UNIVERSIDAD LATINA

CAMPUS SUR

ESCUELA DE DERECHO

Sistema Universidad Abierta

"DERECHO A LA PROTECCIÓN DE LA INTIMIDAD Y LOS DATOS PERSONALES ENTRE PARTICULARES"

T E S I S

QUE PARA OBTENER EL TÍTULO DE :

LICENCIADO EN DERECHO

P R E S E N T A :

MIRIAM ANGELICA PALMA LEÓN

MÉXICO, D.F. **DICIEMBRE 2009**

A mi padre, fuente de sabiduría y fortaleza, que aún después de tantos años de ausencia, sigo recordando tus palabras.

A mi madre, luz, vida y amor incansable.

A mis hermanos, que sin ellos mi vida no habría sido forjada igual.

A mi patito, amado compañero de lucha; nunca olvidaré la forma filosófica en que trataste de explicarme la diferencia entre el derecho objetivo y el derecho subjetivo.

A Max, mi mar de paz y amor, que en cada una de nuestras pláticas, siempre me haces crecer un poco más.

A Rodrigo, que siempre has sabido sacarme una sonrisa con tu mirada inocente y tu sonrisa picára.

A Paty, porque estás ahí siempre apoyándonos, ten la confianza que cuidaré de tu fruto, mientras tenga fuerzas.

A Adri, Ana, Mónica y Vero, compañeras de vida.

A Lily, Ale, Paty, por permitirme trabajar a su lado, hombro con hombro y seguir siendo su amiga.

A Maricela, que sin tus llamadas y preocupación constante, quizá este trabajo se habría alargado más.

A Sandy, porque viviste conmigo tiempos amargos y hoy día disfrutamos la satisfacción de obtener justicia.

A mis maestros, que en cada clase transmitieron sus conocimientos y amor a la carrera.

A Adolfo Hernán Ramírez, porque con tu asesoría y seguimiento esta investigación cumplió con su objetivo.

Y a todos aquéllos que han estado presentes en mi vida y gracias a ello, me han ayudado a crecer.

UNIVERSIDAD LATINA, S.C.

INCORPORADA A LA U.N.A.M.

México, Distrito Federal a 30 de noviembre de 2009.

DRA. MARGARITA VELÁZQUEZ GUTIÉRREZ
C. DIRECTORA GENERAL DE INCORPORACIÓN
Y REVALIDACIÓN DE ESTUDIOS, UNAM.
P R E S E N T E.

La **C. MIRIAM ANGÉLICA PALMA LEÓN** ha elaborado la tesis profesional titulada **"DERECHO A LA PROTECCIÓN DE LA INTIMIDAD Y LOS DATOS PERSONALES ENTRE PARTICULARES",** bajo la dirección del Lic. Adolfo Hernán Ramírez Vargas, para obtener el Título de Licenciada en Derecho.

La alumna ha concluido la tesis de referencia, misma que llena a mi juicio los requisitos marcados en la Legislación Universitaria y en la normatividad escolar de la Universidad Latina para las tesis profesionales, por lo que otorgo la aprobación correspondiente para todos los efectos académicos correspondientes.

Atentamente,

LIC. JOSÉ MANUEL ROMERO GUEVARA
DIRECTOR TÉCNICO DE LA LICENCIATURA
EN DERECHO.
CAMPUS SUR

JMRG/ISV

CAPÍTULO I. TEÓRICO CONCEPTUAL. DERECHO Y TECNOLOGÍA

Los avances científicos y tecnológicos han revolucionado la vida del hombre a lo largo de la historia, creando lazos tan fuertes, que la vida misma no pudiera concebirse sin el uso de estas herramientas que facilitan las tareas diarias, sin embargo, en el último siglo, la velocidad con que dichas tecnologías han avanzado influyen de manera directa e indirecta en el desarrollo de la sociedad[1], obligando entonces a crear las normas necesarias para regular su uso, aplicación y límites, debido a que no puede descartarse que si bien por un lado la sociedad puede verse beneficiada, también puede llegar a ser afectada por una mala aplicación de estas, aunado al hecho de que la finalidad del Derecho es regular la vida del hombre en sociedad en cualquiera de sus aspectos, para lograr el adecuado disfrute y protección de sus derechos así como establecer los límites de los mismos respecto de los de otra persona.

Es así como en este primer capítulo, se desarrollan los conceptos de los temas principales de esta investigación, para una mejor comprensión de como estos se van concatenando y afectando en la actualidad al individuo, y por lo tanto, entender la importancia de crear el marco jurídico necesario para que la sociedad continúe con la convivencia armoniosa a la que siempre ha aspirado.

1.1 Derecho Informático

A partir de la segunda mitad del siglo veinte[2], el desarrollo de la Informática fue tan acelerado que esto dio pie a que la sociedad quedara inmersa en los diferentes sistemas de información generados, creando distintos problemas entorno a ello, desde problemas sociológicos muy parecidos a los existentes en el siglo XIX con la revolución industrial, hasta problemas jurídicos tales como los de seguridad y

[1] KAPLAN, Marcos. *Ciencia, Estado y Derecho en las primeras revoluciones industriales*. UNAM, Instituto de Investigaciones Jurídicas, México, 2000, Pags. 46-55.
[2] En 1944, la Universidad de Harvard desarrolló el MARK I, el cual es considerado el prototipo de las computadoras actuales.

confidencialidad de la información, robo de programas de cómputo, comisión de delitos informáticos, etcétera.[3]

De ahí la importancia de la definición y estudio de la problemática surgida, con el fin de crear un marco jurídico capaz de proteger a los individuos del mal uso que pueda realizarse a partir del simple manejo de cualquier programa de cómputo, red o sistema de información.

1.1.1 Concepto de Derecho Informático

Antes de desarrollar el concepto de Derecho Informático debemos analizar que es el Derecho, ya que a partir de esto, podremos entender el objetivo principal del porque la sociedad necesita un orden para mantener un balance en sus relaciones interpersonales.

Ahora bien, en el presente trabajo no pretendemos establecer un concepto de derecho, pues es bien sabido que no tenemos un concepto real, solo aproximaciones, por lo tanto; expondremos algunas ideas previas de diferentes autores para poder sugerir una idea que se acerque al derecho y a lo que deberíamos entender por Derecho Informático.

Tomaremos entonces en cuenta a Thomas Hobbes, quien en su obra "Leviatán" establece: "El derecho de la naturaleza, lo que los escritores llaman comúnmente *jus naturale*, es la libertad que cada hombre tiene de usar su propio poder como quiera, para la conservación de su propia naturaleza, es decir, de su propia vida; y por consiguiente, para hacer todo aquello que su propio juicio y razón considere como los medios más aptos para lograr ese fin."[4]

[3] TÉLLEZ VALDEZ, Julio. *Derecho Informático*. UNAM, Instituto de Investigaciones Jurídicas, México, 1991, Pags. 38-40.
[4] HOBBES, Thomas. *Leviatán*. Tomo I. Clásicos Ciencia Política, Número 13, quinta edición, Gernika. México. 2005. Pag. 134

Para Hobbes, la razón es la fuente de la libertad, todo lo que se haga dentro de ella, resulta en una acción humana tendiente a usar su fuerza o poder para su propia conservación. Siendo esta una visión naturalista, necesita del reconocimiento de dicha razón por el Estado, siendo así entonces que éste deberá asegurar que ninguna persona ejerza su poder contra otras para demeritar su calidad humana.

Lo anterior se puede deducir de la lectura líneas adelante cuando el mismo Hobbes escribió: "aunque quienes se ocupan de estas cuestiones acostumbran confundir *jus* y *lex*, derecho y ley, precisa distinguir estos términos, porque el DERECHO consiste en la libertad de hacer o de omitir, mientras que la LEY determina y obliga a una de esas dos cosas. Así la ley y el derecho difieren tanto como la obligación y la libertad, que son incompatibles cuando se refieren a una misma materia."[5]

De lo anterior, podemos entonces argumentar que, el derecho y la ley son diferentes y ya que debido a nuestra razón, tenemos la facultad de ejercer nuestra libertad, la ley será la que nos oponga las condiciones para ejercer esa libertad.

Por su parte, Hans Kelsen sostenía que existe una estricta separación entre el "deber ser" y el "ser", debido a que le interesaba la forma de la norma y no su contenido por lo que le preocupaba la validez formal de la norma jurídica, de ahí que llega a igualar el concepto de derecho con el de la ley reconocida por el Estado y en consecuencia a éste con el derecho[6]; ubicando al derecho como un objeto de la ciencia positiva utilizando el método normativo para señalar cuales son las normas vigentes, por lo que la diferencia entre las normas jurídicas de las demás es la coercibilidad ejercida por el Estado, quien por medio del uso de la fuerza pública puede imponer su cumplimiento.

[5] Idem, Pag. 134
[6] FLORES MENDOZA, Imer Benjamín; *La concepción del Derecho en las corrientes de la filosofía jurídica*. UNAM, Instituto de Investigaciones Jurídicas, México, En: Boletín Mexicano de Derecho Comparado, Nueva Serie, Año XXX, número 90, sept.-dic., 1997, pag.1016

Ahora bien, Ronald Dworkin rechaza el positivismo al señalar que "éste reduce y simplifica el derecho de una comunidad al sólo conjunto de normas empleadas por la comunidad, con el propósito de determinar qué comportamiento será castigado o sometido a coerción por los poderes públicos"[7], por lo que reconoce que existe una vinculación entre las normas y la moral, ejemplificándolo con el poder decisorio de los jueces, los cuales se hacen valer de las normas, principios y directrices, los que sirven para resolver asuntos, que en algunas ocasiones, con la sola aplicación de la ley no se podría dar un sentido de justicia, esto es, si existe un asunto que no es contemplado con la norma, el juzgador podrá hacerse valer de los principios morales, y a partir de su razonamiento poder solucionar el problema.

Como hemos visto, cada una de las teorías anteriormente expuestas, ven al derecho de distinta manera, una da mayor peso a los valores axiológicos y reconoce al hombre como el hacedor de las normas que lo organizan en sociedad; otra, únicamente reconoce que a partir de los hechos, el hombre crea las normas y a partir de la vigencia su aplicación y la última, de alguna manera, considera estas dos posturas para establecer que una es complementaria de la otra y que tanto las normas como la moral, son base para el actuar del derecho. Ahora bien, a partir de estas, podemos entonces reconocer, que valor, norma y hecho, coexisten en la vida del derecho, lo que resulta en una interacción dinámica y dialéctica de estos tres elementos, por lo tanto, para entender que es el derecho debemos comprender a estos tres elementos:

- *Hecho*, como la existencia de un fenómeno jurídico.

- *Valor*, como el que confiere un significado a ese hecho, por el que los hombres buscaran alcanzar o preservar cierto fin u objetivo.

[7] SALDAÑA, Javier. ¿Derechos morales o derechos naturales?: Un análisis conceptual desde la teoría jurídica de Ronald Dworkin. UNAM, Instituto de Investigaciones Jurídicas, México, En: Boletín Mexicano de Derecho Comparado, Nueva Serie, Año XXX, número 90, sept.-dic., 1997. Pag.1215.

- *Norma*, que representa la relación o medida que los integra.

Sin embargo, definir hoy día el concepto del derecho sigue siendo tan complicado como quizá hace doscientos años, pero a nuestro parecer debe ser entendido como la ciencia que tiene como objeto de estudio la vida organizada del hombre y que busca equilibrar el poder entre los miembros de la sociedad con base en sus valores y normas.

Ahora bien, pasaremos a la definición entonces del derecho informático, el cual es una rama de las ciencias jurídicas que contempla a la informática como objeto de estudio, buscando normar toda la actividad que en torno a ésta se desarrolla, a modo tal de establecer los límites necesarios en el manejo de la información para evitar el uso indiscriminado de esta tecnología que pudiera resultar en el daño o menoscabo de los datos que opera.

Es por ello importante, entender el concepto de esta rama para dar pie a su análisis y dejar establecido el por que de la importancia de su estudio en este trabajo de investigación:

> *"El Derecho Informático es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática"*[8]

Entendiendo por un lado que la Informática (o llamada actualmente como Tecnología de la Información) es la técnica utilizada por la sociedad para tratar, administrar y/o recabar información[9], la cual, tiene diversas aplicaciones, tales como: industrial, comercial, gubernamental, educativa, científica, doméstica; de ahí la importancia que todas las naciones le han puesto al desarrollo de esta tecnología, ya que durante los últimos años esta ha logrado economizar los costos del manejo de la información,

[8] I*dem* Pag. 39.
[9] *Diccionario de Informática*. 2ª. Ed., Ediciones Díaz de Santos, México,1993, Pag.302

logrando de esta forma que cualquiera tenga la posibilidad de manejar e intercambiar datos[10], convirtiéndose en una herramienta de integración tecnológica, económica, política y social.

De esta manera, entendemos que la Informática se presenta ante el Derecho en dos sentidos: como objeto o como medio; siendo la primera que se encargue del estudio del manejo de la tecnología de la información y sus consecuencias en el ámbito social, dando como resultado al Derecho Informático y la segunda, en como se aplican estas tecnologías en la solución de conflictos para dar mayor celeridad a los procesos y seguridad jurídica a las personas, resultando en Informática Jurídica[11].

Es por el hecho de que la informática se convierta en una herramienta de uso diario por la sociedad en general, que la ciencia jurídica deba regular el uso de estas herramientas con miras a la protección de los derechos de las personas.

1.1.2 Objeto de Derecho Informático.

El derecho informático busca principalmente reglamentar sobre problemáticas específicas tales como[12]:

a) *Regulación de la información integrada en bases de datos*, debido a que su contenido puede llegar a considerarse como un bien económico por la implicación de la creación, obtención y la protección de los datos.

b) *Protección de datos personales*, lo cual busca evitar la violación del derecho a la intimidad, provocado por el uso indiscriminado de estos.

---

[10] Al hacer referencia sobre la facilidad del manejo de la información, se destaca que el hecho de que cualquier computadora tenga acceso a programas como MS-Excel, MS-Access o simplemente MS-Word o cualquier otro software manejador de texto o datos, abre la posibilidad de que cualquier usuario de computadora administre información, ya sea para uso personal o para compartir.

[11] GOLIN KRAMMES, Alexandre. *Sistemas Jurídicos e Tecnología : Evoluções e influências*. http://www.alfa-redi.org/rdi-articulo.shtml?x=9334 : 05/06/08: 22:28 hrs.

c) *Flujo de información*, la cual actualmente en cuestión de segundos puede transmitirse a cualquier parte del mundo.

d) *Protección de los programas*, debido a las copias ilegales se atenta contra derechos de propiedad intelectual.

e) *Delitos informáticos*, por la facilidad en que pueden cometerse actos ilícitos con el uso de las distintas herramientas existentes.

f) *Contratos informáticos*, por las implicaciones económicas y sociales de este tipo de instrumentos.

g) *Pruebas electrónica*s, por la falta de aceptación y apreciación de estos elementos derivados de soportes informáticos ante los órganos jurisdiccionales, debido a la facilidad de su manipulación y modificación.

Y debido a la celeridad con la que se desarrollan estas tecnologías es que en muchas ocasiones el derecho es superado y por lo tanto, los individuos quedan desprotegidos de los actos y hechos que de estos se derivan, de ahí la importancia del estudio y comprensión de estas por parte del mundo jurídico para evitar que las normas sean superadas de manera extraordinaria como sucede en la actualidad, lo cual genera que la norma pierda su eficacia y por ende que pueda cumplir con su cometido regulador.

1.1.3 Nuevas Tecnologías

El uso de nuevas tecnologías ha diluido las fronteras, lo cual ha creado nuevos conceptos y problemas jurídicos que repercuten tanto en el derecho privado como en el público. Los actuales sistemas, contienen diversas herramientas que ayudan al usuario a seleccionar entre los datos obtenidos la información realmente necesaria,

[12] *Idem* Pag. 41.

de ahí la importancia de comprender su uso y funcionamiento, entre estas encontramos:

- Computación y cálculo a muy alta velocidad.

- Registro y procesamiento electrónico de datos.

- Telecomunicaciones (radiotelefonía, telefonía digital, telefonía satelital, transmisión telefónica de grandes volúmenes de datos a muy alta velocidad (3G), Internet, televisión digital, transmisión telefónica de fotografía digital, etcétera).

- Información geográfica y fotografía satelital; fotografía digital, sistemas de posicionamiento geográfico.

- Avances en la reducción del tamaño de los circuitos electrónicos y por tanto de los equipos de computación, de televisión, telefonía, radio y fotografía.

- Acceso a una gran variedad de programas de cómputo y de multimedia para la administración.

- Combinación de dos o más medios electrónicos de información y comunicación para un solo fin[13].

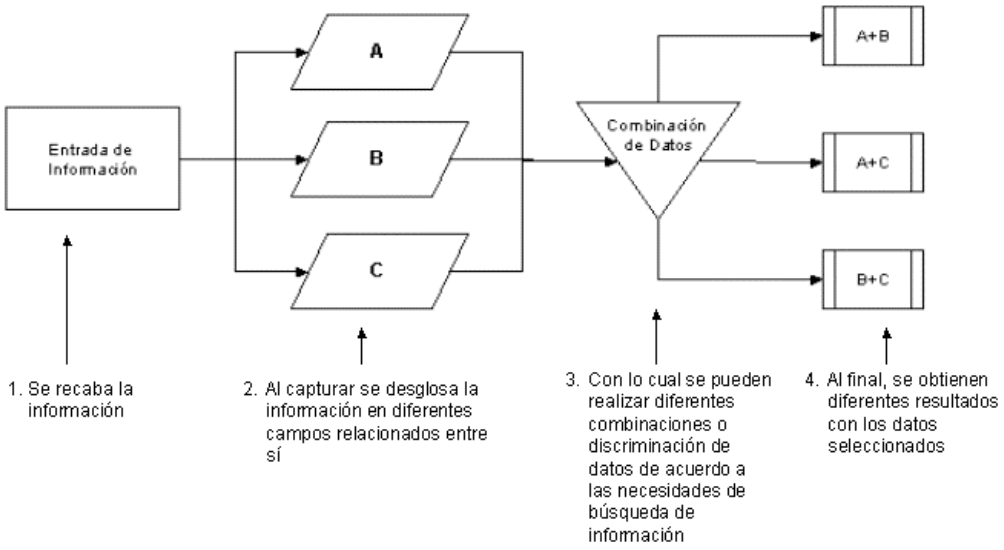
Debido a todas estas ventajas del manejo de las nuevas tecnologías, resulta de importancia entender que son y como funcionan, para que a partir de ello, la regulación que se desarrolle sea planteada de la mejor forma posible, algunas de estas tecnologías se explicarán a continuación.

[13] PICHARDO PAGAZA, Ignacio; *Modernización administrativa: Propuesta para una reforma inaplazable*. El Colegio Mexiquense, UNAM, Facultad de Ciencias Políticas y Sociales, México, 2004, Pag. 335-336.

1.1.3.1 Sistemas de Procesamiento de Datos

Principalmente se refiere a una clase de aplicaciones informáticas, cuya función es la organización de datos que en conjunto conforman diversos archivos que dan como resultado una información estructurada.

Las organizaciones utilizan estos sistemas para que, con la combinación debida de los datos, pueda obtenerse información tan variada como contabilidad, investigación de mercado, planificación y control, hasta el registro personal de todos sus colaboradores, que pudiera contener desde el nombre, hasta número de miembros de la familia, enfermedades, etcétera, a grandes rasgos, funcionan de la siguiente manera:



La estructura de estos sistemas, en realidad es simple, considerando que su objetivo principal es la entrada y salida de información, sin embargo, la parte medular de estos sistemas son los que logran identificar y combinar plenamente los datos que se obtienen y la eficacia con que se logra dicha estructura dará como resultado que el usuario obtenga la información adecuada con un sin fin de combinaciones posibles.

1.1.3.2 Filtros de Información

Son una herramienta utilizada para la selección de elementos dentro de una base de datos, con lo que el usuario logra extraer sólo la información necesaria. Pueden inclusive ayudar a crear subconjuntos del resultado de una consulta, de tal manera que las personas pueden discriminar información y llegar así a datos muy específicos[14].

En la actualidad dichos filtros los encontramos casi en cualquier programa de computación, desde un simple comando "buscar" en un procesador de palabras, hasta aquellos motores de búsqueda como Google, Yahoo!, etc., que ayudan a encontrar información dentro de Internet, inclusive existen organizaciones mundiales como *Dublín Core*[15] que buscan estandarizar la información contenida en los sitios web, para facilitar la búsqueda, distribución y administración de la información, lo cual es muy loable, sin embargo, sin la debida normatividad se podría caer en el uso y abuso de este tipo de herramientas.

1.1.3.3 Tecnología de Punta

Esta se refiere a toda aquella tecnología recientemente inventada y desarrollada, que coadyuva en la mejora de procesos, renovación o reemplazo de la tecnología existente; en muchas ocasiones, al principio esta puede salir al mercado a precios elevados, sin embargo, en la medida que se difunde, bajan los costos.

Por otro lado, la transferencia de tecnología, la cual es el intercambio de conocimientos y técnicas, ya sea de forma onerosa o gratuita, pone al alcance de los

[14] Para comprender mejor, en el caso de una base de datos con la información de 15,000 personas (nombres, fecha de nacimiento, edad, domicilio, etc.) un usuario que busca vender seguros de vida, puede realizar una primera consulta sobre rango de edad y de ese universo solicitar una nueva consulta sobre el domicilio, lo cual podría darle un grupo de personas con características especiales a los cuales ofrecerles el producto; de esta manera los filtros ayudan al solicitante a obtener sólo aquella información que le sea útil, por lo que los poseedores de la información deben llevar un control estricto de quien y cuando se realizan consultas y para que va a ser utilizada la información extraída.

[15] http://dublincore.org/ : 11/06/08: 22:27 hrs.

países menos desarrollados la posibilidad de utilizar estos medios para mejorar y economizar los procesos en sus actividades[16].

Hemos de señalar que en la Tecnología de punta se puede comprender el desarrollo de nuevos equipos (*hardware*) más pequeños, con mayor capacidad y uso más sencillo o aplicaciones más prácticas, así como el desarrollo o mejoramiento de programas de cómputo (*software*) que incorporan nuevas aplicaciones, más complejas y precisas.

1.1.4 Necesaria Regulación ante su uso Indiscriminado

Como hemos visto, la velocidad con la que se desarrollan las nuevas tecnologías de la información han envuelto a la sociedad de tal forma, que la vida actual no podría entenderse sin el uso de estas herramientas, sin embargo, también abre las puertas ha diferentes actos y hechos que deben ser normados para proteger las garantías de los individuos, ya que casi de manera imperceptible, sus derechos pueden ser vulnerados con facilidad, debido a que con acciones tan simples como contestar una encuesta en Internet o enviar un correo, sus datos personales son transmitidos, o bien, la información en los equipos de cómputo puede ser violada, por medio de programas como los llamados "*spyware*"[17] o dañada con los llamados virus informáticos[18].

---

[16] La Conferencia de las Naciones Unidas sobre Comercio y Desarrollo de 1990, define a la transferencia de tecnología como: "transferencia de conocimiento sistemático para la elaboración de un producto, la aplicación de un proceso o la prestación de un servicio".

[17] Los programas "*spyware*" son aplicaciones que recopilan información sobre una persona u organización sin su conocimiento. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en círculos legales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de *software*. Además pueden servir para enviar a los usuarios a sitios de Internet que tienen la imagen corporativa de otros, con el objetivo de obtener información sensible (En: http://es.wikipedia.org/wiki/Spyware : 04/09/08: 21:45 p.m.).

[18] Los virus informáticos, son programas que tienen por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Estos programas, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este; pueden destruir, de manera intencionada, los datos almacenados en un la computadora, aunque también existen otros

Todo esto se da con mayor facilidad al no existir una reglamentación completa y adecuada para limitar el uso de estas tecnologías, lo cual no significa atentar contra la libertad de las personas para acceder al conocimiento o información, si no más bien, evitar la comisión de delitos, violación de derechos de autor, transmisión indiscriminada de información o el mal uso de datos personales.

La tarea no es fácil debido a la falta de conocimiento y entendimiento de la materia informática por parte de la comunidad jurídica y a la constante aparición de nuevas formas de administrar la información a través de medios electrónicos, por lo que el Derecho actualmente se encuentra inmerso en crear la reglamentación necesaria para aspectos tales como:

- Validez legal de los documentos transferidos electrónicamente y régimen aplicable.
- Régimen de la publicidad, sanciones por su uso indebido.
- Infracción de marcas, como por ejemplo la titularidad de los "dominios" en Internet.
- Régimen de venta a distancia en lo que concierne a las normas que rigen las condiciones de oferta pública en la venta de productos y servicios.
- Violaciones al derecho a la imagen y a la vida privada, cuestiones de seguridad, criptografía y protección de datos, responsabilidad relativa a la difusión de información o de imágenes.
- Posibilidad de garantizar los derechos de propiedad intelectual de las obras publicadas en Internet[19].

---

más "benignos", que solo se caracterizan por ser molestos (En: http://es.wikipedia.org/wiki/Virus_inform%C3%A1tico : 04/09/08:21:51 p.m.)

[19] GRANERO, Horacio R. *El impacto de las nuevas tecnologías en el Derecho*. En: Universidad del Salvador, Instituto de Informática Jurídica. (http://www.salvador.edu.ar/ua1-4-hg.htm : 30/07/08 : 14:59 hrs.)

Sin considerar que el desarrollo acelerado va implicando la vida de los seres humanos de manera constante por lo que no debería sorprendernos que esta lista podría incrementarse.

Además dicha situación resulta aun más compleja debido a que la información que se encuentra en la red no tiene límite geográfico alguno por lo cual el uso inadecuado de la misma puede presentarse en un lugar o inclusive país distinto. De ahí la importancia de comenzar a establecer parámetros de regulación de la información los cuales podrían llegar a estandarizarse a nivel mundial.

1.2 Derecho a la Información

El Derecho a la información, es reconocido internacionalmente como un derecho fundamental del cual, se desprenden otros derechos tales como la libertad de expresión, derecho de la información, libertad de imprenta, etc., resumiéndose en tres aspectos principalmente: derecho a **buscar, recibir y difundir** información e ideas.

Recordando que la comunicación y el conocimiento han sido parte fundamental en el desarrollo del hombre de ahí, que no se pueda restringir de forma absoluta el intercambio de información.

1.2.1 Concepto de Derecho a la Información.

El artículo 19 de la Declaración Universal de los Derechos Humanos, establece:

> *"Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión".*

Este artículo es el fundamento del derecho de la información a nivel internacional y del cual, los diferentes países del mundo se han basado para la creación de los distintos mecanismos jurídicos relacionados con el derecho a la información, tales como transparencia, libertad de expresión, derecho de acceso a la información, derecho de la información, etcétera; de su interpretación, podemos definirlo como:

> *"El Derecho a la información son aquellas facultades de investigación, recepción y difusión que tiene como titular a la persona humana y no solo a periodistas y medios de información (como estos han querido interpretar), ya que esta cumple con una función social y se sitúa como objeto central de las relaciones jurídico informativas al calificar cada acto informativo como algo público"*[20].

Toda vez que se trata de un derecho que tiene como titular a la persona humana, sin limitante en razón de su profesión u ocupación, es un derecho general y universal lo cual nos hace considerarlo como un Derecho Humano, pero debemos entender que no es un derecho absoluto y que es precisamente la manera de regularlo en virtud de otro derecho, como es la intimidad que se desarrolla en el presente trabajo de investigación.

Es así como, *"lo público"* siempre será determinante en este derecho: desde el siglo XVIII con la Revolución Francesa se reconoció que todos los hombres tenían iguales derechos y posteriormente con las diferentes revoluciones liberales en el siglo XIX, surge la idea de que la difusión de la información es un derecho del hombre y una libertad que debe configurarse como el fundamento de un nuevo orden jurídico de la información, el cual se ha transformado y desarrollado junto con la sociedad, es así como la UNESCO en 1976, reconoció la evolución de este derecho:

---

[20] NAVARRO, Fidela. *Derecho a la información y Democracia en México*. En: http://www.mexicanadecomunicacion.com.mx/Tables/RMC/rmc87/derecho.html : 01/07/08 : 12:30 hrs.

> *"... Mientras la comunicación interpersonal fue la única forma de comunicación humana, el derecho a la libertad de opinión era el único derecho a la comunicación. Más adelante, con la invención de la imprenta se añadió el derecho de expresión. Y más tarde aún, a medida de que se desarrollaban los grandes medios de comunicación, el derecho a buscar, recibir e impartir información pasó a ser la preocupación principal. Desde este punto de vista, el orden de los derechos específicos enumerados en el artículo 19 de la Declaración Universal traza una progresión histórica: opinión, expresión, información"*[21].

Esto nos hace pensar, que la llegada de la era de la información vino a enseñarnos el poder y la importancia que esta tiene, por lo que la sociedad demanda constantemente ser partícipe en la generación de esta, naciendo así, un derivado de este derecho, conocido como **acceso a la información**, el cual tiene un fundamento político, por ser la salvaguarda y garantía del Estado Democrático y sirve como herramienta para combatir la corrupción ya que es el medio para que el gobernado pueda saber cómo y en qué actúa su gobierno y entonces poder exigir resultados, sin embargo, en el ámbito jurisdiccional significa garantizar el control de la generalidad de la ley y su justa aplicación, respondiendo así al respeto y protección de este derecho.

En México, el Instituto Federal de Acceso a la Información Pública, estableció dentro de su Marco Teórico Metodológico, el siguiente criterio que bien puede funcionar como concepto de acceso a la información:

> *"El acceso a la información es inevitablemente un producto del compromiso político. Sin embargo, éste entra a menudo en conflicto con la protección de secretos comerciales, la*

[21] Informe UNESCO 19 c/93 del 16 de agosto de 1976

> *privacidad personal, la seguridad nacional, la autonomía del Estado y poderosos intereses políticos y económicos. Los errores en el proceso de acceso a la información pueden tener altos costos, ya que si la revelación de información se hace de manera distorsionada o incompleta, se pueden causar malas interpretaciones, confusión o hasta pánico. Por ello, para ser efectivo como un instrumento de política pública, el acceso a la información requiere de un cuidadoso diseño y de un continuo seguimiento"*[22]*.*

De esta manera vemos la importancia del manejo cuidadoso de este derecho, puesto que al confluir con otros, fácilmente puede transgredirse la esfera jurídica de los individuos, o bien, el mal uso o abuso de este derecho, puede distorsionar completamente los fines para los cuales sirve, como es que el ciudadano conozca de manera certera el trabajo de sus gobernantes, con los límites que la misma ley impone tal como la protección de la información clasificada como sensible; de ahí la importancia de la emisión de criterios por parte del mencionado instituto para vigilar el cumplimiento de este.

Por otro lado, el acceso a la información, actualmente se ve vinculado constantemente con el **Derecho de la Información**, por ser complementarios, debido a que por un lado las personas buscan constantemente estar informadas y por otro, hacerse llegar de los medios necesarios para obtenerla, por lo que se puede entender como:

> *"La rama del derecho que tiene como objeto de estudio el conjunto de las normas jurídicas relativas al ejercicio, al alcance*

[22] INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN PÚBLICA. Marco teórico metodológico. IFAI, México, 2003, Pag. 15, En: http://www.ifai.org.mx/TemasTransparencia/#publicaciones :30/09/08: 0:45 hrs.

> *y a las limitaciones de las libertades de expresión e información por cualquier medio"*[23].

En la actualidad, el hambre de obtener información por parte de la sociedad la ha hecho partícipe activa en la forma que los gobiernos toman decisiones políticas, ya que hoy, cualquier político esta al pendiente de la opinión pública cada vez que emite algún comentario o bien, intenta reformar alguna ley, pero también nos ha enseñado que la mayoría de las personas no ha sabido manejar este derecho, cayendo en abusos que violan derechos de terceros, de ahí que las normas que los regulen deben establecer claramente los intereses legítimos que pudieran prevalecer sobre el Derecho a la Información, esto es, entender que se debe proteger la "Privacidad" de las personas, en lugar de pensar solo en la protección de "Archivos personales", ya que esto último es un concepto más limitado, por lo que el acceso debe ser negado en caso de existir un riesgo de dañar un interés legítimo[24], por lo que el peticionario deberá especificar lo más claro posible su solicitud.

Esa necesidad de protección y limitar el uso de información, principalmente de carácter personal ha dado lugar a lo que se conoce como el Derecho a la Intimidad, el cual actualmente en México, y a partir del contenido de la Ley Federal de Acceso a la Información Pública Gubernamental, sólo es obligatorio para los organismos estatales lo cual lo hace limitado e incompleto.

Derivado de lo anterior, podemos distinguir cada uno de los tres aspectos que engloba el Derecho a la Información, para poder definir un concepto de este:

> *"El Derecho a la Información es la garantía que tiene toda persona para obtener información, informar y ser informada, de*

[23] VILLANUEVA, Ernesto. *Temas selectos de derecho de la información*. UNAM, Instituto de Investigaciones Jurídicas. México. 2004. Pag.1

[24] MENDEL, Toby. *Consideraciones sobre el estado de las cosas a nivel mundial en materia de acceso a la información*. UNAM, Instituto de Investigaciones Jurídicas, México, En: Derecho Comparado de la Información, jul.-dic., 2006, Pag. 11

> *forma compatible con otros derechos humanos, engloba tanto libertades individuales como colectivas"*[25].

Reconociendo con este concepto, los límites que la propia sociedad debe reconocer para evitar la violación de otros derechos humanos que pudieran quedar involucrados en el momento de que se solicitara, difundiera o investigara cualquier tipo de información.

