDP, a fin de verificar si los datos del reclamante en el ámbito privado fueron obtenidos lícitamente y si han sido tratados conforme al marco legislativo aplicable.

Este derecho ha sido reconocido expresamente en las Constituciones de algunos países latinoamericanos como Argentina, Colombia, Perú, Brasil, y recientemente en la Constitución Mexicana,[164] asignándole cuatro objetivos a la acción de protección de datos personales:

1) Acceso
2) Rectificación
3) Cancelación
4) Oposición

[164] Argentina (artículo 43); Colombia (artículo 15); Perú (artículo 2); Brasil (artículo 5.71); y México (artículo 16).

Nuestra Constitución mexicana con las reformas garantiza estos derechos, siguiendo el modelo de las legislaciones extranjeras, señalando que 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,[165] veámoslos a continuación de acuerdo a lo establecido por el artículo 22 de la LFPDP, que versa *"Cualquier titular, o en su caso su representante legal, podrá ejercer los derechos de acceso, rectificación, cancelación y oposición previstos en la presente Ley. El ejercicio de cualquiera de ellos no es requisito previo ni impide el ejercicio de otro. Los datos personales deben ser resguardados de tal manera que permitan el ejercicio sin dilación de estos derechos".*

1. **Acceso.** Los titulares tienen derecho a acceder a sus datos personales que obren en poder del responsable, así como conocer el Aviso de Privacidad al que está sujeto el tratamiento (Artículo 23 LFPDP).

Podemos mencionar que la reforma al artículo 16 constitucional en una primera etapa, tutela el ejercicio de la acción de la persona afectada al tomar conocimiento de los datos a ella referidos, es decir que el accionante busca conocer no sólo qué datos se tiene sobre su persona en el registro sino también con qué objetivo ellos están en el registro, de conformidad con el artículo 15 de la Ley.

La toma de conocimiento implica el ejercicio del derecho de acceso a la información. Este derecho de acceso tiene por finalidad permitir al individuo el control sobre la información que le concierne. Una vez que se ha tomado conocimiento del dato y de su finalidad, se deberá probar que existe una falsedad, inexactitud, son incompletos, discriminatorios o desactualizados para poder acceder a los siguientes derechos.

[165] DIARIO OFICIAL DE LA FEDERACIÓN. Primera Sección. Lunes 1 de junio de 2009. DECRETO por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

2. **Rectificación.** El titular de los datos tendrá derecho a rectificarlos cuando sean inexactos o incompletos (Artículo 24 LPFDP).

El caso de la rectificación busca precisión o fidelidad en los datos. Una variante de esta rectificación es la posibilidad de actualización que también debe ser contemplada en la acción de protección de datos personales.

Por medio del derecho de rectificación, se pretende que un dato sea modificado, de manera que refleje la exactitud y situación real del interesado, cumpliendo con el requisito de veracidad, que integra el principio de calidad de los datos, sustituyendo el dato incorrecto y en su caso actualizándolo.

3. **Cancelación**. El titular tendrá derecho en todo momento al derecho de cancelar sus datos personales. La cancelación de datos personales dará lugar a un periodo de bloqueo tras el cual se procederá a la supresión del dato. El responsable podrá conservar exclusivamente para efectos de las responsabilidades nacidas del tratamiento. El periodo de bloqueo será equivalente al plazo de prescripción de las acciones derivadas de la relación jurídica que funda el tratamiento en los términos de la Ley aplicable en la materia. Una vez cancelado se dará aviso al titular. Cuando los datos personales hubiesen sido transmitidos con anterioridad a la fecha de rectificación o cancelación y sigan siendo tratados por terceros, el responsable deberá hacer de su conocimiento dicha solicitud de rectificación o cancelación, para que proceda a efectuarla también (Artículo 25 LFPDP).

El derecho de cancelación, se dará en todo momento que lo solicite el titular del dato, lo cual puede acontecer cuando el dato ha entrado erróneamente al registro o cuando los datos personales ya no sean necesarios para los fines que contemplaron su almacenamiento. También, cuando el dato tenía otra finalidad y llegó al registro al que se accede por una vía ilegítima o sin consentimiento del registrado.

Ello implica un periodo en que el dato es bloqueado y posteriormente se suprime, buscando eliminar información incompleta cuya integridad no sea posible, información almacenada que hubiera cumplido con la finalidad para la que fue recolectada o datos sensibles archivados sin consentimiento del titular, sin embargo, el responsable no estará obligado a cancelar los datos en los términos del artículo 26 de la propia Ley.

4. **Oposición.** El titular tendrá derecho en todo momento y por causa legítima a oponerse al tratamiento de sus datos. De resultar procedente, el responsable no podrá tratar los datos relativos al titular (Artículo 27 LFPDP).

En cuanto al pedido de oposición, el mismo tiende a proteger los datos del individuo aislándolos de su tratamiento. Tal sería el caso del no tratamiento de datos sensibles como las enfermedades que figuren en la historia clínica o de otros considerados dentro de la clasificación de aquéllos.

Ahora bien, el responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales, están obligados a guardar el deber de confidencialidad respecto de los mismos, obligación que deberá de subsistir aun después de finalizada su relación con el titular del archivo de datos, ello lo ha dispuesto el artículo 21 de la Ley.

La abstención de comunicar por cualquier medio del contenido de las informaciones a las que hubieran accedido en virtud de sus labores específicas, y con independencia de su carácter de reservado o no, es importante para el tratamiento de datos personales, y tiene tal trascendencia al punto de que llevó al legislador a implementar sanciones de naturaleza penal para el tratamiento indebido de datos personales (Capítulo XI de la Ley).

Por último queda analizar el límite al hábeas data expreso en la Constitución el secreto relativo a la seguridad nacional: *"Artículo 16.- ... la ley, ...establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad y salud públicas o para proteger los derechos de terceros..."*

Si la Administración se niega a permitir conocer los datos al accionante, éste acudirá a la autoridad competente ¿Cuál es el control de la autoridad sobre esta decisión? La autoridad competente deberá observar y analizar la irrazonabilidad en el objeto del acto o en la finalidad perseguida por la Administración, por lo que esta autoridad debe conservar siempre una amplia potestad para penetrar en el análisis de todos los elementos que hacen a la validez del acto y además para examinar si el acto sometido a su control contiene alguna dosis de discrecionalidad o bien se trata de enjuiciar aspectos reglados, pues es sabido que los datos personales en manos privadas son una mercancía de alto valor económico, pues son manejadas hacia un interés privado que inevitablemente entraran en conflicto con otros intereses del mismo tipo.

Por lo tanto, esta exención dispuesta por la ley, pretende no poner en peligro la integridad nacional al colocarse en manos de personas dejando el campo propicio para la difamación, calumnia, falsedad, mentira, engaño e impunidad.

En éste sentido, los titulares de los Datos Personales podrán ejercer la acción de protección de éstos:

> I. Para conocer los datos personales almacenados en archivos, registros o bancos de datos en posesión de particulares destinados a proporcionar informes, así como la finalidad de aquellos; y
> II. Para solicitar la rectificación, cancelación u oposición de los datos personales en los casos en que se presuma la falsedad, inexactitud, desactualización, discriminación, etc., de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido en la presente ley.

5.1.3.3. Procedimiento.

El procedimiento es previsto en la recientemente aprobada Ley Federal de Protección de Datos Personales en Posesión de Particulares para su aplicación por el IFAI, estableciéndose las facultades procedimentales, sin embargo, debemos resaltar dos momentos que serán competencia de dicho organismo, cuando sea elevada a su conocimiento la acción de Hábeas Data:

a) Acción de Protección del derecho de acceso (Artículo 23).

b) Acción de Protección de los derechos de rectificación, cancelación u oposición (Artículos 24, 25, 26 y 27).

Veamos el procedimiento:

Tratándose del inciso a), primeramente, la solicitud deberá dirigirse directamente ante la persona física o moral privada del que se presume o se tiene la certeza que posee sus datos personales,[166] en los términos del artículo 29 de la Ley, que para el efecto dispone:

> "**Artículo 29**. La solicitud de acceso, rectificación, cancelación u oposición deberá contener y acompañar lo siguiente:
>
> I. El nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud;
> II. Los documentos que acrediten la identidad o, en su caso, la representación legal del titular;

[166] Podemos ver en la Ley que se aprobó una gran deficiencia puesto que se omite señalar la existencia de un Registro Nacional de Bases de Datos en Posesión de Particulares, a fin de que si el titular de los datos desconoce la dirección del responsable del banco de datos, pueda consultar la información de contacto de los responsables inscritos en el Registro, ello ayudaría aun más a la defensa de este derecho. Cuestión que resulta debatible toda vez que la Dirección de Clasificación de Datos Personales del IFAI ha considerado que la creación de este Registro constituye una exigencia innecesaria, empero, considero que con la creación se pudiere llevar aun más el control de los Archivos del sector privado sobre el manejo exacto de los datos personales y el cumplimiento de su finalidad.

III. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y

IV. Cualquier otro elemento o documento que facilite la localización de los datos personales."

La Ley no establece formato alguno para ser considerado sobre el ejercicio de estos derechos, sin embargo, proponemos el siguiente, de acuerdo a lo establecido por el artículo previo pudiendo constituirse en un modelo para el ejercicio del derecho de Acceso:

FORMULARIO PARA EL EJERCICIO DEL DERECHO DE ACCESO

Petición de información sobre los datos personales incluidos en un Archivo, registro, base o banco de datos.*****

DATOS DEL RESPONSABLE DEL BANCO DE DATOS O DEL TRATAMIENTO DE DATOS (Artículo 29, frac. I)

Nombre: .....
Domicilio: .....
C.P..... Delegación o Municipio: .....
Estado: .....

DATOS DEL TITULAR/APODERADO (Artículo 29, frac. II)

Nombre del Titular: .....
Apoderado:..... Acreditación.....
Domicilio: .....
C.P..... Delegación o Municipio:..... Estado: ....., e-mail: ..... Otro medio para ser contactado ..... Identificación:..... No....., del que acompaña fotocopia, por medio del presente escrito vengo a manifestar mi deseo de ejercer mi derecho de acceso, por lo que atentamente

SOLICITO:

1.- Que en términos del artículo 28 y 29, fracción III de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, me facilite gratuitamente (artículo 35) el acceso a los datos existentes sobre mi persona en sus bases o registros en el plazo máximo de 15 días (artículo 32), a contar desde la respuesta de esta solicitud, entendiendo que si transcurre el plazo de 20 días sin contestación expresa, la misma ha sido denegada. En este caso se podré interponer la solicitud de protección de datos ante el Instituto Federal de Acceso a la información y Datos Personales en términos del artículo 45 y 46 de la citada Ley.

2.- Que si la solicitud del derecho de acceso fuese procedente, me sea entregada la misma por medio de (*especificar de qué manera se quiere la información, copias, CD, correo electrónico correo a domicilio, etc.*) en el plazo de 15 siguientes a la fecha en que se comunica su respuesta en términos del artículo 32 de la Ley.

3.- Que esta información comprenda de modo legible e inteligible los datos que sobre mi persona están incluidos en sus registros, y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.

4.- Información Adicional:.....

En la Ciudad de..... a los ..... días del mes de..... de 20.....

FIRMA

*****Los derechos se ejercen ante el responsable del banco de datos: Persona física o moral, para lo cual todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere el artículo 30 de la LFPDP.

En el caso del inciso b), la solicitud procederá cuando se trate de datos:

1. Erróneos
2. Falsos
3. Incompletos
4. Desactualizados
5. Cuando hayan cumplido su finalidad

El pedido de rectificación, cancelación u oposición, deberá hacerse ante el responsable del archivo, registro, base o banco de datos, contando la persona física o moral con el plazo de 20 días para dar respuesta a la primera solicitud referente a alguno de estos derechos, transcurrido este tiempo y en caso de resultar procedente la solicitud, el responsable del archivo, registro, base o banco de datos, realizará la rectificación, cancelación u oposición, dentro del término de 15 días a partir de que se comunique la respuesta.

Es importante mencionar que en cualquiera de los supuestos de acceso, rectificación, cancelación u oposición de los datos personales, el responsable del Archivo, podrá negar el ejercicio de estos derechos cuando:

a) El solicitante no sea el titular de los datos personales;
b) Cuando en su base de datos, no se encuentren los datos personales del solicitante;
c) Cuando se lesiones los derechos de un tercero;
d) Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja o no permita el ejercicio de los derechos ARCO; y
e) Cuando el ejercicio de los derechos ya haya sido realizado.

El siguiente puede ser un modelo para el ejercicio del derecho de rectificación, cancelación u oposición de datos personales:

FORMULARIO PARA LA RECTIFICACIÓN, CANCELACIÓN U OPOSICIÓN DE DATOS PERSONALES INCLUIDOS EN BANCOS DE DATOS*

DATOS DEL RESPONSABLE DEL BANCO DE DATOS O DEL TRATAMIENTO DE DATOS (Artículo 29, frac. I)

Nombre: .....
Domicilio: .....
C.P..... Delegación o Municipio: .....
Estado: .....

DATOS DEL TITULAR/APODERADO (Artículo 29, frac. II)

Nombre del Titular: .....
Apoderado:..... Acreditación.....
Domicilio: .....
C.P..... Delegación o Municipio:..... Estado: ....., e-mail: ..... Otro medio para ser contactado .....
Identificación:..... No....., del que acompaño fotocopia. Por medio del presente escrito vengo a manifestar mi deseo de ejercer el derecho de **rectificación / cancelación / oposición**, de datos de conformidad con el artículo 28 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, por lo que atentamente

SOLICITO:

1. Que dentro del plazo máximo de 15 días hábiles se proceda gratuitamente a la **rectificación** *(para este caso, el titular deberá indicar, las modificaciones a realizarse y aportar la documentación que sustenta su petición. Artículo 31)* **/ cancelación / oposición**, de los datos relativos a mi persona que se encuentren en su base de datos, referente a.....
   Los datos que deberán **rectificarse/cancelarse/oposición** se enumeran en la hoja anexa al presente, se acompañan los documentos que acreditan su veracidad.

2. Que me comuniquen por escrito a la dirección arriba indicada, la **rectificación/cancelación/oposición** de los datos una vez realizada.

3. Que para el caso que el responsable del banco de datos considere que la **rectificación/cancelación/oposición** no procede, lo comunique en forma motivada, por escrito y dentro del plazo de 20 días atento a lo dispuesto por el artículo 32 de la Ley entendiendo que si transcurre el plazo de 20 días para dar respuesta expresa a la presente solicitud, se entenderá que la misma ha sido denegada. En este caso podré interponer la solicitud de protección de datos ante el Instituto Federal de Acceso a la información y Datos Personales en términos del artículo 45 y 46 de la citada Ley.

4. Información Adicional:.....

En la Ciudad de ..... a los ..... días del mes de..... de 20.....

FIRMA

***Los derechos se ejercen ante el responsable del banco de datos: Persona física o moral, para lo cual todo responsable deberá designar a una persona, o departamento de datos personales, quien dará trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere el artículo 30 de la LFPDP.

Ahora bien, en caso de que los derechos ARCO sean violentados por el responsable, para que el Instituto Federal de Acceso a la Información y Datos Personales pueda iniciar el control, es necesario que hayan transcurrido los términos indicados en la solicitud y presentar la copia sellada referente al acceso, rectificación, cancelación u oposición así como la negativa del responsable y demás documentos que se desprendan del trámite ante la responsable.

En caso de que se omita por parte de la responsable dar respuesta, únicamente bastará que el titular de los datos acompañe a su solicitud de protección de datos el documento que pruebe la fecha en que presentó la solicitud del ejercicio de los derechos ARCO y haber transcurrido el término de 2o días según lo dispone el artículo 32 de la LFPDP.

En ambos casos, la solicitud de Hábeas Data ante el IFAI deberá hacerse por escrito libre o en los formatos que al efecto designe el sistema electrónico del Instituto, en el que se deberá contener:

I. El nombre del titular o, en su caso, el de su representante legal, así como del tercero interesado, si lo hay;
II. El nombre del responsable ante el cual se presentó la solicitud de acceso, rectificación, cancelación u oposición de datos personales;
III. El domicilio para oír y recibir notificaciones;
IV. La fecha en que se le dio a conocer la respuesta del responsable, salvo
V. que el procedimiento inicie con base en los previsto en el artículo 50:
VI. Los actos que motivan su solicitud de protección de datos, y
VII. Los demás elementos que se considere procedente hacer del conocimiento del Instituto.

El siguiente puede constituir un modelo de solicitud de protección de datos personales por violación a los derechos ARCO.

SOLICITUD DE
PROTECCIÓN DE DATOS PERSONALES
TITULAR _____
RESPONSABLE_____

C.C. COMISIONADOS INTEGRANTES DEL
INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN
Y PROTECCIÓN DE DATOS PERSONALES ***(O EN SU CASO LA AUTORIDAD QUE SEA FACULTADA DE ACUERDO A LA ESTRUCTURA INTERNA DEL IFAI CONFORME AL REGLAMENTO DE LA LFPDP)***

P R E S E N T E S.

