UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES

ARAGÓN.

LICENCIATURA EN DERECHO.

"LA RESTRICCIÓN DETERMINADA DE DATOS PERSONALES EN PODER DE INSTITUCIONES BANCARIAS, Y LA DIFUSIÓN DE LOS DERECHOS AL PÚBLICO USUARIO".

T E S I S.

Q U E P A R A O B T E N E R E L T Í T U L O D E:

L I C E N C I A D O E N D E R E C H O.

P R E S E N T A:

G I O V A N N Y R E Y E S R O D R Í G U E Z.

ASESOR: MAESTRO JOSÉ ANTONIO SOBERANES MENDOZA.

Nezahualcóyotl, Estado de México, febrero 2016

AGRADECIMIENTOS.

A la Universidad Nacional
Autónoma de México,
(Facultad de Estudios Superiores Aragón).

Por abrirme las puertas a un mundo
que no conocía y por todo
lo que me ha brindado,
durante estos años.

A mis Maestros:
En especial al Dr. Arturo Tinajero
Caballero.

Por haberme dedicado
un poco de su valioso tiempo
y su conocimiento.

A mi asesor.

El maestro José Antonio
Soberanes Mendoza
Por su apoyo incondicional
durante la realización de este trabajo
y esas pláticas tan interesantes que
me ha brindado.

A mis padres:

Por haberme dado la vida y
cuidarme durante todo este tiempo.
Espero que estén orgullosos.

A mis abuelos Agustín y María:

Porque por fin pude cumplir lo que
algún día les prometí.
Los quiero Se los digo desde
el fondo de mi corazón.

A mi abuela Esperanza:

Por qué siempre me recordaras
La importancia de ser un hombre
bueno, aun cuando tus ojos ya no
me puedan ver.

Al amor de mi vida mi esposa
Gabriela, a mi bebe por nacer
y a mi orgullo, mi hijo Gabriel:

Por soportar tantas cosas
a mi lado, para mí, nuestra
familia siempre será primero.

A la vida:

No me importa cuánto trates
de vencerme te adelanto que nunca podrás.

Y al más importante
de todos a Dios:

Por ser el único amigo que
Me escucha cuando estoy
solo y triste.

“LA RESTRICCIÓN DETERMINADA DE DATOS PERSONALES EN PODER DE INSTITUCIONES BANCARIAS Y LA DIFUSIÓN DE LOS DERECHOS AL PÙBLICO USUARIO”.

Índice .Pág.

Capítulo 1.

Antecedentes de los derechos a la protección de datos personales en México y el mundo y los derechos “ARCO”.

Capítulo 2.

Marco legal.

Capítulo 3.

El manejo de información en poder de instituciones bancarias, las formas de obtención de datos personales cedidos a agencias de cobranza o recabados a través de instituciones como el 040 y el desconocimiento de los derechos “ARCO” como defensa.

Capítulo 4.

“La restricción determinada de datos personales en poder de instituciones bancarias y la difusión de los derechos al público usuario”.

I.- Introducción.

Es cierto que los avances tecnológicos, generalmente repercuten de forma positiva y constante en la calidad de vida del ser humano, por lo que es ingenuo desconocer el hecho de que con ellos nacen a la vida cotidiana nuevos conflictos, interrogantes o situaciones a los que el derecho, en su objetivo constante por regular la convivencia social del ser humano, debe dar respuesta.

En la actualidad la tecnología no puede permanecer ajena al derecho ni evidentemente a la Constitución, pues por más que se quieran evitar la velocidad con la que ocurren estas violaciones tecnológicas amenaza, con hacer obsoleto cualquier esfuerzo por regular su impacto y sobre todo el derecho a la vida privada.

La probabilidad de que se susciten abusos de esta índole, aumenta hoy como consecuencia de la llamada “sociedad de la información”, la expansión global, las redes sociales y de información hacen cada vez más frecuente, los casos de robo de identidad, transgresiones constantes, e ilícitos relacionados al mal uso de datos personales de los particulares.

El indiscriminado tráfico de información y perfiles que hacen identificables a las personas en sus patrones tanto de consumo, ahorro, inclinaciones y preferencias, ha propiciado que los medios de protección tradicionales sean insuficientes en la actualidad, en países como el nuestro ya que dichos medios de control adolecen de fuerza impositiva, ante los ojos de quienes comenten dichas violaciones.

En países que suelen estar preocupados por esta situación, se ha decidido otorgar un mayor grado de importancia a la esfera de lo íntimo, a su protección y resguardo, pues por lo general suelen tener un pasado cultural e histórico marcado por experiencias de invasión en la vida privada de las personas.

Sin embargo da la impresión de que en la actualidad instituciones como los bancos entre otras, que prestan servicios relacionados con el manejo de valores, efectivo y productos relacionados con créditos hacia el público consumidor, están exentos de dichos ordenamientos ya que no obedecen a un estatuto interno o código de ética, que se presentan ante quien solicita estos servicios, acompañado de un aviso de privacidad.

Resulta ilógico pensar que estas instituciones no obedecen lo que sus fines establecen en sus propios estatutos o avisos, pero es verdad, pues esto ha causado un desorden constante y molestia en los particulares que proporcionaron estos datos o peor aún, en aquellos casos en que los datos personales no fueron cedidos con autorización de titular, situación que incluso protege a estas instituciones en el artículo 10 de la LFDPPP.

Suena raro creer que en estos tiempos, la practica indiscriminada de tráfico de datos personales entre instituciones bancarias y agencias de cobranza que actúan como intermediarios, para el cobro telefónico de cuentas bancarias, no tiene una sanción o regulación que controle esta costumbre inapropiada, pues haciendo una comparación con otras naciones, esta práctica ya se ha visto erradicada, casi totalmente en otros países tal es el caso de EUA.

La cesión constante de bases personales sin consentimiento alguno del titular, y la duplicidad de los mismos, ha traído como consecuencia una práctica cotidiana, en la cual los bancos obtienen un beneficio económico, a cualquier costo, sin importar que se violente la esfera jurídica de aquellos que confiaron estos datos a su cuidado, violando el secreto bancario existente entre el titular de la cuenta y la institución, propiciando que los datos lleguen a terceros que les dan mal uso.

Aunado a todo esto, la publicidad por parte de la autoridades de los derechos oponibles a este tipo de abusos, es poca y ha provocado un desconocimiento total que incluso los abogados, desconocen muchas veces el significado de que es un

derecho “ARCO”, lo cual conlleva que hasta en nuestra propia profesión estos derechos sean inobservables ante los ojos de la ley, los particulares, permitiendo más abuso por parte de dichas instituciones. Se podría llegar a pensar que existe una clase de proteccionismo, hacia las instituciones bancarias para permitirles realizar dichas prácticas.

Por lo tanto, este trabajo tiene como finalidad, señalar la conveniencia de restringir a las instituciones bancarias el uso de los datos personales, para fines distintos a los de investigación, susceptibilidad o riesgo que representa una persona, al ser sujeto de crédito.

Cuando la utilización de dichos datos conlleve fines de cobranza y se pretenda ceder a instituciones dedicadas a la cobranza telefónica, el almacenamiento no autorizado de datos, información personal de particulares, ocasionando molestias en la esfera de lo íntimo a terceros, y de este acto derivé, afectación, en su domicilio, empleo, deberá traducirse en un acto de molestia, por la presión, amenazas, intimidaciones, que se presentan de manera cotidiana sin que estas importen sanción alguna.

Garantizar que la autoridad, resarza de forma eficaz el daño provocado de manera ilegal y que de esta forma se dé certeza jurídica a los particulares, ante dichas instituciones, debe de ser la verdadera finalidad de los derechos “ARCO”, para que sean respetados y oponibles de manera eficaz, ante instituciones bancarias y de cobranza, y obligarlos a que obedezcan un verdadero procedimiento judicial regulatorio y sancionador.

Por otra parte generar la inclusión de instituciones telefónicas como 040, al padrón del “INAI”, puede evitar la propagación inapropiada de datos personales en manos de particulares que no tengan, relación o parentesco alguno con el titular, procurando que las multas a los bancos por el mal uso de información o propagación indebida de la misma, sean en cierto modo, para que los derechos

“ARCO”, sean mayormente observados ante los ojos de la sociedad, creando una cultura y protección más adecuada de los datos personales en México.

En tal virtud el presente trabajo consta de cuatro capítulos, distribuidos de la siguiente manera:

El capítulo primero “Antecedentes de los derechos a la protección de datos personales en México el mundo y los derechos “ARCO”, se señala cronológicamente las distintas instituciones que han surgido en etapas históricas en México y el mundo y posteriormente en nuestro país, hasta llegar a los derechos “ARCO”, que serán la parte medular en nuestra investigación.

En el capítulo segundo denominado “marco legal” se presenta la legislación que de manera directa o indirecta influye en los derechos de acceso a la información, los derechos “ARCO” así como las instituciones que tengan relación con ellos y a su normatividad.

El capítulo tercero denominado “El manejo de información en poder de instituciones bancarias, las formas de obtención de datos personales cedidos a agencias de cobranza o recabados a través de instituciones como el 040 y el desconocimiento de los derechos “ARCO” como defensa”. Nos presenta una leve remembranza del cómo estas agencias obtienen la información personal de bases de datos alternas y números de servicio privados como el 040, sin autorización alguna de los titulares de dichos datos y sin seguir los lineamientos establecidos por instituciones como el INAI, CONDUSEF y leyes reglamentarias propiciando abusos en el manejo permitido para dicha información, su importancia y los efectos de los derechos “ARCO” frente estas instituciones.

El capítulo cuarto “La restricción determinada de datos personales en poder de instituciones bancarias y la difusión de los derechos al público usuario”, nos menciona la conveniencia que tiene el limitarle la utilización de datos personales a

las instituciones bancarias y agencias de cobranza evitando la propagación innecesaria de estos y las molestias constantes que se ocasionan a terceras personas ajenas a la relación entre el deudor del crédito y la institución bancaria, evitando así que dichas instituciones obtengan datos personales de fuentes aledañas como el 040, que de formar parte del (INAI) bien podría ser una forma más eficaz de dar acceso a la información y localización de datos personales de los particulares que puedan comprobar algún parentesco, relación laboral o de servicio, mediante candados de seguridad que acrediten ese parentesco o relación.

Dar publicidad a derechos como los “ARCO” provocará que las personas estén conscientes, de que pueden defenderse, de abusos de estas instituciones y que existan mecanismos para garantizar el respeto de sus datos, todo esto derivado del análisis de diversas obras y de la legislación existente, en las diferentes épocas de nuestro país y el mundo, lo que provocaría que instituciones como él “INAI” tomarán enserió está problemática e impusieran mayores sanciones a dichas instituciones regulando, modificando o erradicando prácticas como la cobranza telefónica por considerarse una molestia restringiendo así la utilización de los datos personales de los particulares y pérdidas monetarias constantes a los bancos, derivadas de las multas, haciendo esta práctica no rentable.

GLOSARIO.

Aviso de Privacidad: Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales.

Bases de datos: El conjunto ordenado de datos personales referentes a una persona identificada o identificable**.**

Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabadas, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponde.

Consentimiento: Manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

Datos personales: Cualquier información concerniente a una persona física identificada o identificable

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 futura, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual.

Días: Días hábiles.

Disociación: El procedimiento mediante el cual los datos personales no pueden asociarse al titular ni permitir, por su estructura, contenido o grado de desagregación, la identificación del mismo.

Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

Fuente de acceso público: Aquellas bases de datos cuya consulta puede ser realizada por cualquier persona, sin más requisito que, en su caso, el pago de una contraprestación, de conformidad con lo señalado por el Reglamento de esta Ley.

Instituto: Instituto Federal de Acceso a la Información y Protección de Datos, a que hace referencia la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

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

Reglamento: El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

Secretaría: Secretaría de Economía.

Tercero: La persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos.

Titular: La persona física a quien corresponden los datos personales.

Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Transferencia: Toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento.

Capítulo 1.
Antecedentes de los derechos a la protección de datos personales en México y el mundo y los derechos "ARCO".

1.1.-Antecedentes históricos.

A partir del siglo XVIII los derechos humanos al estar presentes y con su reconocimiento en la norma constitucional fueron alcanzando su consolidación con prerrogativas inherentes a todo ser humano.

Esto es, los derechos individuales o bien derechos de primera generación y en particular el reconocimiento de la libertad personal. En este contexto se incorporó el derecho a la intimidad de la persona como una prerrogativa y objeto de tutela, ya no solo en los instrumentos internacionales, sino además en la sede constitucional.

Sin embargo en la época actual este derecho ha provocado una variación considerable. En virtud de que el desarrollo tecnológico ha redimensionado, las relaciones del hombre con sus semejantes, así como su marco de convivencia.

Hoy no podemos negarlo, la información se ha convertido en un símbolo emblemático de la cultura contemporánea. Por ello, el reconocimiento del derecho a la intimidad en sus diversas manifestaciones luego de lograr su consolidación como un derecho fundamental, ha ido alcanzando nuevos matices.

Conceptos como datos personales o "habeas data", son tan ignorados por el ser humano que en ocasiones pasan desapercibidos, tanto que sin darnos cuenta incluso para los abogados, un tema tan simple es desconocido, en otras palabras," no sabemos que es el derecho al acceso a la información".
Es por eso que en este trabajo me he dado a la labor de explicar algunas de las repercusiones que tiene el desconocimiento de dichas normas, siendo más específicos, en el caso de las instituciones bancarias.

Ahora con el tratamiento, la recolección, el almacenamiento de informaciones, que antes solo podía formar parte de la vida íntima de cada ser humano o bien, eran conocidas por un mínimo sector ha provocado, que una variación paulatina rompiera con su entorno y estructura.

Esto quiere decir que la recolección de los datos personales de toda persona se han convertido en una práctica habitual de control y almacenamiento por parte de los sectores tanto públicos como privados, y no solo porque estos datos sean un elemento esencial que integra la condición necesaria para prevenir el arraigo de sistemas autoritarios, si no más por el simple hecho de que es importante que la sociedad y no solo algunos grupos, conozcan del derecho al acceso a la información, ya que permite promover la transparencia de las instituciones públicas para fomentar la participación ciudadana, la toma de decisiones y de otro tipo de contextos tanto sociales, jurídicos y culturales.

Es por ello que el derecho a la intimidad ha tenido que ir modificando su ámbito de protección, donde además de la facultad del individuo de rechazar invasiones a su ámbito privado, ahora busca el reconocimiento de un derecho de control y acceso de sus informaciones, relativas a su persona.

Por tal motivo, el uso y control sobre los datos concernientes a cada persona, debe serle reconocido ya no solo como una mera prerrogativa, sino además como un derecho fundamental, protegido y garantizado por mecanismos de protección idóneos, de este derecho o protección de datos personales con carácter fundamental, derivado del derecho a la intimidad.

En el ámbito europeo se han preocupado por conocer y garantizar una protección de datos personales a sus ciudadanos, en donde toda aquella información relativa a su persona queda libre de intromisiones, salvo consentimiento del interesado.

En otras latitudes por ejemplo en algunos países latinoamericanos, han sido objeto fundamental de estudio como un derecho fundamental, caso particular de México, que reconoce este tipo de derecho fundamental. Cabe mencionar que la protección de los datos personales es un tema nuevo en nuestro país.

Con fecha 26 de abril del 2006, el Comité de Ministros del Consejo de Europa, resolvió declarar el 28 de enero, como el Día de la protección de los Datos Personales, con motivo del aniversario de la firma del Convenio 108, sobre la protección de los datos personales.

El Convenio 108 para la protección de los datos personales, con respecto al tratamiento automatizado de datos de carácter personal, suscrito en 1981, es el primer instrumento vinculatorio de carácter internacional en materia de protección de datos y es el resultado de la decisión del Consejo de Europa, ante el rápido avance en el campo del procesamiento electrónico de información y la aparición de las primeras bases de datos, usadas por las grandes empresas y los gobiernos estatales, que buscó otorgarle un marco legal con principios y normas concretos, al derecho de acceso a la información, para prevenir la recolección y el tratamiento ilegal, de datos personales.

El Convenio 108 los países firmantes se comprometen a realizar las reformas necesarias en su legislación nacional para implementar los principios contenidos en dicho instrumento; los cuales se refieren, en primer lugar, a que los datos personales deben recolectarse y tratarse con fines legítimos y no para otros propósitos distintos, que no deben conservarse más de lo estrictamente necesario; de acuerdo con el fin para el cual fueron recolectados, que sean verdaderos y que no sean excesivos.

Asimismo prevé que deberá garantizarse la confidencialidad de los datos sensibles y reconoce el derecho de los individuos para tener acceso y en su caso solicitar la corrección de sus datos.

Sin embargó este cambio no fue inmediato pues la protección de la información personal fue desligando el derecho a la intimidad, hasta constituirse expresamente en un derecho fundamental con un contenido independiente de Principios internacionales que configuraron el derecho a la protección de datos personales entre los cuales se encuentran los siguientes:

- Las directrices de la OCDE (1980).
- El Convenio 108 (1981).
- La Resolución 45/95 de la ONU (1990).
- La Directiva 95/46/CE(1995).
- El Marco de Privacidad de APEC (1999).
- La Carta de Derechos Fundamentales de la Unión Europa (2000).
- Las Directrices de Armonización de la Red Iberoamericana (2007).
- Los Estándares internacionales o Resolución de Madrid (2009).
- Derecho a la protección de datos personales (1967) .
- El Consejo de Europa.
- La Comisión Consultiva para estudiar las tecnologías de información y su potencial agresividad a los derechos de la persona" (1968).
- La Resolución 509 de CE: "Derechos Humanos y nuevos logros científicos y técnicos (1981).