1.2.2 Objeto de Derecho a la Información

Como hemos visto, el Derecho a la información, busca principalmente garantizar el derecho que toda persona tiene de manejar y administrar cualquier tipo de información y tal como quedo explicado con anterioridad, contiene tres aspectos principalmente:

- *Derecho a atraerse información*, en el cual queda contemplado el acceso a los archivos, registros y documentos públicos y la decisión de qué medios se leen, escuchan o se contemplan.

- *Derecho a informar*, que incluye la libertad de expresión, de imprenta, constitución de sociedades y empresas informativas.

- *Derecho a ser informado*, lo cual significa recibir información objetiva, oportuna, universal, esto es, poder enterarse de todas las noticias de manera completa y sin exclusión alguna.

Esto es, considerando que uno de los principales objetivos de la sociedad internacional encabezada por la Organización de las Naciones Unidas a partir de la segunda guerra mundial, es la protección de los derechos humanos; en el caso de la

[25] NAVARRO, Fidela: *Derecho a la información y Democracia en México*. En: http://www.mexicanadecomunicacion.com.mx/Tables/RMC/rmc87/derecho.html : 01/07/08 : 12:30 hrs.

protección del derecho a la información, como se ha visto, se engloban distintos derechos en uno solo, lo que por una parte pudiera parecer que el sólo hecho de que los Estados promulguen los marcos jurídicos que garanticen el libre acceso a la información o libertad de expresión, por ejemplo, podría suponerse que este derecho fundamental, ha quedado protegido, sin embargo, existen otros derechos que convergen con este, tales como el derecho a la intimidad o vida privada, y el derecho al honor y la reputación; por ejemplo, aquella persona que desea saber cuanto gana un determinado funcionario público, esta en su derecho de que la entidad gubernamental le otorgue esa información, ¿pero que pasa con la información obtenida?, puede que el ciudadano solo la quiera para un trabajo de investigación por lo que le servirá como fin estadístico o de estudio, o bien, como no existen límites al uso de estos datos una vez otorgados, puede que sea utilizada para otros fines, desde comerciales hasta ilícitos.

Por lo tanto, en los casos en que convergen en un solo acto distintos derechos, deben considerarse los límites de estos a fin de evitar daños a terceros, tal y como se explico con anterioridad, por lo que en estos casos deberá aplicarse el principio de proporcionalidad para lograr obtener los beneficios debidos, teniendo como elementos básicos:

a) Existencia de una finalidad legítima y permitida expresamente por la Constitución y los tratados internacionales que forman parte del bloque de constitucionalidad de los derechos.

b) Existencia de idoneidad o utilidad de la restricción para la finalidad legítima exigida, la que debe ser de carácter legal.

c) Existencia de una estricta necesidad de restringir el ejercicio del derecho afectado, es decir, que no existe otro medio idóneo para alcanzar el fin que sea menos restrictivo respecto del derecho.

d) Determinación de que el daño que se provoca con la norma jurídica sea menor que el beneficio producido para el bien común. Cuya carga de la prueba recae en el órgano o autoridad competente que establece la restricción del ejercicio del derecho[26].

En el caso de México, los derechos que confluyen con el Derecho a la Información son los contenidos en los artículos 6° (en los casos de ataque a la moral, los derechos de tercero, provocación de algún delito o se perturbe el orden público), 7° (en lo concerniente al respeto a la vida privada, a la moral y a la paz pública), 3° (interpretado a *contrario sensu*, la educación no podrá favorecer los privilegios de razas, religión, grupos, sexos o individuos) y 130 (en actos de culto o en publicaciones de carácter religioso, los ministros religiosos no podrán oponerse a las leyes del país o sus instituciones) de la Constitución[27].

Sin embargo, a pesar de que constitucionalmente estos derechos son reconocidos y por ende, protegidos, en nuestro país, las normas existentes en materia de información no fueron creadas con una visión de conjunto y debido a esto, responden a intereses diversos que en muchas ocasiones llegan a conflictuar, es por ello, que el Derecho a la Información, toma relevancia pues será la que delimite la estructura y de coherencia a las normas existentes en materia de información.

Por último, esto no significa que este derecho deba ser fiscalizado a tal grado que resulte inoperante, si no que el marco jurídico debe garantizar su funcionalidad de modo tal de que sean ampliadas las libertades y a la vez que la interacción con otros derechos resulte armoniosa para asegurar la creación, pluralidad, difusión y acceso a la información así como la protección de los derechos de terceros, recordando que

[26] NOGUEIRA ALCALÁ, Humberto. *El Derecho a la Información en el ámbito del Derecho Constitucional comparado en Iberoamérica y Estados Unidos*. En: *Derecho a la Información y Derechos Humanos: Estudios en homenaje al maestro Mario de la Cueva* / coords. CARPIZO MCGREGOR, Jorge, CARBONELL, Miguel. UNAM, Instituto de Investigaciones Jurídicas, México, 2000, Pags.47-48

[27] LÓPEZ AYLLÓN, Sergio. El Derecho a la Información como derecho fundamental. En: *Derecho a la Información y Derechos Humanos: Estudios en homenaje al maestro Mario de la Cueva* / coords.

todo el conjunto de leyes existentes deben ser complementarias unas de otras con los límites que la propia constitución establece:

> *"Las Garantías Individuales no son derechos públicos subjetivos absolutos, pues su uso, restricción y suspensión, se arreglan a los casos y a las condiciones que establece la Constitución, dentro de los límites que la misma señala*[28]**"**

1.3 Derecho a la Intimidad

El reconocimiento del Derecho a la Intimidad tiene poco tiempo, ya que es hasta 1890, cuando Samuel D. Warren y Louis D. Brandeis, afirman que los cambios políticos, sociales y económicos obligan al derecho a evolucionar, debido a la injerencia de estos en la vida del hombre, por lo que el derecho a la vida encuentra un nuevo significado: el *derecho a disfrutar*, tal como el derecho a estar solo o el derecho a la libertad, el cual, conlleva a diferentes derechos civiles y al reconocimiento de los bienes tangibles e intangibles[29], siendo esto último materia esencial del derecho a la intimidad, entendiéndose por esto, todo aquello que la persona desea guardarse en su interior y que solo por medio de su voluntad puede ser dado a conocer.

De ahí que toda persona tenga la posibilidad, que debe ser protegida por el Derecho, de mantener parte de su personalidad, que se refleja en ciertos datos e información, en secreto y bajo su resguardo personal.

CARPIZO MCGREGOR, Jorge, CARBONELL, Miguel. UNAM, Instituto de Investigaciones Jurídicas, México, 2000, Pag. 170

[28] Semanario Judicial de la Federación, Quinta Época, Tercera Sala, t. LXXIV, p. 2536 : *IUS:351635*

[29] WARREN, Samuel D. y BRANDEIS, Louis D. *The right to privacy*. En: Harvard Law Review, Vol. IV, no. 5, December 15, 1890. (http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html; 20/08/08: 11:54 a.m.)

1.3.1 Concepto de Derecho a la Intimidad

Debido a los cambios constantes en la sociedad, la protección de los derechos humanos, se ha visto obligada a evolucionar de igual forma, es así, que tenemos por ejemplo, que en sus inicios durante la Revolución Francesa, se exigía el reconocimiento de la igualdad del hombre y en la actualidad, se exige el respeto a la individualidad de cada persona, esto es, las tres primeras generaciones de los derechos humanos, hacen referencia a este como miembro de la sociedad y a partir de la cuarta generación[30], el reconocimiento del hombre, como ser único e irrepetible.

Es a partir de esto, que entra el Derecho a la Intimidad, el cual, podemos definirlo como:

> *"Derecho del individuo de decidir por si mismo en que medida compartirá con otros sus pensamientos, sentimientos y los hechos de su vida privada[31], por lo que se reconoce como un derecho humano fundamental por virtud del cual se tiene la facultad de excluir o negar a las demás personas del conocimiento de ciertos aspectos de la vida de cada persona que sólo a ésta le incumben. Este derecho comprende y se vincula a su vez con varios derechos específicos que tienden a evitar intromisiones extrañas o injerencias externas en estas áreas reservadas del ser humano, tales como la inviolabilidad del domicilio, correspondencia, comunicaciones privadas, derecho a la propia imagen, honor, privacidad informática, a no*

[30] A pesar de los estudios que se realizan actualmente para comprobar la existencia de las nuevas generaciones de derechos humanos, su contenido aún no es claro y no existen propuestas claras, sin embargo, podemos esperar a que en un futuro dichos estudios puedan aterrizar y clarificar la existencia de estos y por lo tanto, exigir su protección; entre ellos se encuentran el derecho a la intimidad y la protección de los datos personales.

[31] http://www.uasnet.mx/derecho/info3.html : 28/08/08: 09:18 a.m.

participar en la vida colectiva, a aislarse voluntariamente y a no ser molestado[32]*"*

Ya Warren y Brandeis, en su artículo "*The Right to Privacy*", publicado en 1890, hacían hincapié en lo importante que era reconocer la individualidad de las personas y el respeto a estas, poniendo como ejemplo la simple toma de una fotografía y su publicación en un periódico sin el permiso expreso de las mismas, así como también la libertad de cada quien de tener pensamientos, escribirlos y de publicarlos, sólo si esa era su *voluntad*, por lo que nadie tendría derecho a acceder a estos si el autor no lo aceptará, estas conclusiones viéndolas en retrospectiva, sirven como base para la protección de asuntos tales como el derecho de expresión, derechos de autor, derecho a la vida privada, acceso a la información, transparencia, etcétera.

Aquí lo importante, sería entender a que nos referimos con intimidad, para que, a partir de este concepto, podamos entender y desprender su importancia en la vida privada de las personas, es así como por ejemplo, el diccionario de la Real Academia Española, define a la palabra íntimo, *"como aquello que viene de lo más interior o interno y relativo a la intimidad"*, e intimidad como la *"Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia"*[33] , por lo que, derivado de esto se puede entender que si la parte más íntima de un ser humano como sus pensamientos o sentimientos, están conectados a hechos o personas de su alrededor como la familia, costumbres o conocimientos y estos a su vez, se derivan en otras cosas como datos de domicilio, lugar de trabajo, capacidad económica, etcétera, por ende, deben ser respetados y protegidos, siendo el Estado quien debe realizar esta tutela y exigir su protección frente a cualquier otra persona, ya sea física o moral, para que el individuo sepa que la sociedad tiene ciertos límites de acercamientos hacía su persona y por ende sienta que su vida privada le

[32] INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN PÚBLICA. Marco teórico metodológico. IFAI, México, 2003, Pag. 17, En: http://www.ifai.org.mx/TemasTransparencia/#publicaciones :30/09/08: 0:45 hrs

[33] http://www.rae.es/rae.html: 28/08/2008: 15:05 p.m.

pertenece y sólo en caso necesario y por medio de su *voluntad*, esa información pueda darse a conocer y no al revés, tal y como sucede en la actualidad.

1.3.2 Objeto del Derecho a la Intimidad

En la actualidad, y a pesar de los años transcurridos, esta línea tan delgada que separa la vida íntima del hombre, con el derecho de la información de la sociedad, se encuentra en conflicto, debido a que por un lado las personas exigen que la información puesta a su disposición, sea lo más amplia posible, sin que muchas veces sea considerada la afectación que esta pudiera tener hacia terceras personas, o respecto del titular de esa información.

Si bien es cierto, que en el caso de México, el Estado tiene límites respecto a los alcances del Derecho a la Información, para proteger datos sensibles de las personas o del propio Estado, también lo es, que entre particulares no existe limitación alguna respecto a la obtención y manejo de información íntima de una persona, basta con ver las noticias en que se cuestiona si cierta persona pública se encuentra relacionado íntimamente con alguien más, o si algún familiar tiene cierta enfermedad, para que la intimidad de esa persona sea violada, por lo que, aspectos de su vida privada son quebrantados en contra de su voluntad, y siendo objetivos, dicha información no causa afectación alguna a la sociedad, por lo que el Derecho a la información supera el derecho del individuo, dejando a este en desequilibrio en comparación a otros.

Ahora bien, esto podemos dimensionarlo en cuanto al uso de las nuevas tecnologías, ya que como quedo explicado anteriormente, estas facilitan a la sociedad a transmitir información en poco tiempo, de ahí la importancia de someter la información sensible a los controles necesarios para evitar la afectación de la persona en su vida privada, y sea el individuo el que decida quien, como y cuando alguien más va a conocer estos aspectos de su vida.

1.4 Derecho a la Protección de Datos Personales

La transmisión de datos ha través de las fronteras hoy es posible gracias al desarrollo de la informática, sin embargo, día a día los países se ven obligados a crear los marcos jurídicos necesarios con el fin de garantizar la protección del Derecho a la Intimidad y evitar el registro ilegal de datos personales, datos inexactos o bien, el acceso y uso indiscriminado de estos.

En 1967, el Consejo de Europa constituyó una Comisión Consultiva con el fin de realizar investigaciones en torno a las nuevas tecnologías de la información y su posible agresividad hacia los derechos de las personas, dando como resultado en 1968 la Resolución 509, sobre "los derechos humanos y los nuevos logros científicos y tecnológicos", conocido posteriormente como "protección de datos personales"[34], más tarde, en 1980 y después de diferentes estudios y convenciones en torno a la protección y transmisión de datos personales, la OECD (Organización para la Cooperación y Desarrollo Económico, por sus siglas en inglés) desarrolla la "*Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[35]", la cual fue presentada en forma de recomendación a los países miembros, con el fin de que se crearán las normas necesarias para asegurar la protección de los datos personales y a su vez facilitar el flujo de información, ya que se reconoce por un lado, la importancia de proteger los derechos fundamentales y por otro, que esta información, contribuye al desarrollo social y económico de los países.

1.4.1 Concepto de Derecho a la Protección de Datos Personales

La privacidad de las personas es un derecho fundamental reconocido hoy en día, y abarca naturalmente, la información que las identifica, o que versa sobre sus

[34] GARCÍA-GONZÁLEZ, Aristeo. *La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado*. UNAM, Instituto de Investigaciones Jurídicas, México, En: Boletín Mexicano de Derecho Comparado, Nueva Serie, Año XL, número 120, sept.-dic., 2007, Pag. 754

[35] "Directrices sobre la protección de la privacidad y el flujo transfronterizo de datos personales" (http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html :29/08/2008:11:28 a.m.)

características o preferencias, es decir, todo aquello que permita identificarlo y conocer sobre su personalidad, vida y familia. En términos generales, estos datos son los que suelen llamarse "personales", pues por su propia definición y naturaleza corresponden e identifican a su titular, ahora bien, la privacidad en cuanto a datos personales es congruente con el desarrollo económico cuando la regulación además de protegerlos, contempla el surgimiento de las sociedades de información[36], por lo tanto es necesario ampliar su ámbito de protección.

Para comprender los límites que deben establecerse en esta regulación, habrá que entender primeramente a que nos referimos con datos personales:

> *"Los datos personales se definen como toda información sobre una persona física identificada o identificable sobre sus características físicas, fisiológicas, psíquicas, económicas, culturales o sociales"*[37]

Por lo que, cualquier dato existente sobre una persona manejado sin el debido cuidado puede arrojar la información suficiente, a modo tal de dejar a la luz pública su vida privada[38], esto es, la intimidad vista como una disciplina jurídica ha perdido su carácter exclusivo individual y privado, para asumir progresivamente un significado público y colectivo a consecuencia de la revolución tecnológica[39] debido a que la informática se ha convertido en el símbolo emblemático de la cultura actual, basta con leer declaraciones como la de Eduardo Arcos, director del *blog ALT140*: *"Estamos haciendo un cambio hacia una generación transparente, que todo el tiempo quiere y desea plasmar su vida en línea para que sea pública (con cierto control ejercido por ellos), publicar fotos de los lugares donde se divierten, mostrar qué*

[36] VILLAR, Rafael, DÍAZ DE LEÓN, Alejandro y GIL HUBERT, Johanna. *Regulación de Protección de Datos y de Sociedades de Información: Una comparación de países seleccionados de América Latina, los Estados Unidos, Canadá y la Unión Europea*. Banco de México, México, En: Documento de Investigación número 2001-07, 2001, Pag. 11.
[37] *Idem*, Pag. 1
[38] *Vid Supra*, 1.1.3.2 Filtros de información. Pag. 14

hacen y dar a conocer su geolocalización en tiempo casi real. Eso no les ha causado ningún problema; todo lo contrario, son más sociales" [40]; afirmaciones como esta, podrían hacernos pensar que las personas mismas son las que provocan la violación de la privacidad de sus datos personales, pero tal y como se explicó en el punto anterior, el individuo sólo a través de su *voluntad* es quien debe decidir quién, como y cuando se accede a esta información, por lo que, su derecho a la intimidad debe ser reconocido y por lo tanto, cualquier acceso a esta información sin el consentimiento de la persona, puede considerarse violatorio.

Por lo que derivado de lo anterior, debemos señalar entonces, la importancia que tiene la protección y manejo de los datos personales para que estos sólo sean utilizados por las personas y para los fines autorizados, por lo que pasaremos al análisis del concepto de este nuevo derecho:

> *"La protección de los datos personales es aquella parte de la legislación que protege el derecho fundamental de la libertad, en particular el derecho individual a la intimidad, respecto del procesamiento manual o automático de datos"*[41]

Esto es, la protección de datos personales concede derechos a los individuos respecto a la información recabada y que es objeto de tratamiento automatizado, como el exigir la existencia de los controles adecuados para evitar que sea vulnerada su libertad y dignidad, e impone obligaciones a todos aquellos que controlan y tienen acceso a las bases de datos[42], cabe aclarar que la recolección de información de los individuos en si, no representa un peligro, si no mas bien que estos pierdan la

[39] GARCÍA-GONZÁLEZ, Aristeo. *La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado*. UNAM, Instituto de Investigaciones Jurídicas, México, En: Boletín Mexicano de Derecho Comparado, Nueva Serie, Año XL, número 120, sept.-dic., 2007, Pag. 750
[40] MICHEL, Víctor Hugo. *Cibernautas soslayan las advertencias del peligro*. En: Milenio: Diario, año 9, número 3174, 8: sept., 2008, Pag.39.
[41] HONDIUS, F.W. *A decade of international data protection*. NILR, vol.30, núm.2, 1983, Pag. 105, citado en: GARCÍA-GONZÁLEZ, Aristeo: *La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado*. UNAM, Instituto de Investigaciones Jurídicas, México, En: Boletín Mexicano de Derecho Comparado, Nueva Serie, Año XL, número 120, sept.-dic., 2007, Pag. 761
[42] *Idem*, Pag. 762

capacidad de disponer de esta información y decidir sobre el manejo que de esta se de, lo cual significa que los sujetos tengan la libertad de elección sobre la revelación y transmisión de la información, por lo tanto, todo organismo, ya sea público o privado que tenga en su poder bases de datos con información de personas físicas deberá preguntar a estas si es posible su utilización para fines distintos a aquellos por los cuales se obtuvieron en un principio.

Pero, por otro lado, también debemos considerar que esto no representa que el individuo tenga absoluta soberanía sobre sus datos personales, ya que así como los organismos arriba mencionados deben tener límites en el manejo y administración de la información, también el individuo tendrá ciertos límites en la protección de estos datos, por el sólo hecho de ser parte de una sociedad en la que la comunicación y la información resultan imprescindibles, ya sea para fines estadísticos, de planeación, control o desarrollo, aquí puede citarse como ejemplo, los criterios sustentados por el Comité de Acceso a la Información de la Suprema Corte de Justicia de la Nación:

> ***Criterio 01/2003***
>
> ***INGRESOS DE LOS SERVIDORES PÚBLICOS. CONSTITUYEN INFORMACIÓN PÚBLICA AUN CUANDO SU DIFUSIÓN PUEDE AFECTAR LA VIDA O LA SEGURIDAD DE AQUÉLLOS****.*
>
> *Si bien el artículo 13, fracción IV, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental establece que debe clasificarse como información confidencial la que conste en expedientes administrativos cuya difusión pueda poner en riesgo la vida, la seguridad o la salud de cualquier persona, debe reconocerse que aun cuando en ese supuesto podría encuadrar la relativa a las percepciones ordinarias y extraordinarias de los servidores*

> *públicos, ello no obsta para reconocer que el legislador estableció en el artículo 7º de ese mismo ordenamiento que la referida información, como una obligación de transparencia, debe publicarse en medios remotos o locales de comunicación electrónica, lo que se sustenta en el hecho de que el monto de todos los ingresos que recibe un servidor público por desarrollar las labores que les son encomendadas con motivo del desempeño del cargo respectivo, constituyen información pública, en tanto que se trata de erogaciones que realiza un órgano del Estado con base en los recursos que encuentran su origen, en mayor medida, en las contribuciones aportadas por los gobernados.*

Ahora bien, lo establecido en el artículo 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, permite que cada ente de gobierno instaure sus propios criterios para el acceso a la información; en el criterio sostenido por el mencionado Comité, el artículo 7° fracciones III y IV de la ley antes mencionada, no es indicativo de relacionar los datos personales de los servidores públicos con la remuneración económica que por sus servicios recibe, por lo que no debería ser considerado otorgar dicha información a los particulares y por lo tanto, tampoco se contravendría con lo establecido en el artículo 13, fracción IV, de la misma ley, veamos pues el siguiente criterio:

> ***Criterio 02/2003***
>
> ***INGRESOS DE LOS SERVIDORES PÚBLICOS. SON INFORMACIÓN PÚBLICA AUN CUANDO CONSTITUYEN DATOS PERSONALES QUE SE REFIEREN AL PATRIMONIO DE AQUÉLLOS.***

> *De la interpretación sistemática de lo previsto en los artículos 3º, fracción II; 7º; 9º y 18, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental se advierte que no constituye información confidencial la relativa a los ingresos que reciben los servidores públicos, ya que aun cuando se trata de datos personales relativos a su patrimonio, para su difusión no se requiere del consentimiento de aquellos, lo que deriva del hecho de que en términos de lo previsto en el citado ordenamiento deben ponerse a disposición del público a través de medios remotos o locales de comunicación electrónica, tanto el directorio de servidores públicos como las remuneraciones mensuales por puesto, incluso el sistema de compensación.*[43]

En este otro criterio, también se establece que el acceso a la información puede quedar sobre los derechos del individuo, a pesar que la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en su artículo 13, fracción IV, establece un equilibrio entre la protección de datos personales y el derecho a la información, aunque analizando detenidamente este criterio, solo se refiere a la difusión de los catálogos de remuneración por puesto y directorio de funcionarios.

Ahora bien, a nuestro parecer dichos criterios resultan excesivos, ya que como se menciono anteriormente[44], una vez obtenida información como la descrita arriba, no hay nada que asegure que esta pueda ser utilizada para un fin ilícito, pero es esto el punto fino de la regulación del manejo de la información personal, los límites tanto del individuo como del organismo para su obtención, manejo y administración.

[43] http://www.scjn.gob.mx/NR/rdonlyres/A8070BE8-07B2-45E3-A53C-036F1CD07D46/0/Principales_Criterios_CAI_06_06_2008.pdf : 08/09/2008 :11:10 a.m.
[44] *Vid Supra*, 1.2.2. Objeto de Derecho a la Información. Pag. 22

1.4.2 Objeto de Derecho a la Protección de Datos Personales.

La protección de los datos personales, como hemos visto, debe ser regulada para asegurar que por un lado tutele el derecho de la intimidad y por otro, que permita el libre flujo de información, lo cual significa que para su regulación, deben quedar bien definidos conceptos tales como “datos personales”, “sistema de aplicación de datos personales” y “datos sensibles” con el objeto de que al quedar claro el por qué de su existencia e importancia se puedan mejorar las reglas que sobre el procesamiento de los datos existan, para que su aplicación sea más práctica y por ende, encontrar un balance entre los intereses de los individuos que proporcionan los datos personales y los organismos (públicos o privados) controladores de datos, con el fin de que sean revisadas las reglas actuales relacionadas con la transferencia de información a terceros países y establecer criterios más simples y flexibles.

Para lograr dicho equilibrio, en algunos países, se ha establecido el *Habeas Data*, el cual es un recurso a disposición de los individuos[45] que contempla cinco objetivos principales[46]:

1. El acceso del individuo a la información que exista de sí mismo en cualquier registro o banco de datos.

2. Actualización de datos atrasados.

3. Rectificación de datos inexactos.

[45] La expresión latina *habeas data* sirve para calificar un derecho de fin de siglo de la informática: *habeas* segunda persona del subconjuntivo *habeo ... habere*, que significa “conserva tu posesión” que es una de las acepciones del verbo y *Data* es el acusativo plural de *Datum* que los diccionarios lo definen como representación de hechos, conceptos o instrucciones de manera apropiada para su comunicación y procesamiento por medios automáticos; es decir, conservar los registros o datos. En: OTÓN SIDOU, J.M. *Las nuevas figuras del derecho procesal constitucional brasileño: mandado de injuncao y habeas data*. UNAM, Instituto de Investigaciones Jurídicas, México, En: Boletín Mexicano de Derecho Comparado, Nueva Serie Año XXIV, número 70, ene.-abr., 1991, Pags.169-187

[46] http://www.aaba.org.ar/bi130019.htm; 27/01/08 : 09:47 p.m.

4. Confidencialidad de cierta información legalmente obtenida para evitar su conocimiento por terceros.

5. Supresión del registro de información sensible, tal como vida privada, ideas políticas, religión o gremial.

De lo anterior, se desprenden diversos criterios existentes en la manera de legislar sobre este tema, por ejemplo, en Europa, la protección de los datos personales es considerado un tema prioritario de materia legislativa, ya que buscan proteger a los ciudadanos en el momento en que estos proporcionan información personal a organismos públicos o privados que se encuentren físicamente en el continente europeo o que tengan sus servidores fuera de este, esto es, restringen el uso de los datos personales para proteger en mayor medida la intimidad de las personas; mientras tanto, tenemos a los Estados Unidos de América en donde las empresas son quienes regulan las políticas de protección de datos y flujo de información, debido a que reconocen que estos mecanismos fomentan y reactivan las inversiones del sector de las tecnologías de la información y sobre todo, permiten que las empresas puedan realizar actividades de comercio electrónico en todos los niveles, lo cual significa que dan prioridad al aspecto económico sobre la privacidad de los individuos[47].

Visto lo anterior, se comprende la importancia de la regulación de la protección de datos personales, ya que al no existir un marco regulatorio que abarque esta protección tanto del sector público como del privado se puede tener como consecuencia:

a) La comercialización y tráfico indiscriminado que realizan empresas dedicadas a la especulación de datos personales.

[47] VELASCO SAN MARTÍN, Cristos. *Privacidad y protección de datos personales en Internet ¿Es necesario contar con una regulación específica en México?*. Instituto Nacional de Estadística Geografía e Informática, México, En: Boletín de Política Informática, número 1, 2003, Pags.1-12

b) Que los titulares de esos datos se encuentren en estado de indefensión ante tal situación, al no poder ejercer sus derechos de acceso y corrección al no ser informados sobre las bases de datos que existen y su finalidad.

c) Que los titulares de esos datos lleguen a ser discriminados o ver disminuidos otros derechos con el mal uso de la información.

d) Que el Estado no pueda garantizar la protección de datos personales a cualquier individuo.[48]

Por lo que la legislación que sea creada con el fin de dar protección a los datos personales deberá contemplar cuatro principios[49]:

1. La persona tiene derecho al acceso de sus datos personales, no importando el soporte en que esta se encuentre, o quien lo tenga.

2. La persona tiene derecho a conocer y controlar la transmisión de la información de sus datos personales, en medida de la afectación que pudiera existir.

3. La legislación deberá garantizar en relación al derecho a la intimidad:

a) El tiempo que dure la conservación de los datos personales.
b) Determinar los fines que persigue la creación de la base de datos.
c) Prohibir la revelación de datos personales sin el consentimiento de su titular, así como también garantizar la veracidad, actualización e integridad.

[48] GÓMEZ-ROBLEDO VERDUZCO, Alonso, ORNELAS NÚÑEZ, Lina. *Protección de datos personales en México: El caso del Poder Ejecutivo Federal.* UNAM, Instituto de Investigaciones Jurídicas, México, 2006, Pag. 29
[49] *Idem*. Pags. 12-13

4. Que los tratados internacionales suscritos contemplen la protección y la forma en que serán transmitidos los datos personales.

Todo ello con vista a buscar un equilibrio entre el derecho a la intimidad y la protección de los datos personales con el flujo de información que garantice el desarrollo económico del país.

Como hemos visto, el desarrollo tecnológico ha superado en muchos aspectos al derecho, debido a que muchos actos que se desarrollaban de manera personal, hoy en día son virtuales, lo que ha propiciado que los individuos deban dar a conocer aspectos de su vida privada para poder realizarlos, dichos aspectos quedan almacenados en bases de datos, las cuales son capaces de administrar una enorme cantidad de información en segundos, lo cual, ayuda a optimizar los recursos dentro de organizaciones tanto públicas como privadas, y es ahí donde encontramos la problemática expuesta en este trabajo de investigación: ¿Cómo establecer un marco normativo acorde a la sociedad actual que por un lado esta deseosa de transmitir información, realizar actos a través del uso de la informática y por otro, que no sean vulnerados sus derechos fundamentales?

La respuesta quizá no sea fácil, debido a que en la actualidad el uso de la informática ha demostrado no tener límites y su desarrollo permite que los usuarios puedan establecer diversas formas de obtener, crear, administrar y compartir información y en muchas ocasiones al poder ser realizadas de manera individual quedan al margen del conocimiento de la sociedad, sin embargo, si pueden crearse recursos jurídicos que coadyuven a que los individuos puedan tener la certeza que sus datos personales serán utilizados **sólo para aquellos fines para los cuales fueron otorgados**, e inclusive si es su voluntad que sean corregidos o eliminados.

En la actualidad diversos países en el mundo han realizado grandes avances en la creación de normas capaces de dar esta certeza, tenemos por ejemplo, a la República Alemana con estrictos controles de datos personales y reconocido el

derecho de la autodeterminación informativa, lo cual significa que sólo las personas pueden decidir quien, como y cuando van a ser utilizados sus datos personales y sólo el Estado puede utilizarlos para fines estadísticos o de planeación, o también como ejemplo podemos tomar el caso de los Estados Unidos de América, en los cuales se reconoce la *privacy* como un elemento de la vida de las personas que debe ser respetada, pero sin embargo, el desarrollo económico siempre estará por encima de esto, debido a que es más importante el flujo de la información con fines económicos y políticos que se reflejan en un beneficio social que la protección de una sola persona, motivo por el cual, a diferencia de Alemania, la transmisión de datos personales no encuentra tantas limitantes.

En el caso de México, existen tres iniciativas de Ley para la protección de datos personales a nivel federal, pero que se encuentran suspendidas en el Congreso y sólo de manera local estados como el de Colima y Guanajuato tienen leyes de protección de datos personales basadas en la legislación española, por lo que resulta importante realizar un estudio de derecho comparado con países afines a nuestra realidad y con aquellos países promotores en la protección de datos personales.

CAPÍTULO II. DERECHO COMPARADO

El Derecho Comparado es la disciplina que se encarga del estudio y análisis de los distintos sistemas jurídicos con el fin de encontrar los elementos comunes y obtener los mecanismos suficientes para realizar una interpretación histórica, crítica, política, y social, para que a partir de este conocimiento puedan realizarse proyectos que permitan crear o mejorar las normas de un país determinado.

De ahí la importancia de este conocimiento, pues permite a cualquier país beneficiarse de la experiencia de otros para utilizar o mejorar las fórmulas ya aplicadas para la solución de problemas jurídicos en específico, que en muchas ocasiones, no son exclusivos de un lugar; pero esto no debe suponer que el legislador haga a un lado las características sociales, políticas e históricas del país al que sirve, sino al contrario, a partir del conocimiento de estas, crear las normas necesarias tomando como base la experiencia de los demás[50].

Es por ello, que en este capítulo, se estudiará la legislación existente en materia de protección de datos personales en cuatro diferentes países, lo que nos servirá para conocer las distintas políticas que de esta materia existen: desde aquélla que esta totalmente a favor de la intimidad de las personas, hasta aquélla en que la transferencia de información esta sobre el derecho individual de las mismas, pasando por las legislaciones que se encuentran en la vanguardia y que buscan un equilibrio entre la transferencia de la información y la protección de la vida privada de los individuos; lo que nos ayudará a entender el manejo que de esta información debe darse en la actualidad en nuestro país, para que por un lado la propuesta de legislación que se haga cumpla con los estándares aplicados a nivel internacional, lo que daría por consecuencia el cumplimiento de los diferentes instrumentos signados por nuestro país en la protección de Derechos Humanos y por otro, a las características particulares de nuestro entorno social.

---

[50] DE PINA, Rafael y DE PINA VARA, Rafael: *Diccionario de Derecho*. – Porrúa: México, 2003. Pags. 230-232

2.1. Francia

2.1.1. Antecedentes

En 1974, se dio a conocer el proyecto gubernamental conocido como SAFARI, con el objetivo de identificar a cada ciudadano por medio de un número, que a su vez, podría interconectar todas aquellas bases de datos personales existentes, este proyecto creó diversas opiniones entre el público, debido a que se destacaba por un lado, el mal uso que pudiera darse a la informática y por otro, el fichaje de cada uno de los individuos capaz de identificarlos de manera particular. Estas inquietudes obligaron al gobierno francés a crear una comisión con el fin de proponer medidas que garantizaran que el desarrollo de la informática se realizaría en cumplimiento y protección de la vida privada, libertades individuales y públicas[51].