_____**,** *(si promueve el representante legal deberá anexar el documento con el que acredite la personalidad con la que se ostenta)*, por propio derecho y en mi calidad de agraviado a mi derecho a la autodeterminación informativa y concretamente del derecho de: *(según corresponda)* ACCESO/RECTIFICACIÓN/CANCELACIÓN/OPOSICIÓN, señalando como domicilio para oír y recibir todo tipo de notificaciones y documentos el ubicado en _____, y autorizando para los mismos efectos a los señores_____, ante ustedes, atentamente manifiesto:

Que con fundamento en los artículos 1, 2, 6, 8, 9, 22, 23,24, 25, 45, 46, 47, 48, 49, 50, 51, 54, 55, 57, 58 y demás relativos y aplicables de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, y encontrándome dentro del término de 15 días, vengo en este acto a presentar **SOLICITUD DE PROTECCIÓN DE DATOS PERSONALES** *(Recurso de Hábeas Data)* en contra de *(especificar el nombre del responsable, persona física o moral, ante el cual fue presentada la solicitud de acceso, rectificación, cancelación u oposición de datos personales)*, el cual puede ser localizado en _____, para que de ser procedente el presente recurso, se le requiera para que dentro del plazo de 10 días siguientes, haga efectivo el ejercicio del derecho, objeto de protección, debiendo dar cuenta por escrito de dicho cumplimiento a esa H. Autoridad dentro de los siguientes 10 días a su notificación.

A fin de dar cumplimiento a lo establecido por el artículo 46, fracción IV de la Ley, manifiesto que la respuesta del Responsable me fue notificada el *(anotar la fecha en que se dio a conocer al titular del dato la respuesta por parte del Responsable cualquiera que esta haya sido)*.

(Este párrafo es únicamente para el caso de que no haya dado respuesta el responsable al titular ante la solicitud presentada) Con fundamento en el artículo 55 de la Ley, solicito a esa H. Autoridad requiera al Responsable para que dentro del término de 10 días contados a partir de que sea legalmente notificado, acredite haber respondido en tiempo y forma la solicitud de *(según corresponda)* ACCESO/RECTIFICACIÓN/CANCELACIÓN/OPOSICIÓN o bien de respuesta a la misma.

Motivan la presente solicitud los presentes hechos: (*Narrar los acontecimientos que fundamentan el accionar del titular ante el IFAI, ya sea que el responsable haya negado la solicitud; haya sido omiso en dar respuesta a la misma; no haya entregado al titular los datos personales solicitados; lo haga en un formato*

incomprensible; se niegue a efectuar modificaciones o correcciones a los datos o el titular no esté conforme con la información entregada por considerar que es incompleta o no corresponde a la información requerida).

Se violan en mi perjuicio el *(los)* artículo *(s)* (*anotar los preceptos legales que se consideran vulnerados, según el derecho que pretenda protegerse)* de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Acompaño al presente recurso la solicitud de fecha _____, presentada ante el Responsable en la que solicito *(según corresponda)* ACCESO/RECTIFICACIÓN/CANCELACIÓN/OPOSICIÓN, así como la respuesta *(si la hubiere, de lo contrario sólo la solicitud será suficiente)* que hoy se recurre *(si no se cuenta con el documento, deberá el accionante proporcionar los datos que permitan su identificación).*

A fin de que esa H. Autoridad cuente con mayores elementos: *(hacer del conocimiento los elementos que se tengan disponibles, así como exhibir toda documentación que pudiere resultar pertinente para la defensa del derecho que se pretende proteger).*

En términos del artículo 54 de la Ley, solicito de esa H. Autoridad instar al Responsable a efecto de buscar una conciliación con el accionante, que conste por escrito y tenga efectos vinculantes. Asimismo acogiéndome al beneficio del artículo 50 de la Ley, solicito sea suplida la deficiencia de la queja, siempre y cuando no se altere el contenido original de mi solicitud de protección en cuanto a los derechos que se pretenden proteger, ni se modifiquen mis hechos o peticiones expuestas en la presente.

Por lo expuesto,

A USTEDES C.C. INTEGRANTES, atentamente pido:

PRIMERO. Tenerme por presentado en términos del presente escrito, solicitando la protección de mi derecho de ACCESO/RECTIFICACIÓN/CANCELACIÓN/OPOSICIÓN relativo a los datos personales.

SEGUNDO. Notificar a la responsable corriéndole traslado del presente recurso para que en el término de 15 días produzca su respuesta, ofrezca las pruebas que estime y manifieste lo que a su derecho convenga.

TERCERO. Una vez desahogado el procedimiento, dictar resolución favorable al titular, en la que se haga efectivo el ejercicio del derecho objeto de protección de la presente solicitud.

FIRMA

_____

TITULAR DEL DATO

(APODERADO LEGAL , en su caso)

México, Distrito Federal a los _____ días del mes de _____ de 20____.

5.1.3.3.1. Principios Generales

Los principios sobre los cuales debe basarse una Institución son el resultado de muchos años de experiencias, en los que han creado un conjunto de normas generales. Con frecuencia esos principios son el trato de la aceptación gradual, generalizada, de los enfoques adoptados por uno o varios organismos en la solución de sus problemas en situaciones nuevas.

En este ámbito se deben adoptar principios que se reconozcan y que sean admitidos en el desempeño de la función pública, amén de los establecidos por la propia Constitución Federal y en la Ley Federal de Responsabilidad de Servidores Públicos.

En este sentido, los siguientes principios o elementos pueden ser tomados en consideración por el Instituto Federal de Acceso a la información y Datos Personales cuando sea determinada la Reglamentación respectiva en cuanto al sistema de protección a la autodeterminación informativa:

1. Deberá establecerse con un objetivo previamente definido y entendido, incluyendo las divisiones o funciones que sean básicas al mismo tiempo: para que el organismo sea eficaz, requiere que sus objetivos sean claros y la consecución de los mismos esté apoyada por un plan de organización que mantenga las políticas para llevar a cabo la acción.
2. La responsabilidad siempre deberá ir acompañada por la autoridad correspondiente: la autoridad no se puede concebir separada de las responsabilidades, es decir, esta debe ser comprendida por la persona que la ejerza y por los demás miembros del organismo.
3. La delegación de la autoridad deberá ser descendente para su actuación: de acuerdo con el sistema de organización que se establezca, la autoridad debe darse de un nivel superior a otro inferior, la falta de una apropiada delineación de autoridad produce demora, mala comunicación, falta de control administrativo y sobre todo fuga de responsabilidad.
4. La división del trabajo adecuado evitará duplicidad de funciones: una lista de todas las funciones que se desarrollan en la empresa sirve de guía para asignarlas a áreas o divisiones especificas, estableciendo y determinando como entidades separadas el menor número de funciones en que pueda ser dividido el trabajo.

5. Cada empleado debe ser responsable ante una sola persona: si no se respeta el principio básico de la "unidad de mando" es imposible establecer responsabilidades. Es necesario diferenciar ante quien se es responsable y las cosas por las que se es responsable.
6. Debe estructurarse una organización lo más sencilla posible: cada estructura deberá ser analizada con el objeto de asegurarse que esta resulte práctica, desde el punto de vista de costos, si la misma implica costos elevados, la organización tendrá que ser modificada.

Por tanto, creada la Ley y facultado el IFAI, es necesario qué en esta organización para alcanzar los objetivos y propósitos, se deban tomar en cuenta las principales experiencias históricas internacionales en la construcción de un nuevo sistema, para el establecimiento de principios acordes con la realidad.

5.1.3.4. Sanciones

Tomando en consideración la naturaleza jurídica del Instituto Federal y sus facultades legislativas para imponer sanciones, podrá imponerlas de carácter administrativo con independencias de las sanciones civiles y penales a las empresas o personas físicas responsables de archivos, ficheros, bases o bancos de datos, que pueden ir desde una amonestación con apercibimiento, multa y hasta la consignación de los hechos al Ministerio Público de la Federación por la comisión de algún hecho delictivo, atendiendo a los daños que se hubieren causado o puedan causarse, el carácter intencional o no de la acción u omisión constitutiva de la inobservancia a la ley y la gravedad de esta o la reincidencia.

Pueden constituir infracciones de naturaleza administrativa las siguientes:

I. No cumplir con la solicitud del titular para el ejercicio de los derechos ARCO, sin razón fundada;
II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de los derechos ARCO;
III. Declarar dolosamente la inexistencia de datos personales cuando exista total o parcialmente en las bases de datos del responsable;
IV. Dar tratamiento a los datos personales en contravención a los

principios establecidos en la presente Ley;

V. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de esta Ley;

VI. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares;

VII. No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64;

VIII. Incumplir el deber de confidencialidad establecido en el artículo 21 de esta Ley;

IX. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12;

X. Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos;

XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;

XII. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley;

XIII. Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible;

XIV. Obstruir los actos de verificación de la autoridad;

XV. Recabar datos en forma engañosa y fraudulenta;

XVI. Continuar con el uso legitimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares;

XVII. Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos ARCO, establecidos en la CPEUM;

XVIII. Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley; y

XIX. Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de los previsto en la presente Ley;

Las mismas serán sancionadas con apercibimiento y multas que podrán aumentarse por la reiteración de conductas, tomando en consideración: 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.