En México, desde el año 2000, se han promovido diversos proyectos legislativos en torno a la protección de datos personales en el Congreso de la Unión, sin que ninguno de ellos fructificara, dada la ausencia de una disposición constitucional que les diera sustento.

Si bien la reciente reforma constitucional en 2007 al artículo 6º, establece en sus fracciones II y III que los datos personales y la información relativa a la vida privada será protegida, así como el derecho de acceder y corregir sus datos que obren en archivos públicos, "arco", el legislador quiso establecer límites al ejercicio del derecho de acceso a la información pública en los tres órdenes de gobierno, federal, estatal y municipal, pero no creó un derecho fundamental e independiente.

La aprobación en 2009 de las reformas a los artículos 16 y 73 constitucionales, introduce al derecho al acceso a la información o habeas data, al más alto nivel de nuestra Constitución, “el derecho de toda persona a la protección de su información” y faculta al Congreso Federal, a legislar en materia de protección de datos personales en posesión de particulares. [1]

Lo anterior es relevante pues las reformas al artículo 16, delimito al derecho al acceso a la información pública y enmarco que los datos personales, se encuentran en manos tanto de gobiernos, particulares, empresas, organizaciones y profesionistas, cabe recordar que el uso indiscriminado de la tecnología, puede originar que los fines para los que estos son destinados sean distintos de aquellos para lo que fueron recabados, causando afectaciones en las esferas jurídicas, de los titulares de esos datos. [2]

Con la aprobación de estas reformas, el Estado Mexicano dio el primer gran avance, al reconocer el derecho de protección de datos personales, como un derecho fundamental, autónomo, contribuyendo así a mejorar la dignidad humana, garantizar la no injerencia y el uso indiscriminado o excesivo de los datos personales, que circulan a través de las bases de datos de diversas instituciones, tanto públicas como privadas, llamadas tecnologías de la información. [3]

Asimismo, se asentaron las bases para la expedición de una ley en la materia que regulara el tratamiento de datos personales en el sector privado, demanda[4]

---

(1) OP. Cit., seminariodatospersonales.INAI.org.mx/index.php/antecedentes

(2) OP. Cit., marco normativo de protección de datos personales en manos de particulares

(3) ídem,. Ley Federal de protección de datos en Posesión de los particulares

(4) ibídem., reglamento de la ley federal de protección de datos personales en posesión de los particulares

Latente desde el año 2000, y que tuvo por objeto, que este sector observe los principios de protección de datos personales y garantizara esta protección a través de los derechos “ARCO”, como un mecanismo de defensa para los ciudadanos.

Cabe destacar, que el Segundo artículo Transitorio del Decreto, por el cual se adiciona la fracción XXIX-O, al artículo 73 constitucional, de 30 de noviembre de 2006, faculta al Congreso de la Unión a expedir la ley en la materia en un plazo no mayor de 12 meses. En este sentido y siendo estrictos, dicho plazo feneció en abril de 2010. [5]

Sin embargo cabe mencionar que gracias a estos supuestos se expidió una la “Ley Federal de Protección de Datos Personales en Posesión de los Particulares”, que fue un gran avance en el largo camino de una legislación adecuada en la materia, en México.

1.2.-Organizaciones y mecanismos internacionales.

La Protección contra injerencias arbitrarias en la vida privada, familia, domicilio o correspondencia y ataques a la honra y reputación ha traído como consecuencia qué en México se hayan tenido que modificar las leyes con relación a las comunidades internacionales, que para opinión de este autor conllevan, un enorme avance en comparación a nuestro sistema de normas de acceso a la información. En México el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos reconoce el derecho a la intimidad y la esfera íntima de la persona, que puede ser vulnerada en otros aspectos, siendo más específicos "sus datos personales".

(5) Constitución Política de los Estados Unidos Mexicanos

Como mencionamos anteriormente este cambio no fue inmediato, la protección de la información personal tuvo que desligarse antes del derecho a la intimidad, hasta constituirse expresamente en un derecho fundamental, con un contenido independiente así como principios internacionales, que configuraron el derecho a la protección de datos personales, entre los cuales se encuentran:

- Las directrices de la OCDE (1980).
- El Convenio 108 (1981).
- La Resolución 45/95 de la ONU (1990).
- La Directiva 95/46/CE(1995).
- El Marco de Privacidad de APEC (1999).
- La Carta de Derechos Fundamentales de la Unión Europa (2000).
- Las Directrices de Armonización de la Red Iberoamericana (2007).
- Los Estándares internacionales o Resolución de Madrid (2009).
- Derecho a la protección de datos personales1967.
- El Consejo de Europa.
- La Comisión Consultiva para estudiar las tecnologías de información y su potencial agresividad a los derechos de la persona".(1968).
- La Resolución 509 de CE: "Derechos Humanos y nuevos logros científicos y técnicos.(1981).
- Convenio 108 de CE: Protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal.(1995).
- Directiva 95/46/CE sobre protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. Antecedentes Constitucionales Constitución Española 1978.Que a la letra decía art. 18.4: "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"
- .La Constitución del Perú art. 2.6: "Toda persona tiene derecho a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad". [6]

---

(6)http://www.itei.org.mx/v3/micrositios/diplomado02/gdl/adjuntos/derecho_proteccion_datos_personales.pdf 15/07/14, 11:30 am.

- La Constitución de Venezuela, art. 60: "…La ley limitará el uso de la informática".

Ahora bien cómo podemos ver el ámbito internacional se ha configurado un auténtico derecho fundamental, así como la protección de los datos personales, derecho distinto al derecho a la intimidad. Ya que este derecho tiene su propio contenido y mecanismo de protección. [7]

Por otra parte podemos señalar que su limitación, deriva según lo dispuesto por el artículo 13 de la Convención Americana de Derechos Humanos (CADH),de fecha (22 de noviembre de 1969), así como de las interpretaciones que ha hecho la Corte Interamericana de Derechos Humanos, bajo este tenor el derecho al acceso a la información, solo puede limitarse si se da cumplimiento estricto de los requisitos establecidos, en el artículo 13, párrafo 2, de la Convención Americana de Derechos Humanos. [8]

Estas condiciones de estricta legalidad, necesidad, idoneidad y proporcionalidad, finalidad, protección de objetivos legítimos autorizados por la CADH", sin olvidar, además, que de conformidad con las características que hemos señalado antes, la máxima divulgación impone un requisito adicional a observarse, esto es, la verdadera excepcionalidad de las restricciones, que se traduce en el limitado número de excepciones que pueden existir para que la información no sea entregada, estableciendo un plazo razonable para que subsista, a fin de que una vez que ha concluído dicho plazo, la información pueda ser consultada, salvo que subsista efectivamente el riesgo cierto y objetivo que haya justificado el establecimiento de la restricción . [9]

———

(7) Corte IDH, caso Claude Reyes y Otros vs Chile. Fondo, Reparaciones y Costas. Sentencias de 19 de Septiembre de 2006. Serie C No. 151, par. 77 .

(8)Idem., Corte IDH, caso Palamara Iribarne vs Chile. Fondo, Reparaciones y Costas. Sentencias de 22 de noviembre de 2005. Serie C No. 135, parr. 77.

(9) Op. Cit. Este Término forma parte del derecho a la intimidad, que algunos señalan que está incluído en el derecho a la vida privada. Pero independientemente de esa discusión, es un concepto estrictamente vinculado con el derecho de acceso a la información, al derivar del llamado habeas data, que es el derecho que toda persona tiene a acceder a la información sobre si misma , sea que esté en posesión del gobierno o de una entidad privada. El derecho incluye el derecho a modificar, eliminar o corregir la información considerada sensible, errónea, sesgada o discriminatoria y que dichos datos no sean conocidos por otras personas.

Así las limitaciones al derecho de acceso a la información para que se puedan establecer deben partir del hecho de que este derecho tiene como escénica el principio de la máxima divulgación, por lo que las restricciones al acceso a la información deben ser taxativas, la excepción y no la regla, así como contar con plazos que permitan que la información se divulgue y la restricción desaparezca.

Asimismo, deben estar previstas en la ley de manera clara y precisa, lo cual implica que esta sea emitida por el órgano legislativo constitucionalmente dispuesto para ello y que no deje a la discrecionalidad de los funcionarios si se divulga o no la información.

Y como toda restricción a un derecho humano, tal y como fue explicado al analizar la libertad de expresión, deben ser necesarias en una sociedad democrática idóneas para alcanzar el objetivo que buscan, proporcionales al interés que las justifiquen y no desnaturalizar , o hacerlo en la menor medida en el derecho de acceso a la información .

1.3 Antecedentes históricos en México.

Como ya lo Hemos mencionado en el anterior segmento En México, desde el año 2000, se han promovido diversos proyectos legislativos en torno a la protección de datos personales en el Congreso de la Unión, sin que ninguno de ellos fructificara dada la ausencia de una disposición constitucional que les diera sustento.

Fue entonces que derivada de la reforma constitucional, en 2007 al artículo 6º estableció en sus fracciones II y III que los datos personales y la información relativa a la vida privada seria protegida, así como el derecho de acceder y corregir sus datos que obren en archivos públicos, el legislador quiso establecer límites al ejercicio del derecho de acceso a la información pública en los tres órdenes de gobierno (federal, estatal y municipal), pero no creó un derecho fundamental e independiente.

En este tenor la aprobación en 2009 de las reformas a los artículos 16 y 73 constitucionales, se introduce al más alto nivel de nuestra Constitución, el derecho

de toda persona a la protección de su información, faculta al Congreso Federal, a legislar en materia de protección de datos personales en posesión de particulares, que como ya vimos anteriormente delimito el alcance de los derechos de acceso a la información. [10]

Asimismo, se sentaron las bases para la expedición de una ley en la materia que regule el tratamiento de datos personales en el sector privado, demanda latente desde el año 2000, y que tenía por objeto que este sector observe los principios de protección de datos personales y garantice los derechos "ARCO" a los ciudadanos.

Cabe destacar, que el Segundo artículo Transitorio del Decreto por el que se adiciona la fracción XXIX-O al artículo 73 constitucional, constriño al Congreso de la Unión a expedir la ley en la materia en un plazo no mayor de 12 meses. En este sentido y siendo estrictos, dicho plazo feneció en abril de 2010 y dio como origen la Ley Federal de Protección de Datos Personales en Posesión de Particulares.[11]

Por otra parte los avances en las Tecnologías de la información (TI) y sus implicaciones para la vida de las personas dieron origen a un derecho distinto, relacionado con la Protección de los Datos Personales (PDP), en nuestro país que fueron en este orden las siguientes:

---

(10) Op. Cit., Becerra Ramírez, Manuel, "El poder judicial y el derecho internacional de los derechos Humanos. El caso del poeta irreverente", en la ciencia del derecho procesal constitucional. Estudios en homenaje a Héctor Fix Zamudio en sus Cincuenta Años como investigador del Derecho, pp455-471

(11)Op. Cit., Faúndez Ledesma Héctor los limites al Derecho a la libertad de expresión. México, UNAM, instituto de Investigaciones Jurídicas, 2004.

A nivel constitucional

Artículo 6 (DOF 20 de julio de 2007).
Artículo 16 (DOF 1º de junio de 2009).
Artículo 73 (DOF 30 de abril de 2009).

A nivel federal.

La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental LFTAIPG. (DOF 27 de abril de 2010).

LA Ley Federal de Protección De Datos en Posesión de los Particulares (DOF 27 de abril de 2010).

La nueva Ley de Transparencia, Publicada por el Gobierno Federal el 4 de mayo de 2015.

La LFTAIPG reconoce por primera vez que en México la protección de los datos personales, limita a las bases de datos del sector público a nivel federal. Es a la vez, una ley de acceso a la información y una ley de protección de datos personales limitada en su ámbito de aplicación (público federal). [12]

Por otra parte tenemos a La Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), que es un cuerpo normativo aprobado por el Congreso de la Unión el 27 de abril de 2010, mismo que tiene como objetivo regular el derecho a la autodeterminación informativa. Esta Ley fue publicada el 5 de julio del 2010 en el Diario Oficial de la Federación y entró en vigor el día 6 de julio del 2010. Sus disposiciones son aplicables a todas las personas físicas o morales que lleven a cabo el tratamiento de datos personales en el ejercicio de sus actividades, por lo tanto empresas como bancos, aseguradoras, hospitales, escuelas, compañías de telecomunicaciones, asociaciones religiosas, o de profesionistas como abogados, médicos, entre otros, que se encuentran obligados a cumplir con lo que establece esta ley.

___

(12)Op. Cit., Fiss, Owen, La Ironía de la libertad de expresión, Barcelona Gedisa, 1999, pp77.

Por último tenemos a la nueva Ley de Transparencia promulgada hace apenas unos pocos meses, en el presente año 2015, la cual vino a modificar no solo el nombre de la institución reguladora por "INAI", cuyas siglas significa Instituto, Nacional, de Acceso a la Información" y que tiene por objeto velar por la transparencia y garantizar el acceso a la información y su protección, tanto en el ámbito público como privado, como ente autónomo capaz de influir con sus determinaciones, en el accionar de la vida jurídica, ya sea de personas morales o físicas, en cuanto a sus datos personales e información que de ellos se derivé.

1.4 La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG).

Como lo hemos mencionado antes la LFTAIPG, reconoce por primera vez que en México la protección de los datos personales, limita a las bases de datos del sector público a nivel federal. Es a la vez, una ley de acceso a la información y una ley de protección de datos personales limitada en su ámbito de aplicación (público federal), que establece la Actuación del INAI, como autoridad garante. Es decir le da la facultad de emitir sus propias resoluciones sin necesidad de que otra autoridad medie en ellas y su ejecución entre las cuales se encuentra:

1.- Expedición de disposiciones administrativas por ejemplo:

- El caso de los Estados de Colima, Jalisco y Tlaxcala que cuentan con sus propias leyes de protección de datos para el sector público y privado.
- Los Estados de Guanajuato, Coahuila, Oaxaca y el Distrito Federal sólo regulan la protección de datos personales en posesión del sector público.
- Es decir que, La mayoría de las legislaciones estatales contienen un capítulo de protección de datos personales expedición de recomendaciones concretas a los sistemas de datos personales.[13]

Y se desglosan en sus primero artículos que a la letra dice:

“La presente Ley es de orden público. Tiene como finalidad proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, y cualquier otra entidad federal”.

“Artículo 2. Toda la información gubernamental a que se refiere esta Ley es pública y los particulares tendrán acceso a la misma en los términos que ésta señala”.

“Artículo 3. Para los efectos de esta Ley se entenderá por: I. Comités: Los Comités de Información de cada una de las dependencias y entidades mencionados en el Artículo 29 de esta Ley o el titular de las referidas en el Artículo 31”;

II. 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 religiosas o filosóficas, los estados de salud físicos o mentales, las preferencias sexuales, u otras análogas que afecten su intimidad; [13]

III. Documentos: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades o la actividad de los sujetos obligados y sus servidores públicos, sin importar su fuente o fecha de elaboración de los documentos.

*(13)*http://seminariodatospersonales.INAI.org.mx/index.php/antecedentes11DE MAYO DE2015, 11:30 *PM.*

Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico;

IV. Dependencias y entidades: Las señaladas en la Ley Orgánica de la Administración Pública Federal, incluidas la Presidencia de la República, los órganos administrativos desconcentrados, así como la Procuraduría General de la República;

V. Información: La contenida en los documentos que los sujetos obligados generen, obtengan, adquieran, transformen o conserven por cualquier título;

VI. Información reservada: Aquella información que se encuentra temporalmente sujeta a alguna de las excepciones previstas en los Artículos 13 y 14 de esta Ley;

VII. Instituto: El Instituto Federal de Acceso a la Información establecido en el Artículo 33 de esta Ley;

VIII. Ley: La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

IX. Órganos constitucionales autónomos: El Instituto Federal Electoral, la Comisión Nacional de los Derechos Humanos, el Banco de México, las universidades y las demás instituciones de educación superior a las que la ley otorgue autonomía y cualquier otro establecido en la Constitución Política de los Estados Unidos Mexicanos;

X. Reglamento: El Reglamento respecto al Poder Ejecutivo Federal, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

XI. Servidores públicos: Los mencionados en el párrafo primero del Artículo 108 Constitucional y todas aquellas personas que manejen o apliquen recursos públicos federales;

XII. Seguridad nacional: Acciones destinadas a proteger la integridad, estabilidad y permanencia del Estado Mexicano, la gobernabilidad democrática, la defensa exterior y la seguridad interior de la Federación, orientadas al bienestar general de la sociedad que permitan el cumplimiento de los fines del Estado constitucional;

XIII. Sistema de datos personales: El conjunto ordenado de datos personales que estén en posesión de un sujeto obligado;

XIV. Sujetos obligados:

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

b) El Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos; c) El Poder Judicial de la Federación y el Consejo de la Judicatura Federal;

d) Los órganos constitucionales autónomos;

e) Los tribunales administrativos federales, y

f) Cualquier otro órgano federal.

XV. Unidades administrativas: Las que de acuerdo con la normatividad de cada uno de los sujetos obligados tengan la información de conformidad con las facultades que les correspondan".

"Artículo 4. Son objetivos de esta Ley:

I. Proveer lo necesario para que toda persona pueda tener acceso a la información mediante procedimientos sencillos y expeditos;

II. Transparentar la gestión pública mediante la difusión de la información que generan los sujetos obligados;

III. Garantizar la protección de los datos personales en posesión de los sujetos obligados;

IV. Favorecer la rendición de cuentas a los ciudadanos, de manera que puedan valorar el desempeño de los sujetos obligados;

V. Mejorar la organización, clasificación y manejo de los documentos, y

VI. Contribuir a la democratización de la sociedad mexicana y la plena vigencia del Estado de derecho.

"Artículo 5. La presente Ley es de observancia obligatoria para los servidores públicos federales."