Es así, como se crea a partir de las propuestas dadas por esta comisión, la ley número 78-17 de 6 de enero de 1978, denominada "Ley de Informática, ficheros y libertades", la cual constituye una referencia en materia de protección de datos personales en toda Europa[52], cabe destacar que a partir de esta ley, fue creada la **Comisión Nacional de Informática y Libertades** (más adelante CNIL), la cual es una autoridad administrativa e independiente que tiene como objetivo primordial velar que la informática este al servicio del ciudadano y que no afecte la identidad humana, vida privada ni a las libertades individuales o públicas, en cumplimiento de esta ley[53].

Posteriormente, con el convenio del Consejo de Europa de 28 de enero de 1981 y la directiva 95/46 de 24 de octubre de 1995, se dieron las primeras directrices en materia de protección de datos personales en Europa, siendo la última, texto fundador de la legislación europea actual, la cual cada Estado miembro debió trasladar a su legislación nacional, por lo que Francia tuvo que actualizar y realizar una reforma profunda a su legislación, por lo que el 6 de agosto de 2004, se

[51] http://www.cnil.fr/index.php?id=36 : 21/09/2008: 21:49 hrs.
[52] BAZÁN, Victor: *El Habeas Data, el derecho a la autodeterminación informativa y la superación del concepto preinformático de la intimidad*. -- UNAM, Instituto de Investigaciones Jurídicas: México. -- En: Boletín Mexicano de Derecho Comparado. -- Nueva Serie Año XXXI, número 94, ene.-abr., 1999. pp. 27-28.
[53] La CNIL en bref. – En: www.cnil.fr : 18/09/2008: 21:06 hrs.

publicaron dichas reformas, siendo este país el último en publicarlas, debido al hecho de que aprovechó todas las opciones abiertas por la directiva para transformar su manera de enfocar la protección de los datos personales y de poner en práctica sus principios.

Entre los aspectos más destacables están:

- La responsabilidad de las empresas en la aplicación de la ley (reconocimiento del interés de la autorregulación)

- La responsabilidad de los ciudadanos en la protección de sus derechos.

- La posibilidad de simplificación y exoneración de las notificaciones, incluso en caso de designación de un "encargado de protección de los datos personales"

- La evolución mayor que se tiene de subrayar que se da un equilibrio entre el control previo de la creación de los tratamientos, que siempre ha sido el modo de acción privilegiado de la CNIL, y el control a *posteriori*, especialmente a través de la instrucción de las quejas, las inspecciones y algo totalmente nuevo: **el ejercicio de la potestad sancionadora**[54].

2.1.2. La Ley Francesa de Protección de Datos de Carácter Personal.

Como se explicó anteriormente, esta Ley es pionera en su tipo, su objeto principal es la protección a la vida privada de las personas[55] y vigilar que el uso de las nuevas tecnologías estén al servicio de la sociedad, entre los derechos en materia de informática y libertades que reconoce, se encuentran:

[54] http://www.cnil.fr : 22/09/2008: 22:18 hrs

[55] En la Constitución Francesa de 1958, no se menciona específicamente el Derecho a la Intimidad o el Derecho a la Protección de Datos Personales, sin embargo, este cuenta con un reconocimiento legal, y considerando que esta constitución toma como preámbulo los principios de la de 1946, que a su vez completó los derechos y libertades de la Declaración de los Derechos del Hombre y del Ciudadano de 1789, podemos considerar entonces, que el principio clave para este Derecho pudiera ser: *la Nación deberá proporcionar al individuo y a la familia las condiciones necesarias para su desarrollo.*

- *Derecho a la información*. Cualquier persona puede dirigirse directamente a un organismo para saber si está fichada o no.

- *Derecho de acceso*. Cualquier persona puede, de manera gratuita, con tan sólo dirigirse al organismo implicado, tener acceso a toda la información que haga referencia a si misma de una manera accesible (debiendo explicitarse los códigos) pudiendo obtener una copia, previo pago, en el caso de generarse algún gasto en concepto de reproducción.

- *Derecho de rectificación y de cancelación*. Cualquier persona puede solicitar directamente a un organismo, que tenga en sus ficheros alguna información relacionada con la misma, que dicha información sea rectificada, completada o aclarada, actualizada o borrada.

- *Derecho de oposición*. Cualquier persona puede oponerse a que se haga uso con fines publicitarios de la información que la concierne o que dicha información se utilice para tareas de prospección comercial o bien oponerse a que esta se ceda a terceros con tales fines.

Las personas implicadas deberán poder ejercer su derecho de oposición a la cesión de sus datos a terceros desde el proceso de obtención de datos.

El uso de llamadas telefónicas automatizadas, faxes o correos electrónicos con fines publicitarios estará prohibido cuando las personas no lo hayan autorizado previamente.

- *Derecho de acceso indirecto*. Cualquier persona puede solicitar a la CNIL para que lleve a cabo comprobaciones de las informaciones relacionadas con si misma y que puedan eventualmente quedar registradas en ficheros que afecten la seguridad del Estado, la defensa o la seguridad pública (derecho de acceso indirecto). La CNIL se encarga de comprobar la pertinencia, la

exactitud y la actualización de estas informaciones, pudiendo solicitar su rectificación o su eliminación.

Con el acuerdo del responsable del tratamiento, las informaciones relacionadas con una persona podrán ser comunicadas a la misma[56].

Como podemos ver, la ley crea los canales necesarios para que los individuos conozcan quien y para que utilizan sus datos personales, así como también, les da la libertad de permitir o restringir el uso de estos para otros fines para los cuales fueron obtenidos y garantiza el acceso a estos cuando los responsables de las bases de datos lo niegan, ahora bien, así como esta ley reconoce los derechos de las personas en cuanto a la protección de sus datos, también deja instauradas las obligaciones de los responsables de la información:

- Notificar a la CNIL la realización de la base de datos y sus características, con excepción de los casos previstos por la ley o por la CNIL.

- Hacer que las personas implicadas puedan ejercer sus derechos recibiendo información al respecto.

- Garantizar la seguridad y la confidencialidad de la información con el objetivo de que éstas no se tergiversen o se pongan en conocimiento de terceros no autorizados.

- Someterse a los controles y comprobaciones que lleve a cabo la CNIL y responder a cualquier solicitud de información que ésta formule en el marco de sus funciones.

Ahora bien, para comprender mejor la estructura de esta ley, explicaremos uno a uno los capítulos que la conforman:

[56] http://www.cnil.fr/index.php?id=1930 : 07/10/08: 20:40 hrs.

El primer capítulo establece los principios y definiciones, y en su primer artículo se constituye el objeto de la ley:

> *"La informática debe estar al servicio de cada ciudadano. Su desarrollo deberá operar en el marco de la Cooperación Internacional. No debe afectar a la identidad humana, derechos del hombre, vida privada, ni a las libertades individuales o públicas*."

Como podemos ver, su objetivo principal es la protección de los ciudadanos, pero no limita el uso de la informática, si no al contrario, vigila que su desarrollo sea en beneficio de la sociedad y que a su vez, cumpla con los requisitos y normas que la comunidad internacional establezca, con esto Francia reconoce por un lado que el Estado debe proporcionar los medios suficientes de protección a sus ciudadanos y por otro, que se encuentra inmersa en un mundo globalizado.

El segundo artículo, define la aplicación de la ley, que son los datos personales y que son los ficheros[57] de datos personales, veamos pues el primer párrafo:

> *"La presente ley aplica al tratamiento automatizado y no automatizados de datos de carácter personal, contenidos o destinados a figurar en ficheros, y con la excepción de los tratamientos aplicados para el ejercicio de actividades exclusivamente personales, cuando su responsable cumple con las condiciones previstas en el artículo 5".*

Quizá una parte importante de esta ley es que no sólo esta dirigida a los bancos de datos electrónicos, si no también abarca los que se encuentran en papel, de esta

[57] En Europa se utiliza el término fichero para referirse a las bases o bancos de datos, con el fin de que en caso necesario este término pueda ser utilizado tanto para archivos en soporte electrónico o en papel.

manera, cualquier dato personal archivado podrá ser controlado, a modo tal, de asegurar que el fin para el cual fue creada la base de datos, sea cumplido.

En los siguientes párrafos define los conceptos de datos personales, procesamiento de datos y fichero de datos, estableciendo conceptos muy similares a los descritos en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental en su artículo 3, fracciones II, XIII, asimismo para abarcar la mayor parte de los medios por los cuales pueden ser procesados los datos, en el tercer párrafo de este artículo, hace hincapié en las distintas maneras en que puede ser procesada la información, de esta manera, logra cubrir ampliamente la información contenida en las bases de datos, así como su acceso y administración:

> *"...*
> *Constituye un tratamiento de datos de carácter personal toda operación o todo conjunto de operaciones referentes a tales datos, cualquiera que sea el método utilizado, y, en particular, la almacenada, el registro, la organización, la conservación, la adaptación o la modificación, la extracción, la consulta, la utilización, la comunicación por transmisión, difusión o cualquier otra forma de poner a disposición, la aproximación o la interconexión, así como el bloqueo, el borrado o la destrucción".*

La parte medular en los artículos 2 y 3 es que establecen al controlador de datos y lo definen como aquella persona, organismo, autoridad pública o prestador de servicios que determina los medios y fines para los cuales recaba los datos personales y que tiene acceso a estos, con ello, se les responsabiliza de la administración de la información, y más adelante en el capítulo V, sección 1ª. Se instituyen sus obligaciones, a diferencia de que en México, sólo se reconoce como sujetos obligados de administrar y proteger estos datos a los entes que conforman al Estado,

quedando fuera de estas obligaciones los particulares[58], debido a que sólo fueron contempladas para su protección y resguardo las bases de datos o ficheros que se encuentran en manos de las autoridades.

En los artículos 4 y 5, establece los conceptos relativos a la transmisión de la información, para lo cual, deja fuera de su protección a las copias temporales que se hagan para este fin, a modo tal, de asegurar el acceso a los datos por parte de los receptores, asimismo, limita su protección a todos los ficheros que sean administrados por los controladores de datos que se encuentren dentro del territorio francés o cuyo responsable del controlador se encuentre en algún Estado miembro de la Unión Europea y que recurra a los ficheros que se encuentran en territorio francés, con esto, trata la ley de proteger la información que se encuentre en su territorio y que pueda ser manipulada desde algún otro punto dentro de la Unión Europea, recordando así, que entre las ventajas (y desventajas) de los medios electrónicos es la facilidad que existe para tener acceso a cualquier información desde cualquier parte del mundo; lo relativo al control de la transmisión de información a otros Estados que no son parte de la Unión Europea, queda establecido en el capítulo XII.

Por último, en el artículo 5, también se determina la facultad de la CNIL, para tener a un representante que se encargue de vigilar el cumplimiento de esta ley.

El segundo capítulo, establece los lineamientos para la creación, procesamiento y protección de los datos personales; entre los fines que establece en el artículo 6° están:

> *“1. Los datos deberán ser recabados de manera honesta y legal.*

[58] Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, artículo 3, fracción XIV

2. Los datos serán obtenidos para los propósitos especificados, explícitos y legítimos, y no serán procesados posteriormente de una forma que sea incompatible con esos propósitos. Sin embargo, el procesamiento que se realice con propósitos estadísticos, científicos e históricos será considerado compatible con los propósitos iniciales de la recopilación de los datos, si se realiza conforme a los principios y los procedimientos señalados ...

3. La recolección y procesamiento posterior de los datos deberá ser adecuado, pertinente y no excesivo respecto al fin para lo cual fueron recabados;

4. Los datos deberán ser exactos, completos, y actualizados si fuera necesario, deberán adoptarse las medidas necesarias para que los datos inexactos o incompletos sean borrados o rectificados;

5. Los datos serán conservados de tal forma que permita la identificación de las personas durante el tiempo necesario que no exceda el fin para el cual fueron obtenidos."[59]

El fin principal será la guarda y protección de la información recabada, a modo tal, de que se cumpla con el propósito para lo cual fueron obtenidos los datos y que los mismos no sean utilizados para otros fines, a menos que sean con propósitos de investigación o estadísticos. Por otro lado, en el artículo 7, también se establecen las condiciones que deberá cumplir el controlador de datos, como por ejemplo, la responsabilidad legal de este en el tratamiento de estos, la protección de la vida privada de las personas y la creación en caso de ser posible de contratos donde se establezcan los derechos del individuo y que el motivo para el cual son recabados los datos debe tener como fin un propósito social y no atente contra los derechos y libertades de las personas; con esto, queda establecido que el controlador de datos

[59] Art. 6 de la ley 78-17 del 6 de enero de 1978

es limitado en cuanto a la recolección, uso y administración de la información, ya que se busca que el individuo sea protegido, cumpliendo con el principio fundamental del derecho a la protección de datos personales que es la facultad del individuo de decidir quien, cuando y como es utilizada su información personal[60].

Ahora bien, en el resto del capítulo la ley busca proteger la vida privada de las personas a través del procesamiento de datos personales que pudieran hacerse, por lo que prohíbe el uso de estos con el fin de identificar cuestiones tales como raza, religión, ideas políticas, ideología, tendencias sexuales, salud y afiliación sindical, a menos que por su *propia voluntad*, el individuo haya otorgado la información, tal y como sucede con las personas públicas, sin embargo, también prevé limitar esta libertad a fin de que la intimidad de la persona sea protegida, como en casos de personas incapaces, expedientes médicos, estudios que tiendan a investigar de forma automatizada la personalidad de los individuos o para limitar a la persona en un contrato o derecho, por la información que se haya obtenido a través del procesamiento de datos y sólo podrá llegar a utilizarse en caso de ser necesario por los órganos judiciales y con fines estadísticos y de investigación permitidos por la CNIL.

En el capítulo III, se establece como órgano regulador a la Comisión Nacional de Informática y Libertades, la cual tiene carácter autónomo, posee libertad de presupuesto al no ser controlado por la autoridad financiera como el resto de los entes del Estado y sólo al Tribunal de Cuentas presenta un informe de sus gastos, así como también, anualmente presenta un informe de su gestión al Presidente de la República, al Primer Ministro y al Parlamento, su objetivo principal es proteger la intimidad y las libertades individuales o públicas[61], entre sus funciones encontramos:

1. Informar. La CNIL informa a las personas sobre sus derechos y obligaciones, propone al Gobierno las medidas legislativas o reglamentarias necesarias para hacer

[60] *Vid Supra,* 1.4.1 Concepto de Derecho a la Protección de Datos Personales. Pag.29
[61] Artículos 11, primer y ultimo párrafo y 12, de la ley.

compatible la protección de las libertades y de la intimidad con la evolución de las tecnologías de la información. Antes de que sea enviado al Parlamento cualquier proyecto de ley relacionado con la protección de los datos personales debe solicitarse a la CNIL su opinión.

2. Garantizar el derecho de acceso. La CNIL vela para que no existan impedimentos en el acceso a los datos personales contenidos en los ficheros por parte de la ciudadanía. Ejerce, a petición de los ciudadanos que así lo deseen, el acceso a las bases de datos que estén relacionados con la seguridad del Estado, la defensa y la seguridad pública, en especial los de información general de la policía judicial.

3. Elaborar la lista de los ficheros. Cualquier procesamiento de datos considerados ”de riesgo”, deberá someterse a la autorización de la CNIL.

Emite opiniones sobre el uso que se realice al número nacional de identificación de personas.

Recibe notificaciones de los distintos tratamientos de datos personales existentes. El incumplimiento de estas formalidades por parte de los responsables de ficheros puede dar lugar a la aplicación de sanciones administrativas o penales.

La CNIL también pone a disposición del público el “archivo de los ficheros”, es decir, la lista de los sistemas notificados, así como sus principales características.

4. Controlar. La CNIL se encarga de comprobar que se respete la ley, vigilando y controlando las diferentes aplicaciones informáticas existentes. La Comisión hace uso de sus poderes de comprobación y de investigación para presentar quejas, disponer de un mejor conocimiento de algunos ficheros, apreciar mejor las consecuencias del uso de la informática en determinados sectores y garantizar un seguimiento de sus deliberaciones. La CNIL supervisa además la seguridad de los sistemas de información asegurándose de que adoptan las debidas precauciones

para impedir que los datos no se tergiversen o sean otorgados a personas no autorizadas.

La CNIL puede establecer diferentes sanciones: apercibimiento, requerimiento, sanciones pecuniarias que pueden alcanzar hasta los 300 000 €, orden de cesar el procesamiento de datos. El Presidente puede solicitar mediante recurso de apremio, presentado ante el órgano jurisdiccional competente, que se decrete cualquier medida de seguridad que sea necesaria, así como también, en nombre de la Comisión, denunciar al ministerio fiscal aquellos casos que violen la Ley.

5. Reglamentar. La CNIL dicta normas simplificadas con el objeto de agilizar los procedimientos más comunes en el ejercicio de las libertades individuales y públicas.

Puede también eximir de la obligación de notificación ciertas categorías de tratamientos que no presenten riesgos.[62]

Ahora bien, en cuanto a su composición, la CNIL esta constituida por un órgano colegiado de 17 miembros, nombrados de la siguiente manera:

- 4 parlamentarios: 2 diputados, 2 senadores designados por la Asamblea Nacional y por el Senado.

- 2 miembros del Consejo Económico y Social, elegidos por ese consejo.

- 6 representantes de los órganos jurisdiccionales superiores: 2 miembros del Consejo de Estado, elegidos por ese órgano, 2 consejeros del Tribunal de Casación, elegidos por su pleno, 2 consejeros del Tribunal de Cuentas, elegidos por su pleno.

[62] Art. 11 de la ley 78-17 del 6 de enero de 1978; véase también: http://www.cnil.fr/index.php?id=1932 : 17/10/2008: 11:56 hrs.

- 3 personas reconocidas y calificadas por sus conocimientos en informática o cuestiones de libertades individuales elegidas por el Consejo de Ministros, mediante decreto.

- 2 personas debidamente calificadas en informática, una nombrada por el Presidente de la Asamblea Nacional y la otra por el Presidente del Senado.

Cada uno de estos miembros tiene una duración de cinco años y puede extenderse por un periodo más, no pueden ser cesados y sólo por renuncia podrán ser sustituidos por el tiempo que falte a su nombramiento; la Comisión elige a su Presidente y dos Vicepresidentes de entre sus miembros, los cuales durarán en su encargo durante el mismo periodo de su nombramiento.

Todos los miembros y el personal designado para realizar actividades de comprobación y regulación de los sistemas de procesamiento de datos, están obligados a mantener la secrecía de su trabajo de acuerdo a lo establecido en el artículo 20:

> *"Se obliga a los miembros y los agentes de la comisión al secreto profesional para los hechos, actos o información cuyo conocimiento pudieron tener debido a sus funciones, en las condiciones previstas en el artículo 413-10 del código penal y, a reserva de lo que es necesario para la elaboración del informe anual, al artículo 226-13 del mismo código."*[63]

Para asegurar su independencia, la Comisión no recibe instrucciones de ninguna autoridad, ya sea pública o privada, y sin embargo, estos no pueden oponerse a las acciones de la CNIL, cualquiera que sea el motivo y deberán adoptar las medidas necesarias para facilitar sus funciones[64].

[63] Art. 20 de la ley 78-17 del 6 de enero de 1978
[64] Art. 21 de la ley 78-17 del 6 de enero de 1978

Por último, las decisiones de la CNIL pueden ser apeladas ante los órganos jurisdiccionales administrativos.

En el capítulo IV, se establecen los lineamientos a seguir para la creación y autorización de bases de datos personales, con el fin de controlar la administración, consulta, uso y demás procedimientos que se realicen con la información recabada, cabe destacar, que cualquier organismo puede nombrar a un administrador independiente que sirva como intermediario ante la Comisión, con solo realizar la notificación debida, por otro lado, este intermediario tiene como beneficios la certificación que la CNIL le otorgue y no podrá ser sancionado por las actividades, contrarias a la ley, que realice el organismo, si no más bien, esta obligado a notificar a la comisión cualquiera de estas actividades.

Ahora bien, el procedimiento para el registro de una base de datos se describe en los artículos 23 a 31, estableciendo como criterios que:

1. La manifestación de la creación de un sistema de procesamiento de datos, deberá realizarse ante la Comisión, ya sea de forma personal o electrónica, en el que se declare que el sistema cumple con la normativa establecida en la ley[65], por su parte, la comisión deberá entregar en ese momento acuse de recibo, con lo cual, el organismo deberá esperar a la resolución de autorización que emita la comisión para poder utilizar la base de datos. Para el caso en que un mismo organismo utilice más de un sistema, podrá registrarlos mediante una misma declaración, e indicando únicamente la descripción de cada uno.

[65] En el artículo 30, se establecen los lineamientos que debe contener esta declaración, tales como: Nombre del responsable del sistema de procesamiento de datos, para el caso de que este no se establezca en territorio francés o dentro de la Unión Europea, el nombre de su representante o quien se presente a su inscripción; descripción del sistema y procedimientos a utilizar, fin para el que será utilizada la información; si existe interconexión con otros sistemas, el tipo de datos personales que serán recabados, así como también el tipo de personas de las que se recabará la información, tiempo que serán utilizados, nombres de las personas que tendrán acceso al procesamiento de los datos y a

2. La CNIL, puede definir los datos y tiempo de conservación que queden excluidos en la declaración, tales como los mencionados en el artículo 8[66].

3. En el caso de que dos o más sistemas de procesamientos de datos estén dirigidos a obtener el mismo tipo de información, podrán ser autorizados por la misma resolución de la Comisión y cada uno de los administradores deberá presentar una declaración de conformidad.

4. La CNIL, tiene dos meses de plazo para otorgar el permiso de uso del sistema de procesamiento de datos, si al término de este tiempo la comisión no ha emitido ninguna resolución, se dará por rechazada y sólo en el caso de que sea solicitado a la comisión un dictamen, si este no es emitido en este mismo plazo, se dará por aceptada.

5. En el caso de sistemas de procesamiento de datos personales por parte del Estado, la comisión emitirá un dictamen y se dará la autorización, solo para los casos de que se trata de seguridad nacional o que tienen como objetivos la investigación, prevención y comprobación, para tomar medidas de seguridad.

6. Quedan excluidos de autorización por parte de la CNIL, aquellos sistemas que sean decretados por medio del Consejo de Estado, siempre y cuando, estos sean administrados a nombre del estado, ya sea por un organismo público o privado, que proporcionen un servicio público y que contengan datos como el número de identificación de la persona o datos biométricos.

7. El responsable del sistema de procesamiento de datos está obligado a informar a la comisión de cualquier modificación en el tratamiento de datos o la supresión de información.

---

las que será entregada la información; medidas de protección de la información y si esta será transmitida y a donde.

[66] *Vid Supra.* Pag. 49

Una vez realizado el registro y autorización de un sistema, la CNIL, tiene como obligación, la publicación de la lista de estos registros, que deberá contener:

a) Fecha de creación del sistema.

b) Denominación y finalidad.

c) Nombre y dirección del administrador del sistema y para el caso de que este no se encuentre dentro de territorio francés o de la Unión Europea, el nombre del representante.

d) Función de la(s) persona(s) que tendrán acceso a la información obtenida

e) Si existe transferencia de datos fuera del territorio francés o de la Unión Europea.

Ahora bien, también la CNIL tiene como obligación de poner a disposición de la ciudadanía los dictámenes y resoluciones que emita, así como también una lista de los países que la Comisión de la Comunidad Europea, reconoce que guardan un nivel de protección y respeto en el manejo de datos personales.

En el capítulo V, se establecen las obligaciones de los responsables de los sistemas de procesamiento de datos, entre las cuales encontramos:

1. Deberá informar a la persona de la que obtendrá los datos el fin para el que son recabados, el nombre del responsable del procesamiento, del carácter obligatorio o facultativo de las respuestas, consecuencias que pudieran existir, el destino de la información recabada y en caso de existir transferencia de datos a un Estado no miembro de la Comunidad Europea.

2. En el caso de medios electrónicos, deberá existir la declaración de privacidad, en el que se indique del posible acceso a la información almacenada en su equipo de cómputo por el hecho de otorgar información del mismo, medios por los cuales puede oponerse a este acceso, si el sitio tiene como única finalidad permitir o facilitar la comunicación vía electrónica, o si es estrictamente necesario otorgar dicha información para otorgar un servicio de comunicación a petición del usuario.

3. Cuando los datos fueron recabados sin la presencia de los individuos, el administrador deberá dar aviso del uso de estos datos y si serán transmitidos a terceros, con excepción de que estos vayan a ser reutilizados para fines estadísticos, históricos o científicos, para lo cual, se aplican las condiciones establecidas en la ley de obligación, coordinación y secreto de estadísticas[67].

4. Cuando los datos vayan a ser procesados con el fin de convertirlos en anónimos, el administrador deberá entregar la información a la persona interesada y se ajustarán a lo establecido en los artículos 1 y 2.

5. Estas obligaciones no son aplicables cuando el tratamiento de datos personales este relacionado con la seguridad pública, y sea el Estado quien los procese, siempre y cuando sea para la defensa, seguridad pública o teniendo por objeto la ejecución de condenas penales o aplicación de medidas de seguridad.

6. La obligación de que el administrador establezca las medidas de seguridad debidas en el tratamiento de la firma electrónica, la cual deberá ser procesada en presencia de la persona interesada, salvo convenio en contrario.

[67] Artículo 7 bis de la ley n° 51-711 del 7 de junio de 1951

7. El administrador deberá preservar los datos personales para evitar el uso y/o procesamiento de estos por terceros.

8. En el caso de que el administrador de datos subcontrate a otro para su tratamiento, este deberá obligarse en los mismos términos que la ley impone, por lo que, el contrato por el que se vinculan deberá señalar las obligaciones del subcontratista en cuanto a protección de la seguridad y la confidencialidad de los datos, así como también contemplará que este no puede actuar sin indicación previa del administrador de datos.

9. El administrador no puede conservar los datos por más tiempo que el indicado para el objetivo establecido, a menos que vayan a ser utilizados con fines estadísticos, históricos y científicos o bien, se obtenga el permiso por parte de la persona interesada o por acuerdo de la CNIL.

Ahora bien, en este mismo capítulo, la ley establece los derechos de las personas en relación con el tratamiento de sus datos personales, en las que encontramos:

1. Toda persona física tiene el derecho de oponerse por motivos legítimos a la recolección de sus datos personales o que sean reutilizados posteriormente con fines comerciales o de investigación de mercado por parte del administrador de datos o cedidos a otro, la gestión de dicho impedimento, por parte de la persona, deberá realizarse de manera gratuita.

2. Previa identificación, toda persona física tiene derecho de la confirmación de la existencia de un procesamiento de sus datos, así como los fines para lo cual fueron recabados y del uso que se le de a estos, así como también el destino y los receptores de la información obtenida.

3. Conocer cuando los datos personales serán transmitidos a un Estado que no sea miembro de la Unión Europea.

4. Saber si el procesamiento de sus datos personales puede llegar a producir efectos jurídicos.

5. En caso de que exista el riesgo de desaparición u ocultamiento de datos personales, el juez competente podrá establecer las medidas necesarias para evitarlo.

6. También la persona física tiene derecho a la corrección, actualización e inclusive eliminación de sus datos personales, cuando compruebe que estos son inexactos, incompletos, ambiguos, que expiró el tiempo para su uso, o que su recolección, comunicación o conservación fueron prohibidas[68] y en caso de conflicto, la carga de la prueba es para el administrador de datos. En el caso de personas difuntas, sus herederos, previa identificación, pueden solicitar la actualización o eliminación de sus datos.

7. En el caso del procesamiento de datos por parte del Estado con fines de seguridad pública, el interesado, puede solicitar a la CNIL, la verificación de sus datos personales, lo cual podrá realizarlo los miembros del Comité que pertenezcan a alguno de los órganos jurisdiccionales, y el resultado de la investigación se dará a conocer al interesado, inclusive en el caso de que la CNIL, compruebe que el tratamiento de datos no tiene como objeto la seguridad nacional, puede exigir que sea dada a conocer a la persona interesada.

[68] Podemos citar como ejemplo una reciente resolución de la Corte francesa, la cual ha sentenciado que las compañías de música y otros titulares de derechos de autor **se abstengan de vigilar** indiscriminadamente a quienes descargan música por Internet, ya que dichas empresas realizaban dichos actos para identificar a las personas que realizaban las descargas para después exigirles el pago compensatorio, por lo que a criterio de la Corte, esto era una violación a la vida privada de las personas. En: http://www.txitua.org/index.php/datos-personales/ : 16/09/2008: 21:15 hrs.

8. Si el procesamiento de datos es con fines médicos, el interesado tiene derecho de que le sean transmitidos los resultados de la investigación, ya sea de manera directa o a su médico tratante.

En el caso de que el administrador de datos considere que la oposición al tratamiento de datos es manifiestamente abusivo por su carácter repetitivo o sistemático, puede oponerse a la solicitudes por parte de la persona física interesada. En el caso de que dicha oposición derivará en conflicto, la carga de la prueba recae en el administrador de datos.

Sin embargo, esta excepción no aplica en el caso de riesgo de violación a la vida privada de las personas interesadas.

El capítulo sexto establece la forma en que la CNIL realizará visitas a las instituciones que manejan bases de datos personales, con el fin de comprobar que el procesamiento de estos se realice de acuerdo al permiso otorgado por la comisión; para que pueda ser realizada esta visita, el agente deberá avisar al administrador de datos con anticipación y este tendrá que dar las facilidades a modo tal de que el agente pueda acceder a toda la información que requiera, así como también en caso necesario podrá ser asistido por algún experto.

En caso de que el administrador de datos se niegue a recibir al agente, sólo el Presidente del Tribunal Administrador podrá otorgar un permiso para que el agente pueda realizar la visita y nombrará a un juez que deberá estar presente durante esta, con la facultad de suspenderla en caso necesario. En cualquiera de los casos, al finalizar la visita, se deberá levantar el acta respectiva.

El capítulo séptimo hace referencia a las sanciones que pueden llegar a aplicarse:

Cuando un administrador de datos no respete las obligaciones descritas en la ley, la CNIL puede realizar una exhortación a su cumplimiento, puede llegar a establecer plazos para que el administrador cese de realizar las actividades que incumplen con

el respeto a la ley, o inclusive después de un procedimiento contencioso administrativo aplicar sanciones[69], las cuales dependerán del tipo de falta y el provecho que se haya obtenido. El procedimiento deberá realizarse ante la comisión a partir de las observaciones realizadas por el agente que realizó la visita al administrador de datos, este no podrá estar presente durante la deliberación de la comisión, y por su parte, el responsable del procesamiento de datos podrá presentar las pruebas necesarias a su favor, en caso de encontrarse culpable, los gastos correrán por parte de él y podrán aplicarse sanciones tales como:

a) Sanción pecuniaria, de 150,000 euros, en caso de ser la primera vez que se incumpla con las obligaciones y hasta de 300,000 euros en caso de ser un incumplimiento reiterativo hasta 5 años después de haber sido probada la falta la primera vez, o inclusive multar hasta con el 5% de las deducciones fiscales del último año siempre y cuando no excedan los 300,000 euros.

b) El cese del procesamiento de datos o la eliminación del permiso concedido por la CNIL para su uso y administración.

En el caso de que un procesamiento o explotación de datos implique la violación de los derechos y libertades indicados en el artículo 1°, la CNIL, después de un procedimiento contencioso administrativo, podrá solicitar:

1. La interrupción de la aplicación del procesamiento de datos hasta por tres meses en caso de tratarse de bases de datos destinados al servicio público o que manejen datos biométricos.

2. Bloqueo de algunos de los datos personales por un período de tres meses.

[69] Debemos recordar, que Francia cuenta con una ley de protección de datos personales con un estándar de protección elevado, citando como ejemplo, que una multa por invasión a la privacidad en dicho país puede llegar hasta 300,000 o 350,000 euros y cinco años de pena privativa de la libertad.

3. Informar al Primer Ministro, para que tome las medidas necesarias para cesar la violación de estos derechos e informar a la comisión las sanciones que se habrán de tomar por dicha inobservancia.

Por último, en caso de que se trate de un ataque grave e inmediato a los derechos y libertades de las personas, el Presidente de la comisión podrá solicitar a la autoridad jurisdiccional competente se aplique una multa coercitiva y se tomen las medidas de seguridad necesaria, con el fin de proteger estos derechos. En el mismo tenor, la CNIL, puede investigar alguna violación en el procesamiento de datos por parte de un administrador o responsable de datos en el caso, de que un organismo, de un Estado de la Unión Europea, con las mismas facultades de la CNIL, se lo solicite.

Ahora bien, el capítulo octavo, describe las sanciones penales que podrán aplicarse en el caso de violación de esta ley, entre las cuales, podemos encontrar:

1. Un año de prisión y 15,000 euros de multa por obstaculizar u oponerse al ejercicio de las facultades de la CNIL, o negándose a entregar la información o documentación que esta solicite para la revisión de los distintos procesamientos de datos, así como también por la falsificación o desaparición de los mismos.