El procedimiento de imposición de sanciones dará comienzo con la notificación que efectúe el IFAI al infractor, sobre los hechos que motivaron el inicio del procedimiento otorgándole un término de 15 días para rendir pruebas y manifestar lo que a su derecho conviniere, admitiendo las pruebas el Instituto y otorgando un término de 5 días para alegatos.

Una vez analizadas las pruebas y demás elementos resolverá dentro del término de 50 días a la fecha en que inició el procedimiento sancionador, notificando la resolución a las partes.

A manera de conclusión podemos señalar que, tomando en consideración las iniciativas presentadas por las diversas fracciones parlamentarias fueron precedente para la creación de una Ley de Protección de Datos Personales en Posesión de Particulares y con ello el fortalecimiento de un organismo ya existente para la salvaguarda de este derecho.

La LFPDP, sustenta la confiabilidad de la protección de datos al Instituto Federal de Acceso a la Información Pública, con la justificación de un ahorro de costos adicionales y gastos que sobrevendrían con la creación de un Instituto nuevo, que bien podrían destinarse a la adecuación de la estructura del IFAI, y aquí, es precisamente, en la adaptación de una estructura nueva tanto orgánica como financiera que deben considerarse las opciones vertidas sobre el manejo de recursos humanos y materiales que son expuestos en el presente capítulo, sobre ello la legislación de la materia en creación es omisa, dejando esta tarea a un Reglamento que aun no ha sido creado.

Opino que al haber sido aprobada la Ley, la unificación de criterios debe ser esencial a fin de evitar conflictos potenciales y que el IFAI, al contar con autonomía plena y especialización no sólo en materia de protección de datos personales, sino también en el ámbito de la administración, organización, calidad y desempeño del sector como lo hemos venido sustentando en el presente proyecto, deberá posicionarse sobre el particular y obtener el grado de conocimiento y confiabilidad que se requiere en nuestro país.

El Instituto Federal de Acceso a la Información, como encargado de velar por el derecho fundamental de protección de datos personales necesita la cooperación del gobierno y de los ciudadanos. Por lo tanto el Instituto tendrá una tarea sumamente compleja, que va desde la protección al individuo de sus datos personales en contra de los abusos públicos o particulares, hasta la de colocar a nuestro país en un ranking de Estados que aseguren el respeto pleno de este derecho fundamental, demostrando que el desarrollo potencial del Estado mexicano va a la par de muchos otros.

C O N C L U S I O N E S

1. La identificación del derecho a la protección de datos personales se ha constituido como un motivo de constantes interpretaciones científicas, legislativas y jurisprudenciales desde su aparición en los primeros textos internacionales en 1973 y años siguientes, hasta el texto internacional más importante sobre la recogida y tratamiento de los datos personales, el Convenio 108 del Consejo de Europa.

2. Los ordenamientos internacionales han ido incrementando poco a poco la formación, reconocimiento y en algunos países la consolidación de este derecho (España y Argentina, recientemente México, que pretende colocarse a la vanguardia de los derechos de tercera generación), pero también motivo de disparidad de criterios y acepciones sobre el mismo y en dónde debe establecerse el derecho de protección de datos personales, si como un derecho de configuración legal o con plena autonomía.

3. La protección de datos personales hoy en día se ha constituido como un derecho fundamental a título propio bajo el reconocimiento de "autodeterminación informativa", pese a las distintas acepciones que ha tenido, es dable denominarlo así por la amplitud de protección de la información personal sobre qué, cómo, cuándo y dónde a través de los distintos medios puede conocerse sobre nosotros; además, de las derivadas de cualquier otro acontecimiento en el que se ponga en riesgo cualquier información, sea sensible o no, íntima o no, en cualquier soporte informático o manual, constituyéndose como verdadero derecho fundamental, ya que existe un titular, un derecho plenamente reconocido y un sujeto pasivo que debe hacer o dejar de hacer para el goce de aquél.

4. El derecho a la protección de datos personales confiere la facultad de poder controlar por parte del individuo lo que se sabe y no sobre sus datos personales, su recogida y tratamiento, es decir impone a terceros la obligación de realizar u omitir determinados actos, poniendo limites y desarrollando el pleno ejercicio del derecho fundamental que ampara elementos más allá del propio derecho a la privacidad e intimidad, amén de que así fue reconocido por la Carta de Derechos Fundamentales de la Unión Europea.

5. Las legislaciones en España y Argentina han respondido gradualmente a las exigencias internacionales sobre la adecuación de estándares de protección acogidos

en sus legislaciones, aportando principios básicos que sitúan a estos países en un nivel adecuado de protección derivado de los Tratados Comerciales con los que estos países cuentan evitando el desinterés del comercio con países de América y la Unión Europea; el Estado mexicano recientemente se ha incorporado a los países que cuentan con una legislación en la materia, pero aun no alcanzando los estándares de calidad que se requieren.

6. Las reforma constitucional de 1 de junio de 2009 en México, incrementó un nivel de protección a la persona respecto de sus datos personales en relación al uso de la información tanto por el sector público como privado dando el primer paso para legislar ordinariamente sobre la materia, lo que dedujo a la creación de una Ley Federal de Protección de Datos Personales en Posesión de Particulares, unificando los criterios en materia de protección de datos personales y confirmando la autodeterminación informativa como derecho autónomo.

7. En este ámbito, la Ley Federal de Protección al Consumidor, dio una protección hasta cierto punto más amplia sobre el uso de la información, protegiendo por vez primera al consumidor de la publicidad, pudiendo exigir a las empresas que utilicen información referente a ellos con fines publicitarios o mercadotécnios no sea cedida o transferida a terceros. Esta ley constituye un intento sobre protección de datos personales con fines publicitarios y mercadotécnios, estableciéndose los primeros principios que rigen sobre la materia: calidad, consentimiento, seguridad y confidencialidad en la recogida y tratamiento de los datos personales, y regulando los derechos de acceso, rectificación y oposición.

8. La Ley Federal de Transparencia y Acceso a la información Pública Gubernamental constituye otro intento de protección de datos personales, enunciando conceptos y principios que rigen los datos personales, su acierto es el acceso a la información pública en poder de entes públicos y recientemente con la creación de la Ley de Protección de Datos Personales Federal y la reforma a la Ley de Acceso, información en posesión de particulares.

9. La nueva Ley Federal de Protección de Datos Personales en Posesión de Particulares es omisa sobre la recopilación de datos con fines publicitarios o mercadotécnios, por tanto no presenta un ámbito integral de protección con las cuestiones de publicidad, venta directa o algunas otras actividades análogas, lo cual no permite establecer

perfiles determinados con fines promocionales, comerciales o publicitarios, ni hábitos de consumo, aun cuando exista consentimiento, lo que si ocurre en las legislaciones española y argentina, pese a ello nuestra legislación constituye un acierto legislativo al considerar el derecho fundamental en nuestro sistema jurídico mexicano.

10. No equilibra del todo el derecho a la protección de los datos personales con las actividades del sector privado de obtener, usar o divulgar información personal, no establece reglas claras y sencillas para el manejo de la información que circula a diario en diferentes operaciones que se realice en el sector empresarial sobre todo en las tecnologías de la información, internet, correo electrónico, teléfono.

11. La creación de la Ley pareciere haber sido legislada por el sector empresarial, en el que las exigencias sociales quedaron parcialmente concedidas, pero sin perder el control y poder total de los datos que quisieren tratar, ya que no se puede concebir que esta legislación no estatuya el régimen de protección de datos en la publicidad, siendo que constituye un factor importante sobre la actividad comercial que debiere ser regulado y más aun remita las condiciones comerciales a la Secretaría de Economía para su regulación. Amén de ello, no se establece la existencia de un Registro de inscripción de Bases de Datos por considerarlo "carga excesiva e innecesaria de cumplimiento".

12. Pese a ello, dentro de las ventajas de la Ley, podemos mencionar las siguientes: reviste las características de ser una legislación moderna, que reconoce los llamados derechos de tercera generación, en particular la autodeterminación informativa; establece todos los derechos reconocidos como derechos ARCO, estableciendo mecanismos para ejercerlos y tutelarlos; facilita la transferencia de datos personales dentro y fuera del país, siempre y cuando el responsable informe en el aviso de privacidad la realización, la finalidad de la transferencia y el titular acepte o consienta; prevé una serie de conductas consideradas como infracciones e incluso prevé penas por delitos especiales; reconoce que los particulares pueden impugnar las decisiones del IFAI mediante el juicio de nulidad ante el Tribunal Federal de Justicia Fiscal y Administrativa; y, prevé mecanismos de autorregulación.