Derivado de los artículos anteriores, podemos concluir que todas las demás leyes en la materia derivan esencialmente de esta ley.

1.5.- La Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP).

La Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), es un cuerpo normativo de México, aprobado por el Congreso de la Unión el 27 de abril de 2010, mismo que tiene como objetivo regular el derecho a la autodeterminación informativa. Esta Ley fue publicada el 5 de julio del 2010 en el Diario Oficial de la Federación y entró en vigor el día 6 de julio del 2010. Sus disposiciones son aplicables a todas las personas físicas o morales que lleven a cabo el tratamiento de datos personales en el ejercicio de sus actividades, por lo tanto empresas como bancos, aseguradoras, hospitales, escuelas, compañías de telecomunicaciones, asociaciones religiosas, y profesionistas como abogados, médicos, entre otros, se encuentran obligados a cumplir con lo que establece esta ley.

Un dato personal, de acuerdo al artículo 3 fracciones V, de la Ley antes mencionada es toda aquella información que permita identificar a una persona.

En la actualidad no es raro recibir una llamada telefónica con el fin de ofrecernos servicios, no requeridos o llamadas de extorsionadores, que parecen tener mucha más información de nosotros, de la que recordamos tener en nuestros perfiles de Facebook, entre otras redes sociales, provocando que nuestra información se vuelva publica, al publicarse en una red de acceso público. Cabe mencionar que un principio del habeas data es que si alguna información personal, es publicada de manera abierta y pública en alguna fuente de acceso a la que todas las personas puedan acceder sin restricciones, no podrá vedarse de nueva cuenta el derecho de acceder a ella, es decir si nosotros publicamos un número de cuenta privado, como por ejemplo:

- Una cuenta bancaria.
- Número del seguro social.
- Contraseña.
- Tipo de sangre.
- Preferencias.

Incluso datos sensibles como la fecha de nacimiento y dirección, de manera abierta les estamos dando acceso a otras personas a que puedan acceder cuando ellos quieran a nuestros datos, sin que podamos retirar dicha información si esta es ingresada en una fuente de acceso público.

Es tan importante verificar, lo que publicamos pues podríamos erróneamente proporcionar información privada por accidente, por dar un ejemplo simple en nuestro país en el año 2014, se realizó erróneamente una publicación en internet del padrón completo de pensionados beneficiarios del IMSS, que incluía no solo su nombre completo, so no que también contenía el monto y la clínica en donde deberían cobrar dicha prestación, poniendo en riesgo la integridad de los beneficiarios, tan delicado fue este asunto que el Instituto Federal de Acceso a la Información (IFAI), ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), emitió una resolución en donde sanciono al IMSS, por haber revelado esta información de manera

imprudente en una fuente de acceso público, que como ya hemos mencionado anteriormente si publicamos información privada en una fuente pública, por principios rectores del “habeas data”, no podremos retirar y mucho menos negar el acceso a esta.

O peor aún debido que nuestros datos personales sean susceptibles de ser extraídos de instituciones bancarias, crediticias, o servicios como televisión por cable, telefonía celular o fija, e incluso de instituciones gubernamentales o paraestatales.

Estas extracciones de información pueden darse de dos formas:

- *Externas*. Son ataques dirigidos desde el exterior de las instituciones que vulneran su seguridad y extraen información.

Un ejemplo de esto fue reciente *hackeo* a la base de datos de tarjetas de crédito de PlayStation que afectó a cerca de 100 millones de usuarios cuya información personal pudo ser vulnerada. Y del cual se derivó una fuerte sanción a esta institución, en otros países tal es el caso de EUA, pues ellos si cuenta con un sistema que regulan las violaciones de tipo cibernético y son capaces de castigarlas, caso contrario en nuestro país que adolecen bastante de esto con la llamada policía cibernética.

- *Internas*. Son robos de información realizados por personal propio de las instituciones y típicamente no se pueden rastrear y por lo tanto tampoco encontrar a los responsables.

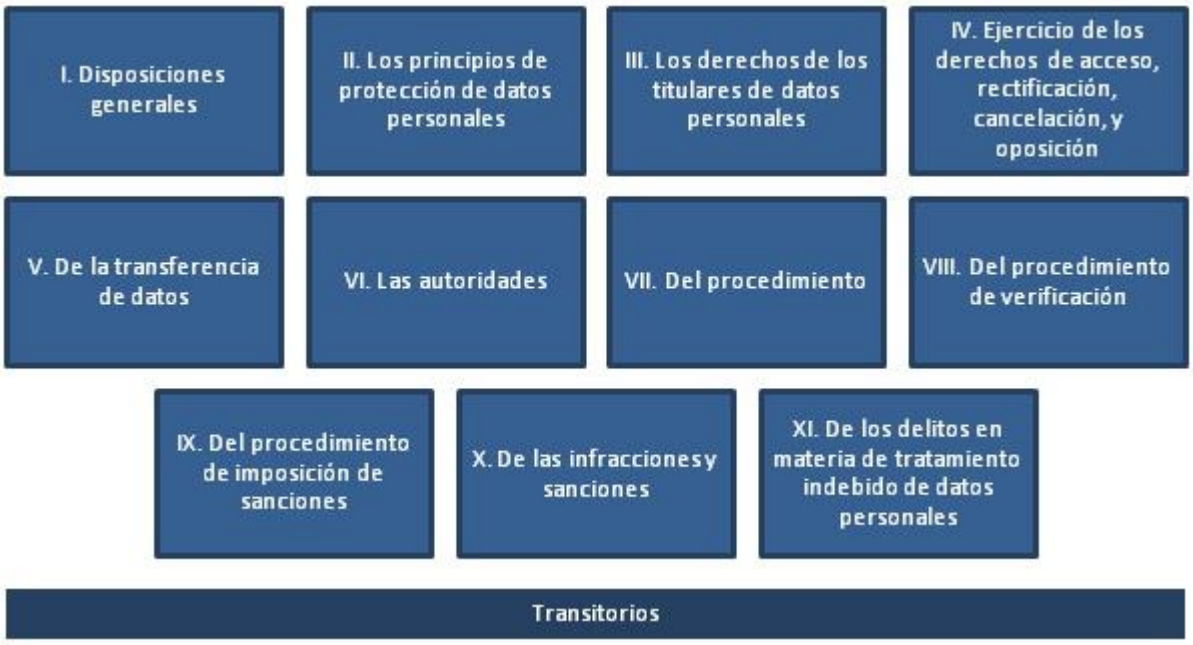
Sea cual fuera la debilidad, las instituciones que proporcionan, información personal a terceras personas deben ser responsables al salvaguardar los datos personales de sus clientes para que solo sean utilizados para los fines autorizados, además de responder por las consecuencias de fallar en este deber.

Por otra parte, tenemos que en el caso de que una misma institución que proporciona varios servicios tenga la información solo dé información personal de

un suscriptor para un servicio específico, aproveche para ofrecerle servicios adicionales que conllevan fines totalmente distintos para los que en un inicio se proporcionó. Es decir, imaginemos un banco que tiene toda nuestra información crediticia y esté por incursionar en el mercado de seguros para automóviles; usa los datos que se le confiaron para hacerse de una cartera de candidatos para el área de seguros haciendo mal uso de la información personal, motivo por el cual tendría que ser sancionado.

Después de un arduo camino y mucha polémica, el 27 de abril de 2010, se aprobó en el Pleno del Senado la Ley Federal de Protección de Datos Personales en Posesión de Particulares, misma que entro en vigor el 5 de julio de 2010, con la finalidad de proteger los datos personales en posesión de los particulares y regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. A decir de expertos es una de las leyes de protección de datos más avanzada del mundo.

La (LFPDPPP) consta de 69 artículos organizados en 11 capítulos, como sigue:



Y está se encuentra estructurada en principios rectores que se definen como:

Principios rectores: aquellos que definen los pilares, en los que se basa la protección de datos personales, los cuales a su vez se componen por:

- Licitud: prohíbe la obtención de datos personales por medios ilícitos, engañosos o fraudulentos.
- Consentimiento: manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los mismos. El consentimiento debe ser tácito, expreso y por escrito.
- Información: Que es aquel principio que menciona, que el titular tiene derecho a conocer quién trata su información personal y qué se hace con ella.
- Calidad: Es aquel principio que señala que los datos personales deben ser pertinentes, correctos y actualizados.
- Finalidad: establece que la obtención y tratamiento de los datos deberá estar relacionada con la finalidad del tratamiento previsto en el aviso de

privacidad – documento que establece lo que se hará con la información del titular y establece los derechos ARCO.

- Lealtad: Es aquel que menciona que se deben respetar una expectativa razonable de privacidad.
- Proporcionalidad: Principio que establece que el responsable sólo debe tratar la mínima cantidad de información necesaria para conseguir la finalidad perseguida.
- Responsabilidad: Establece que el responsable debe velar por el cumplimiento de los principios y rendir cuentas al titular en caso de incumplimiento.

Derivado de lo anterior se puede hablar de principios rectores, que son aquellos que dan origen a los Derechos, que defienden al titular de los datos personales para que pueda ejercer su derecho, a los principios teóricos en los que se basa la ley y que son los denominados derechos “ARCO” cuyas siglas quieren decir que el titular tiene derecho a:

- Acceder a sus datos personales y al aviso de privacidad para conocer qué datos son objeto de tratamiento y con qué objetivo son tratados.
- Rectificar inexactitudes en los datos personales del titular.
- Cancelar sus datos personales, esto obedece al bloqueo de los datos por un periodo en el que el responsable deberá conservarlos bajo su custodia y, cumplido tal periodo, se deberán suprimir.
- Oponerse al tratamiento de los datos personales cuando exista una causa legítima, si este derecho resulta procedente el responsable excluirá los datos del tratamiento.

Estos procedimientos, se dividen en dos tipos:

- El procedimiento de protección de datos.
- Y el procedimiento de verificación.

El primero establece un mecanismo mediante el cual el titular podrá reclamar la protección de los derechos “ARCO” ante el INAI (Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales).

Por otra parte “el procedimiento de verificación”, tiene por objetivo comprobar el cumplimiento de la ley y de la normatividad que se desarrolle por ejemplo:

El reglamento por el cual el INAI tendrá acceso a la información y documentación que considere necesaria y, para que en caso de incumplimiento, la ley preverá sanciones que van desde, una llamada de atención, hasta la imposición de multas entre 100,000 y 320,000 días de salario mínimo vigente en el Distrito Federal, con doble imposición por reincidencia. Además, estas penas y sanciones se duplicarán en los casos relativos a datos personales sensibles y, de acuerdo a la gravedad del delito, podrán existir responsabilidades civiles y penales.

Pero ¿Quién tiene que cumplir con la LFPDPPP y quiénes son los principales actores.

Según lo dispuesto por su texto, la ley es de orden público y de observancia general en toda la república, y 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.
>
> 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 (lucro).Y los principales actores que deberán participar en la implementación de medidas administrativas, técnicas y físicas para proteger la seguridad de los datos, son los siguientes:

Responsable: persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.

Encargado: persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.

Titular: persona física a quien corresponden los datos personales.

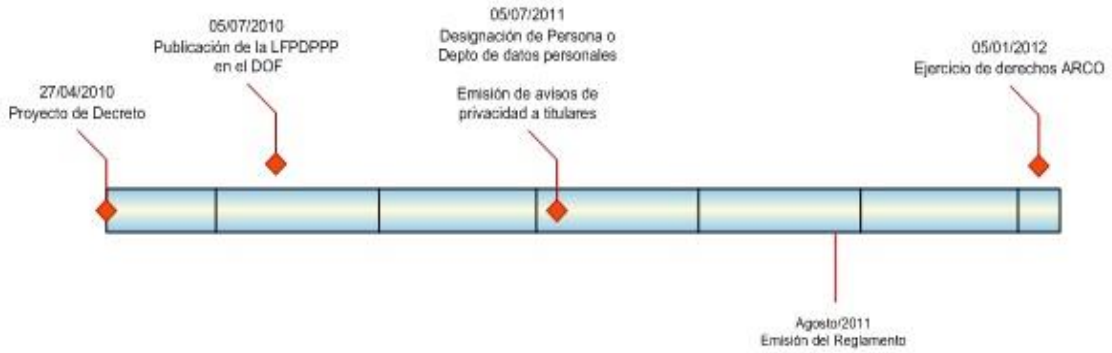
Tercero: persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos.

Por otra parte la Secretaría de Economía, 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 (buenas 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 "INAI", tendrá como función el difundir el conocimiento del derecho a la protección de datos personales, promover su ejercicio y velar por su cumplimiento. Algunas de sus funciones serán:

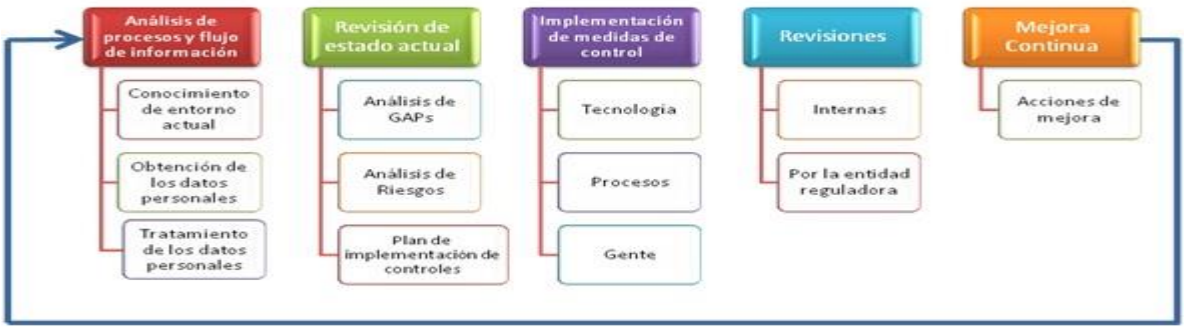
- Vigilar y verificar el cumplimiento de la LFPDPPP.
- Proporcionar apoyo técnico a los responsables que lo soliciten.
- Emitir recomendaciones y normas técnicas para el cumplimiento de la ley.
- Dar capacitación a los sujetos obligados al cumplimiento de la ley.

Ahora, los plazos para el cumplimiento de la LFPDPP se fueron llevando de la siguiente manera, como se muestra en la siguiente figura:



Estrategias, Bases y Términos, para su cumplimiento.

De acuerdo a los requerimientos de la LFPDPPP y con base en el estándar BS10012:2009, por sus siglas en ingles (Data Protection. Specification for a Personal Information Management System), se propuso el siguiente modelo para definir e implementar una estrategia para la protección de datos personales en posesión de particulares, con el objetivo de proporcionar dirección y soporte para el cumplimiento de dicha ley, también denominado, Modelo para la implementación de una estrategia en el cumplimiento de la LFPDPPP y es el siguiente:



El modelo define cinco fases, las cuales se describen a continuación:

Análisis de procesos y flujo de información.

Como primera fase es importante que la empresa realice un análisis y diagnóstico de sus procesos de negocio y cómo estos están siendo operados. La empresa debe identificar si está solicitando información de datos personales a los titulares que no le estén generando algún beneficio ni operativo ni económico, y analizar la factibilidad de dejarlos de recabar y, de esta manera, evitar el uso de recursos para el cumplimiento de la LFPDPPP.

Revisión de estado actual.

En esta fase el objetivo es conocer el grado de cumplimiento y madurez que mantiene la empresa respecto a la LFPDPPP, e identificar desviaciones existentes entre las prácticas de administración y operación actuales, lo cual permitirá identificar los riesgos a los que está expuesta la empresa y, con base en ello, dar prioridad a líneas de acción para la implementación de controles.

Implementación de medidas de control.

Los controles tecnológicos mínimos que se deberán implementar para la protección de datos personales son los siguientes:

Mecanismo seguro para el intercambio de información con terceros.

Mecanismo de retención y eliminación segura de datos personales y datos sensibles.

- Mecanismo de almacenamiento seguro.
- Mecanismo de acceso y autenticación.
- Aseguramiento de bases de datos.
- Mecanismo de prevención de fuga de información.

- Los controles de procesos y políticas mínimas que deberán ser desarrolladas e implementadas son las siguientes:
- Política de protección de datos personales y datos sensibles.

Modelo de responsabilidades que incluya los siguientes actores: responsable, custodio, titular, encargado de seguridad.

- Procedimientos para la obtención de información de datos personales y datos personales sensibles.
- Procedimientos para el tratamiento de información de datos personales.
- Política de retención y eliminación de datos personales y datos personales sensibles.
- Proceso de evaluación formal de riesgos.
- Proceso de control de accesos.
- Proceso de respaldo de datos.
- Proceso de respuesta a incidentes.
- Proceso de investigación forense.
- Proceso de control de cambios.
- Procedimiento de monitoreo.
- Procedimientos de revisión de registros y bitácoras.
- Formatos del aviso de privacidad y del aviso de consentimiento.
- Acuerdos para el intercambio seguro de datos personales y datos sensibles.
- Otros.

En el ámbito de los controles orientados al personal se deberá considerar:

1.-Programa de conciencia de seguridad dirigido a:

- Administradores de red.

- Desarrolladores y analistas.

- Personal involucrado en el manejo de la información de datos

- Capacitación en el entendimiento de la LFPDPPP.[14]

_____

(14) LFPDPPP

Revisiones.

En esta fase se deberán realizar auditorías internas por parte de la empresa a través del departamento de “auditoría” para detectar las áreas de oportunidad en la eficiencia de la implantación de los controles de seguridad y determinar el nivel de cumplimiento con la LFPDPPP, con el objetivo de simular la auditoría por parte de la entidad reguladora (INAI).