2. Cinco años de prisión y 300,000 euros de multa:

    a) Por no haber realizado los trámites debidos para el registro del sistema de procesamiento de datos, así como también, en caso de haber sido sancionado, hacer uso del sistema, antes de levantarse la misma.

    b) Por no cumplir con las obligaciones establecidas por la Comisión al otorgarle el permiso para el tratamiento de datos.

c) Por no establecer las medidas de seguridad en el tratamiento y procesamiento de datos personales.

d) Por recolección de datos personales de manera fraudulenta.

e) Por hacer uso de datos personales, que no se tenga el permiso por parte de persona física, o en caso de difuntos, que no exista el permiso por parte de los deudos.

f) Por el mal uso que pueda hacerse a datos personales con el fin de identificar a una persona por raza, religión, ideas políticas, infracciones, condenas, etc.

g) Por negarle a los interesados el ejercicio de sus derechos con relación al acceso, corrección o eliminación de sus datos, en el caso de tratamiento de datos relacionados con la salud.

h) Por el uso o procesamiento de datos por más tiempo que el establecido por la Comisión en el permiso otorgado por esta y/o del indicado por el responsable del tratamiento en la declaración, con excepción de que sean utilizados con fines estadísticos o de investigación.

i) Por el mal uso y desvió de la información obtenida por parte de un ente distinto al establecido en la declaración para el procesamiento de datos.

j) La revelación de la información obtenida por parte del responsable del procesamiento de datos a un tercero, que viole o afecte, a consideración de la persona interesada, la intimidad o vida privada de esta. En caso de haber sido por negligencia, la condena será por un año de prisión y 100,000 euros de multa.

k) Por la transmisión de datos a un país no miembro de la Comunidad Europea.

3. El borrado total o parcial de datos, cuando el responsable o administrador se haga merecedor de una de estas sanciones, lo cual podrá realizarlo únicamente la CNIL.[70]

Los capítulos nueve y diez indican el procedimiento para el manejo de información relativa a la salud, el cual considera la libertad por parte del médico de transmitir dicha información a otros entes con fines de investigación, siempre y cuando la persona interesada otorgue el permiso debido y que el ejercicio de sus derechos para la rectificación, actualización o eliminación de los datos quede salvaguardada, asimismo, indica que el procesamiento de estos datos puede llegar a identificar plenamente a las personas, por lo que se deberán aplicar los filtros debidos a fin de evitar una violación a la intimidad de las mismas, por otro lado, en el caso de transmisión de información a otro organismo ya sea que este se encuentre dentro o fuera de la Unión Europea, la información deberá ser encriptada con el fin de salvaguardar el derecho de protección a la vida privada de las personas interesadas.

Lo establecido en estos dos capítulos no son aplicables al tratamiento de datos personales con el fin del pago de reembolso o control por parte de seguros de gastos médicos, ni para revisar los tratamientos efectuados en clínicas u hospitales, por parte de los médicos tratantes, dichos datos se regirán en los mismos términos que el resto de las formas de tratamientos de datos personales.

El capítulo once, establece la administración de datos personales por parte de la rama periodística y literaria, en aras de protección de la libertad de prensa y de expresión, por lo que este grupo debe nombrar a un intermediario ante la CNIL, el cual, vigilará el cumplimiento de esta ley dentro de estas profesiones, en caso de que

[70] Dichas sanciones se encuentran dispuestas en los artículos 226-16 a 226-24 del código penal francés.

la comisión encuentre alguna anomalía, solicitará al intermediario que se cumpla con las estas obligaciones, y en caso de reiteración el intermediario será destituido de su cargo.

Por otro lado, esta disposición no significa un halo protector para los periodistas o un obstáculo para la aplicación del resto de las normas que rigen las condiciones del ejercicio del derecho de expresión, establecidas en la ley de prensa, código civil o penal, ya que estas mismas previenen, limitan, reparan y en caso de proceder, reprimen los ataques a la vida privada y al honor de las personas.

En cuanto a la transferencia de datos hacia un Estado que no pertenece a la Comunidad Europea, el capítulo XII, establece que no podrán ser transmitidos datos personales a un país que no prevea dentro de su legislación un nivel adecuado de protección de derechos y libertades personales, así como también, que no contemple los mecanismos de seguridad debidos para la protección de los datos personales, tales como el tipo de procesamiento, tiempo y fines que se persiguen en el tratamiento de estos.

Para ello, en el permiso otorgado por la CNIL, al responsable del tratamiento de datos, se le notificará de esta prohibición y se le solicitará el cese de la transmisión de datos, por otro lado, dará a conocer a la Comisión de las Comunidades Europeas en materia de Protección de Datos Personales dicha determinación, para que realice la investigación correspondiente, en caso de que el país al que se transmitirán los datos cuente con los niveles de protección debidos, se podrá otorgar el permiso al responsable del tratamiento de datos de la transferencia de los mismos, sin embargo, la CNIL podrá otorgar un permiso para la transferencia de datos, que deberá dar a conocer a la Comisión de las Comunidades Europeas, en caso de que tanto el responsable del tratamiento como quien recibirá la información, se ajusten a las condiciones siguientes:

1. Protección de la vida privada de la persona interesada.

2. Protección del interés público.

3. Garantizar el ejercicio y defensa de un juicio justo.

4. Acceso a la información de todo registro público a las personas interesadas.

5. Garantizar medidas precontractuales entre el responsable del tratamiento de datos y la persona interesada, en el que se garantice el cumplimiento de todas sus demandas.

6. Celebración de un contrato entre el responsable del tratamiento de datos y un tercero cuando se trate de un asunto de seguridad nacional.

Como hemos visto, esta ley contempla la protección de los distintos tipos de datos personales existentes, que se encuentren tanto en soporte electrónico como en papel, quizá lo más interesante puede ser el nivel de protección a la intimidad de las personas, ya que el titular de los datos en todo momento es quien decide quien, como y cuando van a ser utilizados, por lo que, cualquier ente de gobierno o particular que pretenda administrar o transmitir información derivada de cualquier tipo de procesamiento de datos, estará sujeto a dicha limitante, ya que este derecho lo antepone a cualquier interés comercial o gubernamental, con la única excepción de que se trate de seguridad nacional, pero aún así establece limitantes como el hecho de que toda información derivada de este tipo de investigaciones deberá ser eliminada una vez que se cumpla con su objetivo.

Asimismo, es de destacar que esta ley contempla la protección de la identidad de las personas para el caso de investigaciones científicas o históricas o con fines estadísticos, con el único fin de evitar cualquier acto de discriminación o represión.

2.2. España

2.2.1 Antecedentes

En 1992, España promulga la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD), atendiendo por un lado a lo establecido en la Constitución de 1978, en la que se señala, en el capítulo II, sección I, la protección de los derechos fundamentales y en particular en el artículo 18, la protección de la intimidad, inviolabilidad de comunicaciones o domicilio y límites a la informática:

> ***Artículo 18.***
>
> *1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.*
>
> *2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en el sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.*
>
> *3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.*
>
> *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*[71]*.*

Y por otro lado, a la ratificación que este país realizó del Convenio Europeo sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1984.

[71] http://noticias.juridicas.com/base_datos/Admin/constitucion.t1.html#c2s1 :10/11/08: 11:06 hrs.

Sin embargo, en 1995, con la Directiva 95/46/CE, el Consejo de Europa, creó un marco regulador que buscó equilibrar la protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea, por lo que, con esta Directiva se fijaron límites para la recolección y uso de los datos personales, así como también la creación en cada Estado miembro, de un organismo independiente encargado de su vigilancia y protección[72], por lo que, el Gobierno de España se vio obligado a reformar la LORTAD, con el fin de actualizar e introducir las nuevas directivas que el Consejo establecía, dando pie a la creación de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal (en adelante LOPD).
De esta forma, se reconoce, a nivel constitucional la protección que el Estado debe dar a los bienes jurídicos propios de la personalidad, ya sea de manera directa o por extensión, como es el caso de la familia, e inclusive, volviendo al mencionado artículo 18, en su fracción 4, deja por sentado el mal uso que pueda hacerse de la informática y no así sus beneficios, por lo que da prioridad a los límites en cuanto al uso de esta herramienta, anteponiendo los derechos fundamentales de los particulares.

Ahora bien, tal y como se realizó con el caso de Francia, analizaremos uno a uno de los capítulos de la LOPD, que de entrada es reconocida por su alto nivel de protección de datos personales y con las sanciones más duras en la Unión Europea.

2.2.1. La Ley Orgánica de Protección de Datos de Carácter Personal

La LOPD, obliga a las personas, empresas y organismos, tanto privados como públicos, que traten con datos de carácter personal, a cumplir con normas estrictas y a aplicar medidas de seguridad para almacenar dichos datos, garantizando al titular de los mismos, su libertad y sus derechos fundamentales en honor a la intimidad personal y familiar[73]; en su primer capítulo, se establecen las disposiciones generales y en el primer artículo se indica el objeto de la misma:

[72] http://europa.eu/scadplus/leg/es/lvb/l14012.htm : 12/11/2008: 13:40 hrs.

> *La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*[74]

Así como la ley francesa, busca proteger las libertades públicas y derechos fundamentales como la intimidad, los cuales, como ya vimos son reconocidos constitucionalmente, cabe hacer mención especial que la ley española además, extiende esta protección al ámbito familiar del titular de los datos, reconociendo de esta forma, la interconexión que pudiera realizarse con estos, lo cual puede resultar en una violación a la intimidad de las personas[75].

En el artículo 2, fracción 1, se establece el ámbito de aplicación:

> *1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores* ***público y privado****.*

Nótese, que contempla la aplicación de esta ley a cualquier sector ya sea público o privado, garantizando ampliamente la protección de los datos personales, de esta manera, se reconoce también que cualquier registro[76] de datos debe ser protegido debido a la información que contiene.

---

[73] http://www.lopd-proteccion-datos.com/ley-proteccion-datos.php :02/10/2008: 14:19 hrs.
[74] http://noticias.juridicas.com/base_datos/Admin/lo15-1999.t1.html :10/11/2008: 15:19 hrs.
[75] *Vid Supra* 1.3.1. Concepto de derecho a la intimidad, pag. 26
[76] Aquí también es de destacarse que esta fracción contempla cualquier **soporte físico** de estos registros, por lo que puede interpretarse que protege tanto a los archivos electrónicos como los de papel.

Ahora bien, en este mismo artículo también se contempla para su ámbito de protección, el lugar en el que se encuentra situada la base de datos, es así como quedan bajo su jurisdicción aquéllas que:

a) Se encuentren dentro de territorio español

b) Cuando el responsable del tratamiento de datos personales le sea aplicable la ley, en relación con normas internacionales

c) Cuando el responsable del tratamiento se encuentre fuera de la Unión Europea, pero utilice medios que dentro de territorio español, salvo cuando sólo los utilice como medios de tránsito.

Considerando lo anterior, establece entonces el tipo de bases de datos que contempla para su regulación la LOPD, de esta manera, excluye primero 3 categorías:

1. Las que son administradas exclusivamente de forma personal o doméstica

2. Las que se someten a la normativa sobre protección de materias clasificadas

3. Las que se establecen para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

E incluye 5 categorías de bases de datos, las cuales podrán ser regidas al mismo tiempo por alguna otra ley de aplicación específica:

- Los ficheros regulados por la ley electoral.

- Los que sirven exclusivamente para fines estadísticos y se encuentren amparados por la legislación estatal o autonómica.

- Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación, que se encuentran contemplados en la legislación del régimen del personal de las Fuerzas Armadas.

- Los que se deriven del registro civil y del registro central de penados y rebeldes.

- Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Cabe destacar en este apartado, que para la LOPD, las imágenes captadas por cámaras de seguridad o fotografías, así como también las grabaciones, son considerados datos personales, por lo que si esta información es dada a conocer sin el permiso del interesado puede llegar a considerarse una violación a su intimidad[77].

De esta manera, podemos darnos cuenta que el ámbito de aplicación de la LOPD, es amplísimo ya que los legisladores trataron de que cualquier información obtenida de una persona, ya fuera con su consentimiento o sin él, fuera protegida, garantizando entonces la protección a su intimidad.

Continuando con este primer capítulo de la ley, en el artículo 3, los legisladores consideraron incluir un glosario con lo que trataron de dejar claros los conceptos de

[77] La instrucción 1/2006, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras estableció: “En relación con la instalación de sistemas de videocámaras, será necesario ponderar los bienes jurídicos protegidos. Por tanto, toda instalación deberá respetar el principio de proporcionalidad, lo que en definitiva supone, siempre que resulte posible, adoptar otros medios menos intrusivos a la intimidad de

los tecnicismos que se utilizan a lo largo de la misma y con eso evitar interpretaciones erróneas que pudieran resultar en una mala aplicación de la ley, encontramos entonces los siguientes conceptos:

- *Datos de carácter personal*: cualquier información concerniente a personas físicas identificadas o identificables.

- *Fichero*: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

- *Tratamiento de datos*: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

- *Responsable del fichero o tratamiento*: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

- *Afectado o interesado*: persona física titular de los datos que sean objeto del tratamiento.

- *Procedimiento de disociación*: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales".

- *Encargado del tratamiento*: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

- *Consentimiento del interesado*: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

- *Cesión o comunicación de datos*: toda revelación de datos realizada a una persona distinta del interesado.

- *Fuentes accesibles al público*: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

En el título II, la ley establece los principios que regirán la protección de los datos, en este apartado se encuentran similitudes con la legislación francesa, pero con la existencia de una rigidez más específica en cuanto a la secrecía que deben guardar los administradores y responsables del sistema.

Ahora bien, en el artículo 4, se enlistan los principios que deben guardarse en cuanto a la calidad de los datos, en los que encontramos:

1. Los datos personales solo podrán ser recabados y procesados, siempre y cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que fueron obtenidos.

2. Los datos personales podrán ser usados para fines distintos para los cuales fueron obtenidos, salvo que el tratamiento posterior sea con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio del derecho de acceso que el interesado tiene.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.

   No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.

   Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento integro de determinados datos

6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.

7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos

En correspondencia con la calidad de datos, la ley en el artículo 5°, establece el derecho a la información que debe ser garantizado a los titulares de los datos, por lo que, al momento en que sea solicitada la información, deberá ser informado de:

a) La existencia de un fichero o tratamiento de datos de carácter personal

b) La finalidad de la obtención de éstos y los destinatarios de la información.

c) El carácter obligatorio o facultativo de su respuesta a las preguntas que le fueron planteadas.

d) De las consecuencias de la obtención de los datos o inclusive de la negativa a suministrarlos.

e) Del derecho de acceso, rectificación, cancelación y oposición.

f) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante; para el caso de que el responsable del procesamiento no se encuentre en territorio español o utilice medios dentro de éste, deberá nombrar a un representante dentro de España.

Como podemos observar estos principios son parecidos al caso francés, la diferencia es que en aquella legislación, estos los consideran dentro del capítulo de derechos de los titulares de datos, en cuanto a los incisos a) a e) y en relación al inciso f) este se encuentra dentro de las obligaciones de los responsables del procesamiento de datos y en los lineamientos para el registro de ficheros. Cabe señalar, que entre otras medidas indicadas dentro de esta legislación es incluir en la recepción de datos, las encuestas y cuestionarios, en las cuales deberán venir escritas estas medidas para que el titular de los datos tenga conocimiento de sus derechos, asimismo, en el caso de que éstos hayan sido obtenidos por otro medio, el responsable del tratamiento tendrá tres meses para informar de manera expresa al titular de los mismos.

En lo relativo al consentimiento del titular, este tiene la opción de negarse o revocarlo, siempre y cuando la ley no estipule lo contrario, lo cual podrá suceder en el caso de contratos o en el ejercicio de la función de la administración pública[78], sin embargo, inclusive para este tipo de casos, el titular podrá oponerse en caso de que existan motivos fundados y legítimos que pudieran resultar en una afectación personal[79].

Por otro lado, el tratamiento de datos que tengan como finalidad la identificación de las personas de acuerdo a su raza, religión, ideología, afiliación sindical, salud o vida sexual son expresamente prohibidas, con excepción de que dicho tratamiento resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o la gestión de servicios sanitarios, siempre que dicho tratamiento se realice por un experto sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente[80].

En relación a la seguridad de los datos, este mismo capítulo en sus artículos 9 y 10, estipula que el responsable del fichero, así como también el administrador del tratamiento de datos, deberán garantizar que éstos no podrán ser manipulados por persona ajena al sistema, ya sea para su transmisión, modificación o eliminación, por lo que si el sistema no cumple con estos requisitos, no podrán ser recabados los datos. Por último, también se obligan los responsables, administradores y cualquier otra persona que intervenga en el procesamiento de datos a guardar secrecía antes, durante y después de finalizado este.

En cuanto a la transmisión de datos a terceros, en el artículo 11 se establece que esta sólo podrá realizarse con el previo conocimiento y permiso de los titulares de los datos, siempre y cuando esta transmisión mantenga la finalidad para lo cual fueron

[78] Como ejemplo podemos citar el procesamiento de datos personales de delincuentes o sujetos a investigación o con fines estadísticos e históricos.
[79] Artículo 6 de la LOPD
[80] Artículo 7 y 8, de la LOPD

recabados, por obvias razones estos terceros quedan obligados a sujetarse a las disposiciones establecidas, salvo que antes de efectuarse la transmisión de datos, se realice un procedimiento de disociación.

Por último, cabe señalar que el permiso por parte de los titulares de los datos puede llegar a revocarse a petición suya, o inclusive, existen excepciones para solicitar dicho permiso, como son:

a) Cuando la cesión está autorizada en una ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. Para lo cual, la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas.

   De igual manera, será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

Por último, el artículo 12 indica que el acceso a datos por parte de terceros, puede llegar a realizarse cuando esto sea parte de la prestación de un servicio al responsable del fichero o cuando el procesamiento de los datos vaya a ser realizado por un tercero (lo cual deberá estipularse por medio de un contrato, así como también este deberá cumplir con las medidas de seguridad establecidas por la ley). Asimismo, una vez que el procesamiento de datos haya concluido todos los documentos, archivos y soporte deberán ser destruidos o devueltos al responsable del tratamiento, por lo que, en caso de que el encargado de este procesamiento llegue a transmitir o utilizar con otro fin la información, este responderá de acuerdo a las infracciones que haya cometido.

El título III, hace referencia a los derechos de los titulares de los datos; el artículo 13 describe primeramente la protección que el particular tiene en cuanto a la valoración de su personalidad a partir de los datos obtenidos, este artículo queda relacionado con el artículo 7.4, en el que se prohíbe la recolección de información con la finalidad de identificar a la persona a partir de su ideología, sexualidad, afiliación, etc., por lo que este artículo, robustece la protección de la personalidad con el fin de evitar la identificación de la persona a través del tratamiento indiscriminado o control de la información, toda vez que a la letra establece:

“1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.

2. *El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.*

3. *En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.*

4. *La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado."*

Tal y como podemos ver, la fracción cuarta señala una excepción a la valoración de la persona a través del tratamiento de información, y sólo esta se dará en caso de que el titular de los datos lo solicite, por lo que una vez más podemos ver, que sólo a partir de la voluntad de la persona es que se abre esta posibilidad[81].

Por otro lado, y con el fin de garantizar el acceso a la información por parte de los particulares, esta ley, otorga la facultad a todo ciudadano de conocer cuales son las bases de datos personales existentes mediante el registro nacional que lleva la Agencia Española de Protección de Datos, por lo que puede conocer desde la finalidad del tratamiento hasta el responsable del mismo sin costo alguno[82]; y el artículo 15 señala que los titulares de los datos pueden solicitar toda información relativa al tratamiento de los mismos, para lo cual, el responsable deberá otorgar dicha información de manera sencilla a modo tal de facilitar este acceso al titular de los datos; ahora bien, este último, tiene el derecho de solicitarlo una vez cada doce

[81] *Vid Supra* 1.3.1 Concepto de Derecho a la Intimidad, pag. 26
[82] Artículo 14 de la LOPD

meses sin costo alguno[83] a menos que se acredite un interés legítimo para lo cual podrá solicitarse antes de este periodo.

Ahora bien, para garantizar el derecho a la rectificación o cancelación de datos, en el artículo 17 se establece primeramente, que el responsable del tratamiento tiene la obligación de hacer efectivo este derecho en un plazo de diez días; el titular de los datos podrá solicitar la rectificación o cancelación de estos, cuando el tratamiento no se ajuste a lo dispuesto por la ley o por que la información sea inexacta, para lo cual, en caso de que hayan sido transmitidos a un tercero, el responsable deberá notificar a este, para que realice la modificación o cancelación del mismo; para el caso de cancelación de datos, estos deberán ser bloqueados inmediatamente y dejarse a disposición de la autoridad administrativa o jurisdiccional para su atención, para en caso de que existan responsabilidades derivadas del tratamiento de estos. Cabe señalar, que estos datos personales podrán estar a disposición de las autoridades sólo durante el período de prescripción que haya sido convenido entre el titular y el responsable, por lo que, al finalizar dicho tiempo serán eliminados.

Por último, el titular de los datos puede acudir a la Agencia Española de Protección de Datos[84], en caso de que le sea negado su derecho de acceso, rectificación o cancelación, para lo cual, esta tendrá seis meses para resolver la improcedencia o procedencia de la negación. Cualquier resolución emitida por la Agencia, puede ser impugnada por medio de un procedimiento contencioso-administrativo[85].

Continuando con este título, para el caso de que el titular de los datos haya sufrido daño o lesión en sus bienes o derechos, a raíz del incumplimiento con lo dispuesto por la ley por parte del responsable o encargado del tratamiento de datos, tendrá derecho a una indemnización, si el daño fue causado por un ente de la

[83] Dicho derecho de acceso es parecido al señalado en el artículo 41 de la Ley para Regular Sociedades de Información Crediticia, con la diferencia que en esta no se establece excepción alguna para poder solicitar un reporte crediticio en un período menor, para lo cual, en caso de que el titular de los datos así lo requiera, el buró de crédito puede cobrar por emitir este reporte.
[84] O en su caso, podrá acudir al organismo competente de cada Comunidad Autonómica
[85] Artículos 17 y 18 de la LOPD

administración pública, esta será acorde con lo que dicte la regulación de responsabilidades administrativas, y para el caso de ficheros de **titularidad privada**, esta acción se ejercitará ante los órganos de jurisdicción ordinaria.[86] Para efectos de este trabajo de investigación es importante hacer hincapié en esta última observación, ya que establece la obligación de los particulares de hacer guardar la ley y responder por cualquier daño o lesión derivado de una mala administración de la información que se encuentre bajo su resguardo, de esta manera se protege al titular de los datos sobre cualquier interés extraordinario que un ente privado tenga sobre la información obtenida por parte de estos, evitando así, que dicho tratamiento quede al margen de la ley y manejo discrecional por parte de los responsables, recordando de esta forma, que si bien estos entes privados son dueños de la plataforma de la base de datos, no son dueños de la información particular de los titulares, por lo que, no podrá ser utilizada con un fin diferente al establecido en el momento de su obtención, esto es, sin que se haya conseguido el permiso expreso del titular[87].

Más adelante, el Título IV, divide en sector público y privado las obligaciones que deben cubrir los responsables del tratamiento de datos para la creación, administración y uso de las bases de datos, lo cual resulta interesante, debido a la naturaleza jurídica de cada ente y la forma en que pueden ser responsabilizados; hecho importante y que puede servir de ejemplo, ya que en nuestro país, esto no ha sido contemplado (con excepción del Estado de Colima), quizá por la falta de interés de regular a los entes privados en el manejo de la información, o realizar la relación de estas obligaciones existentes en las diferentes leyes que pudieran contemplarlas, podemos citar, como ejemplo, a la Comisión de Administración Pública Local de la Asamblea del D.F., cuando realizó el dictamen a la iniciativa de la Ley de Protección de Datos Personales para el D.F., vigente a partir del mes de octubre de 2008:

[86] Artículo 19 de la LOPD
[87] *Vid Supra* 1.4.1. Concepto de Derecho a la Protección de Datos Personales, pag. 29

> *"Es importante destacar que en el presente dictamen se establece únicamente como sujetos obligados a los entes públicos del Distrito Federal y no a entes privados, debido a la complejidad que acarrea y al hecho de que cada ente privado es sujeto de una ley en específico, ya sea local o federal, que regula su actividad …"*[88]

De esta manera, el propio Estado deja al margen de la ley a los entes privados, por lo que se vuelve difícil para el ciudadano común responsabilizar a éstos de cualquier daño que pudiera resultar por el mal manejo de sus datos personales[89].

Volviendo a la LOPD, en cuanto a los ficheros de titularidad pública, señala que para la creación, modificación o supresión de información, sólo podrá realizarse por medio de la publicación a través del Boletín Oficial del Estado.

Para el caso de la creación o modificación, las disposiciones deberán contener:

1. La finalidad del fichero y los usos previstos para el mismo.

2. Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

3. El procedimiento de recogida de los datos de carácter personal.

4. La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

---

[88] Dictamen que presenta la Comisión de Administración Pública Local por el que se crea la Ley de Protección de Datos Personales del Distrito Federal. -- http://seguridad2008.politicadigital.com.mx/lectura.html 05/12/2008: 14:28 hrs.

[89] Podemos citar como ejemplo, la existencia de empresas que venden por Internet bases de datos personales de funcionarios públicos, ejecutivos de empresas, etc., sin importar a quien ofrecen esta información, como ejemplo puede verse www.pro-email.com.mx o http://www.alarechiga.4realhost.com/CatalogoBD.xls, lo cual puede ayudarnos también a dimensionar la cantidad de información que circula en el mercado negro.

5. Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

6. Los órganos de las Administraciones responsables del fichero.

7. Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

8. Las medidas de seguridad con indicación del nivel básico, medio o alto exigible[90].

Cuando se trate de la supresión de datos, las disposiciones deberán establecer también el destino de los mismos o en su caso, las previsiones que se adopten para su destrucción.

En el artículo 21, se establecen los casos en que los entes de la Administración Pública pueden transmitir datos, como cuando un ente elabora una base de datos con destino a otra, cuando tenga por objeto el tratamiento posterior con fines estadísticos, históricos o científicos, y sólo podrán transmitirse a ficheros de titularidad privada en caso de que exista consentimiento por parte del titular de los datos o cuando alguna ley prevea su transmisión; prohibiéndose esta cuando la administración pública tenga como objetivo utilizar los datos para actos diferentes a los establecidos, cabe señalar, que como excepción a esto último, el primer inciso de este artículo permitía la transmisión salvo que "*la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso*"[91], sin embargo, dicha consideración fue declarada inconstitucional por medio de la sentencia 292/2000 en el que el Tribunal Constitucional reconoció:

[90] Art. 20 de la LOPD
[91] Art. 21.1 de la LOPD

> *"El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre estos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con que fin ..."*

Por lo que de esta forma se reconoció que la ley no imponía limites al derecho a la cesión de datos personales entre los entes de la administración pública con fines distintos a los que motivaron su recolección, dejando a un lado el derecho del titular de los datos de decidir el destino y uso de estos.

Lo anterior también resulta contrario a la propia ley, debido a que el artículo 22 establece, en lo referente al manejo de bases de datos administradas para la seguridad pública, que los organismos encargados sólo podrán hacer uso de los datos personales mientras dura la investigación para lo cual fueron recabados y al final de esta tendrán que ser cancelados, o bien, también se indica que los datos obtenidos, sin consentimiento del titular, serán almacenados y clasificados de acuerdo a su categoría y grado de fiabilidad y sólo serán utilizados con fines de *"prevención de un peligro real de seguridad pública o para represión de infracciones penales"*[92], de este modo, los datos personales son protegidos aún en situaciones en que al bien común pareciera dársele prioridad por encima de los derechos individuales, sin embargo, con el solo hecho de que los entes de seguridad pública tengan la obligación de cumplir con ciertos lineamientos para el uso y procesamiento, quedan salvaguardados los derechos individuales aún con el desconocimiento del propio titular.

[92] Art. 22.2 de la LOPD

Por último, en los artículos 23 y 24, se establecen las reglas para negar el acceso, rectificación o cancelación de datos por parte de los titulares, lo cual sólo podrá hacerse cuando se encuentren relacionados con la seguridad nacional o cuando la Hacienda Pública realice una investigación o auditoria al titular de los datos, sin embargo, aún en estos casos, el interesado podrá recurrir a la Agencia Española de Protección de Datos Personales[93], para que esta determine si es procedente o no dicha negación.

Respecto del artículo 24, el Tribunal Constitucional, declaró la inconstitucionalidad parcial de dicho artículo, debido a que se le otorgaban a la autoridad administrativa facultades discrecionales en el manejo de la información, esto es, podía negar el acceso, rectificación o cancelación a los datos por parte del titular, si dichos derechos impedían las funciones de la administración pública o quedaban por encima de terceros más dignos de protección o cedían a intereses de bien público, y la autoridad sólo debía dictar la resolución correspondiente invocando este artículo y debía instruir al titular de los datos su derecho de poner en conocimiento de la Agencia Española, dicha negación, por lo que, el Tribunal estimó que proteger los derechos fundamentales de terceros, era lo mismo que otorgar y proteger los derechos de los titulares de los datos, puesto que se entregaba a la entera discrecionalidad de la Administración Pública el manejo de la información, lo cual contravenía a los artículos 18.4 y 53.1 de la Constitución Española[94], por lo que en su resolución, indicó:

> *"... cabe entender que la restricción fundada en el interés público o de un tercero más digno de tutela que el derecho a la protección de datos personales del interesado lo es al ejercicio mismo de esos derechos de acceso, rectificación y cancelación de los datos que forman parte del contenido esencial de esos derechos*

[93] O a la agencia correspondiente de la Comunidad Autónoma, o a la agencia de policía o administración tributaria encargada del procesamiento de datos.
[94] El artículo 18.4, indica los límites al uso de la informática y el artículo 53.1 indica que los derechos y libertades reconocidos son vinculantes a todos los poderes públicos.

> *fundamentales. Sin perjuicio de que su denegación en ese caso pueda ser impugnada ante el Director de la Agencia de Protección de Datos. Denegación cuya consecuencia será la prórroga del plazo legal para proceder a la cancelación y rectificación de esos datos personales, de lo que se infiere que la restricción no es en rigor al plazo para rectificar y cancelar, sino a los derechos mismos a que se rectifiquen y cancelen los datos."*[95]

Ahora bien, la parte que no fue declarada inconstitucional hace referencia a la negación de estos derechos en caso de bases de datos que tengan que ver con cuestiones de seguridad pública, lo cual es entendible dada la situación de terrorismo existente en España.

Continuando con este mismo título, en su segundo capítulo establece los lineamientos para los ficheros de titularidad privada, siendo en los artículos 25 y 26, se establecen las reglas para la creación de los ficheros, para lo cual, estos ficheros deben tener como finalidad la necesidad de ayudar con el objeto legítimo de la entidad privada y respetar los derechos individuales establecidos en esta ley, para su inscripción ante la Agencia Española de Protección de Datos, estos entes deberán:

1. Notificar previamente a la Agencia Española de Protección de Datos, la creación del fichero.

2. Indicar de forma detallada nombre del responsable del fichero, finalidad del fichero, ubicación, tipo de datos de carácter personal que contiene, las medidas de seguridad y la indicación del nivel básico, medio o alto exigible de las mismas, las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a terceros países.

[95] Sentencia 292/2000 del Tribunal Constitucional.

3. Comunicar a la Agencia Española de Protección de Datos los cambios que se produzcan en cuanto a la finalidad del fichero automatizado, en el responsable y en la dirección de su ubicación.

Una vez cumplidos los requerimientos, el Registro General de Protección de Datos inscribirá el fichero, en caso de faltar alguno de estos, podrá solicitar que sean completados o que se proceda a su subsanación, posteriormente, transcurrido un mes desde la presentación de la solicitud de inscripción, si la Agencia Española de Protección de Datos, no ha resuelto sobre la misma, se entenderá inscrito el fichero automatizado[96] para todos sus efectos.

Para la cesión de datos el artículo 27 indica que el responsable del fichero deberá hacer del conocimiento de esto a los titulares de los datos, una vez que se haya realizado *la primera transmisión*, indicando la finalidad del fichero al que fue transmitido, nombre del responsable y tipo de datos cedidos; aquí cabe señalar, que de alguna forma los derechos individuales del titular son vulnerados, debido a que no se le solicita su consentimiento para la cesión de los datos, si no sólo es informado de ello y hasta que esta ha sido realizada, por lo que el ente privado cuenta con facultades en el uso de los datos que van contrarias a la protección de los mismos. En este mismo orden de ideas, el mismo artículo señala que el responsable del fichero no tiene la obligación de dar conocimiento de la cesión de datos al titular en el caso de que la información sea transmitida a otros ficheros que la complementen, sea utilizada para fines estadísticos o históricos o inclusive si para su transmisión llevo primeramente un procedimiento de disociación[97].

En el caso de ficheros de acceso público, como lo serían directorios de asociaciones o colegios, sólo podrán contener la información estrictamente necesaria para cumplir con su función y no podrá ser transmitida con fines publicitarios o comerciales,

[96] Es de destacar que en el artículo 26, sólo se hace referencia a ficheros automatizados, lo cual excluye a ficheros de cualquier otra naturaleza como aquellos en soporte físico.
[97] *Vid Supra*, artículo 11, pag. 75

teniendo el titular en cualquier momento el derecho de solicitar la exclusión de sus datos de estos ficheros de forma gratuita, así como también, el responsable del fichero deberá indicar gratuitamente que dicha información no puede ser utilizada para fines distintos.

Cuando sea solicitada la exclusión de los datos, la entidad responsable del fichero tendrá 10 días para responder a la petición, cuando se trate de ficheros automatizados y para el caso de ficheros impresos o editados, tendrá hasta la siguiente edición para realizar la eliminación[98].