13. El derecho fundamental protegido por la Ley Española está sustentado en el artículo 18.1 y 18.4 de la Constitución. Una de las más importantes constataciones del

marcado carácter jurídico del objeto de la ley, la encontramos en la Sentencia del Tribunal Constitucional 292/2000 que permite el nacimiento de un nuevo derecho fundamental, todo ello confirma además la voluntad expresa de la Ley 15/99 de disfrutar de un objeto expansivo tanto en su configuración como en su aplicación.

14. Es tarea constante de los países adoptar las medidas y estándares internacionales que aseguren una plena eficacia en el nivel de protección de datos personales con el fin de incrementar la competitividad a nivel mundial, y que no sólo permita al gobernado ejercer eficazmente un nuevo derecho fundamental, sino también traerá consigo un reconocimiento externo que amplíe las relaciones comerciales con los bloques económicos de América y de la Unión Europea.

15. Los medios de comunicación y las tecnologías de la información han afectado directamente al individuo en el disfrute de los derechos fundamentales, al verse menoscabado con el uso de la informática, la computación y el internet, pese a que el éxito de internet es la libertad; internet se ha convertido en el nuevo canal de comunicación en todo el mundo que permite el envío y recepción de información a través de una conexión de computadoras donde se puede interactuar con los demás.

16. Internet constituye una nueva forma de acción y mercado para las empresas que aprovechan la Red para la interacción con los consumidores y ofertan sus productos mediante la publicidad, allegándose cada día de más bases de datos, derivadas de los registros que las personas realizan al ingresar a la web.

17. La recopilación de datos y su tratamiento automatizado dan lugar a la aparición de los bancos de datos, programas destinados a dar información en soportes contenidos en una computadora lo que llega a constituirse como base de datos públicos y privadas. México se constituye como un país más vulnerable al flujo de datos por internet, por su deficiencia normativa en la materia.

18. El marketing utiliza técnicas de publicidad y estrategias de mercado para posicionarse del consumidor, muchas veces con ofertas engañosas para la adquisición de un producto o servicio, lo que lleva al tratamiento de datos personales, poniéndolos en un grave riesgo por el posible robo de ellos.

19. El marketing y la publicidad utilizan a la base de datos como principal herramienta para aperturar el negocio, lo que se traduce en ventajas para el vendedor, puesto que

se tiene conocimiento de todos sus hábitos, consumos, gustos, aficiones, afecciones, con personalización, cobertura geográfica, presupuestos, gastos, y en general una radiografía de la actividad del individuo lo que incluye desde luego sus datos personales, constituyendo la publicidad y marketing una perspectiva de venta que se ha venido realizando a través de las diferentes TIC's.

20. Las cuentas de correos electrónicos han servido de almacenamiento de mensajes entre los que se encuentran los de publicidad textual o gráfica. Las cuentas de correo electrónico o e-mail, ofrecen a las empresas verdaderos bancos de datos que son recopilados en el momento del registro en la apertura de la cuenta, y con ello las comunicaciones se encuentran guardadas y archivadas.

21. La irrupción masiva en la utilización de nuevas tecnologías en transferencia de datos, mensajes e información, visitas a las páginas web, ocasiona la posibilidad de violación a los correos electrónicos y llegadas de *spam y cookies*, de ahí que sea necesario regular estas actividades dentro de la web, pues la cuenta de correo electrónico debe ser considerada como un dato de carácter personal. Un sistema de seguridad de carácter criptográfico para el envío de mensajería o archivos , es una solución viable.

22. Los bancos de datos son previamente elaborados, comprados, o clasificados mediante la información del comportamiento crediticio y de consumo, compras, encuestas, participación en sorteos, concursos, solicitudes de empleo, tarjetas bancarias, guías telefónicas o listas públicas y privadas que posteriormente son utilizadas para el telemarketing (teléfono), por la cuenta de correo electrónico o simplemente por el uso del internet al entrar a navegar en el ciberespacio en donde ingresar a los sitios web con ese solo hecho quedan registros de las paginas que visitamos y por ende la captación de los datos personales.

23. Los sitios web recurren a los datos personales que componen a los perfiles de usuarios e informaciones obtenidas de sus blogs etc., clasificándolos por categorías según sus gustos, ello para hacerles llegar publicidad referente a sus hábitos de consumo.

24. En México no existe una protección integral ante el uso indiscriminado de los datos personales para fines de publicidad, de consumo, e incluso ilícitos, lo que no permite

que se adopten mecanismos de control sobre la protección de datos. La nueva Ley Federal de Protección de Datos no establece de manera específica el tratamiento de datos con fines de publicidad. De ahí que no se permite disociar la información con respecto a la persona, lo que tendría un grado de seguridad para proteger la identidad del individuo sobre el uso y tratamiento de sus datos.

25. La Ley Federal de Protección al Consumidor, constituye la única legislación en México que protege de manera somera los datos personales en materia de publicidad.

26. En México, el ejercicio de los derechos ARCO "en materia de publicidad", no se encuentra regulado específicamente por la nueva Ley de Protección de Datos Personales, sino que se da una remisión a otros sectores de la Administración Pública, concretamente, se dota a la Secretaría de Economía de atribuciones para reglamentar lo referente a los aspectos comerciales y al tratamiento de datos personales, tópico que aun sigue pendiente, lo que deja únicamente para tutela a la Ley Federal de Protección al Consumidor, que es incompleta sobre los principios y derechos de la autodeterminación informativa, motivo por el cual la Ley Federal de Protección de Datos Personales en Posesión de Particulares es insuficiente.

27. El IFAI como organismo garante para proteger los datos personales en México debe crear ante la insuficiencia de la Ley, lineamientos, parámetros, programas, políticas, buenas prácticas, recomendaciones y criterios que complementen los derechos de los titulares de los datos para no ser molestados con ofertas publicitarias y marketing, salvo que haya consentimiento expreso o por lo contrario la negativa a que dicha información sea tratada con fines diversos por los que fueron recopilados o finalmente que se tenga la potestad de disociar los datos con fines publicitarios del individuo, esto es que el perfil pertenezca a un grupo y no a un individuo, ante la sesión del banco de datos a otras empresas por la competencia del mercado.

28. Es necesaria la creación de un Registro Nacional de Bases de Datos en México, la cual la norma de Protección de Datos Personales vigente no establece, ciertamente, ello constituye otra deficiencia en el desarrollo de nuestra legislación en la materia, pues al no contar con un registro como tal, es difícil llevar un control de los archivos y las bases de datos tanto públicas como privadas, que excedan el uso personal. Por tanto, es dable la exigencia de un registro que sea habilitado por la autoridad de control a

fin de ser supervisado constantemente de acuerdo a su funcionamiento y con base en las disposiciones legales vigentes atendiendo los principios que rigen la materia sobre confidencialidad y seguridad en los ficheros.

29. La falta de un Registro de Bases de Datos, no permite al individuo gozar plenamente del derecho a la autodeterminación informativa, porque al no recoger la Ley Federal de Protección de Datos Personales esta obligación, limita el derecho de control por parte de las autoridades reguladoras, no permitiendo un ejercicio pleno del derecho fundamental, ya que con esta obligación se implementa y complementa el mismo.

30. Ante las deficiencias legislativas, el IFAI y la Secretaría de Economía, deben crear en conjunto, altos estándares de protección a fin de complementar la Ley, a través de las diversas disposiciones administrativas según las competencias y atribuciones conferidas por mandato legal, constituyéndose el Instituto como coadyuvante del sector empresarial para regular el tratamiento de los datos personales en la publicidad, actuando según los parámetros de sus facultades.

31. No constituye un acierto legislativo el haber considerado al IFAI como Instituto de Protección de Datos Personales por lo siguiente: la creación de un Instituto de Protección de Datos Personales, debe de ser completamente independiente y autónomo con el fin de contribuir a mejores prácticas y políticas en la defensa del derecho que pretenda protegerse, y evitar el excesivo poder que pueda generarse por la descomunal cantidad de información que manejen, y el otorgarle un absoluto control de entes públicos y privados, centraliza el manejo de información, más aun por la obligatoriedad que se le dan a sus resoluciones, por lo que considero que debió de haberse creado un Instituto autónomo e independiente del IFAI.

32. Nadie puede asegurar que un sistema de información es totalmente seguro, si alguien se empeña en acceder a los datos lo hará, costará más o menos, pero lo hará. Al fin y al cabo, las medidas de seguridad son simples barreras que colocamos en determinados lugares para impedir el acceso, empero cuantas más barreras dispongamos, más difícil será el acceso. Lo único que podemos garantizar es que con el cumplimiento exacto y puntual de la Ley Federal de Protección de Datos Personales y sus leyes complementarias, nuestra responsabilidad quedará a salvo y en caso de necesitarlo podremos siempre decir quién fue, es decir, trasladar la responsabilidad de la acción, objetivo final de cualquier Ley.