Mejora continua.

En esta fase la empresa deberá implementar las acciones correctivas derivadas de las auditorías realizadas. Algunas actividades a contemplar son: dar prioridad a las acciones correctivas y preventivas identificadas, e identificación de los responsables de llevar a cabo las acciones correctivas.[15]

1.6 - Los derechos “ARCO”.

Los derechos “ARCO” son aquellos derechos que toda persona puede ejercer, en relación con el tratamiento de sus datos personales. Cada sigla representa un derecho diferente, por ejemplo:

Acceso: Derecho acceder a la información personal proporcionada, de manera pronta y expedita.

Rectificación: Derecho a corregir datos erróneos o errores, en los datos del titular.

Cancelación: Derecho a pedir la cancelación de datos que perjudiquen o información, que pare un perjuicio al titular de los datos personales, en poder de los particulares.

Oposición: Es el derecho que todo titular de los datos personales, tiene a oponerse al tratamiento de sus datos personales por considerarlo inadecuado o indebido.

---

(15)Carpizo Jorge y Ernesto Villanueva, El derecho a la información. UNAM, 2001, México, pp 71-102

Pero para hablar de los derechos “ARCO”, primero debemos adentrarnos en un punto de suma importancia que no podemos dejar pasar desapercibido, tan importante que influye en la esencia de la existencia de estos derechos y este elemento tan esencial son, los datos personales,

¿Pero que son los datos personales?

Los datos personales son toda aquella información relacionada con el ámbito privado de tu vida, y conforme al tipo de dato de que se trate, se resguardará con diferentes niveles de seguridad, tales como:

Nivel básico de seguridad.

1. De Identificación: Por ejemplo tu nombre, domicilio, número de teléfono particular y celular, correo electrónico, firma, RFC, CURP, cartilla militar, edad, nombres de familiares dependientes y beneficiarios, fotografía, idioma o lengua, entre otros.
2. Laborales: Por ejemplo tus documentos de reclutamiento y selección, de capacitación, puesto, domicilio de trabajo, correo electrónico institucional, referencias laborales y personales, entre otros.

Nivel medio de seguridad.

1. Datos Patrimoniales: Bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos y egresos, cuentas bancarias, seguros, afores, fianzas, entre otros.
2. Datos sobre procedimientos jurisdiccionales o administrativos seguidos en forma de juicio: Información relativa a una persona que se encuentre sujeta a un procedimiento.
3. Datos Académicos: Trayectoria educativa, títulos, cédula profesional, certificados, reconocimientos, entre otros.

4. Tránsito y movimientos migratorios: Información sobre el movimiento de las personas dentro y fuera del país e información migratoria de las personas, entre otros.

Nivel <u>alto</u> de seguridad.

1. Datos Ideológicos y religiosos: Creencia religiosa, ideología, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas, entre otros.
2. Datos de Salud: Estado de salud, historial clínico, alergias, enfermedades, cuestiones de carácter psicológico y/o psiquiátrico, incapacidades médicas, uso de aparatos oftalmológicos, ortopédicos, auditivos, prótesis, entre otros.
3. Características personales: Tipo de sangre, ADN, huella digital, u otros análogos.
4. Características físicas: Tu color de piel, de cabello, de iris, tu, estatura, peso, entre otros.
5. Vida sexual: Preferencia y hábitos sexuales, entre otros.
6. Origen: Étnico y racial.

Estos 6 tipos de datos personales se deben resguardar con un nivel alto de seguridad, ya que abordan temas más sensibles de cada persona, es por ello que se les conoce también como datos sensibles. [16]

Ahora bien una vez abordado el tema de los datos personales, podemos entender mejor el porqué de los derechos "ARCO", y desglosar cada una de sus siglas referentes a cada uno de los derechos que tiene una persona como titular de sus datos personales, los cuales son:

___
(16)http://seminariodatospersonales.INAI.org.mx/index.php/antecedentes14/08/15,19:15

Acceso:

El acceso, es el derecho que tiene todo titular de datos personales, a solicitar a los sujetos responsables, el acceso a su información según obre en el poder de alguna institución privada, siempre y cuando obren en su sistema de datos personales y se encuentre en posesión de los responsables.

Por lo tanto en este tipo de solicitudes, se pedirá que acredite su identidad o bien, la de su representante legal (si se nombra a uno con facultades para ello).

Procedimiento de solicitud.

Presentar una solicitud de información confidencial, (directamente o a través de su representante legal), en términos respetuosos y elegir del formulario electrónico la sección de Solicitud de Información, posterior a ello, la opción de acceso a mis datos personales. Para poder presentar la solicitud de manera verbal o por escrito y debe contener:

- Nombre completo.
- El domicilio o dirección electrónica que autorizas, para recibir la información que requieres y las notificaciones correspondientes.
- La descripción de manera clara y precisa de los datos personales sobre los que buscas ejercer alguno de tus derechos, en este caso, referir que requieres acceder a ellos, y adicionalmente señalar, en su caso, cualquier otro elemento que facilite la localización de la información.

Rectificación:

Es el derecho que tiene el titular de los datos personales, para que se corrijan sus datos personales en las bases de datos de los sujetos obligados, cuando exista un error en ellos, sean inexactos o incompletos. Para ello igualmente se deberá presentar una solicitud de información confidencial (directamente o a través de un representante legal), en términos respetuosos y elegir del formulario electrónico de

la sección que solicita información, la opción de rectificación de mis datos personales, anqué también puede presentar su solicitud de manera verbal o por escrito ante el órgano competente.

La solicitud debe contener, adicionalmente a lo señalado en el punto anterior sobre el acceso a datos personales, las modificaciones a realizarse y aportar la documentación que sustente tu petición.

Cancelación:

Es el derecho que tiene el titular de los datos personales, para que se cancelen los datos personales en las bases de datos de los sujetos obligados, cuando el tratamiento de los mismos no se ajuste a lo dispuesto por la Ley de Transparencia, sus Reglamentos o los Lineamientos respectivos; o cuando se ejercite el derecho de oposición y éste haya resultado procedente.

Para ello igualmente deberá presentar una solicitud de información confidencial (directamente o a través de su representante legal), en términos respetuosos y elegir del formulario electrónico la sección de Solicita Información, la opción de cancelación de mis datos personales y presentarla de manera verbal o por escrito.

La solicitud debe, adicionalmente contener a lo señalado en el punto sobre el acceso a datos personales, la autorización para revocar el consentimiento, otorgado al sujeto obligado.

Efectos de la cancelación:

La cancelación da lugar al bloqueo de los datos, esto es, que se conserven únicamente a disposición de los sujetos obligados, para atender las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas, para que una vez que se haya cumplido el mismo se proceda a su supresión, en términos de la normatividad aplicable y el cual cabe señalar es de 5 años.

Oposición:

Es aquel derecho que tiene el titular para oponerse al tratamiento de sus datos personales, en posesión de los sujetos obligados, cuando estos se hubiesen recabado sin su consentimiento o cuando existan motivos fundados para ello y la Ley no disponga lo contrario.

Para ello igualmente se deberá presentar una solicitud de información confidencial (directamente o a través de su representante legal), en términos respetuosos y elegir del formulario electrónico en la sección de Solicita Información, la opción de oposición de mis datos personales y de igual forma se podrá presentar su solicitud de manera verbal o por escrito. [17.]

La solicitud deberá, contener adicionalmente a lo señalado en el punto sobre el acceso a datos personales, los motivos fundados para tal determinación de oposición. Para lo cual Los sujetos obligados al tratar los sistemas de datos personales, deberán observar los siguientes principios:

1. De consentimiento, es decir, contar con la aceptación del titular de los datos.
2. Información previa, esto es, te debemos informar para qué serán recabados y tratados y a ellos se le llama aviso de privacidad.
3. Finalidad, es decir, para qué los estamos recabando.
4. Licitud, que significa que tenemos que contar con atribuciones legales para ello.
5. Calidad de la información, que deben ser adecuados y no excesivos en atención a la finalidad para la qué los estamos recabando.

---

(17) Op Cit., Gainero Guadaña, Bruno J. La regulación procesal del habeas data. Montevideo, B de f, 2010.

6. Confidencialidad, es decir, que sólo los sujetos obligados con atribuciones pueden tener acceso a tus datos personales y no cualquier funcionario
7. Seguridad, las medidas que debemos adoptar para resguardar tu información.

Los principios anteriores deberán ser esencialmente observados, con la finalidad de Garantizar el ejercicio de los derechos “ARCO”, del titular.

1.7 - La nueva Ley de Transparencia y Acceso a la Información y el “INAI”.

También llamada, Ley General de Transparencia y Acceso a la Información Pública, es básicamente lo mismo que sus antecesoras de orden público y de observancia general en toda la República, es reglamentaria del artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, en materia de transparencia y acceso a la información, tal y como lo describe el artículo 1 de la misma.

Por otra parte tiene por objeto establecer los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información en posesión de cualquier autoridad, entidad, órgano y organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad de la Federación, las Entidades Federativas y los Municipios.

Y sus objetivos primordiales son:

I. Distribuir competencias entre los Organismos garantes de la Federación y las Entidades Federativas, en materia de transparencia y acceso a la información;
II. Establecer las bases mínimas que regirán los procedimientos para garantizar el ejercicio del derecho de acceso a la información;

III. Establecer procedimientos y condiciones homogéneas en el ejercicio del derecho de acceso a la información, mediante procedimientos sencillos y expeditos;
IV. Regular los medios de impugnación y procedimientos para la interposición de acciones de inconstitucionalidad y controversias constitucionales por parte de los Organismos garantes;
V. Establecer las bases y la información de interés público que se debe difundir proactivamente;
VI. Regular la organización y funcionamiento del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, así como establecer las bases de coordinación entre sus integrantes;
VII. Promover, fomentar y difundir la cultura de la transparencia en el ejercicio de la función pública, el acceso a la información, la participación ciudadana, así como la rendición de cuentas, a través del establecimiento de políticas públicas y mecanismos que garanticen la publicidad de información oportuna, verificable, comprensible, actualizada y completa, que se difunda en los formatos más adecuados y accesibles para todo el público y atendiendo en todo momento las condiciones sociales, económicas y culturales de cada región;
VIII. Propiciar la participación ciudadana en la toma de decisiones públicas a fin de contribuir a la consolidación de la democracia, y
IX. Establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio y las sanciones que correspondan.

En otro aspecto importante a señalar de esta ley, incorpora algunas nuevas figuras y términos como son:

I. Ajustes Razonables: Modificaciones y adaptaciones necesarias y adecuadas que no impongan una carga desproporcionada o indebida, cuando se requieran en un caso particular, para garantizar a las personas con discapacidad el goce o ejercicio, en igualdad de condiciones, de los derechos humanos;

II. Áreas: Instancias que cuentan o puedan contar con la información. Tratándose del sector público, serán aquellas que estén previstas en el reglamento interior, estatuto orgánico respectivo o equivalentes;

III. Comisionado: Cada uno de los integrantes del Pleno del Instituto y de los Organismos garantes de los Estados y del Distrito Federal;

IV. Comité de Transparencia: Instancia a la que hace referencia el artículo 43 de la presente Ley;

V. Consejo Nacional: Consejo del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales al que hace referencia el artículo 32 de la presente Ley;

VI. Datos abiertos: Los datos digitales de carácter público que son accesibles en línea que pueden ser usados, reutilizados y redistribuidos por cualquier interesado y que tienen las siguientes características:

a) Accesibles: Los datos están disponibles para la gama más amplia de usuarios, para cualquier propósito;

b) Integrales: Contienen el tema que describen a detalle y con los metadatos necesarios;

c) Gratuitos: Se obtienen sin entregar a cambio contraprestación alguna;

d) No discriminatorios: Los datos están disponibles para cualquier persona, sin necesidad de registro;

e) Oportunos: Son actualizados, periódicamente, conforme se generen;

f) Permanentes: Se conservan en el tiempo, para lo cual, las versiones históricas relevantes para uso público se mantendrán disponibles con identificadores adecuados al efecto;

g) Primarios: Provienen de la fuente de origen con el máximo nivel de desagregación posible;

h) Legibles por máquinas: Deberán estar estructurados, total o parcialmente, para ser procesados e interpretados por equipos electrónicos de manera automática;

i) En formatos abiertos: Los datos estarán disponibles con el conjunto de características técnicas y de presentación que corresponden a la estructura lógica usada para almacenar datos en un archivo digital, cuyas especificaciones técnicas están disponibles públicamente, que no suponen una dificultad de acceso y que su aplicación y reproducción no estén condicionadas a contraprestación alguna;

j) De libre uso: Citan la fuente de origen como único requerimiento para ser utilizados libremente;

VII. Documento: Los expedientes, reportes, estudios, actas, resoluciones, oficios, correspondencia, acuerdos, directivas, directrices, circulares, contratos, convenios, instructivos, notas, memorandos, estadísticas o bien, cualquier otro registro que documente el ejercicio de las facultades, funciones y competencias de los sujetos obligados, sus Servidores Públicos e integrantes, sin importar su fuente o fecha de elaboración. Los documentos podrán estar en cualquier medio, sea escrito, impreso, sonoro, visual, electrónico, informático u holográfico;

VIII. Entidades Federativas: Las partes integrantes de la Federación que son los Estados de Aguascalientes, Baja California, Baja California Sur, Campeche, Coahuila de Zaragoza, Colima, Chiapas, Chihuahua, Durango, Guanajuato, Guerrero, Hidalgo, Jalisco, México, Michoacán, Morelos, Nayarit, Nuevo León, Oaxaca, Puebla, Querétaro, Quintana Roo, San Luis Potosí, Sinaloa, Sonora, Tabasco, Tamaulipas, Tlaxcala, Veracruz, Yucatán, Zacatecas y el Distrito Federal;

IX. Expediente: Unidad documental constituida por uno o varios documentos de archivo, ordenados y relacionados por un mismo asunto, actividad o trámite de los sujetos obligados;

X. Formatos Abiertos: Conjunto de características técnicas y de presentación de la información que corresponden a la estructura lógica usada para almacenar datos de forma integral y facilitan su procesamiento digital, cuyas especificaciones están disponibles públicamente y que permiten el acceso sin restricción de uso por parte de los usuarios;

XI. Formatos Accesibles: Cualquier manera o forma alternativa que dé acceso a los solicitantes de información, en forma tan viable y cómoda como la de las personas sin discapacidad ni otras dificultades para acceder a cualquier texto impreso y/o cualquier otro formato convencional en el que la información pueda encontrarse;

XII. Información de interés público: Se refiere a la información que resulta relevante o beneficiosa para la sociedad y no simplemente de interés individual, cuya divulgación resulta útil para que el público comprenda las actividades que llevan a cabo los sujetos obligados;

XIII. Instituto: El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

XIV. Ley: La Ley General de Transparencia y Acceso a la Información Pública;

XV. Ley Federal: La Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental;

XVI. Organismos garantes: Aquellos con autonomía constitucional especializados en materia de acceso a la información y protección de datos personales en términos de los artículos 6o., 116, fracción VIII y 122, apartado C,

BASE PRIMERA, Fracción V, inciso ñ) de la Constitución Política de los Estados Unidos Mexicanos;

XVII. Plataforma Nacional: La Plataforma Nacional de Transparencia a que hace referencia el artículo 49 de la presente Ley;

XVIII. Servidores Públicos: Los mencionados en el párrafo primero del artículo 108 de la Constitución Política de los Estados Unidos Mexicanos y sus correlativos de las Entidades Federativas y municipios que establezcan las Constituciones de los Estados y el Estatuto de Gobierno del Distrito Federal;

XIX. Sistema Nacional: Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales;

XX. Unidad de Transparencia: Instancia a la que hace referencia el artículo 45 de esta Ley, y

XXI. Versión Pública: Documento o Expediente en el que se da acceso a información eliminando u omitiendo las partes o secciones clasificadas. Así como garantizar el derecho humano de acceso a la información comprende solicitar, investigar, difundir, buscar y recibir información.

Capítulo 2.
Marco legal.

2.1 .-El derecho a la protección de datos personales y los derechos “ARCO” en la constitución.

El derecho a la protección de datos personales y los derechos se encuentra regulado a nivel constitucional en los siguientes artículos:

- Artículo 6 (DOF 20 de julio de 2007).
- Artículo 16 (DOF 1º de junio de 2009).
- Artículo 73 (DOF 30 de abril de 2009).

Referente a lo antes señalado tuvimos como consecuencia, la reforma al artículo 6º Constitucional, de cuyo primer antecedente encontramos la reforma realizada en el año 2007, al artículo 6 constitucional en la que se adicionó un párrafo segundo a este numeral, sentando las bases respecto al derecho a la información (transparencia), e incluyendo la protección de datos personales por parte de las entidades públicas y reconociendo los derechos de acceso y rectificación.

Por otra parte, tenemos la reforma del artículo 16 Constitucional. En esta reforma se adicionó un párrafo segundo al artículo, y se establece que toda persona tiene derecho a la protección de sus datos personales, a ejercer los derechos denominados “ARCO” cuyas siglas significan acceso, rectificación, cancelación y oposición.

El texto constitucional también señala que este derecho sólo podrá limitarse por razones de seguridad nacional, disposiciones de orden público, seguridad y salud pública o para proteger los derechos de terceros. La Ley Federal de Protección de Datos en Posesión de los Particulares, (LFPDPPP) por su parte, recoge estos supuestos dentro de su artículo 4.