Para el caso de servicios de información crediticia, el artículo 29 indica que dichas entidades sólo podrán hacer uso de la información obtenida de registros y fuentes accesibles al público o por información que el mismo interesado haya facilitado, también podrá utilizarse la información recabada por los acreedores o quién actúe por su cuenta o interés, teniendo el responsable del fichero treinta días a partir de la recepción de la información de notificarle al titular de la existencia de dichos datos, la referencia de quien los haya incluido y de su derecho de recabar toda la información relativa a los mismos, por otro lado y a solicitud del titular de los datos, el responsable del fichero le comunicará los resultados del análisis de la información obtenida, así como también los datos de la entidad a quien fue cedida la información.

Ahora bien, y en cumplimiento a uno de los principios que consideramos toda ley de protección de datos debe contener, en este mismo artículo se incluye el “derecho al olvido”, lo cual significa que toda la información adversa que sea determinante para indicar la solvencia económica de una persona, podrá ser transmitida siempre y cuando no rebase una antigüedad de seis años y que responda con veracidad a la situación actual del titular de los datos.

En cuanto al procesamiento de datos con fines comerciales o de publicidad, sólo podrán ser utilizados los datos obtenidos de ficheros de accesibilidad pública, o

[98] Artículo 28 de la LOPD

cuando hayan sido obtenidos por consentimiento del titular. Para el caso de que los datos provengan de ficheros públicos, cada vez que el responsable del tratamiento envíe información o propaganda al titular de los datos, deberá indicarle a este el fichero del cual obtuvo los datos y los derechos que le asisten en cuanto a la protección y acceso a sus datos personales, de igual manera, el titular podrá oponerse al tratamiento (previa solicitud y de forma gratuita) de sus datos, por lo que, el responsable realizará la cancelación de la información de manera inmediata[99].

El artículo 31 de esta ley, contempla la creación de un "censo promocional", a partir del registro de ciudadanos con derecho a voto, el cual sirve a las empresas para enviar publicidad, venta a distancia, investigación comercial, etcétera, a los titulares de los datos; dicho censo, tiene como fin eliminar la venta fraudulenta de datos personales y el órgano encargado de su creación y mantenimiento es el Instituto Nacional de Estadística, el uso del listado del censo tiene una vigencia de un año y el instituto puede exigir una contraprestación por facilitar esta información, sin embargo, cuando este instituto se dio a la tarea de la creación de dicho censo, se encontraron con diferentes cuestionamientos, debido a que contrario a la LOPD[100], sólo excluirían, en un principio, a aquéllas personas que contestaran por escrito a la carta de invitación que haría el instituto, por lo que, por *default* todos los datos serían ingresados y solo a solicitud del titular serían excluidos[101], y por otro lado, se violaría la Ley de Régimen Electoral, en la que se prohíbe el uso del registro de electores para fines y actividades comerciales[102], por lo que, al ser corregida la postura por parte de este instituto, la exclusión de las personas sería por *default* y su inclusión

[99] Artículo 30 de la LOPD

[100] Artículo 6.1 de la LOPD: El tratamiento de los datos de carácter personal ***requerirá el consentimiento inequívoco del afectado***, salvo que la ley disponga otra cosa.

[101] El Diputado Diego López Garrido, en ese entonces defendía la postura que el censo promocional debería de crearse a partir de los datos de aquéllos ciudadanos que expresaran su consentimiento, excluyendo de esta forma tanto a quienes expresaban no estar interesados, como aquéllos que no realizaran pronunciamiento alguno. En: NOGUEIRA, Charo. *El INE venderá datos del censo electoral si la persona no se opone por escrito*. -- En: El Pais, 02-OCT-2002 (http://www.elpais.com/articulo/sociedad/INE/vendera/datos/censo/electoral/persona/opone/escrito/elpepisoc/20021002elpepisoc_2/Tes : 07/01/2009: 13:36 hrs.)

[102] *¿Censo o Publicidad?*. -- En: El País, 02-OCT-2002 (http://www.elpais.com/articulo/opinion/Censo/publicidad/elpepiopi/20021002elpepiopi_4/Tes : 07/01/2009: 13:20 hrs.)

sólo en caso de que el titular así lo deseara, de esta forma, las empresas tienen acceso a esta información de manera indirecta, debido a que el titular no da su consentimiento directamente a estas.

Por lo que se refiere al artículo 32, establece que las empresas u organismos sectoriales tanto públicos como privados pueden crear códigos tipo, los cuales son un conjunto de normas deontológicas o de buena práctica que son adaptadas para determinar las pautas a tener en cuenta, en cuanto al tratamiento y utilización de datos de carácter personal, en el desarrollo de su actividad[103], dichos códigos deberán ser inscritos en el Registro General de Protección de datos y en caso de no ajustarse a la LOPD, denegará el registro y solicitará las correcciones a los solicitantes.

El título V hace referencia a la transmisión de datos a nivel internacional, para lo cual, el artículo 33 establece la prohibición de ésta a países que no contemplen una protección de datos personales equiparable a la contenida en la LOPD, salvo que el país garantice las medidas de seguridad óptimas para la transferencia de la información, para lo cual, la Agencia Española de Protección de Datos evaluará dichas garantías así como también la naturaleza, finalidad, duración del tratamiento de datos, legislación vigente, informes de la Comisión de la Unión Europea, normas profesionales y medidas de seguridad en vigor en dichos países.

El artículo 34, contiene las excepciones en la aplicación del artículo anterior, entre las cuales podemos encontrar:

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

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

[103] http://www.microsoft.com/spain/empresas/faqs/6_codigos_tipo.mspx :07/01/2009: 14:35 hrs.

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

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

e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.

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

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

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

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

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

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

Continuando con este análisis, el capítulo VI, esta dedicado a la Agencia Española de Protección de Datos (más adelante AEPD) y en el artículo 35.1 se establece su naturaleza:

> *"La Agencia Española de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno."*

Como podemos ver, se trata de un organismo de carácter autónomo, lo cual busca que las resoluciones y opiniones que dicte se encuentren libres de cualquier injerencia del Gobierno, por otro lado y continuando con este artículo, dispone que la AEPD, se regirá por un estatuto interno y por la ley del Régimen Jurídico de las Administraciones Públicas y el Procedimiento Administrativo Común; con respecto al personal contratado por la agencia tendrán carácter de funcionarios públicos y deberán guardar secreto sobre los datos personales que administren durante el desarrollo de sus funciones.

Por lo que respecta a los medios económicos con los que cuenta para el desarrollo de sus funciones, esta podrá disponer, de:

- Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.

- Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.

- Cualesquiera otros que legalmente puedan serle atribuidos[104].

Ahora bien, el artículo 36, hace referencia al Director de la AEPD, el cual será designado por el Consejo Consultivo de la agencia por un período de cuatro años, para el ejercicio de sus funciones, atenderá sólo a las propuestas que el Consejo presente, todo esto con la finalidad de que su desempeño se desarrolle de forma objetiva y con independencia. En el caso de que el Director estuviera desempeñando una función pública, pasará al régimen de servicios especiales, debido a que este puesto es de consideración de "alto cargo", si estuviera desempeñando una función judicial o fiscal, pasará al régimen administrativo de servicios especiales, esta aclaración se debe al tipo de sistema de servicio profesional de carrera existente en España.

Por último, el Director de la AEPD, sólo podrá dejar el cargo antes del tiempo estipulado en los siguientes casos:

a) A solicitud propia

b) A petición del Gobierno (previa instrucción de expediente en el que necesariamente serán escuchados todos los miembros del Consejo)

c) Incumplimiento grave de sus funciones

d) Incapacidad para el ejercicio de sus funciones

e) Incompatibilidad

f) Condena por delito doloso

[104] Artículo 36 de la LOPD

En cuanto a las funciones de la AEPD, independientemente de que estas pudieran aumentar, el artículo 37 señala:

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

2. Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.

3. Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios establecidos en la Ley.

4. Atender las peticiones y reclamaciones formuladas por titulares de los datos afectados.

5. Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de datos personales.

6. Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del procesamiento de datos a las disposiciones contempladas en la Ley y, en su caso, ordenar el cese de los tratamientos y la cancelación de los ficheros, cuando no se ajusten a las disposiciones.

7. Ejercer la potestad sancionadora de acuerdo a las infracciones y sanciones contempladas en la Ley.

8. Informar acerca de los proyectos de disposiciones generales que se desarrollen para la LOPD.

9. Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.

10. Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.

11. Redactar un informe anual, el cual será enviado al Ministerio de Justicia.

12. Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.

13. Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recolección de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y aplicar las sanciones que en su caso existieran a la Administración Pública.

Asimismo, las resoluciones de la AEPD, deberán ser publicadas preferentemente en medios electrónicos y/o informáticos después de ser notificadas a los interesados, con excepción de aquéllas resoluciones referentes a la inscripción de un tratamiento de datos personales o de un código tipo.

Continuando con la organización de la AEPD, el artículo 38 señala que el Director de la agencia estará asesorado por un Consejo Consultivo que se regirá por las normas reglamentarias establecidas por la agencia y deberá reunirse por lo menos una vez cada seis meses, teniendo entre sus funciones la emisión de informes sobre todas

las cuestiones que solicite el Director de la agencia y la creación de propuestas en materia de protección de datos[105], dicho consejo estará conformado por:

- Un Diputado, propuesto por el Congreso de los Diputados.
- Un Senador, propuesto por el Senado.
- Un representante de la Administración Central, designado por el Gobierno.
- Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.
- Un miembro de la Real Academia de la Historia, propuesto por la misma.
- Un experto en la materia, propuesto por el Consejo Superior de Universidades.
- Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente[106].
- Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.
- Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente[107].

El artículo 39, establece el objeto del Registro General de Protección de Datos, el cual, es un órgano integrado en la AEPD y los procedimientos de inscripción,

[105] https://www.agpd.es/portalweb/conozca/estructura/index-ides-idphp.php#consejo :07/01/2009: 23:41 hrs.
[106] Se propone una terna por parte del Consejo de Consumidores y Usuarios de España.

contenido de la inscripción, modificación, cancelación, reclamaciones y recursos contra las resoluciones de éste, también este artículo establece el tipo de ficheros que estarán sujetos a este registro, entre los cuales encontramos:

- Los ficheros de que sean titulares las Administraciones públicas.
- Los ficheros de titularidad privada.
- Las autorizaciones a que se refiere la presente Ley.
- Los códigos tipo[108].
- Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

Otra de las facultades perteneciente a la AEPD, es la de inspeccionar los ficheros de datos personales, para lo cual, pueden solicitar informes o la exhibición de documentos relativos al tratamiento de los datos, así como también realizar visitas a los lugares en que físicamente se realizan los procedimientos, para la revisión de los equipos informáticos. En cuanto a los funcionarios que realicen la inspección, serán considerados autoridad pública, por lo que a su vez, éstos tendrán la obligación de guardar secreto sobre la información recabada, aún después de haber concluido en sus funciones[109].

Para terminar con este título, en cada una de las Comunidades Autónomas podrá crearse un órgano de protección de datos personales, que será independiente a la AEPD y podrá ejercer facultades de control sobre los ficheros creados en la administración local de su ámbito de territorio, dichas facultades serán iguales a las otorgadas a la agencia[110], con excepción de las referentes a la transmisión internacional de datos; por otro lado, el Director de la AEPD, podrá convocar a estos órganos a efectuar una cooperación institucional y coordinación de criterios o procedimientos de actuación, así como también, podrán solicitarse información

[107] Se propone una terna por parte del Consejo Superior de Cámaras Oficiales del Comercio, Industria y Navegación de España.
[108] *Vid Supra*, Artículo 32 de la LOPD. Pag. 89
[109] Artículo 40 de la LOPD

mutua para el cumplimiento de sus funciones; por último el Director de la AEPD, cuando constate que el mantenimiento o tratamiento de un fichero en una Comunidad Autónoma contraviene a lo dispuesto en la LOPD podrá requerir al órgano correspondiente se adopten las medidas necesarias en un plazo determinado y en caso de que esto no sea cumplido, el Director de la agencia podrá impugnar la resolución adoptada por ese organismo[111].

El título VII, hace referencia a la regulación de las infracciones y sanciones, el cual, ha nuestro punto de vista es el título más característico de esta ley, debido al grado de sanciones que impone y de ser la más estricta en la Unión Europea.

Primeramente, el artículo 43, menciona que tanto los responsables de los ficheros como de los tratamientos estarán sujetos a este régimen sancionador y para el caso de ficheros públicos, los responsables estarán sujetos al régimen disciplinario de las administraciones públicas.

En cuanto a la calificación de las infracciones, las clasifican en:

1. Leves, aquellas que no cumplan con alguna solicitud o procedimiento, siempre y cuando no constituyan una infracción grave, entre las cuales tenemos:

    a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

    b) No proporcionar la información que solicite la Agencia Española de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

[110] *Vid Supra*, artículo 37 de la LOPD. Pag. 93
[111] Artículo 42 de la LOPD

c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d) Proceder a la recolección de datos de carácter personal de los propios afectados sin haber sido previamente informados de modo expreso, preciso e inequívoco, del derecho de acceso a sus datos[112].

e) Incumplir el deber de secreto por parte del responsable del fichero o por cualquier otra persona que intervenga durante el tratamiento de los datos, salvo que constituya infracción grave[113].

2. Graves, cuando se incumplan procedimientos para el registro, acopio y aseguramiento de la información de acuerdo a lo que la LOPD dicta, entre las cuales encontramos:

a) Proceder a la creación de ficheros de titularidad pública o iniciar el acopio de datos de carácter personal, sin autorización de disposición general, publicada en el *Boletín Oficial del Estado* o Diario oficial correspondiente.

b) Proceder a la creación de ficheros de titularidad privada o iniciar la recolección de datos de carácter personal con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recolección de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

[112] De acuerdo a lo establecido en el artículo 5° de la LOPD
[113] En concordancia con lo establecido en el artículo 10 de la LOPD

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la LOPD o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la LOPD ampara.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia Española de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos

documentos e informaciones deba recibir o sean requeridos por aquel a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia Española de Protección de Datos.

l) Incumplir el deber de información a los titulares de los datos, establecidos para los ficheros de acceso público y los de información crediticia, cuando los datos hayan sido recabados de persona distinta del afectado.

3. Muy graves, cuando el tratamiento y procesamiento de los datos personales resulte en violaciones a los derechos individuales o en el uso y abuso de estos al margen de los lineamientos indicados en la LOPD, como son:

a) La recolección de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar los datos de carácter personal referentes a la ideología, religión, creencias cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referentes a salud, vida sexual y origen racial cuando no lo disponga una ley o el afectado no haya consentido expresamente, o la creación de ficheros que revelen la ideología, religión, creencias, salud, vida sexual y origen racial[114].

[114] *Vid Supra*, artículo 37 de la LOPD. Pag. 93

d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia Española de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia Española de Protección de Datos.

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia al apartado c), así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Con relación a la cuantía de las infracciones, el artículo 45 determina que estas serán fijadas de acuerdo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, grado de intencionalidad, reincidencia, daños y perjuicios causados a los titulares de los datos

y terceras personas y cualquier otra circunstancia que determine el grado de antijuridicidad y culpabilidad del acto, sin embargo, en caso de apreciarse una disminución de la culpabilidad del imputado, se establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracción que le preceda inmediatamente, dichas escalas, se encuentran establecidas de la siguiente forma[115]:

a) Infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.

b) Infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas.

c) Infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas.

Por lo que, en ningún caso podrá imponerse una multa que quede fuera del rango establecido por la ley y dichas multas serán actualizadas por el Gobierno de acuerdo a las variaciones que se den al índice de precios.

Para el caso de que las infracciones sean cometidas por las Administraciones Públicas, el Director de la AEPD dictará la resolución en que se indique la forma en que cesaran las anomalías, como serán corregidas y será comunicada al responsable del fichero, al órgano jerárquico superior y a los titulares afectados. De igual forma, el Director de la agencia podrá solicitar el inicio de los procedimientos administrativos a que hubiese lugar y a su vez, las resoluciones dictadas deberán ser

[115] Las cantidades establecidas en la LOPD, se encuentran en pesetas debido a que la fecha de promulgación de la ley es de 1999, la entrada del Euro se efectúo hasta el 2001, por lo que, la conversión que la misma AEPD utiliza para la aplicación de las infracciones, es de la siguiente manera: Infracciones leves de 600 a 60,000 euros; infracciones graves de 60,000 a 300,000 euros; infracciones muy graves de 300,000 a 600,000 euros (fuente: AEPD, mediante consulta vía correo electrónico).

informadas a la AEPD, así como también el Director de la agencia deberá comunicar al Defensor del Pueblo las actuaciones que efectúe y las resoluciones tomadas[116].

En relación a la prescripción, esta se contará a partir del día en que la infracción hubiese sido cometida y será interrumpida cuando de inicio el procedimiento correspondiente, reanudándose nuevamente en caso de que el procedimiento estuviese detenido por más de seis meses por causas no imputables al presunto infractor.

De acuerdo al tipo de infracción será el tiempo de prescripción, considerando así que las muy graves serán a los tres años, las graves a los dos años y las leves al año. En cuanto a las sanciones, están prescribirán a los tres años para las faltas muy graves, dos años para las graves y un año para las faltas leves, y el plazo de la prescripción de las sanciones comenzará a contarse desde el día siguiente a aquél en que sea de la resolución por la que se impone la multa[117].

Ahora bien, en lo que se refiere al procedimiento sancionador, la AEPD establecerá la reglamentación necesaria para que se lleve a cabo y de esta forma establecer las sanciones correspondientes; las resoluciones dictadas por la agencia agotaran la vía administrativa y tendrán una duración máxima de seis meses[118].

Por último, en los supuestos, constitutivos de infracción muy grave, de uso o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad, el Director de la AEPD podrá, requerir a los responsables de los ficheros, ya sean de titularidad pública como privada, la cesación en el uso o la cesión ilícita de los datos; en caso de no atender a este requerimiento la AEPD

[116] Art. 46 de la LOPD
[117] Art. 47 de la LOPD
[118] Art. 48 de la LOPD

podrá, mediante resolución, inmovilizar tales ficheros con el fin de restituir los derechos de las personas afectadas[119].

Como podemos ver, la LOPD es una legislación que busca privilegiar la protección de la intimidad y datos personales de los individuos sobre la comunidad y aún cuando la seguridad pública esta por encima de los derechos individuales, se procuró proteger dichos derechos a modo tal de evitar que se le de un mal uso a la información obtenida a partir de estos, por lo que, los organismos responsables de manejar dicha información tienen la obligación de eliminar los datos obtenidos una vez que dejen de tener utilidad para lo cual fueron recabados. Por otro lado, es de suma importancia como se hace la distinción para el tratamiento de datos entre ficheros públicos y privados, con esto queda demostrado que existe la posibilidad de reglamentar la información en manos de particulares, y de esta forma evitar el uso abusivo de los datos en su poder, recordándoles en todo momento que estos no les pertenecen y por lo tanto, deberán respetar los derechos de los titulares de los mismos.

Es también importante destacar, que con todas las medidas tomadas en la estructuración de la LOPD, se abre la posibilidad de considerar dato personal todo lo relacionado con el individuo, desde su nombre hasta su silueta tomada en una fotografía, tal y como se pudo constatar en la instrucción 1/2006, en que la AEPD, dictamina que el uso de videovigilancia solo podrá ser empleado para fines de seguridad pública y no dar motivos para que el individuo llegue a pensar que su intimidad ha sido violada por el solo hecho de encontrarse en el ángulo de grabación de la cámara.

[119] Art. 49 de la LOPD

2.3. Argentina

2.3.1. Antecedentes

En 1968, la promulgación de la ley 17.622 estableció que todos los datos recabados por el Sistema Estadístico Nacional debían guardar secrecía, por lo que estos solo podrían ser suministrados y publicados únicamente en compilaciones de conjunto, de tal modo que se buscaba proteger el secreto comercial o patrimonial y por lo tanto no podría individualizarse a las personas o entidades.

Fue hasta 1986, que se presentó ante el Congreso un proyecto de ley de protección de datos personales, elaborado por la Subsecretaría de Informática y Desarrollo del Ministerio de Justicia, el cual respondía a la recomendación hecha por el Consejo para la Consolidación de la Democracia, la cual señalaba que debía consagrarse el derecho a la privacidad, principalmente para evitar que las personas se vieran afectadas por los avances de la informática en materia de registro de datos.

Este primer proyecto, estaba basado principalmente en la Ley de Informática, ficheros y libertades (78-17) de Francia, sin embargo, esta no pudo ser consolidada y fue hasta con la reforma constitucional de 1994 que retomó un nuevo impulso, debido a que en el artículo 43, párrafo tercero se establecía:

> *"Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere, amenace, con arbitrariedades o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva. Podrán interponer esta acción contra cualquier forma de discriminación y en lo relativo a los derechos que protegen al ambiente, a la competencia, al usuario y al consumidor,*

> *así como a los derechos de incidencia colectiva en general, el afectado, el defensor del pueblo y las asociaciones que propendan a esos fines, registradas conforme a la ley, la que determinará los requisitos y formas de su organización. Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o banco de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos. No podrá afectarse el secreto de las fuentes de información periodística. Cuando el derecho lesionado, restringido, alterado o amenazado fuera de la libertad física, o en caso de agravamiento ilegítimo en la forma o condiciones de detención, o en el de desaparición forzada de personas, la acción de habeas corpus podrá ser interpuesta por el afectado o por cualquiera en su favor y el juez resolverá de inmediato, aun durante la vigencia del estado de sitio"*[120].

Como podemos ver, en este artículo también fue incluido dentro de la acción de amparo, el *habeas data* con el fin de que el titular de los datos personales tuviera conocimiento de los registros existentes, ya fueran **públicos o privados**, destinados a otorgar información relativa a su persona y de esta forma tener la oportunidad de exigir su supresión, rectificación, confidencialidad o actualización y evitar cualquier tipo de falsedad o discriminación.

Por otro lado, comenzaron a realizarse diversos proyectos de ley, muchos de los cuales estaban basados en la Ley Orgánica de Protección de Datos de Carácter Personal de España, sin que alguno de éstos pudiera llegar a ser consolidado, dando por consecuencia que al no poder existir una ley reglamentaria para el ejercicio del *habeas data*, está tuvo que ser desarrollada por vía jurisprudencial.

[120] Constitución Nacional de la República de Argentina. Texto vigente.

Más adelante, en 1996 el Congreso aprobó la ley número 24.745, sin embargo, esta ley fue vetada por parte del Poder Ejecutivo mediante el decreto 1616/96; por lo que hasta 1998, el Senado presentó una nueva ley, la cual fue aprobada bajo el número 25.326 el 4 de octubre de 2000 y promulgada mediante el decreto número 995 el 30 de octubre del mismo año, en esta ocasión el Poder Ejecutivo vetó los incisos 2 y 3 del artículo 29 que hacían referencia a la autonomía del organismo de control y el artículo 47 que señalaba que los bancos de información crediticia suprimieran toda información relacionada con deudas canceladas[121].

Ya con la ley promulgada, mediante decreto 1558/2001 se creó la Dirección Nacional de Protección de Datos Personales como organismo de control.

Como pudimos ver, tuvieron que transcurrir 32 años desde el primer intento de regulación para que Argentina tuviera una ley de protección de datos personales, aquí lo destacable fue que un principio partieron de la experiencia francesa y española para crear su legislación, dando por resultado a ser uno de los mejores ejemplos a seguir como ley general, ya que a partir de esta experiencia buscaron que la ley cumpliera con los lineamientos marcados por la Unión Europea en la directiva 95/46 y debido a ello, Argentina es el único país latinoamericano que goza del *ut-supra* el cual es un estatus de "nivel de protección adecuado" con respecto a los datos transmitidos por la Comunidad Europea, por decisión de la Comisión reguladora[122].

2.3.2. Ley 25.326. Protección de los Datos Personales.

Al igual que las otras dos legislaciones revisadas, comenzaremos con el análisis del objeto de esta ley, el cual se encuentra plasmado en el primer artículo:

[121] TANÚS, Gustavo Daniel. *Protección de datos personales. Principios generales, derechos, deberes y obligaciones*. Argentina: Revista Jurídica El Derecho, 19 de julio de 2002. En: http://www.protecciondedatos.com.ar/ 16/01/2009 : 22:01 hrs.
[122] Decisión C (2003) 1731 de 30 de junio de 2003, dictada por la Unión Europea

> *"La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.*
>
> *Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.*
>
> *En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas"*[123].

Al revisar este artículo, podemos darnos cuenta de distintas cuestiones que busca proteger esta ley, por lo cual resulta interesante desglosar cada una de las garantías que protege:

a) La protección integral de datos personales que se encuentren en cualquier registro de datos *u otros medios técnicos de procesamiento de datos*, haciendo hincapié en esto último, debido a que es el que nos abre la posibilidad de que se trate de cualquier tipo de registro ya sea electrónico o en papel, como lo veremos más adelante con el análisis del artículo 2 que trata de las definiciones técnicas contempladas en la ley.

b) Busca la protección del derecho al honor y a la intimidad de las personas, con lo que se reconoce que ninguna persona debe ser

[123] Artículo 1° de la Ley 25.326

molestada como resultado de cualquier procesamiento de datos y garantizar que la información contenida en estos registros sea fidedigna.

c) Garantiza el derecho de acceso a la información, con ello, el titular de los datos puede conocer quien y para que tiene en su poder información en torno a su persona y por lo tanto, solicitar la corrección, supresión o cancelación de sus datos.

d) Aquí lo interesante de esta ley, es que extiende esta protección de datos a las personas morales, reconociendo de esta forma, que es posible hacer extensible este derecho en los casos especiales o que la entidad así lo solicite por su conveniencia.

e) Por último, busca proteger las fuentes de información periodísticas, con lo que se garantiza la libertad de expresión y de prensa, evitando así intromisiones inadecuadas por parte del Gobierno, claro esta que así como lo vimos con la LOPD, esto también responde a la propia experiencia de este país, que ha tenido por los regímenes autoritarios.

El artículo 2, contiene las definiciones de cada uno de los conceptos que se manejan a lo largo de la ley, con ello se evita la mala interpretación que pudiera darse en la aplicación de la misma, por lo que entre estas definiciones encontramos:

1. *Datos personales*: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables. Al ser una definición simple se logra ampliar el espacio de protección, al referirse a *cualquier tipo,* con lo cual todos los datos que pudieran obtenerse serán protegidos, como iremos viendo en el desarrollo del análisis de esta ley.

2. *Datos sensibles*: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales,

afiliación sindical e información referente a la salud o a la vida sexual. Evitando de esta forma, cualquier tipo de discriminación que pudiera darse en el tratamiento de datos.

3. *Archivo, registro, base o banco de datos*: Indistintamente, designan al conjunto organizado de datos personales objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso. Hace referencia a cualquier tipo de soporte del archivo, contemplando por ejemplo, los electrónicos y los de papel[124].

4. *Tratamiento de datos:* Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias. Quizá esta sea la definición más completa de tratamiento de datos de las tres leyes ya estudiadas, debido a que se buscó ampliar el aspecto de protección con el fin de evitar que alguna etapa del tratamiento de datos quedará fuera del ámbito de protección.

5. *Responsable de archivo, registro, base o banco de datos*: Persona física o de existencia ideal pública o privada, que es titular de un archivo, registro, base o banco de datos. Con esto, incluye tanto a las personas que manejan la información como también a los organismos que la administran, de esta forma, se logra ampliar las personas obligadas al cumplimiento de esta ley.

6. *Datos informatizados*: Los datos personales sometidos al tratamiento o procesamiento electrónico o automatizado. Esta definición suena

[124] *Vid Supra*, inciso a). Pag. 108

contraria a la señalada en el inciso 3, debido a que si se piensa en la definición de automatizado[125], como cualquier proceso dirigido a la organización o mecanización de un trabajo se pensaría que solo contempla aquellos procedimientos realizados de manera electrónica, pero si se da una interpretación más amplia, se pueden incluir en caso necesario aquellos procedimientos realizados manualmente, debido a que se realizan de acuerdo a un método establecido.

7. *Titular de los datos*: Toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley. Aquí solo cabe destacar el hecho de que se contempla ampliar la protección también a las personas morales.

8. *Usuario de datos*: Toda persona, pública o privada que realice a su arbitrio el tratamiento de datos, ya sea en archivos, registros o bancos de datos propios o a través de conexión con los mismos. En las otras leyes esta definición esta contemplada como la "cesión de datos", para contemplar también los procedimientos que se generen después de que el responsable del archivo entrega la información obtenida a terceras personas.

9. *Disociación de datos*: Todo tratamiento de datos personales de manera que la información obtenida no pueda asociarse a persona determinada o determinable. Este concepto contempla la protección de la intimidad de la persona, al evitar que esta sea totalmente identificable por el solo hecho de realizar un tratamiento de datos en el que se logre reunir desde aspectos generales hasta aquellos que hacen referencia al interior de la persona como lo sería la ideología[126].

[125] Automátizado: Ciencia que trata de sustituir en un proceso el operador humano por dispositivos mecánicos o electrónicos. Diccionario de la Real Academia Española (http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=automatico)
[126] *Vid Supra,* 1.3 Derecho a la intimidad. Pags. 25 a 28.

El capítulo II, establece diez principios generales en relación a la protección de datos personales, entre los que tenemos:

1. *Licitud de los archivos de datos*. Lo cual significa que todo archivo de datos deberá estar inscrito de acuerdo a lo establecido en la ley y su finalidad, nunca deberá ser contraria a las leyes o moral pública[127].

2. *Calidad de los datos*. Se establece que todos los datos recabados deberán ser ciertos, adecuados, pertinentes y no excesivos con relación al ámbito y finalidad para lo cual fueron recabados, de la misma forma, no podrán ser recolectados por medios fraudulentos o contrarios a la ley y por otro lado, garantizar el acceso, rectificación y cancelación de los datos y la eliminación de los mismos cuando el fin para el que fueron recabados se haya cumplido[128].

3. *Consentimiento*. Se considera que el tratamiento de datos es ilícito cuando no existe el consentimiento expreso por parte del titular, el cual debe ser otorgado de manera libre e informada y sólo en caso de que sean obtenidos de registros de acceso público e irrestricto, o sean para el ejercicio del poder público del Estado, o deriven de una relación contractual, o deriven de operaciones que realicen las entidades financieras, no será necesario el consentimiento por parte del titular de los datos[129].

4. *Información*. El titular de los datos, tiene el derecho de conocer la finalidad del tratamiento de datos, a quien serán transmitidos y las consecuencias de otorgarlos, así como también su derecho de acceso, rectificación o supresión de los datos[130].

[127] Art. 3° de la ley 25.326
[128] Art. 4° de la ley 25.326
[129] Art. 5° de la ley 25.326
[130] Art. 6° de la ley 25.326

5. *Categoría de los datos*. Se garantiza que ninguna persona puede ser obligada a otorgar datos sensibles, y solo podrán ser recabados éstos, en caso de que el tratamiento sea con fines estadísticos o científicos sin que puedan ser identificados los titulares, y sólo las asociaciones religiosas, políticas y sindicales podrán llevar registros de sus integrantes, de igual manera, aquellos datos que hagan referencia a antecedentes penales podrán ser procesados por las autoridades competentes y dentro del marco de las leyes reglamentarias existentes[131].

6. *Datos relativos a la salud*. Los profesionales de la salud, podrán recabar datos relativos a la salud física o mental de aquellas personas que se encuentren o se hayan encontrado bajo tratamiento médico, siempre que se guarden los principios del secreto profesional[132].

7. *Seguridad de los datos.* Por una parte el responsable de los datos, debe garantizar la seguridad y confidencialidad de los datos, a modo tal de evitar la adulteración, supresión o desviación de información, en el tratamiento de los datos y por otro lado, se prohíbe el registro de datos en base de datos que no cuenten con las medidas de seguridad establecidas en la ley[133].

8. *Deber de confidencialidad.* Al igual que la LOPD, el responsable del tratamiento de datos y las personas que intervengan el procesamiento de estos, tienen la obligación de guardar secreto profesional aún después de finalizada la relación con el titular del tratamiento de datos y sólo en caso de resolución judicial y que medien razones de seguridad nacional podrán ser relevados de esta obligación[134].

[131] Art. 7° de la Ley 25.326
[132] Art. 8° de la Ley 25.326
[133] Art. 9° de la Ley 25.326
[134] Art. 10° de la Ley 25.326

9. *Cesión.* Los datos personales sólo pueden ser cedidos para cumplir con los fines establecidos entre el cesionario y el cedente, siendo ambos responsables del tratamiento de los datos, por lo que, ambos responderán solidaria y conjuntamente ante la autoridad responsable y por otro lado necesitarán previa autorización del titular de éstos, sin embargo, por parte de este último, el consentimiento para la cesión puede ser revocada, a menos que sea por disposición de la ley, o que la cesión sea otorgada entre dos órganos del Estado, o que esta sea necesaria para fines de salubridad y siempre y cuando se mantenga en secreto la titularidad de los datos, o bien que se haya realizado un proceso de disociación que evite la identificación del titular de los datos[135].

10. *Transferencia internacional*. Esta prohibida la transferencia con países que no tengan leyes que garanticen los mismos niveles de seguridad en la protección de datos y podrá ser revocada esta prohibición en caso de colaboración judicial internacional, transacciones bancarias o bursátiles, intercambio de datos médicos con el fin de investigaciones epidemiológicas o en el tratamiento del afectado, en el marco de cooperación de tratados internacionales o que se tenga por objeto la cooperación internacional en materia de seguridad, lucha contra el narcotráfico, terrorismo y crimen organizado[136].

Como podemos ver, estos principios están totalmente alineados a los principios que la Unión Europea ha marcado en la directiva 95/46 y que como pudimos analizar anteriormente, se encuentran inmersos en las dos leyes ya estudiadas.