ANEXO I

Ley Federal de Protección de Datos Personales en Posesión de los Particulares[167]

CAPÍTULO I.
Disposiciones Generales

Artículo 1. *Objeto*.
- a) A quiénes alcanza la ley
- b) Garantía de privacidad
- c) Garantía de autodeterminación informativa

Artículo 2. *Sujetos Obligados*.
- a) Personas físicas o morales de carácter privado
- b) Excepciones

Artículo 3. *Definiciones*
Artículo 4. *Límites a los derechos y principios*
Artículo 5. *Supletoriedad*

CAPÍTULO II.
De los Principios de Protección de Datos Personales

Artículo 6. *Principios*
Artículo 7. *Licitud*
- a. Expectativa razonable de privacidad

Artículo 8. *Consentimiento*
- a. Quién lo otorga
- b. Tipos de consentimiento
- c. Datos financieros o patrimoniales
- d. Revocación del consentimiento

Artículo 9. *Consentimiento. Datos Sensibles*
- a. ¿Se pueden crear bases de datos con datos personales sensibles?

Artículo 10. *Casos en que no se requiere el consentimiento*
Artículo 11. *Calidad*.
- a. Pertinencia
- b. Corrección
- c. Actualización
- d. Finalidad
- e. Derecho al olvido

Artículo 12. *Finalidad de los datos previstos en el aviso de privacidad*
Artículo 13. *Tratamiento de datos* de acuerdo a su finalidad previstos en el aviso de privacidad.
- a. Datos sensibles
- b. Limites en los periodos de tratamiento

Artículo 14. *Obligaciones del responsable*
- a. Cumplimiento de los principios
- b. Adopción de medidas para su aplicación
- c. Garantizar el respeto al aviso de privacidad

Artículo 15. *Información*

[167] Sin reglamentar.

CAPÍTULO III
De los Derechos de los Titulares de Datos Personales

CAPÍTULO IV
Del ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición

Artículo 45. *Procedimiento*[168]
- a. Instancia de parte
- b. Término para interponerlo y pruebas
- c. Notificación al responsable y traslado
- d. Término para contestar y ofrecer pruebas
- e. Desahogo de pruebas
- f. Alegatos
- g. Resolución

Artículo 46. *Solicitud de protección de datos personales*
- a. Requisitos

Artículo 47. *Término para resolver sobre el procedimiento de Protección del Derecho*

Artículo 48. *Resolución favorable*
- a. Término para cumplimentarla por el responsable
- b. Obligaciones del responsable

Artículo 49. *Prevención al titular del dato*
- a. Subsanar omisiones
- b. Omisión de desahogo
- c. Interrupción del plazo

Artículo 50. *Suplencia de la queja*

Artículo 51. *Resolución*
- a. Tipos
  - i. Sobreseer
  - ii. Desechar
  - iii. Confirmar
  - iv. Modificar
  - v. Revocar

Artículo. 52. *Causas de improcedencia*

Artículo 53. *Causas de sobreseimiento*

Artículo 54. *Conciliación entre el responsable y el titular*

Artículo 55. *Falta de respuesta a una solicitud en ejercicio de los derechos ARCO*
- a. Acreditación de respuesta por parte del responsable
- b. Resolución del Instituto
- c. Cumplimiento de la Resolución

Artículo 56. *Juicio de Nulidad*
- a. Tribunal Federal de Justicia Fiscal y Administrativa
- b. Contra resoluciones del Instituto

Artículo 57. *Difusión de las resoluciones del Instituto*

Artículo 58. *Incumplimiento de la ley por el Responsable del Instituto*
- a. Indemnización al titular

CAPÍTULO VIII
Del Procedimiento de Verificación

Artículo 59. *Verificación del cumplimiento de la ley por el Instituto*
- a. Oficio
- b. A petición de parte

Artículo 60. *Acceso a la Información y datos por parte del Instituto en el procedimiento de verificación*

[168] La presente Ley aun no cuenta con Reglamento, pues de acuerdo a los dispuesto por el artículo Segundo Transitorio, el Ejecutivo Federal expedirá el Reglamento dentro del año siguiente a la entrada en vigor de la Ley, motivo por el cual no se encuentra reglamentado el procedimiento.

CAPÍTULO VIII
Del Procedimiento de Verificación

Artículo 61. *Incumplimiento de los principios o de la ley*
Artículo 62. *Inicio del Procedimiento*
- a. Notificación
- b. Contestación y rendición de pruebas
- c. Desahogo
- d. Alegatos
- e. Resolución

CAPITULO X
De las Infracciones

Artículo 63. *Conductas que constituyen infracciones a la ley*
Artículo 64. *Sanciones*
- a. Apercibimiento
- b. Multas

Artículo 65. *Fundamentación y motivación de las resoluciones del Instituto*
Artículo 66. *Responsabilidad civil o penal*

CAPÍTULO XI
De los Delitos en materia del tratamiento indebido de Datos Personales

Artículo 67. *Pena privativa de libertad*
- a. 3 meses a 3 años de prisión

Artículo 68. *Pena privativa de libertad*
- a. 6 meses a 5 años de prisión

Artículo 69. *Duplicidad de pena tratándose de datos sensibles*

TRANSITORIOS

PRIMERO. Entrada en vigencia.
SEGUNDO. Expedición del Reglamento
TERCERO. Designación del responsable, expedición de Aviso de privacidad y término para hacerlo
CUARTO. Término para comenzar a ejercer los derechos ARCO
QUINTO. Abrogación y Derogación de disposiciones contrarias a la ley y locales sobre la materia.
SEXTO. Referencias al Instituto Federal Acceso a la Información y Protección de Datos Personales.
SÉPTIMO. Presupuesto para el ejercicio de las acciones previstas por la ley de la materia.
OCTAVO. Presupuesto 2011.

BIBLIOGRAFÍA

- ACKERMAN, John M. *Coordinador. Más allá del Acceso a la Información. Transparencia, Rendición de cuentas y Estado de Derecho.* Textos de Stephen Holmes... *et. Al.,* Siglo XXI, México, 2008.
- ALMUZARA ALMAIDA, Cristina, *et. al. "Estudio Práctico sobre la protección de datos de carácter personal".* Lex Nova, 1ª edición, España, 2005.
- ÁLVAREZ LEDESMA, Mario I. *Introducción al Derecho.* Mc Graw-Hill, 2004.
- ARAGÓN REYES, Manuel. *Coordinador. "Temas Básicos de Derecho Constitucional". "Tribunal Constitucional y Derechos Fundamentales".* Tomo III, 1ra. Edición, Madrid, España, 2001.
- BALLESTEROS MOFFA, Luis Angel. *La Privacidad Electrónica. Internet en el centro de protección.* AEPD, Valencia, 2005.
- BASTERRA, Marcela. *Protección de Datos Personales. Ley 25.326 y Dto. 1558/01 Comentados. Derecho Constitucional Provincial. Iberoamérica y México.* IIJUNAM-Ediar, Argentina, 2008.
- CANGA LAREQUI, Jesús. *La Prensa y las Nuevas Tecnologías. Manual de la Redacción Electrónica*. Ediciones Deusto S.A. Madrid, España. 1988.
- CARRANZA TORRES, Luis R. *Hábeas Data. La Protección jurídica de los datos personales*. Alverone Ediciones, Córdova, Argentina, 1996.
- CASTÁN TOBEÑAS, Alonso, Alonso Martínez, C. *Protección de Datos de carácter personal. El consentimiento en entidades financieras*. Madrid, ASNEF, 2002.
- CESARIO, Roberto. *Hábeas Data. Ley 25.326. Doctrina, jurisprudencia y Legislación.* Ed. Universidad, Buenos Aires, 2001.
- *Compilación de normas y criterios en materia de Transparencia, Acceso a la Información Pública y Protección de Datos Personales de la Suprema Corte de Justicia de la Nación*. Quinta edición, SCJN, México, 2009.
- DALLA VÍA, Alberto y Marcela Basterra. *Hábeas Data y otras garantías constitucionales.* Némesis, Argentina, 1999.
- DÁVARA RODRÍGUEZ, Miguel Ángel. *Manual de Derecho Informático*. Aranzandi Editores, Madrid, España, 1997.
- *Diccionario de la Real Academia de la lengua Española,* 22ª edición, 2001.
- ESTADELLA YUSTE, Olga. *"La protección de la intimidad frente a la transmisión internacional de Datos personales*", Centre d´Investigació de la Comunicación, Generalitat de Catalunya, Tecnos, Madrid, 1995