La reforma al artículo 73 Constitucional por su parte facultó al Congreso de la Unión para legislar en materia de protección de datos personales en posesión de particulares, a través de la adición de la fracción XXIX-O. La justificación para otorgar dicha facultad al Legislativo Federal, fue que los datos personales que se utilizan en diversas transacciones comerciales, y el comercio se encuentren regulados en el ámbito federal, discusión de la cual derivó la siguiente ley:[18]

1. Ley de Transparencia, publicada originalmente en el Diario Oficial de la Federación el 11 de junio de 2002.

2.2 El derecho a la protección de datos personales y los derechos "ARCO" en las leyes federales.

Como ya hemos mencionado antes Después de un arduo camino y mucha polémica, el 27 de abril de 2010 se aprobó en el pleno del Senado la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP), y el pasado 5 de julio de 2010 se publicó en el Diario Oficial de la Federación (DOF); esta ley tiene como finalidad proteger los datos personales en posesión de los particulares y regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. A decir de expertos es una de las leyes de protección de datos más avanzada del mundo.

(18)http://www.finanzas.df.gob.mx/oip/arco/index.html, 15/11/15,21:15

Como lo mencionamos en la página 18, la Ley Federal de Protección de Datos Personales en Posesión de Particulares, (LFPDPPP), consta de 69 artículos organizados en 11 capítulos, que mencionan en los artículos 1 y 2 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, señalan que los objetivos de la misma son garantizar la privacidad de las personas (físicas) y su derecho a la autodeterminación informativa, ya que sus disposiciones se aplicarán al tratamiento automatizado o no automatizado de información personal que realicen la persona física o moral ("Responsable"), con determinadas excepciones que tengan como objeto (fines personales y los que realicen las Sociedades de información crediticia).

En este mismo capítulo se definen los términos centrales de esta normatividad, de entre los cuales resultan fundamentales los conceptos de dato personal sensible, titular, responsable, encargado, tercero y tratamiento tanto en el modelo general y sectorial.

El modelo general es adoptado por la mayoría de los países, especialmente por la Unión Europea y entre sus características se encuentran:

1. Sólo existe un cuerpo normativo en la materia y una autoridad encargada de su cumplimiento.
2. Siempre se requiere el consentimiento de los titulares para el tratamiento de información.
3. Se prohíben las transferencias a países que no tengan un nivel adecuado de protección.

Por su parte, el modelo sectorial es aplicado por los Estados Unidos de América, tiene las siguientes características:

1. No existe un instrumento legal único que regule la materia, las diversas dependencias pueden emitir las normas que estimen convenientes para su sector.

2. Diversas autoridades, en el ámbito de su competencia. Se encargan de velar por la protección de este derecho.
3. Se presume el consentimiento de los titulares para el tratamiento de los datos a menos que los mismos manifiesten su negativa.
4. Este esquema funciona bajo mecanismos de autorregulación.

Es importante conocer lo anterior ya que derivado de su Capítulo II, De los Principios de Protección de Datos Personales, podemos identificar qué tipo de modelo es al que México se adapta, sin embargo debemos considerar que la ley retoma el modelo general y los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad pero no se adapta a ninguno de los dos sistemas más bien es un hibrido de ambos que a su vez deriva de la variación realizada del sistema español. Resulta de suma importancia mencionar este modelo, ya que los principios de consentimiento e información tienen la finalidad de que los responsables sólo puedan realizar el tratamiento de datos personales, si los titulares de los mismos otorgan su consentimiento para las finalidades señaladas en el aviso de privacidad únicamente.

Capítulo VI, De las Autoridades señala que el IFAI ahora INAI (denominado Instituto Nacional de Acceso a la Información y Protección de Datos), a partir de la reforma del 5 de julio de 2006 sería la autoridad encargada de vigilar y verificar el cumplimiento de la Ley de Datos Personales, así como dar trámite a los procedimientos de protección de derechos, verificación y sanción que constaban en sus artículos (Capítulos VII, VIII y IX). Adicionalmente, la ley señala que las Secretarías podrán emitir disposiciones en la materia, otorgando facultades especiales a la Secretaría de Economía.

Por otra parte en su Capítulo VII, Del Procedimiento de Protección de Derechos la ley señala que este procedimiento inicia con una solicitud presentada por el titular de los datos ante el INAI, cuando estime que el responsable negó injustificadamente el acceso, rectificación, cancelación u oposición de sus datos. El capítulo en cuestión señala la forma y los plazos en los cuales se sustanciará

este procedimiento, las causales de improcedencia y sobreseimiento, así como el recurso que procede en contra de la resolución que emita el Instituto.

Capítulo X, De las Infracciones y Sanciones, este capítulo enlista un breve catálogo de infracciones y sanciones correlativas a la Ley, que a su vez contempla sanciones o multas que van de los 100 a los 320,000 días de salario mínimo vigente en el Distrito Federal, las cuales podrán aumentarse por reincidencia, y se duplicarán cuando las infracciones tengan relación con el tratamiento de datos personales sensibles. De conformidad con el salario mínimo del Distrito Federal para el 2013, estas multas oscilan entre los $6,476.00 (mínimo) y $20’723,200.00 (máximo).

Capítulo VIII, Del Procedimiento de Verificación, nos hace una breve remembranza del procedimiento que comenzará cuando los responsables incumplan con las resoluciones emitidas por el INAI, o cuando la autoridad presuma la existencia de algún tipo de incumplimiento. La forma y los plazos para sustanciar este procedimiento se regula en la vía reglamentaria.

Capítulo IX, Del Procedimiento de Imposición de Sanciones, nos habla de que el INAI y sus facultades para dar inicio a un procedimiento sancionador que deriva del trámite de los procedimientos de protección de derechos y verificación, en donde se haya detectado algún incumplimiento de los principios o disposiciones a la Ley. La forma y plazos para sustanciar este procedimiento se regulara en la vía reglamentaria.

Capítulo XI, De los Delitos en Materia del Tratamiento Indebido de Datos Personales contempla las penas privativas de libertad, que van desde los tres meses hasta los 5 años de prisión, mismas que también podrán duplicarse cuando las conductas guarden relación con datos personales sensibles.

(**2) Decreto por el que se adiciona un segundo párrafo con siete fracciones al Artículo sexto de la Constitución Política de los Estados Unidos Mexicanos. Publicado en el Diario Oficial el 20 de julio de 2007.**

(3) Reforma al artículo 16 constitucional Publicada en el Diario Oficial de la Federación el 1 de junio de 2009.

(4)Reforma al artículo 73 constitucional. Publicada en el Diario Oficial de la Federación el 30 de abril de 2009.

(5)Decreto por el que se expide la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, publicado en el Diario Oficial de la Federación el 5 de julio del 2010.

2.3 Los derechos (ARCO) como mecanismos de defensa ante la violación del derecho a la protección de datos personales.

Los Derechos ARCO (acceso, rectificación, cancelación y oposición), son un conjunto de derechos que garantizan al ciudadano el poder de control de sus datos personales.

Lo más importante en el ejercicio de estos derechos es que sólo el titular de los datos personales puede solicitar el acceso, la rectificación, cancelación u oposición, siempre que se encuentren en un sistema de datos personales. Por lo tanto en este tipo de solicitudes será requisito indispensable fundar y motivar el acceso la rectificación o la cancelación de nuestras bases de datos para oponerse a su tratamiento y que acreditada la personalidad del solicitante o bien la del representante legal, se proceda al trámite de dicha solicitud.

Así que cada uno de nosotros, como titulares de datos personales, o en su caso, representante legal, puede ejercer cualquiera de los derechos “ARCO” y puede solicitar a los entes obligados, el acceso a la información según obre en sus archivos, requerir que en caso de algún error en los datos personales sea rectificado; o bien solicitar la oposición o cancelación de sus datos de manera definitiva en sus bases de datos, cabe mencionar que el ejercicio de cada uno de estos derechos es independiente entre sí, y no es necesario agotar uno para ejercer alguno de los otros tres.

Cabe señalar que de estos cuatro derechos conllevan efectos distintos por ejemplo:

- El derecho de **Acceso**: Se ejerce únicamente para solicitar y obtener información de los datos de carácter personal.
- El derecho de **Rectificación**: Procede cuando de los sistemas de datos personales en posesión de algún particular, tales datos resulten inexactos o incompletos, inadecuados o excesivos.
- El derecho de **Cancelación:** tiene como finalidad que cuando el tratamiento que se le dé a los datos personales no se ajuste a lo dispuesto en la Ley y Lineamientos emitidos en materia, conlleve como consecuencia la supresión de los mismos, siempre y cuando dicha solicitud este bien fundada y motivada haciendo énfasis en el o los motivos por los cuales hace esta solicitud.
- El derecho de **Oposición**: Por su parte la oposición procederá cuando los datos personales sean recabados sin consentimiento, o sin que existan motivos fundados para ello y la ley no disponga lo contrario.

Ahora bien y bajo el mismo orden de ideas ya que hemos dado un breve repaso al significado de las siglas, ”ARCO” y de cada uno de los derechos que estas contemplan, por lo cual podemos comprender la interposición dé cada una de las solicitudes relacionadas con el ejercicio estos derechos”, y su forma de presentación en la Oficina de Información Pública, o de los entes públicos; y que deberá cumplir con los siguientes requisitos:

“Artículo 34 de la LFPDPP.- La solicitud de acceso, rectificación, cancelación u oposición de los datos personales deberá contener, cuando menos, los requisitos siguientes:

I. Nombre del ente público a quien se dirija

II. Nombre completo del interesado, en su caso, el de su representante legal;

III. Descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados;
IV. Cualquier otro elemento que facilite su localización;
V. El domicilio, mismo que se debe encontrar dentro del Distrito Federal, o medio electrónico para recibir notificaciones, y
VI. Opcionalmente, la modalidad en la que prefiere se otorgue el acceso a sus datos personales, la cual podrá ser consulta directa, copias simples o certificadas."

Cabe señalar que los requisitos del artículo "34 de la LFPDPP", operan de manera general e indistinta para cada una de las solicitudes, pero cuentan con particularidades que las distinguen entre sí por ejemplo:

- Para Acceso: se debe Indicar la forma en la que prefieres se te otorgue el acceso a tus datos personales, que puede ser mediante consulta directa o impreso.
- Para Rectificación: Señalar qué dato es erróneo y cuál es la corrección que debe realizarse. Adicionalmente, se tendrá que acompañar la solicitud con la documentación necesaria que acredite los datos correctos.
- Para Cancelación: Incluir las razones por las cuales consideras que el uso de los datos no se ajusta a lo que la legislación dispone.
- Para Oposición: Señalar los motivos por los que no estás de acuerdo con el uso o difusión de tus datos.

En el caso de que la solicitud sea negada se interpondrá un recurso de revisión, de ser procedente otorgará mediante un medio de información la información para el efecto solicitada en la Oficina de Información Pública (OIP), para lo cual deberá acreditarse como titular de los datos mediante identificación oficial.

Por otra parte si la solicitud de derechos ARCO, no fue atendida o no se está Conforme con la respuesta. El El Instituto de Acceso a la Información Pública del Distrito Federal (INFODF), será la autoridad encargada de atender las

inconformidades de los titulares de los datos personales ante las respuestas o falta de respuestas y para hacer valer sus derechos ARCO y se realizará a través de un recurso de revisión. Como anteriormente ya hemos señalado

Ahora hay que señalar que como ya dijimos anteriormente en otros capítulos estos entes públicos deben observar algunos principios para solicitar, mis datos personales, ya que debe tratar sistemas de datos y observar los siguientes principios:

I. Licitud, que significa que la posesión y tratamiento de sistemas de datos personales obedecerá únicamente a las atribuciones legales de cada ente público.

II. Consentimiento tu voluntad libre, inequívoca e informada para que los entes públicos lleven a cabo el tratamiento de tus datos personales.

III. Calidad de los datos que deben ser adecuados, pertinentes y no excesivos en atención a la finalidad para la que se están recabando.

IV. Confidencialidad es decir, que sólo la persona interesada, así como los entes públicos con atribuciones pueden tener acceso a los datos personales debiendo guardar absoluta secrecía.

V. Seguridad únicamente el responsable del sistema de datos personales o en su caso el usuario puede llevar a cabo el tratamiento de los datos personales.

VI. Disponibilidad los datos deben de ser almacenados de modo que permitan el ejercicio de los derechos ARCO al titular de los mismos.

VII. Temporalidad, los datos personales deben ser destruidos, cuando hayan dejado de ser necesarios o pertinentes para los fines que hubiesen sido recolectado.[19]

_____

(19)http://www.finanzas.df.gob.mx/oip/arco/index.html 12/02/2015. 11:30 pm

2.4.- Repercusiones por su incumplimiento.

Es de suma importancia conocer que nuestros derechos frente a los abusos que puedan suscitarse en nuestra esfera jurídica pero es más importante aún saber las repercusiones de su incumplimiento, el cual se encuentra en el Capítulo IX. Del Procedimiento de Imposición de Sanciones que nos menciona:

Que si con motivo del desahogo del procedimiento de protección de derechos o del procedimiento de verificación que realice el Instituto, éste tuviera conocimiento de un presunto incumplimiento de alguno de los principios o disposiciones de esta Ley, iniciará el procedimiento de imposición de sanciones, a efecto de determinar la sanción que corresponda.

De este se deriva la facultad que tiene el INAI como órgano independiente para emitir sanciones en caso de incumplimiento de las mismas.[20]

---

(20)http://www.finanzas.df.gob.mx/oip/arco/index.html 15/02/2015 11:40pm

2.5- Sanciones impuestas por la inobservancia a las regulaciones.

Mucho se ha hablado de las sanciones que el instituto como autoridad impone Tratándose de infracciones cometidas, esto en razón de que algunos autores y no consideran que sean correctos ya que no producen un efecto sancionar realmente en proporción de su riqueza ni de su nivel de gravedad, estas infracciones se enumeran a continuación:

Infracción cometida por el responsable de los datos.	Sanción
No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en la Ley.	Apercibimiento
Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales; Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable; Dar tratamiento a los datos personales en contravención a los principios establecidos en la LFPDPP; Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de la LFPDPP; 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; No cumplir con el apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular (derechos ARCO).	Se impondrá por cualquiera de los supuestos señalados en este apartado, multa de $5,980 a $9,569,000 pesos o de (100 a 160,000 días de salario mínimo vigente en el Distrito Federal).

Incumplir el deber de confidencialidad respecto de cualquier fase del tratamiento de datos personales; Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin haber recabado nuevamente el consentimiento del titular; 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; Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable; Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley; Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible; Obstruir los actos de verificación de la autoridad; Recabar datos en forma engañosa y fraudulenta; Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares; Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos ARCO; Crear bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado, y Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la	Se impondrá a los sujetos que se ubiquen dentro de los supuestos enumerados aun lado multa de $11,960 a $19,136,000 pesos O el equivalente de (200 a 320,000 días de salario mínimo vigente en el Distrito Federal).

presente Ley.	
En caso de que de manera reiterada persistan las infracciones citadas en los incisos anteriores, se impondrá una multa adicional que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal.	Se impondrá una Multa de $5,980 a $19,136,000 pesos.
Tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.	Se impondrá una Multa de $23,920 a $38,272,000 pesos.

Para esto el INAI fundará y motivará sus resoluciones, considerando:

a) La naturaleza del dato;

(b) La notoria improcedencia de la negativa del responsable, para realizar los actos solicitados por el titular, en términos de la Ley;

c) El carácter intencional o no, de la acción u omisión constitutiva de la infracción;

d) La capacidad económica del responsable, y

e) La reincidencia.

No es hasta esta última entrega, particularmente después de haber visto los montos de las multas y el tiempo que puede un responsable de datos ir a parar a prisión, que prestamos la debida atención y entendemos la relevancia de cumplir con esta ley.

Desde que se publicó la ley los “despachos de consultores” comenzaron a tener enfoque sobre la misma y brindar asesoría sobre su cumplimiento a sus trabajadores sin embargo se trata de una ley, poco observada por lo estudiosos de la ciencia jurídica, por lo que sólo abogados especialistas están debidamente capacitados para asesorar y dar cumplimiento a su reglamento. Pues aunque suene extraño hay que reconocer que en estos despachos de consultores, están mejor

informados y asesorados en la materia ya que se encuentran respaldados por un Consejo Legal Especializado.

En el Capítulo XI. en su artículo 67 De los Delitos en Materia del Tratamiento Indebido de Datos Personales, se contemplan algunas sanciones leves que por ejemplo:

• Se sancionará con prisión…	• Sanción
• Al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.	• Prisión de tres meses a tres años.
• Al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.	• Prisión de seis meses a cinco años.
• Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.	• Prisión de seis meses a diez años.

Dentro de este capítulo se enlista el catálogo de infracciones a la Ley y sus correlativas sanciones. La ley contempla como sanciones, multas que van de los 100 a los 320,000 días de salario mínimo vigente en el Distrito Federal, las cuales podrán aumentarse por reincidencia, y se duplicarán cuando las infracciones tengan relación con el tratamiento de datos personales sensibles. De conformidad con el salario mínimo del Distrito Federal para el 2013, estas multas oscilan entre los $6,476.00 (mínimo) y $20’723,200.00 (máximo)

Procedimiento de Imposición de Sanciones.

El INAI se encuentra facultado para dar inicio a un procedimiento sancionador en caso de que, derivado del trámite de los procedimientos de protección de derechos y de verificación, haya detectado algún incumplimiento de los principios o disposiciones de la Ley. La forma y plazos para sustanciar este procedimiento se regula en la vía reglamentaria.[21]

(21)http://www.Ley_Federal_de_Protección_de_Datos_Personales#Cap.C3.ADtulo_X.2C_De_las_Infracciones_y_Sanciones ,25/10/15, 21:40pm.