Continuando con esta ley, en el capítulo III se establecen los derechos de los titulares de los datos, entre los que encontramos:

[135] Art. 11° de la Ley 25.326

1. *Derecho de Información*. Se garantiza que toda persona tiene derecho a solicitar al organismo de control información de la existencia de bases de datos o registros de datos, sus finalidades y la identidad de los responsables, además que el registro que dicho órgano lleve será de consulta pública y gratuita[137].

2. *Derecho de acceso*. Previa identificación, toda persona tiene derecho a obtener información de las bases de datos que contengan sus datos personales; el responsable de los datos tiene la obligación de contestar a una solicitud de acceso dentro de los diez días siguientes, si al término del plazo, no otorga la información o esta no satisface al titular de los datos, se podrá dar inicio al recurso de *habeas data*. Ahora bien, dicho derecho de acceso puede ser ejercido en un plazo no menor a seis meses, a menos que se acredite un interés legítimo para acceder en un tiempo menor y en caso de personas fallecidas el acceso a sus datos podrá ejercerlo su heredero universal[138].

3. *Contenido de la información*. La información otorgada al titular de los datos deberá ser entregada en lenguaje claro y de forma amplia, aún cuando la solicitud no lo contemplara y nunca deberá contener información de terceras personas aún cuando se encuentren vinculadas a la información[139].

4. *Derecho de rectificación, actualización o supresión*. El titular de los datos tiene derecho a la rectificación, actualización o supresión de la información relativa a él contenida en una base de datos, el responsable del tratamiento al recibir la solicitud tendrá que realizar la modificación o cancelación en un plazo no mayor a cinco días, en el caso de cesión o transmisión de datos, el responsable deberá notificar al cesionario al quinto día de realizada la modificación en el tratamiento de los datos, sin embargo, dicha modificación o tratamiento no podrá ser realizado en caso de afectación de terceros y durante

[136] Art. 12° de la Ley 25.326
[137] Art. 13 de la Ley 25.326
[138] Art. 14 de la Ley 25.326
[139] Art. 15 de la Ley 25.326

el proceso de rectificación los datos deberán ser bloqueados o informar en caso de solicitud que se encuentra sometida a la revisión. Por último, se contempla también que los datos deberán ser conservados sólo durante el tiempo contractual establecido entre el responsable, usuario y el titular de los datos. En el caso de negación de este derecho, el titular de los datos podrá ejercer la acción de *habeas data* prevista en la ley[140].

5. *Gratuidad*. La rectificación, modificación o supresión de los datos debe ser realizado en forma gratuita[141].

6. *Impugnación de valoraciones personales*. Las decisiones judiciales o actos administrativos que impliquen la apreciación o valoración de conductas humanas únicamente a través del procesamiento automatizado de datos, serán nulos[142].

Dentro de este capítulo, también se establecen las excepciones, al derecho de acceso a información personal, la cuales constan de:

a) Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, denegar el acceso, rectificación o la supresión en cuanto se trate de cuestiones de seguridad o defensa de la Nación o de la protección de los derechos e intereses de terceros.

b) La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando se pudieran obstaculizar las actuaciones judiciales o administrativas vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, en relación a las funciones de control de la salud y del medio ambiente, investigación de delitos y la verificación de infracciones administrativas. Dicha resolución deberá ser fundada y notificada al afectado.

[140] Art. 16° de la Ley 25.326
[141] Art. 19° de la Ley 25.326

c) Deberá brindarse acceso a los registros en cuestión en que el titular de los datos tenga que ejercer su derecho de defensa[143].

Por último, y solo para el caso de seguridad nacional, las Comisiones de Defensa Nacional, la Comisión Bicameral de Fiscalización de los Órganos y Actividades de Seguridad Interior e Inteligencia del Congreso de la Nación y la Comisión de Seguridad Interior de la Cámara de Diputados, tendrán derecho de acceso a la información de los datos personales[144].

El capítulo IV de la ley, establece entre otras cosas, las obligaciones de los administradores respecto a la forma de prestar la consulta y acceso a los registros y los requerimientos que deben cumplirse para el registro de las bases de datos.

Los requisitos para la inscripción y registro de las bases datos se encuentran establecidos en el artículo 21:

1. Todo archivo, registro, base o banco de datos público, y privado destinado a proporcionar informes[145] debe inscribirse en el Registro que al efecto habilite el organismo de control.

2. El registro deberá comprender como mínimo:
    a) Nombre y domicilio del responsable,
    b) Características y finalidad del archivo,
    c) Naturaleza de los datos personales contenidos en cada archivo,

[142] Art. 20° de la Ley 25.326
[143] Art. 17° de la Ley 25.326
[144] Art. 18° de la Ley 25.326
[145] A nuestro parecer el hecho de que se especifique que el destino de las bases de datos sea "proporcionar informes" puede dejar al margen algún otro tipo de bancos que no tenga por objetivo principal dar información, sino por ejemplo, sólo ser utilizado como mecanismo de control.

d) Forma de recolección y actualización de datos,

e) Destino de los datos y personas físicas o morales a las que pueden ser transmitidos,

f) Modo de interrelacionar la información registrada

g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información,

h) Tiempo de conservación de los datos, y

i) Forma y condiciones en que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación o actualización de los datos.

3. Ningún usuario de datos podrá poseer datos u obtener datos personales de naturaleza distinta a los declarados en el registro.

Por otro lado, los archivos que sean creados por particulares y que no tengan como fin exclusivo el uso personal, también deberán ser inscritos de acuerdo a lo establecido en este artículo[146].

Para el caso de banco de datos que sean administrados por organismos públicos, el artículo 22 establece que las normas destinadas a su creación, modificación o supresión deberán ser publicadas en el Boletín Oficial, cumpliendo con los siguientes requisitos:

a) Características y finalidad del archivo,

[146] Art. 24° de la Ley 25.326

b) Personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas,

c) Procedimiento de obtención y actualización de los datos,

d) Estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán,

e) Las cesiones, transferencias o interconexiones previstas,

f) Órganos responsables del archivo, precisando dependencia jerárquica en su caso, y

g) Las oficinas ante las que se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión.

Para el caso de la supresión de datos de bancos informatizados además deberá indicarse el destino que estos tendrán o las medidas que se adoptaran para ello, nuevamente es importante indicar aquí, que la ley hace mención únicamente de bancos informatizados, lo cual deja al margen cualquier otro tipo de registro como lo son los que se encuentran en papel, que a pesar de los avances tecnológicos, no puede descartarse la existencia de este tipo de registros, que muy probablemente continúen funcionando.

En el artículo 23, la ley establece reglas especiales sobre los registros de datos que versan sobre la seguridad nacional, ya sean los administrados por las fuerzas armadas, fuerzas de seguridad, organismos policiales o sobre antecedentes personales, debido a que éstos registros generalmente son concentrados sin el consentimiento de los titulares de los datos, por lo que su uso queda limitado al estricto cumplimiento de una asignación especial, como por ejemplo, la defensa nacional, seguridad nacional o represión de los delitos y los archivos para tales casos deben ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad y en el caso particular de los registros con fines

policiales, estos serán cancelados cuando ya no sean necesarios para la averiguación por la cual fueron recabados.

Más adelante, en el artículo 25, para la prestación de servicios informatizados, se establece que en caso de ser otorgado este servicio por cuenta de terceros (o subcontratación) no podrán usarse con fines distintos a los que figuren en el contrato que para ello se haya realizado, cederlos a otras personas o mucho menos para su conservación y una vez cumplida la prestación contractual, los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquél por cuenta de quien se prestan tales servicios y cuando se presuma la posibilidad de futuros encargos, en cuyo caso pueden almacenarse con las debidas condiciones de seguridad por un período de hasta dos años.

Por su parte, el artículo 26 establece para la prestación de servicios de información crediticia, los siguientes principios:

1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de la información facilitada por el interesado.

2. Pueden tratarse también datos personales relativos al cumplimiento o incumplimiento de obligaciones de carácter crediticio, facilitados por el acreedor o por quien actúe por su cuenta o interés.

3. A solicitud del titular de los datos, el responsable o administrador del registro de datos, le informará de los resultados del tratamiento y de las evaluaciones que sobre el mismo hayan sido otorgadas durante los últimos seis meses y el nombre y domicilio del cesionario en el caso de tratarse de datos obtenidos por cesión.

4. Sólo podrán archivarse, registrarse o cederse los datos personales que sirvan para evaluar la solvencia económico-financiera del titular de los datos durante los últimos cinco años y dicho plazo se reducirá a dos años cuando el deudor cancele o extinga la obligación, debiéndose hacer constar dicho hecho, o lo que es lo mismo, se establece el principio al olvido.

5. La prestación de servicios de información crediticia no requiere el previo consentimiento del titular de los datos a los efectos de su cesión, ni la posterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios, por lo que, a nuestro parecer pudiera dejar en desventaja al titular si este no se entera a tiempo del tratamiento que sobre sus datos se haya realizado, debido a que si existiera algún error en la información obtenida, se le estaría negando el derecho de rectificación.

Para fines publicitarios, el artículo 27 establece que para la compilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, pueden tratarse datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios, o bien, permitan establecer hábitos de consumo, cuando éstos figuren en documentos públicos o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento, por su parte, el titular podrá solicitar, sin cargo alguno, el acceso a sus datos o en cualquier momento, el retiro o bloqueo de estos.

Con relación al registro de datos recabados para encuestas, esta ley no es aplicada en la medida que los datos obtenidos no puedan atribuirse a persona determinada, para el caso de investigación de mercados, científicos o médicos; pero, si se diera el caso de que no resultara posible mantener el anonimato, el responsable del tratamiento deberá utilizar un procedimiento de disociación, a modo tal que no se permita la identificación de persona alguna[147].

[147] Art. 28ª de la Ley 25.326

Continuando con este análisis, el capítulo V esta consagrado a los controles en materia de protección de datos personales y el artículo 29 establece al organismo de control, llamado Dirección Nacional de Protección de Datos Personales (mas adelante DNPDP), el cual goza de autonomía y sus actos son descentralizadas del Ministerio de Justicia y Derechos Humanos del propio país, a diferencia de las dos leyes anteriores la descripción de las facultades, funciones y organización, de esta Dirección, no son tan amplias puesto que sólo se encarga de describir *groso modo* sus funciones, ya para revisar a fondo su organización es necesario recurrir a la reglamentación interna[148].

Por lo tanto, dentro de esta ley, se señalan como funciones de la DNPDP:

a) Asistir y asesorar a las personas que lo requieran acerca de los alcances de la ley y de los medios legales de que disponen para la defensa de los derechos garantizados por la misma.

b) Dictar las normas y reglamentaciones que se deban observar para el desarrollo de las actividades comprendidas por la ley.

c) Realizar un registro de archivos, registros o bancos de datos personales y mantener su registro.

d) Vigilar el cumplimiento de la ley sobre integridad y seguridad de datos por parte de los archivos, registros o bancos de datos, para ello, podrá solicitar autorización judicial para acceder a locales, equipos, o programas de tratamiento de datos con el fin de investigar si se realizan infracciones a la ley.

e) Solicitar información a los organismos públicos y privados, los cuales deberán proporcionar antecedentes, documentos, programas u otros

[148] Decreto Nº 1558/01. En: http://www.jus.gov.ar/dnpdpnew/ 09/02/09: 22:35 hrs.

elementos que estén relacionados con el tratamiento de los datos personales; para estos casos, la autoridad deberá garantizar la seguridad y confidencialidad de la información y elementos suministrados.

f) Imponer las sanciones administrativas que correspondan por la violación a la ley y sus reglamentos.

g) Constituirse en querellante en las acciones penales que se promuevan por violaciones a la presente ley.

h) Vigilar el cumplimiento de los requisitos y garantías, que para obtener la correspondiente inscripción en el Registro, deben reunir los archivos o bancos de datos privados destinados a suministrar informes.

Por otro lado, la DNPDP será dirigida por un Director Nacional, que cuente con la experiencia y conocimientos en la materia, nombrado por el Poder Ejecutivo con acuerdo del Senado. Estará dedicado a sus funciones y podrá ser removido por su mal desempeño por el mismo Poder Ejecutivo, así como también, las leyes en materia de responsabilidad administrativa le son aplicables.

Ahora bien, como se señaló anteriormente, para conocer de la organización de la DNPDP, recurrimos al decreto 1558/2001, el cual estipula que la Dirección Nacional contará con un Consejo Consultivo, el cual se desempeñará *ad honorem* y tendrá entre sus funciones la de asesorar en los asuntos de importancia al Director, dicho Consejo estará integrado por:

a) un representante del Ministerio de Justicia y Derechos Humanos

b) un magistrado del Ministerio Público Fiscal con especialidad en la materia.

c) Un representante de los archivos privados destinados a dar información designado por la Cámara que agrupe a las entidades nacionales de información crediticia.

d) Un representante de la Federación de entidades empresarias de información comercial de la nación.

e) Un representante del Banco Central de la nación.

f) Un representante de las empresas dedicadas a la publicidad, designado por las Cámaras respectivas de común acuerdo[149].

g) Un representante del Consejo Federal del Consumo

h) Un representante del Instituto Argentino de Normalización con especialidad en seguridad informática.

i) Un representante de la Superintendencia de seguros de la nación.

j) Un representante de la Comisión Bicameral de Fiscalización de los órganos y actividades de seguridad interior e inteligencia del Congreso.

Continuando con la ley, el artículo 30 establece la forma en que deberán operar los códigos de conducta establecidos por los organismos privados, los cuales deberán establecer normas para el tratamiento de datos personales que busquen asegurar y mejorar las condiciones de operación de los sistemas de información en función de los principios determinados en la ley. Así mismo, estos códigos deberán ser inscritos en el registro establecido por la DNPDP, quien podrá negar la inscripción cuando considere que no se ajustan a las disposiciones legales y reglamentarias sobre la materia.

En cuanto a las sanciones, la misma ley en su capítulo VI, establece dos tipos de sanciones, administrativas y penales, las cuales podrán aplicarse de manera

separada o en conjunto según sea el caso, es importante señalar, que de la misma forma que sucedió con el capítulo referente a la organización, las sanciones sólo son nombradas en la ley y la disposición 7/2005[150] es la que establece la clasificación de las sanciones, la cual es muy parecida a la LOPD por la forma de dividir las sanciones en leves, graves y muy graves y que más adelante podremos analizar las similitudes entre ambas leyes.

Ahora bien, entre las sanciones administrativas encontramos:

> *"1. Sin perjuicio de las responsabilidades administrativas que correspondan en los casos de responsables o usuarios de bancos de datos públicos; de la responsabilidad por daños y perjuicios derivados de la inobservancia de la presente ley, y de las sanciones penales que correspondan, el organismo de control podrá aplicar las sanciones de apercibimiento, suspensión, multa de mil pesos ($ 1.000.-) a cien mil pesos ($ 100.000.-), clausura o cancelación del archivo, registro o banco de datos.*
>
> *2. La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso."*[151]

Esto es, la cuantía de las sanciones deberá ser de acuerdo a la naturaleza de los derechos personales afectados, a la cantidad y volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia,

[149] *Vid Supra,* artículo 27. pag. 121
[150] Esta disposición deroga la anterior 1/2003, debido a que en esta nueva se buscó que la DNPDP, creara un registro de reincidentes, para llevar un mejor control, cuantía de las sanciones aplicadas a estos, sin embargo, dejaron la limitante de 3 años para seguir considerando a una persona reincidente y por lo tanto mantenerlo dentro de este registro.
[151] Art. 31ª de la Ley 25.326

a los daños y perjuicios causados a los titulares de los datos y a terceros o a cualquier otra circunstancia que sea relevante para determinar el grado de culpabilidad[152], por lo que, con esto queda plasmada la función de control que la DNPDP respecto de la vigilancia de registros y tratamientos de datos personales, sin embargo, revisando el mencionado Decreto 1558/2001 y la disposición 7/2005, a la DNPDP se le limita esta facultad de control debido a que, en caso de que un responsable de fichero o tratamiento de datos, se le compruebe nuevamente alguna infracción dentro del período de tres años después de ser sancionado por primera vez, será considerado reincidente y por lo tanto, las sanciones aplicables pueden llegar a ser más severas, sin embargo, ¿qué pasará con aquella persona que espera a que se cumpla este período antes de violar nuevamente la ley?, desgraciadamente, la propia ley Argentina no lo contempla, lo cual hace pensar que cualquiera puede esperar a que se cumpla dicho período para poder reincidir y sólo hacerse acreedor a una sanción mínima, cuando en realidad debiera ser sancionado de manera más severa.

Ahora bien, el artículo 32 de esta ley, señala las sanciones penales que deberán aplicarse de acuerdo a la violación de los derechos protegidos:

a. Sanción de seis meses a tres años, al que proporcione a un tercero información falsa contenida en un archivo de datos personales.

b. La sanción penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.

c. En caso de que el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, será aplicable además la inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el establecido por la condena.

[152] Art. 31ª del Decreto 1558/2001

d. Sanción de un mes a dos años de prisión a quien viole los sistemas de confidencialidad y seguridad de datos, o accese de cualquier forma, a un banco de datos personales.

e. La misma sanción se establecerá a quien proporcione a otra persona, que no se encuentre autorizada mediante el registro en un banco de datos personales, un secreto que estuviera obligado a preservar por disposición de una ley, y cuando el infractor sea funcionario público se le aplicará además, la inhabilitación de uno a cuatro años.

f. Sanción de un mes a dos años de prisión a quien inserte o haga insertar datos en un archivo de datos personales, y cuando el infractor sea funcionario público se le aplicará además, la inhabilitación de uno a cuatro años.

Ahora bien, para completar la clasificación de estas sanciones y sus infracciones, la disposición 7/2005, establece la clasificación y la graduación de estas:

1. Serán consideradas infracciones leves:

a) No atender la solicitud de acceso, rectificación o supresión de los datos personales objeto de tratamiento cuando legalmente proceda.

b) No proporcionar la información que solicite la Dirección Nacional de Protección de Datos Personales en el ejercicio de las competencias que tiene atribuidas.

c) No solicitar la inscripción de las bases de datos personales tanto públicas como privadas y cuyo registro sea obligatorio en los términos exigidos por la Ley Nº 25.326 y sus normas complementarias.

d) Recoger datos de carácter personal sin proporcionar a los titulares de los mismos la información necesaria acerca de la recolección de los datos personales[153] o sin recabar su consentimiento libre, expreso e informado en los casos en que esto sea exigible.

e) Incumplir el deber de secreto establecido por la Ley 25.326[154], salvo que el responsable del tratamiento vulnere la seguridad de los registros, lo cual constituiría una infracción grave, o bien, que viole el secreto establecido para datos sensibles y los recabados para fines penales, lo que constituiría una infracción muy grave.

f) No respetar el principio de gratuidad al titular de los datos en el acceso, modificación, corrección y supresión[155].

g) Mantener por más tiempo del establecido el registro, archivo o cesión de los datos significativos para evaluar la solvencia económico-financiera de los titulares de los datos.

h) Tratar, dentro de la prestación de servicios de información crediticia, datos personales patrimoniales que excedan la información relativa a la solvencia económica y al crédito del titular de tales datos.

i) Tratar, en los archivos, registros o bancos de datos con fines publicitarios, datos que excedan la información para establecer perfiles con fines promocionales o hábitos de consumo.

j) No cesar en el uso ilegítimo del tratamiento de datos cuando sea requerido por el titular, incluyendo en este supuesto la negativa a retirar o bloquear el

[153] *Vid Supra*, 4. Información. Pag. 112
[154] *Vid Supra*, 8. Deber de confidencialidad. Pag. 113
[155] *Vid Supra*, 5. Gratuidad. Pag. 116

nombre y dirección de correo electrónico de los bancos de datos destinados a publicidad cuando su titular así lo solicite[156].

k) Proceder al tratamiento de datos personales que no reúnan la calidad de ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.

Nótese que dentro de estas infracciones, la disposición contempla también el exceso en el manejo o tratamiento de datos que tengan como finalidad conocer la capacidad crediticia del titular o para fines publicitarios, especificando de esta forma, otras sanciones que en la práctica no habían sido consideradas en otras leyes como la LOPD, con ello, y a partir de la experiencia española, Argentina trató de abarcar un mayor ámbito de protección.

En cuanto a la cuantía, para estas infracciones, se establece que la sanción ira desde dos apercibimientos y/o multa de $ 1,000 a $ 3,000 pesos.

2. Serán consideradas infracciones graves:

a) Tratar los datos de carácter personal en forma ilegítima o con menosprecio de los principios y garantías establecidos en Ley 25.326 y sus normas reglamentarias.

b) Realizar acciones concretas tendientes a impedir u obstaculizar el ejercicio por parte del titular de los datos del derecho de acceso o negarse a facilitarle la información que sea solicitada.

c) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones, actualizaciones o supresiones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares de los datos.

[156] *Vid Supra,* artículo 2. Pag. 109

d) Vulnerar el deber de guardar el deber de confidencialidad y la seguridad de los registros[157].

e) Mantener bases de datos locales, programas o equipos que contengan datos personales sin las debidas condiciones de seguridad establecidas por los reglamentos o disposiciones en la materia.

f) Obstruir el ejercicio de la función de inspección y fiscalización a cargo de la DNPDP.

g) No inscribir la base de datos personales en el registro correspondiente y/o cuando haya sido requerido por la DNPDP.

h) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando haya sido requerido por la DNPDP.

i) Recabar datos de carácter personal mediante el engaño.

En este tipo de sanciones no fueron tan específicos para la clasificación, ni contempla como aspectos “muy graves” aquellos como los establecidos en los incisos h) e i), que en la LOPD, si son sancionados con mayor dureza, quizá esto sea a que en este apartado se contempla de forma general las infracciones, debido a que esta más relacionada con la administración de las bases y los registros de datos personales.

Respecto a la cuantía de las sanciones estas serán de hasta 4 apercibimientos, suspensión, en el manejo o tratamiento de la base de datos, de 1 a 30 días y/o multa de $ 3,001 a $ 50,000 pesos.

[157] *Vid Supra*, en relación al inciso e) Deber de secreto. Pag.128

3. Serán consideradas infracciones muy graves:

a) Conformar un archivo de datos cuya finalidad sea contraria a las leyes o a la moral pública.

b) Transferir datos personales de cualquier tipo a países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, salvo que sean con fines de cooperación internacional[158].

c) Ceder ilegítimamente los datos de carácter personal.

d) Recolectar y tratar los datos sensibles sin que medien razones de interés general autorizadas por la ley o tratarlos con finalidades estadísticas o científicas sin hacerlo de manera disociada.

e) Formar archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles, salvo aquellos registros o bases de datos creados por organizaciones religiosas, sindicales o profesionales.

f) Tratar los datos personales de forma ilegítima o con menosprecio de los principios y garantías establecidos en la constitución y cuando ello impida o atente contra el ejercicio de los derechos fundamentales.

g) Vulnerar el deber de guardar secreto sobre los datos sensibles, así como de los que hayan sido recolectados y tratados para fines penales.

Estas sanciones en comparación con la LOPD, contemplan estrictamente actos que violan derechos fundamentales, contrario a lo establecido por los españoles, para quienes la negación a atender de forma sistemática la notificación o inclusión de datos a un registro es considerado como muy grave, por lo que, a nuestro entender,

[158] *Vid Supra*, 10. Transferencia internacional. Pag. 114

esta legislación trata de forma más mesurada clasificar las infracciones y no caer en extremos como lo que sucedió con la experiencia española, quedando quizá a un nivel intermedio entre la ley 78-17 y la LOPD.

En cuanto a las sanciones, esta contempla hasta 6 apercibimientos, suspensión, en el manejo o tratamiento de la base de datos, de 31 a 365 días, clausura o cancelación del archivo, registro o banco de datos y/o multa de $50,001 a $ 100,000 pesos.

El siguiente capítulo, establece el procedimiento para dar entrada a la acción de protección de datos personales (*habeas data*), la cual se divide en 11 artículos:

1. Procedencia, la cual se da en dos casos[159]:

    a) Para conocer de los registros o bases de datos que almacenen datos personales ya sean públicos o privados y su finalidad.

    b) Para conocer de los casos en que se presuma falsedad, inexactitud o desactualización de la información, para exigir la rectificación, supresión, confidencialidad o actualización, así como también si el tratamiento de datos se encuentra en los supuestos de prohibición establecidos en la ley.

2. Legitimación activa[160]:

La acción de *habeas data* puede ser ejercida por el titular de los datos, tutores y sucesores en línea directa o colateral hasta el segundo grado, por propia persona o por su apoderado y cuando la acción sea ejercida por personas morales, deberá ser

[159] Art. 33ª de la Ley 25.326
[160] Art. 34ª de la Ley 25.326

interpuesta por sus representantes legales o apoderados que designen para ello y podrá coadyuvar el Defensor del Pueblo en este procedimiento.

Es importante señalar aquí, la distinción que se hace de las personas, ya que como se vio al inicio de este análisis[161], la ley Argentina protege también los datos personales de las personas morales, lo que a nuestro parecer se encuentra fuera del objeto principal del derecho de protección de datos personales y derecho a la intimidad, ya que estos derechos son por naturaleza propios del ser humano, y por otro lado, el objeto de las personas morales es darse a conocer para poder ejercer su finalidad, por lo tanto, nos parece extraño el que esta ley busque proteger a un ente el cual no debiera ser ocultado, para este caso, podemos citar como ejemplo, lo que la Suprema Corte de Justicia de la Nación ha interpretado como sujetos de protección de datos:

> ***TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL. LOS ARTÍCULOS 3O., FRACCIÓN II, Y 18, FRACCIÓN II, DE LA LEY FEDERAL RELATIVA, NO VIOLAN LA GARANTÍA DE IGUALDAD, AL TUTELAR EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES SÓLO DE LAS PERSONAS FÍSICAS***[162]*.*
>
> *Si se toma en cuenta que la garantía constitucional indicada no implica que todos los sujetos de la norma siempre se encuentren en condiciones de absoluta igualdad, sino que gocen de una igualdad jurídica traducida en la seguridad de no tener que soportar un perjuicio (o privarse de un beneficio) desigual e injustificado, se concluye que los artículos 3o., fracción II, y 18, fracción II, de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, al tutelar sólo el derecho a la protección de datos personales de las*

[161] *Vid Supra,* 7. Titular de los datos. Pag. 111.
[162] Semanario Judicial de la Federación, Novena Època, Segunda Sala, T. XXVIII, julio 2008, p. 549: *IUS:169167*

> *personas físicas y no de las morales, colectivas o jurídicas privadas, no violan la indicada garantía contenida en el artículo 1o. de la Constitución Política de los Estados Unidos de América Mexicanos, pues tal distinción se justifica porque el derecho a la protección de los datos personales se refiere únicamente a las personas físicas por estar encausado al respeto de un derecho personalísimo, como es el de la intimidad, del cual derivó aquél. Esto es, en el apuntado supuesto no se actualiza una igualdad jurídica entre las personas físicas y las morales porque ambas están en situaciones de derecho dispares, ya que la protección de datos personales, entre ellos el del patrimonio y su confidencialidad, es una derivación del derecho a la intimidad, del cual únicamente goza el individuo, entendido como la persona humana.*

Como podemos observar, la interpretación que, en México y otros países, se ha dado al derecho de protección de los datos personales, deriva de un derecho personalísimo que es el derecho de la intimidad, siendo este último reconocido como un derecho fundamental del ser humano, por lo que, buscar proteger a las personas morales de la violación de datos personales es un tanto riesgoso puesto que se les estaría dando el mismo tratamiento que a los seres humanos, lo cual, dejaría en situación de desigualdad a las personas físicas con respecto de las morales, entre las cuales se encuentra el Estado, por lo que se estaría abriendo la puerta para que otros derechos humanos pudieran ser violentados.

Por último, el Defensor del Pueblo puede participar como coadyuvante en este procedimiento.

3. Legitimación pasiva[163]:

Esta acción procede contra los responsables y usuarios de bancos de datos públicos, y de las bases de datos privadas destinadas a proveer informes.

4. Competencia[164]:

La competencia a elección del actor puede darse por su domicilio, domicilio del demandado, lugar del hecho, lugar del acto en que pudiera surtir efecto.

Puede ser también de competencia federal en los casos en que se interponga el *habeas data* en contra de archivos de datos públicos de entes de gobierno o cuando los archivos de datos se encuentren interconectados en redes nacionales o internacionales.

5. Procedimiento aplicable[165]:

La acción de *hábeas data* se tramita de acuerdo a las disposiciones de la Ley 25.326 y por el procedimiento que corresponde a la acción de amparo común y de forma supletoria por las normas del Código Procesal Civil y Comercial de la Nación, en lo concerniente al juicio sumarísimo.

6. Requisitos de la demanda[166]:

a) Deberá presentarse por escrito, señalando nombre y domicilio del archivo, registro o base de datos y, en su caso, el nombre del responsable o usuario y en el supuesto de que el archivo, registro o base de datos sean públicos, deberá indicarse el ente de gobierno del cual dependen.

[163] Art. 35ª de la Ley 25.326
[164] Art. 36ª de la Ley 25.326
[165] Art. 37ª de la Ley 25.326
[166] Art. 38 de la Ley 25.326

b) El actor debe exponer de forma clara las razones por las cuales supone que el archivo, registro o banco de datos obra información sobre su persona; los motivos por los cuales considera que la información resulta discriminatoria, falsa o inexacta y demostrar que ha procurado proteger los derechos que le reconoce la ley.

c) El actor puede solicitar que mientras dure el procedimiento, en el registro o base de datos se asiente que la información cuestionada está sometida a un proceso judicial.

d) El Juez puede solicitar el bloqueo provisional del archivo en lo referente a los datos personales motivo del juicio cuando en el caso se manifieste discriminación, información falsa o inexacta.

e) Con el fin de hacerse llegar de mayor información, a criterio del Juez, se podrá requerir al archivo, registro o banco de datos involucrado, la ampliación de la información establecidas en los incisos a) y b).

7. Trámite[167]:

Admitida la acción de *habeas data*, el juez requerirá en un termino de cinco días hábiles al archivo, registro o base de datos la contestación a la demanda, asimismo puede solicitar informes sobre el soporte técnico de datos, documentación de base relativa a la recolección y cualquier otro aspecto que resulte conducente a la resolución de la causa que estime procedente, dicho término, puede llegar a ampliarse a discreción del juez.

[167] Art. 39 de la Ley 25.326

8. Confidencialidad de la información[168]:

Los registros, archivos o bancos de datos privados no pueden alegar confidencialidad de la información que se les requiere, salvo que se afecten las fuentes de información periodística.

En el caso de que se opongan al envío del informe solicitado invocando las excepciones al derecho de acceso, rectificación o supresión, autorizadas por la ley o por una ley específica, deberá ser acredita fehacientemente, y en tales casos, el juez puede conocer de forma personal y directa los datos solicitados asegurando su confidencialidad.

9. Contestación del informe[169]:

Al contestar, el archivo, registro o base de datos debe expresar las razones por las cuales incluyó la información cuestionada y aquellas por las que no contestó a la solicitud del interesado, de conformidad a lo establecido en la ley.[170]

10. Ampliación de la demanda[171]:

Después de contestado el informe, el actor puede en el término de tres días, ampliar el objeto de la demanda solicitando la supresión, rectificación, confidencialidad o actualización de sus datos personales, en los casos que resulte procedente, ofreciendo las pruebas necesarias. De esta ampliación se correrá traslado al demandado por el término de tres días.

[168] Art. 40 de la Ley 25.326
[169] Art. 41 de la Ley 25.326
[170] *Vid Supra,* capítulo III de la ley. Pag. 116

11. Sentencia[172]:

Al vencerse el plazo para la contestación del informe o ampliación de la demanda y de haber sido contestada, el juez dictará sentencia, para lo cual, en el caso de estimarse procedente la acción, especificará si la información debe ser suprimida, rectificada, actualizada o declarada confidencial y establecerá un plazo para su cumplimiento.

Ahora bien, en caso de que el juez rechace la acción de *habeas data*, no constituye presunción respecto de la responsabilidad en que hubiera podido incurrir el demandante.

Para cualquiera de los casos, la sentencia debe comunicarse a la DNPDP, quien deberá llevar un registro de los asuntos.

Después de la descripción del procedimiento de *habeas data*, el artículo 44 establece el ámbito de aplicación de la ley 25.326, por lo que, lo referente a las disposiciones generales (capítulo I), principios generales (capítulo II), derechos de los titulares de los datos (capítulo III), obligaciones de los responsables de los tratamientos (capítulo IV) y las sanciones penales (art. 32), serán de orden público y de aplicación federal, asimismo, establece que la jurisdicción federal regirá con respecto de los registros, archivos, bases de datos interconectados en redes de alcance interjurisdiccional, nacional o internacional.

Por lo que pudimos ver, esta ley cuenta con un nivel de protección adecuado de acuerdo a los lineamientos marcados por la Unión Europea, sin embargo, a pesar de esto, a Argentina no se le ha facilitado el intercambio de información internacional, debido a que por ejemplo, para los Estados Unidos de América de América este país interpone demasiados candados para que se pueda dar un flujo de información, por

[171] Art. 42 de la Ley 25.326
[172] Art. 43 de la Ley 25.326

lo que a opinión de ellos Argentina se niega al libre intercambio de datos y a su vez, esta por ley tiene la necesidad de exigir al país con el que intercambie información que este cuente con los niveles de seguridad y protección adecuados con el fin de evitar el mal uso o abuso de la información.