- GILS CARBÓ, Alejandra. *Régimen Legal de las Bases de Datos y Hábeas Dat*. La Ley. Argentina, 2001.
- GÓMEZ GALLARDO, Perla. *IFAI: Avances y Retrocesos. Análisis jurídico de sus resoluciones*. Universidad de Guadalajara, Editorial e, México, 2007.
- GOZAINI, Osvaldo Alfredo. (Coordinador). *La Defensa de la intimidad y los datos personales a través del Hábeas Data. Ley 25.326*. Ediar, Argentina, 2001.
- GOZAINI, Osvaldo Alfredo. *Derecho Procesal Constitucional. Hábeas Data. Protección de datos personales. Ley 25.326 y reglamentación (decreto 1558/20001)*. Rubinzal Culzoni, 2002.
- HASSEMER, WINFREIED y Alfredo, Chirino Sánchez. *El derecho a la autodeterminación informativa y los retos del procesamiento automatizado de datos personales*. Editorial del Puerto, Argentina, 1997.
- HERRÁN ORTIZ, Ana Isabel.*"La violación de la Intimidad en la Protección de Datos Personales*, Dykinson, Madrid, 1999.
- IBAÑEZ, Álvaro. *El libro de internet. Una visita guiada al mundo digital*. 1996.
- JIMENEZ GUZMÁN, Luis. *Regulación en México de la protección a la vida privada en Internet*. (Tesis de Maestría). UNAM, 2007.
- LANDERIA PRADO, Renato Alberto, et. Al. *Colección de Derecho de las Nuevas Tecnologías. Diccionario Jurídico de los Medios de Comunicación*. Reus, España, 2006.
- LESSIG, LAWRENCE. *El Código y otras leyes del ciberespacio*. Traducción de Ernesto Alberola, Taurus, España, 2001.
- MURILLO DE LA CUEVA, Lucas . *La Protección de Datos en la Administración de Justicia*. Cuadernos de Derecho Judicial, número IX, perteneciente a Derecho a la Intimidad y Nuevas Tecnologías, Centro de Documentación Judicial, España, 2004.
- MÁRQUEZ ALURRALDE, Maximiliano. *Régimen Jurídico de las Comunicaciones*. Depalma. Buenos Aires, Argentina, 1986.
- NAVARRO SOLANO, Sonia y Carlos G. Gregorio. *Coordinadores. Internet y sistema judicial en América Latina*. Ad Hoc, Buenos Aires, 2004.
- PECES-BARBA MARTÍNEZ, Gregorio, *Derecho y Derechos Fundamentales*, Centro de Estudios Constitucionales, Madrid, 1993.
- PÉREZ LUÑO, Enrique. *Ensayos de Informática Jurídica*. Distribuciones Fontamara, México, 1996.
    - *El derecho a la Intimidad en Constitución y Derechos Fundamentales*. Centro de Estudios Políticos y Constitucionales, España, 2004.
- PHILIP JONES, John. *Cuando la publicidad si funciona. Nuevas pruebas de que anunciar dispara sus ventas*. Grupo Editorial Norma, Traducción de Manuel Lorenzo Villegas, Colombia, 1997

- PIERINI, et.al. *Hábeas Data. Derecho a la Intimidad.* Editorial Universidad, Argentina, 2002.

- PIZARRO, Ramón Daniel. *Responsabilidad civil de los medios masivos de comunicación*. 2ª edición, colección Responsabilidad civil vol. 8. Ed. Hammurabi S. de R.L. Argentina, 1999.
- R. PUCCINELLI, Oscar. *"Protección de Datos de carácter personal",* Astrea, Buenos Aires, 2004.
- REBOLLO DELGADO, Lucrecio. *El derecho a la fundamental a la intimidad.* Dykinson, España, 2000.
- RUIZ MIGUEL, Carlos. *La configuración constitucional del derecho a la intimidad*. Tecnos, 1995.
    - *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*. Civitas, 1994.
- S. FAYT, Carlos. *La Omnipresencia de la Prensa. Su juicio de Realidad en la jurisprudencia Argentina y Norteamericana*. La Ley, Argentina, 1994
- SALAZAR UGARTE, Pedro. *Coordinador. El derecho de acceso a la información en la Constitución Mexicana: razones, significados y consecuencias*. UNAM/IFAI, México, 2008.
- SCHWABE, Jürgen. *Jurisprudencia del Tribunal Constitucional Federal Alemán. Extractos de las sentencias más relevantes*. Sentencia BVerfGE 65, [Censo de Población]. Ed. Konrad Adenauer Stiftung, Alemania, 2009.
- SIBILIA, Paula. *La intimidad como espectáculo.* Fondo de Cultura Económica, Argentina, 2008.
- SIDOU, Othon. J.M. *Las nuevas fronteras del derecho procesal constitucional brasileño: mandamientos de ejecución y hábeas data. Colombia, 1992.*
- SILVERMAN, Mónica Ana. *Comunica Comunicador. Desafíos y tendencias e la publicidad en el fin de siglo*. Ed. Belgrano, Argentina, 1996.
- TÉLLEZ VALDÉS, Julio. *Derecho Informático.* Mc Grw Hill, 3ª edición, México, 2004.
- VILLANUEVA, Ernesto. *Coordinador. Derecho de la información. Culturas y Sistemas jurídicos comparados*. UNAM, México 2007.
- WARREN AND BRANDIS. *The right to privacy*. Trad. a cargo de Benigno Pendás y Pilar Baselga, Civitas, España, 1995.

LEGISLACIONES

NACIONALES

- Código Civil Federal
- Código de Comercio
- Código Federal de Instituciones y Procedimientos Electorales
- Código Federal de Procedimientos Civiles
- Código Federal de Procedimientos Penales
- Código Penal Federal, Ediciones
- Compilación Jurídica de los otros sujetos obligados por la Ley Federal de Transparencia y Acceso a la información Pública Gubernamental.
- Ley de Protección de Datos Personales del Estado de Colima
- Ley de Protección de Datos Personales del Estado de Oaxaca
- Ley de Protección de Datos Personales para el Distrito Federal
- Ley de Protección de Datos Personales para el estado y los Municipios de Guanajuato
- Ley Federal de Protección al Consumidor
- Ley Federal de Protección de Datos Personales en Posesión de Particulares.
- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
- Ley General de Población
- Ley General de Salud
- Lineamientos de protección de datos personales.
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares.
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento y trámite de las solicitudes de acceso a la información gubernamental que formulen los particulares, así como en su resolución y notificación, y la entrega de la información en su caso, con exclusión de las solicitudes de acceso a datos personales y su corrección.
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de acceso a datos personales que formulen los particulares, con exclusión de las solicitudes de corrección de dichos datos.
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal para notificar al Instituto el listado de sus sistemas de datos personales.
- Reglamento de Acceso a la Información Pública del Municipio de Gómez Palacio Durango
- Reglamento de Acceso a la Información Pública del Municipio de San Felipe
- Reglamento de Acceso a la Información Pública Gubernamental del Municipio de San Pedro Garza
- Reglamento de Acceso a la Información Pública para el Municipio de Victoria
- Reglamento de Derecho de Acceso a la Información Pública del Municipio de Monterrey

- Reglamento de la Coordinación de Enlace de Acceso a la Información Pública del Municipio de Culiacán
- Reglamento de la Ley de Acceso a la Información Pública del Estado de Sinaloa para el Municipio de Cosalá
- Reglamento de la Ley de Acceso a la Información Pública del Estado de Sinaloa para el Municipio de Rosario
- Reglamento de la Ley de Acceso a la Información Pública del Estado de Sinaloa para el Municipio de Escuinapa
- Reglamento de la Ley de Acceso a la Información Pública del Estado de Sinaloa para el Municipio de Mazatlán
- Reglamento de la Ley de Acceso a la Información Pública del Estado de Sinaloa para el Municipio de Mocorito
- Reglamento de la Unidad de Acceso a la Información Pública del Municipio de Celaya
- Reglamento de Transparencia y Acceso a la Información del Municipio de Piedras Negras
- Reglamento de Transparencia y Acceso a la Información Pública del Municipio de Torreón
- Reglamento de Transparencia y Acceso a la Información Pública del Gobierno Municipal de Metepec
- Reglamento de Transparencia y Acceso a la Información Pública del Municipio de Guadalajara
- Reglamento de Transparencia y Acceso a la Información Pública del Municipio de Allende
- Reglamento de Transparencia y Acceso a la Información Pública para el Municipio de Durango *(Capítulo IV. De la clasificación de la Información Pública*
- Reglamento de Transparencia y Derecho a la Información del Municipio de Ramos Arizpe
- Reglamento de Transparencia y Derecho a la Información del Municipio de Zapotlán el Grande
- Reglamento Municipal de Transparencia y Acceso a la Información Pública de Tlalnepantla de Baz
- Semanario Judicial de la Federación y su Gaceta. Poder Judicial de la Federación. 2009.