Capítulo 3.
El manejo de información en manos de instituciones bancarias, las formas de obtención de datos personales cedidos a agencias de cobranza o recabados a través de instituciones como el 040 y el desconocimiento de los derechos (ARCO) como defensa.

3.1 El Manejo de la información personal por parte de las instituciones bancarias y el aviso de privacidad.

La información personal en este tiempo es tan poderosa que el conocimiento o desconocimiento de cierta información adecuada a las sociedades y sus gobiernos, así como el manejo "adecuado" de la información, puede ayudar a los grandes propietarios del capital a definir gustos y patrones de los consumidores, puede ser utilizada incluso para manipular la información política que ayuda a tomar decisiones que convienen a las empresas transnacionales.

Hablar de acceso a la información en este tiempo puede significar incluso un arma para desprestigiar a figuras públicas o políticas, por el simple hecho de que tengan ideas adversas a las necesidades de los dueños del dinero o de algún partido político, influyendo directamente en la sociedad y en sus ganancias. Por su parte las instituciones bancarias y sus estudios de campo, sirven para calcular que éste tipo de riesgos no afecten su inversión determinando de esta manera si una actividad es o no rentable. Esta doble función de la información que por una parte le permite la manipulación y por la otra a la población estar mejor o peor enterada de los factores que influyen en la toma de decisiones produciendo "virtudes que

Pueden ser exploradas y explotadas por los capitalistas para sus propios fines, dejando indefenso al pueblo.[22]

Lo antes señalado en el párrafo anterior trae como consecuencia un uso indiscriminado de la información no sólo daña a la sociedad sino que perjudica a cada individuo. No sólo nos referimos a la información pública si no también a la privada, que es manipulada para obtener ciertas respuestas sociales o de consumo, cuando es utilizada con fines extra particulares, que ameriten o tengan de por medio una especulación comercial.

Por otra parte puede sonar atrevido lo que voy a referir, pero aquellos datos que proporcionamos al Estado que los bancos y las aseguradoras tienen de nosotros, es información que proporcionamos por internet a las escuelas o para conseguir un trabajo u obtener algún apoyo social y que podrían estar en posesión de particulares con intereses diferentes a los nuestros y a los de la sociedad en su conjunto.

Es por eso que nace mi idea del que se deba cuestionarse la alta concentración de datos personales en entes públicos o privados porque la información es Poder. Un poder que conlleva incluso la pérdida absoluta del control por parte del interesado sobre sus datos y la posibilidad de que sus derechos y libertades sean vulnerados, por aquellos que disponen de la tecnología necesaria para recolectar, almacenar y procesar grandes cantidades de información, los cual debería preocuparle no solo al acreditado si no también a la autoridad en cuestión.

---

(22) Op Cit. Ekmenkdjian, Miguel Ángel y Pizzolo, Calogero, *Hábeas data. El derecho a la intimidad frente a la revolución informática*, 2a. ed., Argentina, Depalma, 1998, pp45.

Antes, la información sobre cada individuo podía estar parcializada en diferentes instituciones públicas y privadas. Pero, ahora, con las nuevas tecnologías, puede hacerse un compendio absoluto de todas las actividades de un individuo y, por lo tanto, tenerlo totalmente observado y controlado para fines tanto legales como ilegales.

Esta información personal influye bastante en términos de cobranza que es la actividad que nos ocupa en la presente investigación, información que puede ser no solo extraída e identificada en ocasiones provocando una molestia en casos de un homónimo.

Ahora parece que, para las instituciones bancarias existe un "exceso" de transparencia en la búsqueda de "la riqueza" y puesto que en su práctica todo se basa sustancialmente en "información" que debe ser comunicada al instante por lo que toda vida privada, se convierte o pasa a ser pública. Como dice Galindo Garfias, "es una ironía de la historia, que uno de los mayores logros de la modernidad, que es la democratización de la información, se banalicé". [23]

En este sentido, se producen dos consecuencias que afectan la percepción de los ciudadanos sobre la información. Por una parte, la información pierde relevancia al ser transmitida sin ninguna jerarquización o responsabilidad no objetividad por las autoridades e instituciones bancarias, con el único fin de que los intereses de unos pocos no se vean afectados y sigan operando de manera clandestina e ilegal en la mayoría de los casos.

(23)Op. Cit., Galindo Garfias, Ignacio. Derecho Civil Primer Curso, México, Porrúa, 19 ED. 1995, Pág. 334-335. 8 Burgoa

Por dar un ejemplo los hechos verdaderamente importantes forman parte de un torrente informativo que, la mayoría de las veces, carece de trascendencia en estos temas para evitar que la sociedad comience a presentar descontento con dichas situaciones que afecta a un sistema muy complejo de tráfico de datos personales de un particular a otro o de una institución bancaria a otra. Responsabilidad que radica, por un lado, en ejercer el derecho a la información buscando y publicando información veraz, trascendente y, por el otro lado, reconociendo que hay un derecho de la ciudadanía a estar informados, por lo tanto, lo que se comunica por parte de las autoridades debe ser en apoyo a la población no en su perjuicio. [24]

Debemos ser conscientes que lo que hacemos público transforma nuestra Sociedad", pero como transformar una sociedad que se encuentra regida en la actualidad por un modelo económico que protege al capitalista o en su caso las instituciones bancarias. Es así que las instituciones autorizadas por la propia ley para transferir los datos una y otra vez, transfieren también constantemente los datos personales que en un principio les fueron otorgados por el titular para ¿un fin distinto al que ahora ellos mejan?

El argumento de que basado en el artículo 10 de la LFPDPP, ellos pueden ejercer su derecho al cobró, violando directamente las garantías del acreditado sin importar el que ni el por qué. Peor aún es el caso, cuando estos no les fueron otorgados y dichas instituciones se justifican en algo llamado aviso de privacidad que sigue un código de ética que persigue unos fines y el cual deben de cumplir supuestamente estas instituciones, pero no es así no siempre se cumple con eso.

---

(24)Orihuela, Ignacio. Las garantías individuales, México, Porrua, 30ª ED., 1998, Pag. 161.

Y bueno es entonces que nos preguntamos ¿qué es el aviso de privacidad? Que no es más que un texto en el cual se explica el uso que se le dará los datos al titular de los mismos, y se genera en forma impresa o electrónica (aparece como una liga en una página Web). La ley y su reglamento mencionan en varios de sus artículos la forma que tendrá este aviso de privacidad. En forma adicional, el día 17 de enero de 2013 la Secretaría de Economía publicó en el Diario Oficial de la Federación los lineamientos para la generación del Aviso de Privacidad, a efectos de minimizar la necesidad de que se deba recurrir a empresas privadas para obtener asesoramiento en su creación. En dicha publicación se diferencian tres formas del Aviso de Privacidad: Integral, Simplificado y Corto, según su aplicación, por ejemplo:

www.banamex.com//avisodeprivacidad , que es con lo que el banco justifica el uso y tratamiento de los datos personales no así el uso que les dan las agencias de cobranza o despachos, lo cual acarrea un descontento pues dichas agencias se identifican en representación del banco y hasta mencionan su aviso de privacidad en el cual pues si buscamos a la agencia jamás se encontrará en el pues la información se trasfiere de mano en mano y por ejemplo Banamex tiene millones de agencias en el Distrito Federal, lo que nos hace pensar en las lagunas que tiene nuestra ley y en la decadencia jurídica que vivimos en la actualidad en este rubro en el cual si bien estamos comenzando, también lo estamos haciendo de mala manera pues aún se le dan demasiadas libertades a los bancos para hacer casi lo que sea con dichos datos o de obtenerlos en su defecto de donde sea y nadie se ha dado a la tarea de investigar el por qué.[25]

(25)http://inicio.INAI.org.mx/Publicaciones/ensayos9.pdf 07/11/15, 21:40

3.2 La cesión y venta de datos personales a las agencias de cobranza a través de carteras.

En la actualidad es muy común que si alguien tiene un tarjeta de crédito préstamo o un crédito personal y no esté al corriente reciba aproximadamente de 20 a 50 llamadas por día con un contenido más o menos así:

Hola que tal señor, x buenos días mi nombre es; y ; le llamo de; x agencia, en representación de; x banco , con relación a un asunto de su, tarjeta de crédito, terminación; 1234, y esta llamada puede ser grabada o monitoreada con fines de calidad.

A esto se le llama script y es una forma de homologar las llamadas para que todas suenen igual, lo que ocasiona disgusto entre las personas pues piensan que el Banco cuenta con una sola agencia para cobrar y que siempre son las mismas personas las que hablan, lo cual es totalmente falso pues como ya explique antes el banco tiene millones de agencias especializadas en esto lo que quiere decir que es muy raro que se vuelva hablar con una misma persona dos veces en un día.

A menudo una pregunta muy frecuente entre las personas que son llamadas por estas agencias es ¿Quién les proporcionó mi número? o ¿quién les proporcionó mis datos?, el problema no es si son 20 o 50 llamadas diarias, pues tal vez es justificable cuando el deudor es el titular de los datos, pues este adquirió una obligación de carácter civil con el Banco.

El problema es cuando es un número equivocado, pues Dichas instituciones pueden transferir la información de un lado a otro contratando a otras agencias de cobranza que en ocasiones suelen ser poco ortodoxas o falsean información de los titulares para obtener un beneficio traficando con los datos de los mismos

o bien obtienen datos personales de otras fuentes donde pueden buscar y localizar a el titular sin su permiso.

Cabe decir que dichas agencias tienen aproximadamente un lapso de uno a tres meses para cobrar dicha cuenta si no lo hacen pasa a la siguiente agencia de cobranza, la cual tendrá el mismo tiempo para hacerlo y un copia exacta de la información anteriormente adquirida por una agencia o proporcionada a propósito para su búsqueda, la cual en ocasiones no es actualizada ni dados de baja los números erróneos lo que produce un circulo de molestias constantes que pueden extenderse hasta varios meses o varios años sin que las autoridades hagan nada y los procesos como hemos podido ver son demasiado lentos, lo que ocasiona que instituciones como el Banco en cierto punto pretendan recuperar su pérdida de esta forma al no tener otra manera de hacer el cobro de las mismas pues en la actualidad no hay un mecanismos que les de la pauta a los Bancos para dejar de hacer este tipo de prácticas.

Pero como no lo hay no tienen otra salida más que acudir a las agencias de cobranza que no siempre actualizan la información y que en ocasiones revenden la cartera que les fue otorgada por no ser redituable, lo que también significa que en cierto punto trafican con los datos que les fueron vendidos u otorgados provocando que los Bancos rompan con el secreto bancario, y vulneren las esferas de los titulares de los mismos en su intimidad pues en cierto punto el titular de la línea telefónica al pagar por el servicio tiene derecho a no ser molestado en sus pertenecías ni en sus bienes, como lo es su línea telefónica, pero al dejar de ser respetado este principio se ocasionan molestias entre las personas titulares de dichos datos, o de terceros que no tienen relación contractual alguna con el Banco.

3.3 La obtención no autorizada de datos personales por parte de estas agencias (040 y bases alternas).

Como bien lo habíamos mencionado antes tenemos que a menudo una pregunta muy frecuente entre las personas que son llamadas por estas agencias es ¿Quién les proporciono mi numero? o ¿quién les proporciono mis datos?, la pregunta medular de todo esto sería de donde obtienen los datos personales de otras fuentes donde pueden buscar y localizar al titular, conocido como 040 que es una institución privada que forma parte de Telmex, que con el simple hecho de proporcionar nombre dirección y estado puede proporcionar todos los numero hasta los de celular de un titular que tenga cuentas en Telmex o Telcel, con el simple hecho de marcar al 040 tú puedes obtener todos los medios necesarios para ubicar al titular de una cuenta sin la autorización de utilizar sus datos ni de obtener sus números de teléfono, además buscando en páginas de Internet como todo teléfono puedes encontrar a cualquier persona que radique en la República Mexicana sin problema.

Pero quien autoriza al 040, para transferir los datos de esta manera y sin seguir los procesos de acceso a la información la respuesta es nadie, pero aun así sigue operando de la misma forma sin que instituciones como el Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales, haga algo por corregir esta situación que cada vez es más utilizada por las agencias de cobranza.

3.4 El desconocimiento de los derechos (ARCO) como defensa por parte de los particulares y los licenciados en derecho.

Podrá resultar gracioso el hecho de que siendo licenciados en derecho desconozcamos la norma que nos rige y nos protege pues no es tan común que a diferencia de otras personas nosotros no sepamos qué ley se nos puede aplicar o beneficiar.

La mayoría de la población tiene un desconocimiento total de los derechos ARCO pues ni siquiera en las campañas informativas nos mencionan que son y peor aún es tal el desconocimiento de esta norma que hasta los mismos abogados desconocen que es un derecho ARCO si no en una parte sin en su totalidad yo me di a la tarea de preguntar dentro de un grupo de 50 abogados quien sabía que era un derecho arco, y ninguno me supo contestar

Lo anterior implica que la sociedad no solo está desprotegida sino también en un serio problema pues no tiene respaldo jurídico alguno por parte de los abogados que llegaran a atenderlos, fue entonces que me dirigí a las oficinas del INAI fingiendo desconocer la norma para ver qué era lo que me decían a diferencia de lo que se anuncia en las campañas televisivas me di cuenta que en ningún momento me ofrecieron la opción de oponer mis derechos arco aun y cuando les dije a propósito que no estaba de acuerdo con el uso de mis datos lo que refleja que a la autoridad no le interesa en realidad atender las irregularidades como debe de ser.

Si nosotros vemos los spots y leemos la ley, pareciera que las instituciones en cargadas de ello cumplen al cien con su finalidad pero no es así.

Capítulo 4

La restricción determinada de datos personales en poder de instituciones bancarias para fines de cobranza, y la publicidad de los derechos (ARCO) al público usuario.

4.1 La restricción del uso de la información y la transferencia indefinida de los datos personales en manos de instituciones bancarias

Como ya lo hemos mencionado con anterioridad la problemática de que las instituciones puedan tener ilimitadamente los datos de una persona por así decirlo es una situación que atañe a nuestro país pero como es que la ley permite estas irregularidades si ella misma las prohíbe y las respuesta se encuentra en una sola palabra que no está bien delimitada en el artículo 3 fracción XIX de la LFPPP y la palabra es transferencia.

Si bien es cierto que al contratar algún producto bancario nosotros al revisar el aviso de privacidad estamos aceptando tácita o expresamente los términos y condiciones, tal y como si se tratare de un contrato por el que las partes deben pasar cual si fuera su voluntad.

En muchos de estos contratos y en la ley no está descrito de manera correcta un término que debería ser explicado al titular la palabra es “remisión”, es importante que nosotros, la conozcamos pues es a través de ella que nosotros hacemos una transferencia al responsable para que trate y administre nuestros datos personales de acuerdo a los términos establecidos en su aviso de privacidad, que debe de obedecer además a un código de ética dichos lineamientos que de acuerdo al modelo español se conocen como buenas prácticas, estas no son otra cosa más que una manera correcta de tratar al

titular de los datos personales que cede los datos a través de una transferencia indefinida, lo cual la no ha sido reglamentada.

Es lamentable pero cierto que aun y en estas épocas donde las leyes han evolucionado tanto, no se pueda limitar a una institución bancaria, un número definido de veces para que esta transfiera la información de sus titulares a cualquier persona, sin que se tenga la certeza alguna por parte de una institución gubernamental, provocando de alguna manera, incertidumbre entre los titulares de los datos que no saben si su información está en buenas manos.

Cuando una persona deja de cumplir con una obligación de carácter civil que ha contraído con el Banco incurre en una mora o capitalización de intereses por pagos tardíos que como ya hemos mencionado antes le produce una perdida contable al Banco, que al ser un acreedor genera un vínculo entre ambos; también es cierto que dicha relación es entre el deudor y el acreedor o (responsable), pero gracias el aviso de privacidad dicha relación se ha extendido a un tercero que actúa mediante una (tercerización) como él (encargado) de los datos del titular.

Cuando el acreedor principal o (responsable), no puede cobrar en un principio la deuda, y que propicia que el responsable de los datos o (acreedor principal), transfiera indefinida y arbitrariamente los datos de los titulares a cuantos encargados, decida en un lapso de indefinido de tiempo sin que opere algún tipo de prescripción, con la finalidad de rescatar la mínima cantidad de capital o de alguna cuenta.

Ahora bien dicho lo anterior que le faculta al responsable para realizar esta actividad una y otra vez e incluso hasta ceder o vender carteras de datos personales a otros indefinidamente o realizar simulaciones para que no opere la prescripción del acreedor una y otra vez, sin ser sancionado o apercibido,

como es que la ley evoca en su artículo primero, que dicha busca la protección de los datos personales en manos de particulares y el derecho a la privacidad y a la autodeterminación de la personas ya sean físicas o morales, a través del tratamiento legítimo, controlado e informado, si en vez de ponerle restricciones a las empresas les da amplio criterio para hacer con los datos personales del titular prácticamente lo que sea y no les da pauta si quiera a los propios profesionistas, de demostrar un interés en el tema.

El artículo 10 de la LFPDPP, nos exhibe como un país que tiene muy poco control sobre la información de los ciudadanos y las fuentes por las que acceden estando realmente desprotegidos y sin avances en la legislación de esta materia y que en la opinión de este autor debería, dedicarse a velar por los intereses del titular y no del Banco quien con solo mencionar la fracción IV, puede hacer prácticamente lo que sea con los datos del titular de los datos personales, trasfiriendo o remitiendo cuantas veces quiera a cuantas empresas desee, rompiendo incluso con un derecho humano intrínseco de la persona o titular de origen, derecho a la privacidad.