Asimismo, la novedad en esta ley, es la protección a las personas morales otorgada, ya que a diferencia de otros países, Argentina reconoce derechos de privacidad y de protección de datos de éstas, lo cual nos resulta extraño, debido a que a nuestro entender estos derechos son inherentes al ser humano y que por otro lado, en nuestro país leyes como la de sociedades mercantiles establecen mecanismos de control con el fin de evitar la intromisión de personas ajenas a actos privados de las sociedades, tales como asambleas de accionistas o el conocimiento de las personas físicas que conforman una sociedad anónima, etcétera.

2.4 Estados Unidos de América.

2.4.1. Antecedentes.

Estados Unidos de América no considera la protección de los datos personales como un derecho fundamental, por el contrario, sus políticas, suelen considerarlos como una mercancía sujeta al libre comercio[173], de ahí que no exista una ley en específico de protección de datos personales, sin embargo, cuenta con una ley general que regula las Sociedades de Información tales como controladores de datos, empresas públicas y privadas, que venden reportes con datos personales (historial crediticio, de empleo, médico, de pago de bienes y servicios, de arrendamientos, etcétera) y con otras leyes que en general regulan la protección de datos personales tratados en diferentes sectores[174], como por ejemplo, la "*Freedom of information act*" (FOIA) que

[173] http://lared.wordpress.com/2005/12/10/derechos-delitos-y-libertades-en-internet/ : 21/09/2008: 17:37 p.m.
[174] VILLAR, Rafael; Díaz de León, Alejandro y GIL HUBERT, Johanna. *Regulación de Protección de Datos y de Sociedades de Información: Una comparación de países seleccionados de América Latina,*

regula el acceso a bases de datos personales del sector público, o el "*Fair Credit Reporting Act*" (FCRA), que vigila el procesamiento de datos personales por parte de las agencias de reportes sobre consumidores, también existen otras tales como el título V del "*Gramm-Leach-Bliley Act*" de 1999 y el "*Financial Information Privacy Protection Act*" de 2000 que regulan la protección de datos personales dentro del sistema financiero, y en cuanto a la protección de datos sensibles, existe la Ley del Seguro Social, la cual contiene un capítulo destinado a la protección de datos relativos con la información médica.

Pero quizá la mayor evolución que se ha dado en torno a la regulación de la protección de datos en E.U.A. es a través de las decisiones y controversias judiciales suscitadas en relación con la operación de las sociedades de información, dada la naturaleza del sistema jurídico anglosajón.

Retomando el principio de este tema, sobre la forma en que son considerados los datos personales, no debe sorprendernos que para identificar a los titulares de estos, en E.U.A. se utiliza el término consumidor, para de esta forma englobar un universo de información crediticia, de empleo, salud, arrendamiento de vivienda, etcétera de los individuos, pero esto no debe hacernos pensar que el titular de los datos es considerado un objeto, ya que dentro de las regulaciones sectoriales mencionadas arriba, se establecen ciertas condiciones para la transmisión de la información, como el permitir la autorregulación de las instituciones financieras en cuanto a las políticas que estas utilizarán para la transferencia de información de sus clientes sin dejar de reconocer el derecho que estos tienen de negarse a ésta y aquéllas instituciones que no se sujeten a estas políticas son sancionadas, así como también establecen un régimen estricto para los casos de acceso fraudulento, por lo que, a pesar de no contar con una ley en específico sobre la protección de datos personales si se contemplan en las diferentes legislaciones los principios de acceso, corrección y cancelación de datos.

---

los Estados Unidos, Canadá y la Unión Europea. Banco de México, México, 2001, En: Documento de Investigación, número 2001-07, pag.13

Debido a esta política de dejar libremente que cada sector se autorregule es que en E.U.A. se facilita por consecuencia el flujo de información que da como resultado un importante factor de progreso económico y los consumidores confían en que las sociedades de información no transmitirán sus datos a terceros por que saben que estas empresas no transmiten la información arbitrariamente, sino únicamente cuando existe un derecho o interés legítimo del destinatario de la información, por lo que, este método de procesamiento de datos garantiza que las empresas puedan acceder a la información que sea efectivamente benéfica al consumidor.

En cuanto a seguridad se refiere, en E.U.A. no existen requisitos legales para constituir una base de datos personales, pero si una regulación detallada de la forma en que deben operar y disposiciones que establecen que los datos deben ser protegidos de riesgos de destrucción, pérdida o transmisión, así como también la *Associated Credit Bureaus* (ACB) desarrolló junto con las compañías de software el *ACB Security Certification Program*; dicha certificación sólo es otorgada a las sociedades de información que cumplen con los controles y estándares de seguridad establecidos.

Como podemos ver, aunque existe una certificación para proteger la información en una base de datos esto no es suficiente, ya que el control sólo se limitará al acceso de las bases de datos por terceras personas que no tengan permisos, pero, para el procesamiento de datos, y que es materia importante en este estudio, no existen lineamientos para evitar el mal uso que se le de a la información obtenida en el manejo o procesamiento de la información, por lo que de cualquier forma los datos personales se encuentran desprotegidos, ya que si los responsables en el tratamiento de datos no tienen limitantes para el manejo de esta información, ¿qué les impide ser ellos mismos quienes transmitan o hagan un mal uso de esta?

Con relación a las sanciones, el Fair Credit Reporting Act establece sanciones tanto para los usuarios como para las sociedades de información y distingue entre

sanciones intencionales y negligentes, las primeras equivalen a la suma de los daños efectivamente ocasionados al consumidor, el daño punitivo que el juez determine, las costas judiciales y los honorarios de los abogados; en cuanto a las infracciones por negligencia, la sanción equivale a la suma de los daños efectivamente ocasionados al consumidor, costas judiciales y honorarios de los abogados, por lo que la forma de sancionar es mucho más simple que las establecidas en las leyes anteriormente estudiadas, debido principalmente a que en los E.U.A. se considera que las sanciones elevadas pueden desincentivar el flujo de información en la economía e inhiben el desarrollo de las sociedades de información, debido a que los controladores serán más cautelosos en el manejo de los datos con el fin de evitar costos por algún error cometido.

Como podemos ver, en E.U.A. al no existir una ley que regule la protección de los datos personales en particular es que se ha tenido que recurrir a la creación de distintas normas, para solventar esta carencia, por lo que, en las próximas páginas se analizará algunas leyes y jurisprudencia que contengan elementos de protección de datos personales y su comparativo con las legislaciones estructuradas existentes.

2.4.2 Legislación.

Para iniciar con el análisis de la forma en que se regula la protección de datos personales en E.U.A., tendremos que revisar primero la fundamentación constitucional de esta protección, la cual encontramos en la quinta enmienda:

> *Fifth Amendment - Rights of Persons*
> *No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against*

> *himself, nor be deprived of life, liberty, or property, without due process of law;* ***nor shall private property be taken for public use, without just compensation***[175]*.*
>
> *(Quinta enmienda – Derechos de las personas. No se podrá detener a ninguna persona para responder por una falta capital o crimen a menos que exista la presentación de una acusación por parte de un jurado, a excepción en los casos que se presentaran en las fuerzas navales o en la milicia, y cuando se encuentre en servicio activo, peligro de guerra o del bien público; ninguna persona será sujeta a juicio por la misma ofenda dos veces, tampoco será obligado a testificar en contra de sí mismo, ni ser privado de la vida, libertad o propiedad sin el debido proceso de ley;* ***ni la propiedad privada será tomada para uso público, sin la justa compensación***[*]*)*

Aunque la quinta enmienda sólo hace mención de *propiedad privada*, podemos hacer una interpretación de esta, y considerar como parte de la propiedad del individuo, los datos personales, por lo que el uso público que pudiera darse a estos tendría que ser sólo mediante la compensación justa al titular de los datos, podemos aquí darnos cuenta entonces de la simplicidad y practicidad con la que los E.U.A. busca dar solución a problemas comunes como estos, ahora bien, podemos también revisar un caso en el que la Corte de apelaciones reconoce el derecho de los consumidores a decidir si la información relativa a su persona deba ser incluida en bases de datos de compañías telefónicas y transmitidas por terceros a otras empresas, y de como las normas establecidas por sectores de la sociedad ayudan a regular y cubrir lagunas en la legislación existente, lo cual ha ayudado a solventar la violación a la intimidad de las personas en este país:

> ***Court:*** *U.S. D.C. Circuit Court of Appeals*
>
> ***Topic:*** *Administrative Law, Communications Law, Consumer Products, Consumer Protection Law*

[175] http://www.uslaw.ibls.com/uslaw/home.htm :06/03/2009: 22:46 hrs.
[*] Traducción del autor de este trabajo de investigación.

Title: *Nat'l Cable & Telecomm. Ass'n v. Fed. Communications Comm'n*

Date: *02/13/09*

Case Number: *07-1312*

Summary: *a case involving the validity of the FCC's latest order specifying how carriers are to obtain their customers' approval for use of the customers' information, In telecommunications association and companies' petition for review of the order is denied where: 1) the FCC returned to a limited "opt-in" consumer consent requirement in response to the increasing activity of data brokers; and 2) it gave sufficient reasons for singling out the relationships between carriers and third-party marketing partners*[176]*.*

(***Sumario:*** *en el caso de la validez de la última disposición de la FCC se específica que los transmisores (de datos) deberán obtener la aprobación por parte de sus clientes para el uso de la información de los consumidores, en la asociación de telecomunicaciones y compañías la solicitud de revisión se negará cuando: 1) la FCC requiere el consentimiento por parte del consumidor de ser incluido, en respuesta a la actividad cada vez mayor de los corredores de datos; y 2) se dieron las suficientes razones seleccionar la relación entre los transmisores y los terceros socios de empresa.*[*]

Como podemos ver, la corte resuelve que para hacer uso de información personal por parte de una empresa (en este caso de comunicaciones), el consumidor deberá tener el derecho de optar por decidir si acepta su inclusión en la transmisión de datos a terceros, debido al aumento considerable de corredores de datos o lo que es lo mismo de agencias dedicadas a la búsqueda y obtención de información personal para su posterior entrega o venta a empresas, de igual forma, el titular de los datos tendrá derecho de conocer a quien se le transmitirá la información y quienes obtendrán los resultados del procesamiento de los datos.

[176] *Idem*

Ya en el contenido de la sentencia, podemos encontrar algunas de las razones por las cuales la corte, en este caso en particular, decide reconocer como prioridad el que se le de la opción al individuo de proteger su privacidad por encima de la actividad comercial de las empresas:

> *"…*
> *The 2002 Order also allowed carriers to share customer information with joint venture partners or independent contractors for marketing communications-related services. But the Commission recognized a heightened personal privacy risk associated with these third parties because they did not qualify as "carriers" under the Telecommunications Act and thus were not subject to confidentiality requirements. The Commission therefore ordered carriers and their joint venture partners or independent contractors to enter into confidentiality agreements to safeguard customer information, in addition to the opt-out notices sent to customers. Carriers were apparently content with this state of affairs; no challenges were mounted against the 2002 Order.*
> *…"*[177]

> *(La orden 2002 permite a los transmisores compartir la información del cliente con los socios o los contratistas independientes de los servicios de comunicación relacionados con la comercialización. Pero la Comisión reconoció el aumento del riesgo en la privacidad de las personas asociado con estos terceros porque no calificaron como "transmisores" de acuerdo a la ley de telecomunicaciones y por lo tanto, no estaban de acuerdo con los requerimientos de confidencialidad. La Comisión por lo tanto, solicitó a los transmisores y sus socios o contratistas independientes a firmar acuerdos de confidencialidad de salvaguardar la información del consumidor, además de notificar al consumidor la opción de ser excluidos. Los*

[*] Traducción del autor de este trabajo de investigación.
[177] http://caselaw.lp.findlaw.com/data2/circs/dc/071312p.pdf : 05/03/2009:19:49 hrs.

> *transmisores al parecer quedaron contentos con esta situación; ya que no se inició ningún litigio contra la orden 2002.*[*])

El análisis que la corte realizó de la norma de 2002 de la Comisión de Telecomunicaciones, deja ver que el cumplimiento de esta por parte de los encargados de transmitir información de los consumidores debían cumplir con acuerdos de confidencialidad en el caso de subcontratación del procesamiento de datos, así como también darle la opción al consumidor de que sus datos fueran excluidos de dicha transmisión, de esta forma, la Comisión de Telecomunicaciones establecía límites a la transmisión de información, dando prioridad a la protección de la privacidad de las personas, y como podemos ver, una simple norma establecida por parte de un sector de la sociedad puede llegar a solventar posibles violaciones a los derechos humanos, o viéndolo de otra forma, en E.U.A. de manera indirecta se estaba cumpliendo con principios establecidos internacionalmente en materia de protección de datos aún cuando el propio Estado no tiene como prioridad establecer legislación concreta, lo que aunado a otro tipo de acuerdos, la transmisión de datos entre empresas de telecomunicaciones a nivel internacional si puede llegar a concretarse por la simple existencia de este tipo de lineamientos.

Más adelante, en la misma sentencia, la corte incluye, el reconocimiento que el Congreso de los E.U.A. da a la existencia de esta norma y de la importancia de proteger la privacidad de las personas:

> *"…*
> *Congress found that unauthorized disclosure of customer information "not only assaults individual privacy but, in some instances, may further acts of domestic violence or stalking, compromise the personal safety of law enforcement officers, their families, victims of crime, witnesses, or confidential informants, and undermine the integrity of law enforcement investigations.*

[*] Traducción del autor de este trabajo de investigación.

…"

> *(El Congreso encontró que el consumidor no estaba autorizado a acceder a su información, lo cual "no solamente ataca a la privacidad individual, debido a que puede fomentar actos de violencia o acecho en el hogar, compromete la seguridad personal de autoridades, de sus familias, víctimas de un crimen, testigos, informantes confidenciales, y minar la integridad de las investigaciones en la aplicación de la ley.)*[*]

Esto es, el hecho de proteger la privacidad de las personas evita no solo la intromisión de extraños a su información personal, sino también puede llegarse a abrir la puerta a la violación de la seguridad de los mismos y a las personas cercanas a ellos, lo que puede llegar a ocasionar inseguridad e ineficacia en la aplicación de la ley, tal y como lo hemos visto en el análisis de las otras legislaciones, el hecho de proteger la intimidad de las personas debe ser prioritario para la seguridad nacional, debido a que la simple intromisión a la vida privada puede derivar en actos de intimidación o inclusive, desenvolverse en otro tipo de crímenes debido a que una sola persona se encuentra concatenada a otros individuos[178], organismos o instituciones, por lo que de alguna manera el mismo Congreso de los E.U.A., reconoció que normas de este tipo ayudaban de manera indirecta al propio Estado en aspectos de seguridad y por lo tanto, los datos de las personas dejaban de ser, en ese momento, objetos mercantiles para convertirse en información digna de protección, es así como en las conclusiones de esta sentencia encontramos:

> *"…*
> *Accordingly, because the Commission returned to a limited opt-in consent requirement in response to the increasing activity of data brokers, and because it gave sufficient reasons for singling out the relationships between carriers and third-partymarketing partners, we*

[*] Traducción del autor de este trabajo de investigación.
[178] *Vid Supra* 1.3.1 Concepto de derecho a la intimidad. Pag. 26

> *hold that the Commission adequately provided the reasoned analysis State Farm requires."*
>
> *(Por consiguiente, debido a que la Comisión volvió a incluir como requisito que existiera el consentimiento de inclusión (en una base de datos), fue en respuesta a la actividad cada vez mayor de los agencias de datos y por que dio las suficientes razones de distinguir la relación entre los transmisores de datos y los terceros, es que sostenemos que la Comisión proporcionó los elementos adecuados que el Estado necesitaba para elaborar su análisis)*·

Por lo que, la misma corte de apelaciones reconoce que la Comisión de Telecomunicaciones ha demostrado que da prioridad a los consumidores en optar por su inclusión o exclusión para la transmisión de sus datos personales, estableciendo límites a las empresas dedicadas a realizar estas gestiones, por lo que, en este caso a la empresa que impugnaba esta norma y que argumentaba que existían demasiadas restricciones para el desarrollo de su actividad le niega su petición y por lo tanto, al declararse la corte en este asunto crea un precedente en la protección de los datos personales, en cuanto a la transmisión de estos, pero respecto al procesamiento de datos no se hace ninguna mención.

Ahora bien, en relación a la protección de datos personales con información sensible, podemos tomar como ejemplo la sentencia de la Suprema Corte de Estados Unidos de América Whalen v. Roe (1977) 429 U.S. 589[179], en dicha sentencia, se cuestiona la constitucionalidad de la ley del Estado de Nueva York sobre sustancias controladas de 1972, la cual establece la creación de un registro de datos personales de los pacientes que por prescripción debían tomar drogas, para de esta forma llevar un control del número de recetas prescritas y evitar de esta forma que estos medicamentos fueran desviados hacía canales ilegales de distribución.

· Traducción del autor de este trabajo de investigación.

[179] http://www.ugr.es/~redce/REDCE7/articulos/16sentenciasupremoamericano.htm#12bis :19/03/2009: 21:36 hrs.

Para dicho control, el médico debe llenar un formulario por triplicado, el cual identifica al médico que prescribe, la farmacia que entrega el medicamento, el nombre, dirección y edad del paciente, así como el tipo de droga y la dosificación; la tercera copia de este formulario se remite al Departamento de Salud, donde es clasificado, identificado con un código y registrado, posteriormente son enviados a otra área para su procesamiento informático; después de dicho procesamiento se devuelven al Departamento de Salud donde serán resguardadas por cinco años; en cuanto a los encargados del procesamiento de datos, tienen prohibido por esta misma ley la divulgación de cualquier información concerniente a la base de datos y cualquier violación dolosa a estas disposiciones constituye un delito que es sancionado hasta con un año de reclusión y una multa de $2,000.00 dólares[180].

Viendo el procedimiento de este control, podría pensarse que esta ley cumple con algunos de los lineamientos de protección de datos establecidos en otros países como los anteriormente analizados, sin embargo y debido a que los niveles de protección no son tan estrictos y la penalización por la falta de secrecía es muy baja, es que la protección de datos personales sigue estando en un segundo plano, como lo veremos a continuación:

En el planteamiento del problema, los demandantes establecían que los pacientes podrían rechazar el tratamiento por miedo a que un error en el uso de los datos automatizados pudiera llevarlos a señalarlos como drogadictos, por su parte, el Tribunal de Distrito que conoció primero de este asunto, sostuvo que la protección de la relación doctor-paciente es uno de los ámbitos de intimidad que se encuentran constitucionalmente protegidos y que el hecho de aplicar filtros de información[181] para realizar la comparación de la cantidad de medicamento prescrito contra la identificación de los pacientes, resultaba ser un procesamiento de datos innecesariamente amplio, por lo que eliminó la aplicación de los preceptos de la ley que obligaban a dar el nombre y dirección del paciente.

[180] Artículo 3371 de la Ley de Salud Pública del Estado de Nueva York
[181] *Vid Supra*, 1.1.3.2. Filtros de información, pag.14

Sin embargo, dicho planteamiento para la Suprema Corte no era contundente, puesto que reconocía que los Estados al momento de crear las diferentes legislaciones, tienen ciertos efectos sobre la libertad individual o la intimidad de las personas y por lo tanto, eso no da lugar a plantear la inconstitucionalidad de una ley simplemente por que un Tribunal encuentre innecesaria su aplicación ya sea de forma total o parcial. Asimismo, se planteó que el uso de la información personal de los pacientes podía ayudar al Estado a experimentar nuevos mecanismos de control en el uso ilegal de drogas, puesto que al poder identificar a los pacientes se podría esperar que tuviera un efecto disuasorio en los posibles infractores, por lo que, el contenido de la ley apoya al Estado (en este caso de Nueva York) en el ejercicio de sus poderes de policía, y por lo tanto, lo planteado por el Tribunal de Distrito resultaba insuficiente para calificar dicha ley de inconstitucional.

De igual forma, la Suprema Corte planteaba que en la remota posibilidad de que el control judicial en el uso de la información resultante del procesamiento de datos no la protegiera debidamente no constituía una razón suficiente para anular el programa de identificación de los pacientes, puesto que, el permitir que los representantes del Estado pudieran conocer dicha información no representaba automáticamente una lesión a la intimidad de las personas, máxime si en la práctica médica moderna, la divulgación de información sobre pacientes, es dada a conocer por los médicos a las aseguradoras, personal de hospitales, etcétera y no representa una violación a la intimidad de los pacientes.

Ahora bien, también reconocía la Suprema Corte que existía una amenaza latente a la intimidad de las personas por el uso indiscriminado de la información derivado del procesamiento de datos, en caso de que los funcionarios del Estado dieran una amplia difusión a la información obtenida, sin embargo, la cuarta enmienda establece los límites que el propio Estado tiene no solo para el tipo de información que puede obtener, sino también a los medios que puede utilizar para obtenerla, aunque no se descartaba la posibilidad de crear los mecanismos necesarios para restringir el uso

de la tecnología en el manejo de información. Veamos pues lo que señala esta cuarta enmienda:

> *"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."*
>
> *(El derecho de la persona a estar segura en su persona, casa, papeles y efectos contra investigaciones desmedidas e incautación, no resultaran en garantías violadas, sobre causa probable soportada por juramento o afirmación, así como la descripción del lugar de investigación y las personas o cosas que serán incautadas.)*

Es así como a nivel constitucional el Estado tiene límites para la obtención de información y de acuerdo a la interpretación que la Suprema Corte daba en esta sentencia, le parecía que el sólo hecho de que la ley estableciera el *porque* de la obtención de la información y el *como* en el manejo de esta, era más que suficiente para resolver que no existía ninguna violación a la intimidad de las personas puesto que se estaba indicando el motivo de la investigación (uso ilegal de drogas) y los datos de los cuales se iban a valer para obtener dicha información (o lo que podría interpretarse como los objetos del individuo que serían incautados por parte del Estado con motivo de la investigación).

Por otro lado, dentro del planteamiento del problema, también se cuestionaba la violación a la Décima cuarta enmienda, la cual consigna entre otras las garantías de privilegios e inmunidades, misma protección ante la ley y debido proceso y *establece que ningún Estado promulgará ni dará validez a ley alguna que restrinja los privilegios e inmunidades de los ciudadanos de E.U.A.*, ni los Estados privarán a persona alguna de su vida, libertad o posesiones sino mediante el debido proceso establecido en la ley, ni tampoco negarán a las personas la misma protección ante la

ley[182], sin embargo, para la Suprema Corte, esta ley no representaba violación alguna, debido a que a pesar del temor de algunos pacientes, también se había probado que se continuaban registrando recetas en el Departamento de Salud, por lo que, se deducía que la ley no había privado a los pacientes del acceso a las drogas, es mas, utilizando por analogía lo señalado en la sentencia "Katz v. Estados Unidos, 389 USA. 347 señalaron:

> *"El Tribunal dejó claramente establecido que aunque la Constitución protege frente a ciertas clases de intrusiones del gobierno en cuestiones personales y privadas, "no hay un derecho constitucional general a la intimidad" (p.608). La protección del derecho de una persona a la intimidad ... su derecho a estar sólo, como la protección de su propiedad y de su misma vida, queda en gran medida a resguardo de la voluntad de los estados individuales"*[183]

Por lo tanto, la Suprema Corte resolvió que el registro y procesamiento de datos, en este caso en particular, no suponían una lesión de ningún derecho o libertad de las contenidas en la cuarta y décimo cuarta enmienda, lo que a nuestro parecer es indicativo de que en E.U.A. los intereses de la comunidad estarán siempre por encima de los derechos individuales, puesto que en el particular no importaría procesar la información y divulgar información personal con tal de obtener como resultado el uso ilegal de las drogas, pero en ningún lado se contempla que después de usar esta información con fines de investigación y seguridad nacional, esta sea desechada o vuelta a la confidencialidad para evitar un mal uso o abuso de esta, tal y como sucede con las otras legislaciones en las que el ejercicio de investigación por parte del Estado contempla solo el período en que dure esta y terminado este tiempo, la información obtenida será desechada y se volverá a dar prioridad a la

---

· Traducción del autor de este trabajo de investigación.

[182] PUENTE DE LA MORA, Ximena. *Privacidad de la información personal y su protección legal en Estados Unidos*. Alfa Redi, Revista de Derecho Informático. Núm. 096, agosto de 2006. España. En: http://www.alfa-redi.org/rdi-articulo.shtml?x=6956 : 26/03/2009: 20:24 hrs.

[183] Citado en: http://www.ugr.es/~redce/REDCE7/articulos/16sentenciasupremoamericano.htm#12bis :19/03/2009: 21:36 hrs.

protección de datos personales con el fin de proteger la intimidad de la persona y de todas aquellas relacionadas a esta.

Con relación a la información crediticia el código de comercio en su capítulo III, relativo a las agencias dedicadas a dar información crediticia[184], establece que estas podrán dar a conocer la información crediticia de cualquier consumidor sin el consentimiento o conocimiento de este, mientras dure algún tipo de investigación que tenga interés jurídico (pago de alimentos, litigios) o público incluyendo entre estos la verificación que las compañías pudieran llegar a hacer por motivo de una posible adquisición de algún bien, solicitud de algún crédito o inclusive si la persona fuera parte de la negociación en la fusión de empresas u otro tipo de transacción realizada por las bancas de inversiones[185].

Para el caso de seguridad nacional y que se requiera realizar una investigación crediticia, esta podrá ser elaborada de igual forma sin el consentimiento del titular de los datos, sin embargo, al final de dicha investigación la persona deberá ser informada de los alcances de esta y el Gobierno podrá reservarse la información clasificada si esto fuera necesario[186].

Por último, existe también el *Privacy Act of 1974*, el cual establece un código de prácticas para el manejo de información sobre datos personales que se encuentren en poder de cualquier agencia federal y otorga derechos a los ciudadanos de acceso, corrección, actualización de sus datos personales, mas no así de la cancelación o eliminación de estos.

Asimismo, esta ley requiere que los entes de gobierno publiquen los sistemas de información existentes; y cualquier información obtenida a través del procesamiento de datos deberá ser informada al titular de estos, a menos que se encuentre en posesión de la Agencia Central de Inteligencia (CIA) o de alguna agencia dedicada a

[184] http://www4.law.cornell.edu/uscode/15/ch41schIII.html : 01/04/2009: 23:16 hrs.
[185] http://www.export.gov/safeharbor/eu/sh_en_docs1.asp : 01/04/2009: 23:30 hrs.
[186] Código de comercio, 1681b. *Permissible purposes of consumer reports*, fracción 4, incisos A) y B)

la investigación criminológica, sin embargo, en estos casos, deberán establecer las razones por la cual esta base datos debe ser eximida del cumplimiento de lo establecido en esta ley.

Para concluir, el modelo seguido por los Estados Unidos de América, se basa en la práctica ausencia de previsiones legales, quedando dicha regulación reducida al establecimiento de códigos de conducta o, la denominada, "autorregulación industrial" desarrollada esencialmente por el sector privado, y cuya efectividad depende, en gran parte, del poder de coacción de quien formula dichos códigos y de la aplicación de las sanciones previstas en ellos,[187] así como también, el hecho de que solo los entes de gobierno federales tienen una reglamentación para el manejo de datos personales, pero sin dejar de establecer que dicha información le pertenece al gobierno y por lo tanto el individuo, si así lo quisiera, no puede solicitar la cancelación o eliminación de sus datos, por lo tanto, podemos concluir que no existe un reconocimiento real del derecho a la protección de datos personales en este país, aún y cuando en la actualidad han firmado distintos tratados comerciales con la Unión Europea y tratan de solventar la ausencia de una regulación.

Por último y analizando el objeto de cada una de las normas de estudio, anteriormente descritas, es necesario considerar que Francia, España y Argentina tienen por objeto regular el tratamiento de los datos de carácter personal tanto a nivel público como privado, mientras que en México la protección de datos, sólo está reglamentada a nivel entes de Gobierno, debido a que su objeto principal no es la regulación y protección de datos personales, sino que la referencia surge como consecuencia de permitir el acceso a la información pública que maneja la Administración Pública Federal y por ningún motivo considera a los particulares.

Por lo tanto, la norma que se desarrolle para la regulación de la protección de datos personales en México, deberá considerar que su objeto principal es garantizar el

[187] Estudio sobre protección de datos a nivel internacional. – Instituto Federal de Acceso a la Información: México, 2004. p.8

derecho a la privacidad de las personas (o titulares de los datos), siendo su concreción del derecho a la intimidad, así como también darle el reconocimiento como derecho fundamental en nuestra Carta Magna a la protección de estos datos, tal y como se ha hecho en diferentes Estados, tanto de la Unión Europea, como de América Latina[188].

[188] Estudio sobre protección de datos a nivel internacional. – Instituto Federal de Acceso a la Información: México, 2004. p.12

CAPÍTULO III. ANÁLISIS DEL INTERCAMBIO DE INFORMACIÓN ENTRE PARTICULARES EN MÉXICO

Actualmente, en México no existe una regulación vigente sobre protección de datos personales y las iniciativas existentes no cumplen con los lineamientos establecidos internacionalmente, tal y como se estudiaron en el capítulo anterior, algunas de las fallas más representativas son por ejemplo la falta de un organismo regulador especializado en este Derecho, puesto que se pretende ampliar las funciones del Instituto Federal de Acceso a la Información Pública para dar cabida a la vigilancia y protección de esta información y por otro lado, no se contemplan las bases de datos administradas por particulares, argumentando que existen diferentes legislaciones que contemplan la obligación de estos de proteger la privacidad de esta información, sin embargo, el hecho de que exista dispersa normatividad, también abre la posibilidad de que sólo algunos sectores de la sociedad sean regulados y obligados a proteger los datos personales y por lo tanto, algunos otros no quedan contemplados en esta normativa por lo que, la posibilidad de la violación de este derecho queda latente, de ahí la importancia de la existencia de una sola ley que contemple el derecho de la protección de datos personales y la intimidad de las personas, en la que se incluya como sujetos obligados tanto a los entes de gobierno como a los particulares.

A continuación estudiaremos la problemática actual en México en relación al intercambio de información entre particulares, enfocándonos en este sector principalmente, el cual no es contemplado en las iniciativas existentes en el ámbito de protección de datos personales.

3.1 Estudio de la legislación a nivel Federal y local

3.1.1 Constitución Política de los Estados Unidos Mexicanos

El derecho a la protección de los datos personales y a la vida privada dentro de nuestra Constitución, es un derecho nuevo, el cual, ha tenido que evolucionar poco a poco, un primer paso para su existencia se dio con la aprobación de la Ley Federal de Transparencia y Acceso a la Información Pública en 2002, en el que se estableció en el artículo 3, fracción II, la definición de datos personales, posteriormente, en julio de 2007, se público la reforma al artículo 6° Constitucional en el que se constituyó como un derecho independiente al derecho de acceso a la información pública, pero limitándose a la información en poder de cualquier ente de los tres niveles de gobierno, en lo que concierne a este trabajo de investigación, dicha reforma quedó de la siguiente manera:

> "Artículo 6. ...
>
> II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
>
> III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.
>
> ..."

Como podemos ver, se garantizó la protección a la vida privada y a los datos personales, salvo disposición en contrario, de igual forma, se garantizó la gratuidad del acceso y rectificación de datos, pero no así del derecho de cancelación, eliminación u oposición.

En virtud de que faltaba precisar que era el derecho a la protección de datos personales, indicando sus alcances y límites, se presentó una iniciativa, en la

Cámara de Senadores, para reformar el artículo 16 constitucional en el que se insertaría un segundo párrafo y por consiguiente el resto de los párrafos serían recorridos. La iniciativa fue aprobada por parte del Congreso de la Unión, quedando de la siguiente forma[189]:

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

Por lo que con esta modificación, se elevó a rango Constitucional la protección de datos personales, garantizando el acceso, rectificación, cancelación y oposición que el titular de los datos tiene como derechos, limitándolos para los casos de seguridad nacional, orden público, salud o protección de terceros, debido a que, a criterio de la Comisión de Puntos Constitucionales del Senado, "*un derecho fundamental no puede ser un derecho superior a cualesquier (sic) otro o bien a intereses sociales o públicos*"[190]; por lo que, con esta reforma se abrió el camino para la creación de una ley de protección de datos personales a nivel federal.

[189] Dicha iniciativa fue aprobada por la Cámara de Senadores y turnada a la de Diputados el 4 de Diciembre de 2008; el pasado 15 de abril de 2009, la Cámara de Diputados aprobó la iniciativa de reforma al artículo 16 constitucional con 18 votos a favor por parte de los Congresos de los Estados, en el que se estableció el derecho de protección de datos personales, cubriendo todos sus aspectos: acceso, rectificación, cancelación y oposición. En el momento de realizar este trabajo de investigación, dicha iniciativa fue revisada por la Cámara de Senadores y turnada el 21 de abril de 2009 al Ejecutivo Federal, y publicada el 1º de junio de 2009 (Anexo 1).

[190] Proyecto de decreto que adiciona un párrafo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (anexo 1, pag.7)

Sin embargo, y a criterio de esta Comisión, este derecho otorgado a los titulares de los datos, no interfiere con la dinámica del comercio, ya que existe la posibilidad de que el titular de los datos de manera tácita otorgue esta información sin límite alguno, mientras no exista manifestación de voluntad en contrario[191], lo cual, a nuestro parecer es incorrecto, ya que como se mencionó en el capítulo anterior[192], los datos personales no deben ser incluidos en bases de datos comerciales por *default* y ser transmitidos sin el consentimiento expreso del titular, lo que deberá ser corregido en el momento de la creación de una ley de protección de datos personales.