INTERNACIONALES

- Ley 15/99 Española de Protección de Datos Personales
- Ley 25.326 Hábeas Data
- Ley 25/1990, de 20 de diciembre, del Medicamento.
- Ley 26/1984, de 19 de julio, general para la defensa de los Consumidores y Usuarios.
- Ley 30/1992 del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común,
- Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de

comercio electrónico.

- Ley 45/2003, de 21 de noviembre, por la que se modifica la Ley 35/1988, de 22 de noviembre, sobre Técnicas de Reproducción Asistida.
- Ley 50/1980, de 8 de octubre, de Contrato de Seguro.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.
- Ley 9/1968, de 5 de abril, reguladora de los Secretos Oficiales.
- Ley 12/1989, de 9 de mayo de la Función Estadística Pública.
- Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.
- Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.
- Ley Orgánica 10/2007, de 8 de octubre, reguladora de la base de datos policial sobre identificadores obtenidos a partir del ADN.
- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.

CONVENIOS Y TRATADOS INTERNACIONALES

- Carta de Derechos Fundamentales de la Unión Europea
- Convención Americana sobre Derechos Humanos
- Convenio 108 del Consejo de Europa de 1981, para la Protección de Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal
- Convenio Europeo sobre Televisión Transfronteriza de Estrasburgo de 5 de mayo de 1989
- Convenio para la Protección de los Derechos y Libertades Fundamentales;
- Declaración Universal de los Derechos del Hombre
- Directiva 2000/31/CE, del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos de los servicios de la sociedad de la información,
- Directiva 95/46 de la Comunidad Europea sobre Protección de Personas Físicas en lo que respecta al Tratamiento de Datos de Carácter Personal y Libre Circulación
- Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores.
- Pacto Internacional de los Derechos Civiles y Políticos

CONSTITUCIONES

- Constitución de la Nación Argentina
- Constitución de la República Federal de Brasil
- Constitución Española
- Constitución Política de Colombia
- Constitución Política de los Estados Unidos Mexicanos
- Constitución Política del Perú

DECRETOS

- Decreto 1558/01 que reglamenta la Ley 25.326 de Hábeas Data
- Decreto 1892/02, que designa y pone en funciones al titular del órgano de control de la Dirección Nacional de Protección de Datos Personales en Argentina.
- DECRETO por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Diario Oficial de la Federación, 1 de junio de 2009.
- Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de entes Particulares y se reforman los artículos 3, fracciones II y VII, y 33, así como la denominación del Capítulo II, del Titulo Segundo, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. 5 de julio de 2010.

SENTENCIAS

- Amparo en revisión 191/2008. Grupo Senda Autotransporte S.A. de C.V. 7 de mayo de 2008. *Semanario Judicial de la Federación y su Gaceta,* Novena Época, Tomo XXVII, julio de 2008, Segunda Sala, p. 549, Tesis, 2ª XCIX/2008, IUS: 169167.
- Amparo en revisión 50/2008. Rosario Liévana León. 12 de marzo de 2008. *Semanario Judicial de la Federación y su Gaceta,* Novena Época, Tomo XXVII, abril de 2008, Segunda Sala, p. 733, Tesis, 2ª XLIII/2008, IUS: 169772.
- Corte Federal Argentina. Sentencia de la Sala IV, en autos "Farrel Desmond, Agustín c/BCRA y otros, s/amparo", 5 de septiembre de 1995, Jurisprudencia, 1995-IV-350.
- Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Sentencia de la Sala de lo Contencioso Administrativo de la Audiencia Nacional de España, de 9 de marzo de 2001.
- Sentencia de la Sección Novena de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 5 de noviembre de 1998.
- Sentencia de la Sección Octava de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 18 de octubre de 2000.
- Sentencia de la Sección Octava de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 26 de mayo de 1999,
- Sentencia de la Sección Octava de la Sala de lo Contencioso Administrativo del Tribunal Superior de Justicia de Madrid, de 9 de febrero de 2000
- Suárez Mason s/homicidio y Privación Ilegal de la Libertad. Fallos, 319:71. CSJN Argentina.

REVISTAS

- DE MIGUEL Asensio, Pedro Alberto. *La Protección de Datos Personales a la luz de la reciente jurisprudencia del TJCE.* Revista de la Facultad de Derecho de la Universidad de Granada, 3ª época, número 7, 2004.

    - *El derecho a la protección de los datos personales en la carta de derechos fundamentales de la Unión Europea*. Revista de Derecho Comunitario Europeo, Año 7, número 14, enero-abril, 2003.

- FREIXES Montes, Jordi. *Libertad de Expresión y Publicidad Comercial en los Estados Unidos de América: Una aproximación a la reciente jurisprudencia del Tribunal Supremo* Comunicación y Pluralismo. Actas del Congreso Internacional. España, 1994.

- RUIZ MIGUEL, Carlos. *En torno a la protección de los datos personales automatizados*. Revista de Estudios Político (Nueva Época), No. 84, abril-junio, 1994.

- Corte Suprema de Justicia de la Nación, *"Hábeas Data"*, Revista de Derecho Procesal, No. 5, Sección Jurisprudencia Temática, Argentina, agosto-septiembre de 1999.

- Revista alemana Deutschland, No. 19 10/93. Ed. Societäs Verlang y la Oficina de Prensa e Información del Gobierno Federal, Boon. 1993.

OTROS

- *Sexto Seminario Nacional e Internacional de Protección de Datos Personales. Éxitos e Innovaciones hacia el bicentenario de la República Argentina.* Buenos Aires, Argentina, 14 de mayo de 2009.

- IV Encuentro Iberoamericano de Protección de Datos Personales. IFAI, México, 2005.

- DÁVARA y Asociados. *Conferencia sostenida en la IV Semana de Transparencia y Acceso a la información Pública*. Instituto Federal de Acceso a la Información, México, 2005.

- Solicitud de Acceso a la Información de fecha 17 de agosto de 2010, presentada por Aldo González Gutiérrez a la Directora de Clasificación y Datos Personales del Instituto Federal de Acceso a la Información, referente a la estructura interna del IFAI para atender sus nuevas obligaciones derivadas de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, así como la posición del IFAI respecto de la Ley y sus nuevas atribuciones. No omitiendo establecer que estas consideraciones no prejuzgan sobre las determinaciones que en su caso el Pleno pudiere adoptar posteriormente.

- Dirección Nacional de Protección de Datos Personales, Sarmiento 1118, 3er piso, Capital Federal, Argentina, 2009

PÁGINAS WEB CONSULTADAS

- http://blogs.clarin.com/oscarschiavetta/2008/3/27/curriculum
- http://es.wikipedia.org/wiki/Programa_esp%C3%ADa
- http://es.wikipedia.org/wiki/Seguridad_en_Internet/
- http://es.wikipedia.org/wiki/Wikipedia:Consultas
- http://gaceta.diputados.gob.mx/Gaceta/59/2005/dic/20051214-VIII.html
- http://gaceta.diputados.gob.mx/Gaceta/59/2006/feb/20060223-I.html#Iniciativas
- http://gaceta.diputados.gob.mx/Gaceta/59/2006/mar/20060322-I.html#Iniciativas
- http://senado.senado.gob.mx/gace2.php?sesion=2006/04/05/1&documento=9
- http://sitiosargentina.com.ar/tv-online/
- http://web.archive.org/web/19990427222839/bbs.seker.es/~alvy/que_es_internet.html
- http://www.csjn.gov.ar/consultaexp/documentos/expedientes/cons_expe.jsp
- http://www.diputados.gob.mx/LeyesBiblio/
- http://www.en.us.ar/php?option=com_conterd/12_1.htm
- http://www.en.us.ar/php?option=com_conterd/12_1.htm
- http://www.en.us.es/araucaria/nro18/ideas18_1.htm
- http://www.ib.edu.ar/bib2004/Finalistas/AlejandroBenitezLlambay.pdf
- http://www.ifai.org.mx/Vinculacion/legisMunicipal
- http://www.informatica-juridica.com/autodeterminacion_informativa.asp
- http://www.jus.gov.ar/dnpdpnew/
- http://www.jus.gov.ar/dnpdpnew/
- http://www.markalliance.com/index.php?parlamento/63
- http://www.radiosonlinefm.com/
- http://www.scribd.com/doc/305468/Definiciones-de-Medios-de-Comunicacion-Social-MCS.
- https://www.agpd.es/portalweb/canaldocumentacion/legislacion/index-ides-idphp.php
- https://www.orkut.com
- www.google.com.ar.
- www.inegi.org.mx/est/contenidos/español/rutinas/ept.asp?t=tinf204&s=est&c=5931