Cuánto tiempo más el legislador seguirá permitiendo esto, de esta razón nace el hecho de que se deba limitar a los Bancos la trasferencia de datos personales del artículo 3, o remisión de datos, mediante una cláusula en el aviso de privacidad, que prevea tan solo a las personas que realmente estén dentro de una lista de agencias que certificadas por el INAI y a avale que este cuenta con la capacitación correcta para realizar el, tratamiento, transferencia o remisión de los datos, obligando a la institución bancaria a decir exactamente a quien para que y cuánto tiempo estará en posesión de estas personas los datos, esto en relación a que de acuerdo a la LFPDPP no podrá ser mayor a 5 años, lo que los obligara tomar en consideración que existe una prescripción y obligando de esta manera a la institución a que se apegue más a la normatividad civil.

Como lograr esto si dichas acciones se fundamentan en la voluntad de las partes en el aviso de privacidad que obliga al titular a que proporcione sus datos aun y contra su voluntad puede ocasionar cierto dolo pues en cuestiones económicas por necesidad o por urgencia es una forma de aprovecharse de la dignidad humana ya que en ocasiones ni siquiera se les explica a los titulares en qué términos o condiciones se expresa dicho contrato. Es por eso que en lo personal pienso que la solución a este problema sería que el aviso de privacidad como menciona el artículo 16 de la Ley Federal de Protección de Datos en Posesión de los Particulares, que además de contener los 6 requisitos de forma también contiene las personas que estarán como encargadas o responsables de los mismos.

Hacer público el derecho a la información para todas las personas y obligar a los Bancos a mencionar desde un inicio al titular que en caso de incumplimiento de sus obligaciones sus datos serán remitidos para el cobro y transferencia de la deuda solamente a las personas que se estipulen en el aviso de privacidad

Prohibir la cesión de derechos de los datos ya que la ley solo permite la transferencia y remisión de los datos no la venta, pues si bien es cierto los Bancos tienen derecho a recobrar su dinero tan bien es cierto que hablamos de dos tipos diferentes de situaciones, pues al involucrar los datos personales de una persona no solo estamos poniendo en riesgo la seguridad de una persona, le podemos ocasionar algún daño perjuicio e incluso una pérdida o menos cabo que tal vez no pueda ser reparada.

4.2.- La prohibición a la cesión de los datos de agencias de cobranza y la imposición de sanciones más rigurosas a instituciones bancarias.

La situación más penosa de todo esto es que las multas o sanciones impuestas por la autoridad sinceramente no son efectivas ni producen efecto alguno o cambio en estas instituciones pues es muy común que empresas como Banamex, Bancomer, Santander etc.. Que cuentan con miles de agencias telefónicas que actúan en el carácter de encargados de los datos personales por remisión de los mismos sean sancionadas.

El problema realmente no es la remisión de los datos personales a los encargados o responsables si no las subcontrataciones de servicios que estos pueden hacer y que muchas veces derivan responsabilidades de carácter civil o penal que realmente no provocan un gran impacto en el ámbito de respeto a la ley de la materia y sus reglamentos por ejemplo:

consideremos la situación que nos atañe, con relación a los Bancos suponiendo que la multa más alta que se puede imponer al Banco es de 320.000 veces días de salario mínimo en el Distrito Federal y to manado en consideración que en el caso de un solo Banco que tiene varias agencias recibe por lo menos 8 millones de pesos libres de impuestos por la cobranza que realiza en un solo mes y que el procedimiento tarda hasta 50 días después de emitida la solicitud de acceso a la información podríamos decir que bien una multa de 10 millones no es nada para un Banco por lo que lo que realmente lo seguirán haciendo constantemente como lo hacen ya que realmente estas multas son muy escasas y las sanciones no son efectivas.

Se supone que una sanción es un castigo que se impone con la finalidad de obtener un cierto comportamiento por parte del sancionado en este caso se esperaría qué de las pérdidas, también le son redituables al mismo por lo que seguirá con estas prácticas, es por eso que las sanciones impuestas deben de ser

más duras y más rígidas con las instituciones bancarias para frenar el descontrol que provocan en nuestro sistema legal y de acceso a la información.

Lo que se propone en este trabajo es poner multas ejemplares a los Bancos como en el caso de Estados Unidos de América a PLAY STATION, para provocarles un menoscabo importante en su ganancia y evitar así, que se vuelva a propagar estas malas costumbres que deben ser erradicadas de nuestro sistema obligando a los Bancos a hacer mención los titulares en su aviso de privacidad del lapso de 5 años que tienen para el cobro de las deudas de carácter civil ya que aunque los datos son transferidos de mano en mano y de responsable en responsable o en su defecto de responsable a encargado y a su vez se realiza una sub contratación de servicios por cada uno de ellos no se genera ninguna novación en cuanto al contrato de apertura de crédito o el adeudo, a menos que expresamente el titular estructure dicho adeudo evitando así que opere la prescripción negativa para evitar la propagación por mas años de la información del titular.

Por otra parte el limitar ciertas fuentes de acceso público a los Bancos para cuestiones de cobranza extrajudicial sin consentimiento expreso del titular, traerá como consecuencia la descripción de dicha búsqueda en el aviso de privacidad obligando de cierta manera que el mismo tenga que generar expresamente en su aviso de privacidad la búsqueda del consentimiento del titular.

No basta con un apartado especial, o leyenda en el aviso de privacidad que busque dicho consentimiento, sino más bien generar por parte del INAI un apartado obligatorio en el que se haga mención de que para su mayor información acerca de la cobranza, que se le realizará al titular se le debe indicar de un inicio lo siguiente:

Le recordamos que todos sus datos incluso los nuevos datos que sean obtenidos durante el proceso de cobranza serán usados por un lapso de x tiempo con la finalidad de ejercer nuestro derecho al cobro.

Exceptuando de este aviso los que son de tipo sensible, por la naturaleza del negocio y para evitar la propagación de dichos datos para la formación indebida de bases de datos que son formadas con la finalidad de venta de seguros médicos de vida etc.

De esta manera y brindando dichas facultades al INAI para conocer irregularidades y sancionar mediante la creación de un órgano especializado de atención ciudadano que pueda tratar las solicitudes de acceso a la información que tengan como característica común la violación de la ley por parte de las instituciones bancarias generará que dichas instituciones sean más cuidadosas en cuanto a la vulneración de la norma por el temor de ser sancionado más cada vez, por su reincidencia. Disminuyendo de cierta manera el hecho de que una llamada telefónica de sus agencias deje de ser un acto consecutivo de molestia, constante y que trascienda en la vida, pertenencias y en ocasiones en la dignidad humana, de las personas que son afectadas, sancionando de manera correcta al responsable de forma administrativa y no penal como en el artículo 109 del Código Penal del Distrito Federal, siempre y cuando tomando en consideración las buenas prácticas y su actuar como un trabajo, personal y subordinado y lícito, que se rige mediante un contrato de servicios, pues si bien es cierto que dichas personas causan una molestia también es cierto que a cambio reciben un salario, que aunque de manera curiosa contraviene lo dispuesto por el artículo 5 constitucional que a la letra dice:

"A *ninguna persona podrá impedirse que se dedique a la profesión, industria, comercio o trabajo que le acomode siendo lícitos. El ejercicio de esta libertad sólo podrá vedarse por determinación judicial, cuando se ataquen los derechos de terceros,* siempre y cuando no amerite que se les sancione".

Lo anterior será siempre y cuando estos no utilicen prácticas fuera de los lineamientos que establecen las buenas prácticas del modelo español que anteriormente ya expusimos en el capítulo de derechos ARCO:

Considerando el enunciado anterior y las palabras subrayadas, esta actividad pude ser infundada e ilegal, al causar una molestia a terceros, pero no puede vedarse el derecho a este trabajo por lo cual no debería de ser considerado como ilícito como lo menciona el artículo 109 del Código Penal para el Distrito Federal:

Siempre y cuando no que de demostrado fehacientemente que:

> 1.-El desempeño de esta actividad afecta a terceros de las siguientes maneras.
> 2.-Causa molestias en sus pertenecías bienes, al no ser el titular buscado, o exista un caso de homonimia, pues al ser el titular de la línea tiene derecho a reclamar que se le esta violentando su esfera íntima.
> 3.-Causa molestias en el domicilio y pertenencias tanto del deudor como de terceros ajenos a la obligación principal del mismo

Por lo cual para mí la mejor forma de solucionar esta problemática es, restringir la información a las instituciones bancarias, reforzado más el artículo 16 constitucional, pues en cierta medida hablamos que estas llamadas podrían considerarse un acto de molestia, que afecta los bienes y los derechos de pertenencia del titular de la línea, que se producen al momento de contratar un servicio delimitado en específico por tiempo limitado en el artículo 3 de la LFTPPP, lo que evitaría un tráfico indebido a estas instituciones solo con las instituciones que el INAI y el titular autoricen de inicio y a nadie más.

4.3.-La publicidad de los derechos ARCO ventana a la creación de una cultura de la información en México.

Siempre he dicho que la información es poder y el poder controla a las masas pareciera que no pero el simple y sencillo hecho de que las personas no conozcan que es un derecho arco, no acarrea ninguna complicación.

Pero que sucede cuando decimos que ese desconocimiento e ignorancia incluso de los abogados trae como consecuencia abusos y que los mismos abogados no sepan cómo defender a sus clientes y si lo hacen resultan ser presas fáciles para las empresas que si lo saben, y no es solamente que el hecho de que el campo del derecho al acceso a la información sea poco considerado en la rama del derecho administrativo, sino lo que implica esto.

Es necesario que instituciones como el INAI comiencen a considerar la publicidad de estos derechos pues el que ellos pongan como requisito a las instituciones de crédito, la obligación de hacer mención en su aviso de privacidad al público usuario no quiere decir que las personas sepan lo que son los derechos ARCO, realmente cuantas personas saben que es un derecho ARCO, los empleados de estas instituciones no hacen mención de ellos, lo que debería de ser ya que cuando alguien firma un contrato de servicios sus términos y condiciones deben ser explicados y detallados por estos empleados y aun así el hecho de que ellos le hagan mención a las personas del término arco no quiere decir que la persona comprenda que es, a lo que la empresa podría excusarse diciendo que el desconocimiento de la norma no exime de la misma, en pocas palabras si no conoces no te puedes defender, porque ya diste tu aceptación como dice la ley.

El dar publicidad a estos derechos evitará problemas y mal entendidos, además generara tanto en las personas como en los abogados una cultura como en el caso de los derechos humanos, evitando no solo injusticias y abusos, de parte de los bancos, al saber cómo defenderse ante ellos cuando se considere que existe realmente un abuso u hostigamiento en el servicio comprobable, provocando que ellos realmente busquen una certificación para evitar ser multados y sancionados, prestando realmente un verdadero servicio en la cobranza que realizan expresando el que y el para qué y con qué fines, se requiere la información solicitada.

El expresar puntualmente en el aviso de privacidad y la adquisición de nueva información en caso de que sea encontrada además la limitación para acceder a la información sensible en el caso de aseguradoras de los bancos que vendan paquetes de seguros médicos por tratarse de datos sumamente personales y de los cuales solo la persona puede acceder.

Pues cabe destacar que el hablar de datos el Término remite al derecho a la intimidad, que algunos señalan que está incluido en el derecho a la vida privada.

Independientemente de esa discusión, es un concepto estrictamente vinculado con el derecho de acceso a la información, al derivar del llamado habeas data, que es el derecho que toda persona tiene a acceder a la información sobre sí misma , sea que esté en posesión del gobierno o de una entidad privada.

El derecho incluye la facultad de modificar, eliminar o corregir la información considerada sensible, errónea, sesgada o discriminatoria y que dichos datos no sean conocidos por otras personas.

Y ya que como hemos dicho antes en el ámbito internacional se ha configurado un auténtico derecho fundamental a la protección de datos personales, distinto al derecho a la intimidad.

Este derecho tiene su propio contenido y mecanismos de protección e incluso puede ser limitado según lo dispuesto por el artículo 13, de la Convención Americana y las interpretaciones que de este ha hecho la Corte Interamericana Derechos Humanos.

4.4.- La restricción determinada de datos personales, en poder de instituciones bancarias y la difusión de los derechos al público usuario

Según la Convención Americana de Derechos Humanos (CADH), e l derecho al acceso a la información solo puede limitarse si se da cumplimiento estricto de los requisitos establecidos, en el artículo 13, párrafo 2, de la Convención Americana de Derechos Humanos (CADH), esto es si se satisfacen las condiciones de estricta legalidad, necesidad (idoneidad y proporcionalidad) y finalidad (protección de objetivos legítimos autorizados por la misma), sin olvidar, además, que de conformidad con las características que hemos señalado antes, la máxima divulgación impone un requisito adicional a observarse, esto es, la verdadera excepcionalidad de las restricciones, que se traduce en el limitado número de excepciones que pueden existir para que la información no sea entregada y en establecimiento de un plazo razonable para que subsistan, a fin de que una vez que concluya dicho plazo la información pueda ser consultada, salvo que subsista efectivamente el riesgo cierto y objetivo que haya justificado el establecimiento de la restricción .

Así las limitaciones al derecho de acceso a la información para que se puedan establecer deben partir del hecho de que este derecho tiene como escénica el principio de la máxima divulgación, por lo que las restricciones al acceso a la información deber ser taxativas, la excepción y no la regla, así como contar con plazos que permitan que la información se divulgue y la restricción desaparezca.

Asimismo, deben estar previstas en la ley de manera clara y precisa, lo cual implica que esta sea emitida por el órgano legislativo constitucionalmente

dispuesto para ello y que no deje a la discrecionalidad de los funcionarios si se divulga o no la información.

De conformidad con lo anterior los alcances del derecho al acceso a la información que se tiene en el sistema interamericano, los Estados así como las instituciones privadas tienen la obligación de garantizar a los individuos el derecho acceder a los archivos que contengan violaciones graves a dicho derecho, destacando que este derecho implica también la posibilidad de acceder a los lugares físicos donde se encuentra la información.

De esta manera, toda la información relativa a las graves violaciones de este derecho como parte del derecho a la verdad que está estrechamente vinculado al acceso a la información.

Si creamos una verdadera cultura de acceso a la información podemos evitar que se propague dicha falta de información y el abuso de las instituciones la publicidad es la solución a un problema como este, el hecho de que el Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales, realizare todas estas situaciones traería como consecuencia que tengamos una mejor cultura de acceso a la información y que nuestros profesionales del derecho se preocupen por estudiar más las situaciones derivadas de estas leyes y las múltiples lagunas que contiene esta ley, a la cual le falta mucho para ser realmente una regulación para el acceso a la información en manos de particulares, obligando a el legislador a generar acuerdos y avances mejores en cuanto al tema, dando realmente una verdadera certeza al titular de los derechos y no al responsable de su información.

El camino hacia una mejor legislación de estos temas tiene que ver no solo con quien legisla de manera que nosotros los abogados podemos aportar o generan debates o discusiones en cuanto al tema entre nuestras autoridades responsables.

Por último me resta decir que México puede ser uno de los mejores países en cuestión de legislación de acceso a la información haciendo, proposiciones en el caso de acceso a la información para que otras naciones tomen el modelo mexicano como un ejemplo y puedan dar más avances en estas situaciones, provocadas, por los Bancos evitando el control que ellos ejercen sobre nosotros al tener nuestra información.

Por tal motivo debe ser un objetivo esencial y primordial el crear o generar una cultura del acceso de la información entre instruyendo a la gente de manera correcta,

1.- en recomendaciones en materia de seguridad de datos personales sobre todo del artículo 19 de la Ley Federal de protección de datos personales en Poder de Particulares y sus elementos principales contenidos en su recomendación general, trayendo a su vez como consecuencia;

2.- Difundir la materia de acceso a la información entre los profesionales del derecho para obtener una mejora circunstancial y un mayor número de opiniones, que generen una conciencia de la importancia que tiene este derecho y su impacto social.

De lo anterior se puede decir que al considerar más el tema podemos comenzar a plantearnos en generar o mejorar el sistema general de datos personales en nuestro país, para evitar que se den tantos desvíos como hoy en día, estableciendo mecanismos jurídicos que regulen a los Bancos de manera correcta y conforme al derecho, reduciendo de cierta forma su camp de maniobra.

3.- Generar o reorganizar al INAI, en el ámbito de sus funciones, de tal manera que no solo sea una autoridad que pueda conocer si no resolver el asunto, creando tribunales especializados en la materia que resuelvan sobre el fondo y

de la inconformidad instaurada por alguna de las partes, determinando si procede o no el habeas data, creando apartados más específicos, para el caso de los datos ultra sensibles esto beneficiará mucho en generar mejoras en el formato de aviso de privacidad, que tantas lagunas posee, haciéndolo más específico de acuerdo al género del negocio jurídico aplicando distinciones, estableciendo el que para qué y quienes además del responsable de los datos puedan dar tratamiento a los datos del titular, evitando actos de molestia hacia alguna de las partes o en su defecto terceros ajenos a la relación.

4.- Por otra parte el Implementar obligatoriamente las buenas prácticas, de manera más estricta en los avisos de privacidad, de las instituciones bancarias que tengan como objeto la recuperación de su cartera vencida en caso de pérdidas monetarias, derivadas del incumplimiento de alguna obligación civil, respetando siempre leyes y reglamentos del INAI, para evitar que se generen incidencias de parte del responsable.

Mejorar y actualizar continuamente las funciones de seguridad y el contenido del artículo 59 y 62 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de manera continua así como la adecuada división de los negocios jurídicos que causan normalmente situaciones de vulnerabilidad en cuestiones de acceso a la información y su distinción.

Esto obligará tanto a empresas como a Instituciones Gubernamentales a cumplir correctamente con la publicidad de las leyes y reglamentos para dar mayor paso a una mayor propagación para el conocimiento del público usuario y de las figuras que ellos tienen para defenderse ante los abusos de estas instituciones, frenando de esta manera las prácticas de agencias o instituciones que no cumplan con las disposiciones impuestas por el INAI.

Y a regular y controlar mejor las fuentes de acceso público general, como son la internet y otras fuentes de telecomunicaciones como el 040, locatel y redes

sociales, creando organismos con las competencias necesarias para desempeñar tales tareas, evitando o disminuyendo las fugas de información tal y la como establece SGSDP, (Sistema de Gestión de Datos Personales).

Conclusiones.

Primera.-Es necesario crear o generar una cultura del acceso de la información instruyendo a la gente de manera correcta con recomendaciones en materia de seguridad de datos personales, sobre todo del artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, que forman parte fundamental de los elementos principales de la recomendación general.

Segunda.-Difundir la materia de acceso a la información entre los profesionales del derecho para obtener una mejora circunstancial y un mayor número de opiniones para generar una conciencia de la importancia que tiene este derecho y su impacto social.

Tercera.-Generar o mejorar el sistema general, para evitar que se generen tantas evidencias como hoy en día estableciendo mecanismos jurídicos que regulen a los bancos de manera correcta y conforme a derecho, reduciendo de cierta forma su campo de impacto.

Cuarta.- Generar o reorganizar al Instituto Nacional de Transparencia y Acceso a la Información y Protección de Datos Personales, en el ámbito de sus funciones, de tal manera que no solo sea una autoridad que pueda conocer si no resolver el asunto, creando tribunales especializados en la materia que resuelvan sobre el fondo y de la inconformidad instaurada por alguna de las partes, determinando si procede o no el habeas data, creando apartados más específicos, para el caso de los datos ultra sensibles.

Quinta.-Generar mejoras en el formato de aviso de privacidad, que tantas lagunas posee, haciéndolo más específico de acuerdo al género del negocio jurídico aplicando distinciones, estableciendo el qué para qué y quienes además del responsable de los datos puedan dar tratamiento a los datos del titular, evitando

actos de molestia hacia alguna de las partes o en su defecto terceros ajenos a la relación.

Sexta.-Regular y controlar mejor las fuentes de acceso público general, como son la internet y otras fuentes de telecomunicaciones como el 040, locatel y redes sociales, creando organismos con las competencias necesarias para desempeñar tales tareas, evitando o disminuyendo las fugas de información tal y la como establece el Sistema de Gestión de Datos Personales, también conocidas por sus siglas (SGSDP).

Séptima.-Implementar obligatoriamente las buenas prácticas, de manera más estricta en los avisos de privacidad, de las instituciones bancarias que tengan como objeto la recuperación de su cartera en caso de perdidas monetarias, derivadas del incumplimiento de alguna obligación civil, respetando siempre leyes y reglamentos del Instituto Nacional de Transparencia y Acceso a la Información y protección de Datos Personales (INAI), para evitar que se generen incidencias de parte del responsable de los datos personales.

Octava.-La traducción de un mayor número de autores a nuestro idioma español ya que la mayor parte de los libros en materia de datos personales se encuentran en otro idioma, lo que generaría la mayor asimilación de este derecho, ya que para los estudiosos del derecho de este país muchos de los avances en esta materia les son desconocidos derivado del no entendimiento del idioma Inglés o algunos otros como el caso del idioma Alemán de donde provienen gran parte de los autores en la materia.

Novena.-Cumplir correctamente con la publicidad de las leyes y reglamentos para dar mayor paso a una mayor propagación para el conocimiento del público usuario y de las figuras que ellos tienen para defenderse ante los abusos de estas instituciones, frenando de esta manera las prácticas de agencias o instituciones que no cumplan con las disposiciones impuestas por el Instituto Nacional de

Transparencia y Acceso a la Información y Protección de Datos Personales (INAI).

Décima - Mejorar y actualizar continuamente las funciones de seguridad y el contenido del artículo 59 y 62 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de manera continua así como la adecuada división de los negocios jurídicos que causan normalmente situaciones de vulnerabilidad en cuestiones de acceso a la información y su distinción.

Décima Primera.-Implementar de manera obligatoria el registro de la oficina o departamento encargado de recibir las solicitudes de acceso a la información ante el Instituto Nacional de Transparencia y Acceso a la Información y Protección de Datos Personales (INAI), con la finalidad de mantener vigiladas a las empresas que mantengan entre sus actividades cotidianas el tratamiento de los datos personales, de los titulares que les hayan proporcionado acceso a su in formación personal.

Décima segunda.-Creación de un órgano de vigilancia nacional de gestión informativa, encargado únicamente de realizar inspecciones y auditorias tanto a las bases de datos personales que resguarden, entidades privadas tanto empresas como Instituciones bancarias que pretendan el resguardo de datos personales, asegurando de esta manera que las cancelaciones u oposiciones que se hayan determinado se cumplan y lleven a cabo en los plazos establecidos por las leyes de la materia y en caso contrario se lleve a cabo la imposición de las sanciones en el momento por cada uno de dichos incumplimientos.

Décima tercera.-La no satanización de la cobranza judicial mediante la creación de artículos que adolecen y complican situación actual como e l caso del código penal del Distrito Federal., pues si bien es cierto las violaciones deben de ser perseguidas y castigadas también lo es que resulta muy subjetivo para cada persona el hablar de lo que para ellos causaría una molestia o una falacia, motivo

por el cual en muchos de los casos la gente actuaria premeditadamente con la única finalidad de evadir sus deudas y obligaciones pendientes.

Décima cuarta.-La creación de normas en la materia de carácter penal más especializadas en castigar cuestiones únicamente de acceso a la información y no cuestiones que no tengan que ver con situaciones que se deriven de una relación laboral, derivada a su vez por un contrato de servicios, como es el caso de estas agencias pues su fuente de empleamiento resulta legal desde un inicio.

Décima Quinta.-Programar un plazo legal como en el caso de las declaraciones fiscales para llevar acabo auditorías a las personas morales para reforzar la vigilancia y el cumplimiento de las normas en la materia mediante un reporte completo y detallado de la gestión de los datos así como las trasferencias y destino de los datos personales, que están siendo gestionados por una persona distinta del encargado de los mismos.

Bibliografía:

1. - Ackerman, John M., Fix-Fierro, Héctor,
Más allá del acceso a la información: Transparencia, rendición de cuentas y
Estado de Derecho, presentación de Héctor Fix-Fierro.
=México= Siglo Veintiuno Editores =2008=404 p.

2.- Albor, Mariano.
La denuncia.
México =sin.editorial.= 2001, 126 p.

3.- Araujo Carranza, Ernesto.,
El Derecho a la Información y la Protección de Datos Personales en México.
México, Editorial Porrúa, 2009
xv, 292 p.

4.- Castellanos Hernández, Eduardo de Jesús, coord.
El Sistema de Compilación y Consulta del Orden Jurídico Nacional.
México, Secretaría de Gobernación, 2007
82 p.

5.-Cantoral Domínguez, Karla.
Villanueva, Ernesto, pról.
Derecho de protección de datos personales de la salud =prólogo de Ernesto
Villanueva=.
=México= Editorial Novum =2012=
xiv, 224 p.

6.- Cantú Aguillén, Ricardo.
Martino, Antonio A. Puccinelli, Oscar R.,
Derecho de la Información en América Latina y en México; Legislación, Jurisprudencia y Habeas Data, prólogo de Antonio A. Martino

7.- Carbonell Sánchez, Miguel.
Constitución y transparencia: Consideraciones Para Sonora.
=Hermosillo, Son., México= Instituto de Transparencia Informativa del Estado
de Sonora =2009,92 p.

8.- Carbonell, Miguel.
El régimen constitucional de la transparencia.
México, Universidad Nacional Autónoma de México, 2008
viii, 96 p.
(Instituto de Investigaciones Jurídicas, Ensayos Jurídicos, 33)

9.-Carbonell, Miguel, coord.
Davara, Isabel, coaut.
Luna, Issa, coaut.
Ley de Protección de Datos Personales para el Distrito Federal Comentada, coordinado =por= Miguel Carbonell, Isabel Davara =e= Issa Luna.
México, Instituto de Acceso a la Información Pública del Distrito Federal, 2010. 322 p.

10.-Carbonell, Miguel.
Acceso a la información y protección de datos personales en el ámbito de la justicia.
=México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2012=
61 p. (Ensayos para la Transparencia de la Ciudad de México, 20)

11.-Coahuila. Instituto Coahuilense de Acceso a la Información Pública.
Ley de Acceso a la Información Pública y Protección de Datos Personales para El Estado de Coahuila.
=Saltillo, Coahuila, México= Instituto Coahuilense de Acceso a la Información Pública =2009= 70 p.

12.-Distrito Federal. Instituto de Acceso a la Información Pública del Distrito Federal.
Tú Derecho a la Privacidad: La Protección de tus Datos Personales.
=México= Instituto de Acceso a la Información Pública del Distrito Federal=2009, 20 p.
(Colección Educación Cívica, 4)
13.-Distrito Federal. Instituto de Acceso a la Información Pública del Distrito Federal. Manual de Autoformación

sobre la Ley de Protección de Datos Personales para el Distrito Federal. (Capacitación a Distancia, 5)=México, Instituto de Acceso a la Información Pública del Distrito Federal, 2009, 201 p.

14.- Gaiero Guadagna, Bruno J. La regulación procesal del Habeas data: protección de Datos personales y acceso a la información pública Montevideo, B def, 2010.

15.- González Padilla, Roy.
Protección de datos personales en posesión de particulares..(Cuadernos de Trabajo, 11)=México= Senado de la República, Instituto Belisario Domínguez, 2011 35 p

16.- Gómez-Robledo, Alonso.
Ornelas Núñez, Lina, Protección de Datos Personales en México: El Caso del Poder Ejecutivo Federal =por= Alonso Gómez-Robledo =y= Lina Ornelas Núñez. México, Universidad Nacional Autónoma de México, 2006, viii, 104 p. (Instituto de Investigaciones Jurídicas. Serie Estudios Jurídicos, 97)

17.- López Ayllón, Sergio,
Código de buenas prácticas y alternativas para el diseño de leyes de Transparencia y acceso a la información pública en México.
=México= Instituto Federal de Acceso a la Información Pública =2007,119 p.

Legislación.

1.- Constitución política de los Estados Unidos Mexicanos.

2.-Ley Federal de Protección de Datos Personales en, Posesión de los Particulares;

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

4.- Reglamento de la Ley Federal de Protección de Datos Personales en, Posesión de los Particulares.

5.- México. Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.
5° concurso de ensayo; Universitarios construyendo transparencia 2012. =México= Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal =2012=172 p.

6.- México. Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal.
6° concurso de ensayo; Universitarios construyendo transparencia 2013.=México= Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal =2013=189 p.

7.-México. Instituto Federal de Acceso a la Información Pública.
Transparencia, acceso a la información y datos personales; Marco normativo. Instituto Federal de Acceso a la Información Pública Gubernamental,
México, 2003=140 p.

8.- México. Poder Judicial de la Federación.
Primer Seminario de Transparencia Judicial Federal.- (Tópicos de Transparencia, II)=México= Comisión para la Transparencia, Acceso a la Información Pública Gubernamental y Protección de Datos Personales, 2011 230 p.

9.- Oscar R. Puccinelli.
=México= Universidad Autónoma de Nuevo León =2005., 438 p.

10.- Ovilla Bueno, Rocío.
Correas Vázquez, Óscar, La Protección de los Datos Personales en México, comentario de Óscar Correas Vázquez. México, Editorial Porrúa, 2005
xix, 72 p. (Breviarios Jurídicos, 28)

11.-Pérez Fuentes, Gisela María,
Gómez Gallardo, Perla, Temas Selectos de Derecho a la Información, Derecho a la Intimidad, Transparencia y Datos Personales =prólogo de Perla Gómez Gallardo=.- Villahermosa, Tab., México= Universidad Juárez Autónoma de Tabasco =2010=308 p.

12.- Ponce Báez, Gabriela, García Tinajero, Leonel,
Las fronteras del derecho de la información, coordinado =por=Gabriela Ponce Báez =y= Leonel García Tinajero.
=México= Editorial Novum =2011=xiii, 168 p.

13.-Téllez Valdés, Julio.
Lex cloud computing; Estudio jurídico del cómputo en la nube en México. México, UNAM, Instituto de Investigaciones Jurídicas, 2013 xv, 733 p.

14.- Villanueva, Ernesto,
Derecho de la información; Culturas y Sistemas Jurídicos Comparados. México, UNAM, Instituto de Investigaciones Jurídicas, 2007 xiii, 462 p. (Instituto de Investigaciones Jurídicas. Serie Doctrina Jurídica, 378)

15.- Villanueva, Ernesto,
Nucci, Hilda, coord. Comentarios a la Ley Federal de Protección de Datos Personales en Posesión de Particulares, coordinado =por= Ernesto Villanueva =e= Hilda Nucci.=México= Editorial Novum =2012=447 p.

16.- Villamil, Jenaro.
Acceso a la Información, Periodismo y Redes Sociales. Escenarios Futuros. =México, Instituto de Acceso a la Información Pública del Distrito Federal, (Ensayos para la Transparencia de la Ciudad de México, 18) 2010., 53 p.

REVISTAS

1. Acuña, Juan Manuel.
La protección de datos personales y la
autodeterminación informativa como
respuesta desde el derecho ante el poder informático.
ARS IURIS No. 33, 2005
México, D. F

2. Aveleyra, Antonio M.
La comunicación de mensajes de datos personales en
México. El predecible
Estado del arte: La administración pública, los
desarrollos privados y los
esfuerzos legislativos 2003-2004.
DERECHO COMPARADO DE LA INFORMACIÓN
No. 4, Julio-Diciembre, 2004 México, D. F.

3. Blanco Tatto, Alejandro.
¿Es constitucional el Buró Crédito?
EL MUNDO DEL ABOGADO. UNA REVISTA ACTUAL
Año 6, No. 58, Febrero, 2004 México, D. F.

4. Bailón Cabrera, Lorenzo.
El Derecho Fundamental de la Protección de Derechos
Personales.
PODIUM NOTARIAL. REVISTA DEL COLEGIO DE
NOTARIOS DEL ESTADO DE JALISCO
No. 32, Diciembre, 2005 Guadalajara, Jal., México

5. Ceballos De la Mora, Carlos Alberto.
Consideraciones sobre la protección de los datos
personales automatizados.
REVISTA INTERCONTINENTAL DUCIT ET DOCET
DE INVESTIGACIÓN Vol. IV, No. 1,
2003 México, D. F.

6. Cervantes Gómez, Juan Carlos.
Protección de datos personales.
QUÓRUM No. 86,
Julio-Septiembre, 2006 México, D. F.

7. Domínguez, Luis Alberto.
La evolución de la Protección de los

datos personales.
EL MUNDO DEL ABOGADO
Año 8, No. 77, Septiembre, 2005
México, D. F.

8. Flores Dapkevicius, Rubén.
Algunas consideraciones sobre el amparo mexicano.
REVISTA DE DERECHO PÚBLICO Año 13, No. 25,
Junio, 2004 Montevideo, Uruguay

9. García Murillo, José Guillermo.
Puente de la Mora, Ximena, coaut.
Límite al Derecho a la Información: La Protección de
Datos Personales en el Derecho Comparado.
REVISTA JURÍDICA JALISCIENSE
Año 16, No. 1, Enero-Junio, 2006
Guadalajara, Jal., México

10. García González, Aristeo.
La protección de datos personales: derecho
fundamental del siglo XXI. Un
Estudio comparado.
BOLETÍN MEXICANO DE DERECHO COMPARADO
Nueva Serie, Año XL, No. 120, Septiembre-Diciembre,
2007 México, D. F.

11. García González, Aristeo.
La protección de datos personales en el ámbito judicial:
el caso del Poder
Judicial del Estado de Michoacán.
DERECHO COMPARADO DE LA INFORMACIÓN
No. 10, Julio-Diciembre, 2007 México, D. F.

12. Gudiño Pelayo, José de Jesús.
Tratamiento jurídico de datos personales.
LEX. DIFUSIÓN Y ANÁLISIS
Tercer Época, Año IX, No. 125, Noviembre, 2005
México, D. F.

13. Jiménez Guzmán, Luis.

La libertad de libre circulación de comunicaciones privadas y correspondencia: La protección del correo electrónico y de los datos personales en México. REVISTA DE LOS TRIBUNALES AGRARIOS Segunda Época, Año IV, No. 41, Enero-Abril, 2007 México, D. F.

14. Lechuga Maternach, Vicente.
Derecho, Intimidad e Informática.
ESCRIVA. REVISTA DEL COLEGIO DE NOTARIOS DEL ESTADO DE MÉXICO Año 2, No. 4, primavera, 1999 Toluca, Edo. de Méx., México

15. Martí Capitanachi, Luz del Carmen.
Comentario a la reforma al artículo 6o. de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
CUESTIONES CONSTITUCIONALES. REVISTA MEXICANA DE DERECHO CONSTITUCIONAL No. 16, Enero-Junio, 2007 México, D. F.

16. Mirón Reyes, Jorge Antonio.
Ataques a la vida privada y a la intimidad frente al derecho de acceso a la información.
DERECHO COMPARADO DE LA INFORMACIÓN No. 8, Julio-Diciembre, 2006, México, D. F.

17. Morales Campos, Estela.
Sociedad e Información. OMNIA Año 6, No. 20, Septiembre, 1990 México, D. F.

18. Pérez Cázares, Martín Eduardo.
El habeas data o respeto a la intimidad en el derecho informático. REVISTA JURÍDICA JALISCIENSE, Año 13, No. 2, Julio-Diciembre, 2003 Guadalajara, Jal., México.