Por otro lado, para completar la reforma en esta materia y por lo tanto, para que fuera posible la creación de una ley que englobara tanto a entes públicos como privados, fue necesario adicionar la fracción XXIX-O al artículo 73 de la Constitución[193], en el que se estableció como facultad del Congreso legislar en materia de datos personales en posesión de particulares, quedando dicha adición de la siguiente forma:

> *"Artículo 73. El Congreso tiene facultad:*
> *I. a XXIX-N.* ***...***
>
> *XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares.*
>
> *XXX. ..."*

De esta forma, el Congreso buscó consolidar este derecho de protección a la persona en relación con el uso que se de a su información personal en posesión tanto de entes públicos como privados. Desafortunadamente, para llegar al

[191] *Idem*
[192] 2.2.2. La Ley Orgánica de Protección de Datos de Carácter Personal. Artículo 31 de la LOPD, pag. 49 y 2.4.2. Legislación (E.U.A.). pags. 105-109
[193] Esta adición, fue publicada el 24 de marzo de 2009 en el Diario Oficial de la Federación.

reconocimiento de este derecho, en relación con el resto del mundo México lleva un atraso de 30 años, por lo que la creación de una ley en esta materia deberá realizarse en el menor tiempo posible y contemplando los estándares establecidos a nivel mundial, para garantizar por un lado, la protección de la intimidad de la persona y por el otro, el flujo de información necesario en este mundo globalizado.

3.1.2 Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

Uno de los objetivos principales de esta ley es garantizar la protección de datos personales que se encuentren en posesión de un sujeto obligado[194] y como se señaló anteriormente, en el artículo 3, fracción II, de esta Ley, se define que es un dato personal:

> *"Artículo 3. Para los efectos de esta Ley se entenderá por:*
>
> *I. ...*
>
> *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;*
>
> *III..."*

Lo importante de esta definición, es que se trata del primer paso que a nivel federal se da en materia de protección de datos personales y de protección a la intimidad.

[194] Artículo 4 de la LFTAIPG

Más adelante en la fracción XIII del mismo artículo, se define que un sistema de datos personales es un conjunto ordenado de datos que este en posesión de un sujeto obligado, el cual lo define en la fracción XIV, y contempla sólo a los órganos federales como obligados a cumplir con esta Ley.

Dentro de las obligaciones establecidas, se establece la exigencia de clasificar la información para su publicación, por parte de los sujetos obligados, para el caso de datos personales se contempla "*Poner en riesgo la vida, la seguridad o la salud de cualquier persona*"[195], así como también considerar como información confidencial "*Los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos de esta Ley*"[196] y en el caso de la publicación de las sentencias que hayan causado estado o ejecutoria, a las partes se les concede el derecho de oponerse a la publicación de sus datos personales[197].

Entre otras medidas establecidas en esta Ley, se incluye un capítulo dedicado a la protección de datos personales, en el que se contempla la obligatoriedad por parte de los entes de gobierno, de establecer los mecanismos necesarios para la seguridad de la información, confidencialidad, registrar el sistema de datos, informar al titular de los datos el objeto de estos sistemas, actualizar y otorgar el acceso y rectificación de datos personales a los titulares, así como también crear Comités de vigilancia que establezcan los criterios que el organismo utilizará para el manejo y procesamiento de datos[198].

Otros derechos que tiene el titular de los datos, es establecer un recurso de revisión ante el Instituto Federal de Acceso a la Información Pública (más adelante IFAI), en

[195] Artículo 13, fracción IV de la LFTAIPG
[196] Artículo 18, fracción II de la LFTAIPG
[197] Artículo 8 de la LFTAIPG
[198] Artículos 20 a 26 y 61 de la LFTAIPG

el caso de que le sea negado el acceso, corrección o información que el organismo tiene sobre sus datos personales[199].

Como podemos ver, al IFAI le fueron otorgadas facultades para vigilar el cumplimiento de esta normativa por parte de los entes de gobierno, de ahí que algunas de las iniciativas existentes para la creación de una ley de protección de datos, contemplen a este organismo como el regulador, entre algunos de los motivos utilizados es que este Instituto cuenta con la infraestructura y experiencia necesarios que redundaran en evitar más gastos al erario, pero a nuestro parecer, el IFAI, podría quedar sobrepasado en sus funciones y por lo tanto, no podría realizarlas eficazmente, ya que tendría que vigilar por un lado, a todos los entes tanto públicos como privados, que tengan en su posesión un sistema de datos personales y por otro, vigilar que todos los entes de gobierno cumplan con su obligación de garantizar la transparencia y el acceso a la información de sus actividades, además que en ambas materias deberá establecer los criterios que regularán el procesamiento de toda la información relativa, por lo que, dos derechos que son reconocidos como independientes en la Constitución, quedarían relacionados en la práctica.

3.1.3 Lineamientos de Protección de Datos Personales del Instituto Federal de Acceso a la Información Pública

Los artículos 47 y 48 del Reglamento de la LFTAIPG, establecen la obligatoriedad por parte del IFAI de crear los lineamientos a seguir por parte de la Administración Pública Federal en cuestión de protección de datos personales, así como también la obligación de inscribir cualquier sistema de datos personales ante este Instituto para dar su debido seguimiento y control.

Debido a lo anterior, en septiembre de 2005 se publicaron los lineamientos de Protección de Datos Personales, en los cuales el mismo IFAI reconoció:

[199] Artículo 50 de la LFTAIPG

"...

Admitiendo que la sociedad de la información, fundada en el avance vertiginoso de la tecnología, ofrece al individuo ventajas diversas que contribuyen a mejorar su calidad de vida y, en el caso del Estado, a mejorar la actividad administrativa, el desarrollo económico, social y cultural, así como el cumplimiento de las obligaciones ciudadanas frente a éste, pero que, al mismo tiempo, una mala utilización de las herramientas tecnológicas puede convertirse en un factor de amenaza a la privacidad y seguridad de las personas al permitir que se generen formas de exclusión o condiciones de incertidumbre y riesgo, ya que las nuevas tecnologías facilitan ilimitadas posibilidades para mover un gran volumen de información y de interrelacionarla, de manera que se constituyen perfiles que pueden limitar la libertad o condicionar el modo de actuar de las personas;

..."[200]

A partir de la lectura de este párrafo, podemos ver que existía una preocupación por parte del Estado de brindar protección a los datos personales, pero sólo de aquellos que se encontraban en su posesión, por lo que, a través de la lectura de los mencionados lineamientos, podemos encontrar diversas reglas de operación en el procesamiento de datos personales basadas principalmente en los lineamientos establecidos por la Unión Europea y las Naciones Unidas, los cuales de alguna manera fueron revisados durante el análisis de las leyes expuestas en el capítulo anterior; entre estas reglas podemos mencionar:

1. Principios rectores de la Protección de los Datos Personales (licitud, calidad, acceso y corrección; seguridad, custodia y consentimiento de transmisión)[201]

2. Tratamiento de los datos personales:

[200] Lineamientos de Protección de Datos Personales. Texto vigente.
[201] Capítulo II de los Lineamientos.

a) Exacto. Información actualizada y veraz.

b) Adecuado. Medidas de seguridad.

c) Pertinente. Procesamiento en cumplimiento de las atribuciones de las dependencias y entidades que hayan recabado la información.

d) No excesivo. La información es estrictamente la necesaria para cumplir con los fines establecidos.

e) Corrección de oficio.

f) Conservación de los datos. Los plazos que deberán establecerse para la conservación de la información y de su transmisión.

g) Información. Hacer del conocimiento del titular de la base de datos, fines, fundamento y objetivos.

h) Disociación de datos.

i) Tratamiento de datos por terceros. Obligación de establecer la implementación de medidas de seguridad y custodia de acuerdo a la legislación y lineamientos existentes en el caso de la contratación de terceros para el procesamiento de datos[202].

3. Transmisión de la información. Las dependencias deberán realizar un informe al Instituto cuando hayan realizado una transmisión de datos personales y para el caso de solicitar al Titular el consentimiento de transmisión, el Instituto estableció dos criterios para delimitar la obligatoriedad de esta solicitud:

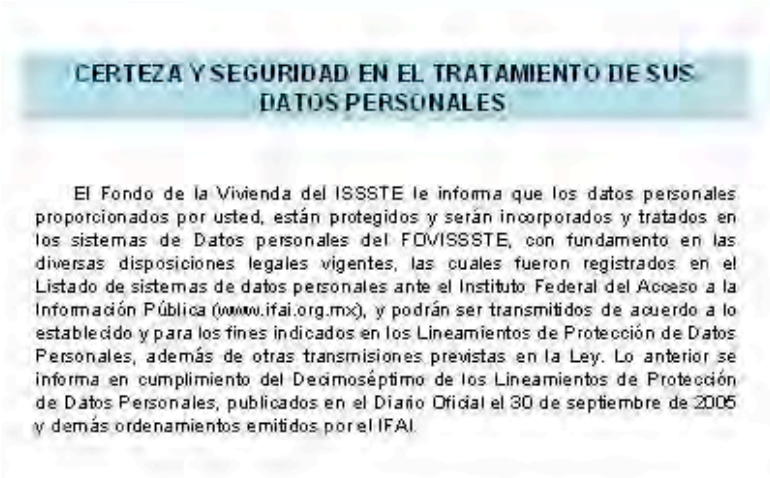
a) *Sin el consentimiento del titular*, aplicado a los datos personales de los servidores públicos, los que se encuentren en registros públicos, para el uso de estadísticas e informes, para la transmisión entre dependencias

y entidades federales[203], por orden judicial y cuando sean contratados terceros para su procesamiento.

b) *Con el consentimiento del titular*, el cual deberá ser otorgado por escrito, con firma autógrafa y copia de identificación oficial.

4. Seguridad de los sistemas de datos personales. El Instituto emitirá una vez al año las recomendaciones sobre los estándares mínimos a cumplir por parte de las dependencias, independientemente de las medidas y acciones que estas lleven a cabo para la reserva, resguardo y seguridad, de los sistemas, así como también la expedición de documentos en los que se detallen las medidas administrativas, físicas y técnicas que se llevarán a cabo.

Cabe mencionar, que en cumplimiento de estos lineamientos en diversas páginas de la Administración Pública Federal se ha incluido una leyenda en la que se avisa al titular de los datos que la información recabada será protegida de acuerdo a lo establecido en la ley, para ilustrar lo anterior, se tomó como ejemplo la página del Fondo de la Vivienda del ISSSTE:



CERTEZA Y SEGURIDAD EN EL TRATAMIENTO DE SUS DATOS PERSONALES

El Fondo de la Vivienda del ISSSTE le informa que los datos personales proporcionados por usted, están protegidos y serán incorporados y tratados en los sistemas de Datos personales del FOVISSSTE, con fundamento en las diversas disposiciones legales vigentes, las cuales fueron registrados en el Listado de sistemas de datos personales ante el Instituto Federal del Acceso a la Información Pública (www.ifai.org.mx), y podrán ser transmitidos de acuerdo a lo establecido y para los fines indicados en los Lineamientos de Protección de Datos Personales, además de otras transmisiones previstas en la Ley. Lo anterior se informa en cumplimiento del Decimoséptimo de los Lineamientos de Protección de Datos Personales, publicados en el Diario Oficial el 30 de septiembre de 2005 y demás ordenamientos emitidos por el IFAI.

[202] Capítulo III de los Lineamientos.

[203] En relación a la transmisión entre dependencias y entidades federales, quizá valdría la pena considerar para la actualización de este criterio, la experiencia española, establecida en la sentencia 292/2000, citada en el capítulo II, pags. 77 y 78, en el que se consideró inconstitucional el artículo 21 de la LOPD, al no limitar las facultades de la Administración Pública en la transmisión de información, debido a que entre ellos no se consideraba exigir medidas de seguridad, plazos y fines para su uso.

Ahora bien, y para dar cumplimiento a estos lineamientos, el Instituto creó el "Sistema Persona", el cual es una base de datos que integra un listado de todos los sistemas de procesamiento de datos personales existentes en la Administración Pública Federal y para lo cual, los responsables de las bases de datos deberán registrarlo o actualizarlo dentro de los primeros diez días hábiles de enero y julio de cada año. Asimismo, las dependencias y entidades deberán permitir al IFAI la supervisión del cumplimiento de los lineamientos y en caso de encontrar alguna irregularidad, el Instituto deberá informar al Órgano Interno de Control correspondiente y las sanciones a las que se haga acreedor el servidor público estarán fundamentadas en el capítulo IV de la LFAIPG y en la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.

Con estos lineamientos, podemos ver que en lo referente a la Administración Pública, México ha tratado de cumplir con los lineamientos establecidos internacionalmente, al menos al interior de la estructura gubernamental, puesto que se contemplan los principios, medidas de seguridad y sanciones por la violación al derecho de protección de datos personales, sin embargo, como ha sido indicado a lo largo de este estudio, el individuo ha quedado parcialmente protegido, debido a que en relación a la información en manos de particulares no existe una reglamentación específica que contemple de manera global cualquier violación a este derecho, por lo que quizá estos lineamientos pudieran servir de base para crear una ley federal de protección de datos personales.

3.1.4 Acuerdo por el que se establecen las reglas de operación y funcionamiento del Registro Público de Consumidores.

Con las reformas a la Ley Federal de Protección al Consumidor en 2004, se estableció en el artículo 18 la creación del Registro Público de Consumidores (en adelante RPC), el cual fue establecido como un mecanismo de protección y que con relación al artículo 17, segundo párrafo otorga a los consumidores el derecho a no

ser molestados en su domicilio, lugar de trabajo, dirección electrónica o cualquier tipo de medio:

> *"Artículo 17. ...*
>
> *El consumidor podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad. Asimismo, el consumidor podrá exigir en todo momento a proveedores y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicial.*
>
> *Artículo 18.- La Procuraduría podrá llevar, en su caso, un registro público de consumidores que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios. Los consumidores podrán comunicar por escrito o por correo electrónico a la Procuraduría su solicitud de inscripción en dicho registro, el cual será gratuito."*

Para noviembre de 2007, la Procuraduría Federal del Consumidor (en adelante PROFECO), publicó el Acuerdo por el que se establecieron las reglas de operación y funcionamiento del RPC, contemplando "en su primera etapa a los consumidores que no deseen recibir publicidad en su número telefónico o que su información sea utilizada para fines mercadotécnicos o publicitarios"[204], por lo que deberemos esperar a que en un futuro se establezcan otros mecanismos de protección a la privacidad en cualquiera de los otros medios mencionados en el artículo 17, lo cual, abre una

[204] Acuerdo por el que se establecen las reglas de operación y funcionamiento del Registro Público de Consumidores. Texto vigente.

enorme posibilidad para las empresas de obtener información personal de cualquier individuo en este país y utilizar esta información de manera indiscriminada.

Continuando con el tema, en estas reglas de operación se establece que los sistemas informáticos deberán llevar todos los mecanismos de seguridad necesarios para salvaguardar la información, así como también, el registro de los números telefónicos deberá ser disociado de los datos de identificación del consumidor, para que de esta forma se garantice la seguridad en la identificación del titular de los datos[205].

Por otro lado, en relación al consumidor, éste tiene derecho a ser inscrito en el RPC por un período de tres años a partir del día siguiente a su solicitud, al finalizar este plazo puede renovar la inscripción, ya que de forma automática esta es cancelada al final del período, a nuestro parecer, este es una de las fallas más significativas en relación a la protección de los consumidores debido a que sólo se protege la privacidad de las personas que así lo deseen y por un período corto de tiempo, cuando a nuestro parecer, debiera ser al revés, que sólo los proveedores tuvieran acceso a la información de aquellos consumidores que deseen recibir información de bienes o servicios en su número telefónico, por un período delimitado[206].

Ahora bien, los proveedores y empresas pueden realizar consultas al RPC, con el fin de conocer los números de los consumidores que no deseen recibir información de bienes o servicios, con esto espera la PROFECO que dichos proveedores no utilicen esta información para un fin distinto, sin embargo, existen excepciones para utilizar esta información como es, para fines estadísticos, políticos, de cobranza, por lo que, por un lado una empresa puede consultar el RPC para saber a quien **no** llamar para ofrecerle un bien o servicio, pero sin importar que el individuo no desea ser molestado, su número telefónico si puede ser utilizado para otros fines, por lo que podemos cuestionarnos aquí, ¿qué pasa con aquellas empresas que además de

[205] Artículo 5 de las Reglas
[206] Artículos 6-21 de las Reglas

ofrecer bienes o servicios, también ofrecen servicios de encuestas, o de promoción política?, pues de acuerdo a las reglas de operación, no importa si el individuo expresó no ser molestado, de cualquier forma seguirá recibiendo información no deseada, afectando además su derecho a la intimidad al hacer público su número de teléfono.

Para acceder al Registro, las empresas deberán realizar una solicitud, la cual la podrán tramitar a través de la página web de la PROFECO, en dicha solicitud deberán señalar los datos de la empresa y del representante legal y en caso de que publiciten sus bienes o servicios a través de terceros deberán proporcionar también los datos de éstos, posteriormente, a los dos días hábiles de haber realizado la solicitud, deberán pagar la tarifa correspondiente al área del país del cual deseen conocer los números y al período de consulta, ya sea por 6 meses o un año, la PROFECO, les proporcionará una clave de acceso y contraseña para acceder al listado y la información les será actualizada de manera semanal o quincenal[207].

Por último, si se contemplan sanciones para el caso de los proveedores o empresas que continúen llamando a los teléfonos inscritos en el RPC, las cuales están contempladas en el artículo 18 bis, en relación con el 127 de la Ley Federal de Protección al Consumidor:

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

[207] Artículos 22-33 de las Reglas

> *del manejo de la información de consumidores cuando dicha publicidad la envíen a través de terceros.*
>
> *...*
>
> *"Artículo 127.- Las infracciones a lo dispuesto por los artículos 7 BIS, 13, 17, 18 BIS, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 45, 47, 48, 49, 50, 52, 53, 54, 55, 57, 58, 59, 60, 61, 62, 66, 67, 68, 69, 70, 72, 75, 77, 78, 79, 81, 82, 85, 86 QUATER, 87 BIS, 90, 91, 93, 95 y 113 serán sancionadas con multa de $345.58 y en un máximo de $1'105,856.25 "*

Y de acuerdo a lo indicado en las Reglas de Operación y Funcionamiento del RPC, la PROFECO verificará el cumplimiento de estas reglas por parte de las empresas y proveedores.

Como podemos observar, la creación del RPC, es un intento de protección de datos personales, debido a que se espera que los consumidores sean quienes soliciten su inscripción, pero de acuerdo a la información publicada en la página web de la PROFECO, a un año de haber sido establecido el RPC, sólo se han inscrito 134,101 números telefónicos y de celulares, lo cual nos indica que no todos los poseedores de líneas telefónicas y de celulares en el país saben que pueden ejercer este derecho, de ahí la importancia que la prioridad sea proteger al individuo y no al revés como sucede en este momento, pero también esto es consecuencia de la disgregación de normas que protegen la privacidad de las personas, de ahí la importancia de la existencia de una sola ley que regule y proteja este derecho y que de pauta a que el resto de las leyes que lleguen a contemplar la protección de datos personales remitan a esta para facilitar tanto a los mecanismos de control como a los de protección, y de esta forma se evitarían las lagunas legales.

3.1.5 Ley de Protección y defensa de los usuarios de servicios financieros

Con fecha 15 de junio de 2007, se publicó en el Diario Oficial de la Federación el "Decreto por el que se abroga la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, publicada el 26 de enero de 2004, se expide la Ley para la Transparencia y Ordenamiento de los Servicios Financieros y se reforman, adicionan y derogan diversas disposiciones de la Ley de Instituciones de Crédito y de la Ley de Protección y Defensa al Usuario de Servicios Financieros y la Ley de la Comisión Nacional Bancaria y de Valores" a efecto de complementar un esquema adecuado de protección al usuario de servicios financieros, que fomentara el equilibrio en las relaciones entre el usuario y las entidades financieras.

En esa reforma se otorgaron mayores atribuciones y competencia a la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (en adelante CONDUSEF), al facultarla para crear y operar, entre otros, el Registro Público de Usuarios (en adelante REUS), para que aquellas personas que no desearan que sus datos personales fueran utilizados para fines mercadotécnicos o publicitarios.

Es así como en el artículo 8°, párrafos III al VI, se establece la obligación de esta Comisión a llevar este registro de usuarios, así como también, la prohibición de que las Instituciones Financieras usen esta información para ofrecer bienes o servicios:

> *"Artículo 8o.- ...*
>
> *La Comisión Nacional establecerá y mantendrá actualizado, un Registro de Usuarios que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios.*
>
> *Queda prohibido a las Instituciones Financieras utilizar información relativa a la base de datos de sus clientes con fines mercadotécnicos o*

publicitarios, así como enviar publicidad a los clientes que expresamente les hubieren manifestado su voluntad de no recibirla o que estén inscritos en el registro a que se refiere el párrafo anterior. Las Instituciones Financieras que sean objeto de publicidad son corresponsables del manejo de la información de sus Clientes cuando dicha publicidad la envíen a través de terceros.

Los usuarios se podrán inscribir gratuitamente en el Registro Público de Usuarios, a través de los medios que establezca la Comisión Nacional, la cual será consultada por las instituciones de crédito.

Las Instituciones Financieras que incumplan lo dispuesto por el presente artículo, se harán acreedoras a las sanciones que establece esta Ley."

Por lo que, la CONDUSEF comenzó a trabajar en la creación de este Registro Público, estableciendo los lineamientos para su operación, muy parecidos a los del RPC y en una primera etapa protegerá número telefónico de domicilio y lugar de trabajo, teléfono móvil y correo electrónico tanto particular como de trabajo, cabe señalar que este registro si esta vinculado directamente a la persona, por lo que en caso de que un mismo número telefónico sea utilizado por varias personas cada una por separado deberá registrarse para evitar ser molestada al contrario del RPC en que el número queda bloqueado para cualquier tipo de publicidad, y para varias personal al mismo tiempo.

3.1.6 Lineamientos del Registro de Usuarios

Como se señaló anteriormente, el REUS involucra todos los datos personales, por lo que se podrá vincular a la persona con su número telefónico y por ende con su domicilio y en caso de registrar también el número del lugar de trabajo, el domicilio de este, por lo que la CONDUSEF debe establecer mecanismos máximos de

seguridad para evitar la extracción indebida de información que pudiera dar cómo resultado la violación de la intimidad de la persona. De acuerdo a lo establecido en estos lineamientos, la CONDUSEF solo indicará al Titular de los datos que su información se encuentra salvaguardada en términos del artículo 13 de la LFTAIPG[208].

En relación a la vigencia del registro, este sólo es por dos años y al término de este plazo la CONDUSEF cancelará el registro, teniendo la persona que volver a solicitar su inscripción en el REUS[209].

De igual forma que el RPC, el REUS puede ser consultado por las instituciones financieras para evitar utilizar la información del usuario para fines mercadotécnicos o de publicidad, para ello, deberá pagar a la CONDUSEF $60,000.00 anuales, y la Comisión le dará acceso a la información del REUS en toda su amplitud[210]:

- Información de todos los usuarios registrados.
- Los registros de los usuarios inscritos en los últimos quince días al momento de la consulta.
- Información de todos los usuarios dados de baja.

Por lo que, en caso de existir algún uso indebido de esta información, la Institución Financiera podrá hacerse acreedora de una multa; asimismo, el usuario registrado podrá presentar un aviso de infracción a la CONDUSEF en el caso de recibir publicidad de algún bien o servicio. La Comisión investigará y en caso de declarar procedente el aviso de infracción contabilizará los avisos que reciba con respecto a una Institución Financiera por trimestre calendario, al final de cada uno de estos, notificará a la Institución y está tendrá un plazo de diez días para manifestar lo que a su derecho convenga[211].

[208] Artículo 7, segundo párrafo de los lineamientos.
[209] Artículo 13 de los lineamientos.
[210] Artículos 23 a 32 de los Lineamientos.
[211] Artículos 36 a 41 de los Lineamientos.

La CONDUSEF revisará y en caso de proceder contabilizará por trimestre las infracciones e impondrá la multa correspondiente[212]:

a) Multa de 250 días de salario cuando el número de infracciones registradas en el trimestre sea de 1 a 20.
b) Multa de 251 a 325 días de salario cuando el número de infracciones registradas en el trimestre sea de 21 a 40.
c) Multa de 326 a 1000 días de salario cuando el número de infracciones sea de 41 a 60.
d) Multa de 1001 a 1600 días de salario, cuando el número de infracciones sea de 61 a 80.
e) Multa de 1601 a 2000 días de salario cuando el número de infracciones sea de 81 o más.

Como se puede ver, estos lineamientos son en estructura parecidos a los del RPC, sin embargo, subsisten diferencias que debieran revisarse y por lo tanto homologarse, como es el caso del tiempo en que los datos del usuario serán mantenidos en el registro o la información recabada, así como también los costos para acceder a la base de datos por parte de las empresas o instituciones, ya que a nuestro parecer el hecho de que para un mismo objetivo –la negación por parte de los titulares de los datos de recibir información para ofrecer bienes o servicios- se tomen diferentes criterios desde el tipo de datos a solicitar hasta la forma de imponer infracciones crea inseguridad en el ciudadano que desea proteger su información. Esto también se debe a la falta de una sola regulación que establezca los criterios que deberán tomarse en consideración en el momento de crear cualquier tipo de procesamiento de datos, para que de tal forma, el ciudadano sepa que todas las bases de datos existentes manejaran un mínimo de medidas de seguridad, criterios de protección y de transmisión de información, asimismo, se ahorrarían recursos cada vez que se quisiera implementar algún nuevo procesamiento de datos.

[212] Artículo 42 de los Lineamientos.

Además de que se establece la adquisición de información previo pago de los derechos pero no se indica nada respecto al consentimiento del titular para que su información aún sin utilizarse pueda volverse "pública".

3.1.7. Ley de Transparencia y Acceso a la Información en el Distrito Federal

Esta ley, en su estructura busca tutelar la protección de datos personales, para así servir de fundamento para la Ley de Protección de Datos Personales recientemente aprobada por la Asamblea Legislativa del D.F., sin embargo y a nuestro parecer es ambiguo el tratamiento que se le dio a esta materia, empezando con la definición que se estableció de datos personales:

> *"Artículo 4. Para los efectos de esta Ley se entiende por:*
> *...*
> *II. Datos Personales: Toda información relativa a la vida privada de las personas;*
> *...*
> *VII. Información Confidencial: La que contiene datos personales relativos a las características físicas, morales o emocionales, origen étnico o racial, domicilio, vida familiar, privada, íntima y afectiva, número telefónico privado, correo electrónico, ideología, preferencias sexuales y toda aquella información que se encuentra en posesión de los entes públicos, susceptible de ser tutelada por el derecho fundamental a la privacidad, intimidad, honor y dignidad;*
> *...*
> *XV. Protección de Datos Personales: La garantía que tutela la privacidad de datos personales en poder de los entes públicos;*
> *...*
> *XVIII. Sistema de datos personales: El conjunto ordenado de datos personales que estén en posesión de un Ente Público; ..."*[213]

[213] Artículo 4 de la LTAIPDF

Como podemos observar, las fracciones II y VII bien pudieron ser parte de una sola, pero el legislador las separo quizá para buscar ser más específico en cual sería la protección a este derecho, sin embargo, al tratar de ser tan descriptivo en la fracción VII, podría llegarse a argumentar, por ejemplo, que una imagen fotográfica de la persona no entra en la descripción de este numeral y por lo tanto, no es susceptible de protección.

De igual forma, la fracción XV, deja ambiguo lo que significa el derecho a la protección de datos personales, así como también lo limita a solo aquella información en poder de los entes públicos. Aquí cabe recordar que en el capítulo anterior se hizo mención que a los legisladores no les interesó dar una protección integral a este derecho "*debido a la complejidad que acarrea y al hecho de que cada ente privado es sujeto de una ley en específico, ya sea local o federal, que regula su actividad*"[214] por lo que a nuestro parecer, si en un principio no esta bien definido que se va a proteger, no puede esperarse una buena protección de este derecho.

Considerando lo anterior, pasemos pues al análisis de la Ley de Protección de Datos Personales del D.F. publicada en octubre de 2008, la cual retoma muchos principios de la LOPD.

Esta ley fue publicada el pasado 3 de octubre de 2008, antes de la reforma constitucional al artículo 16, por lo que a nuestro parecer a muy poco tiempo de haber sido creada, deberá ser modificada y ajustada para cumplir con el precepto constitucional, ya que al no hacerlo podría llegar a convertirse en una ley con problemas de inconstitucionalidad, debido a que de acuerdo a su artículo 3°, deberá ser interpretada conforme a la Constitución y a todos los preceptos internacionales firmados por México:

[214] *Vid supra*, capítulo II. Pags. 80 y 81

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

Por otro lado, al no existir una ley federal de la materia, la Asamblea Legislativa trató de abarcar todos los principios aceptados a nivel internacional, sin embargo en lo referente a la conservación de datos con fines históricos el artículo 5° en su último párrafo indica:

> *"Únicamente podrán ser conservados de manera integra, permanente y sujetos a tratamiento los datos personales con fines históricos."*

Lo cual llama la atención, debido a que si la intención era realizar una ley lo más apegada a los estándares aceptados internacionalmente, en estos se prohíbe la "conservación integra" de los datos personales para fines históricos, ya que lo único que se espera es que el Gobierno mantenga la información que sirva para controles estadísticos e históricos y el resto sea destruida, ya que lo único que necesita para establecer programas de gobierno son aquéllos indicativos que sirvan para conocer a la población de manera general e imparcial y saber de esta forma que es lo que se necesita y donde debe aplicarse primordialmente; al permitir que en el Distrito Federal se guarde de manera "integra" la información, podría caerse en la suspicacia que ésta servirá para crear otro tipo de controles lejanos a la democracia e igualdad.

Por lo que, la Asamblea Legislativa deberá considerar modificar la ley y ajustarla al artículo 16 Constitucional, o bien, después de creada una ley a nivel federal,

apegarse a lo que se establezca, para permanecer en concordancia con la federación.

3.2 Problemática Actual

Hoy día, es difícil concebir la realización de las diferentes actividades del hombre sin el uso de las tecnologías de la información, pero el uso indiscriminado de estas nos han llevado a cuestionarnos sobre los límites que deben imponerse para evitar el mal uso y abuso de estas en contra de las mismas personas, tales como el robo de información o la invasión de la privacidad.

Existen sectores de la sociedad que están en contra de limitar el uso de estas tecnologías por que es parte del derecho a la información que todo ser humano tiene, pero también existen otros que se encuentran preocupados por la falta de controles que impongan sanciones adecuadas a quienes violentan la seguridad e intimidad de las personas a través de estos medios tecnológicos.

A continuación, analizaremos la problemática en torno a la protección de datos personales y su consecuencia con la intimidad de las personas en el uso de las nuevas tecnologías de la información.

3.2.1 Transmisión de datos indiscriminado entre particulares

En la actualidad la mayoría de las personas de manera constante y de manera casi imperceptible, hace uso de sus datos personales para realizar casi cualquier trámite, desde la compra de algún bien o servicio, en el que con solo utilizar una tarjeta de crédito la institución bancaria transmite al vendedor la información necesaria del cliente para aprobar la transacción, hasta el uso simple del correo electrónico en el que el remitente por “*default*” transmite su nombre a quien le envía un correo.

Sin embargo, ¿Qué sucede cuando estos simples movimientos comienzan a realizarse sin el consentimiento de las personas?

Esto es, cuando los creadores de bases de datos personales creen ser dueños de la información contenida en estas comienzan a transmitir los datos a terceros sin el consentimiento de los titulares; como ya se ha visto, en México sólo los entes de Gobierno tienen límites en la obtención, procesamiento y transmisión de la información contenida en sus bases de datos, pero los particulares no, los cuales son los que en la mayor parte de las ocasiones tienen más facilidad para hacerse de estos datos y de utilizarlos para distintos fines sin que el titular tenga conocimiento de ello; como ejemplo podemos tomar el "Programa de Transporte Escolar Obligatorio" decretado por el Gobierno del Distrito Federal el pasado mes de febrero de 2009, en dicho programa a las escuelas particulares se les obliga a aplicar el transporte escolar a todo el alumnado, para ello, cada escuela tiene la obligación de dar a conocer al Gobierno del Distrito Federal el nombre, edad, año escolar, horario, clases extracurriculares, domicilio y nombre de padres o tutores de cada menor, y por el solo hecho de que no existe alguna restricción para las escuelas privadas, en la transmisión de la información a terceros, estas, sin que medie la aprobación del titular de los datos (o en este caso del tutor) transmite la información, la cual es reunida por el Gobierno del Distrito Federal para su procesamiento, y como esta información no es reunida de manera directa por este, el Gobierno del Distrito Federal no tiene obligación de cumplir con lo establecido en la LPDPDF, en sus artículos 6 al 12, en el que se establece el procedimiento para la creación y procesamiento de bases de datos.

De esta forma, un decreto administrativo (nombrado así por el Jefe de Gobierno del Distrito Federal) obligatorio a ciertos particulares, hace que estos procesen y transmitan la información obtenida por ellos, para el uso de un tercero sin que sea necesaria la autorización de los titulares de los datos[215].

[215] Para el caso concreto, se puede señalar lo acontecido en el Colegio Madrid, A.C., en el mes de mayo del presente, cuando el GDF solicitó esta información a la escuela, aún no entraba en vigor la reforma al artículo 16 constitucional, por lo que esta transmitió la información al GDF, aún y cuando

El anterior es un ejemplo de cómo la autoridad puede hacer que los particulares violen derechos de terceros al cobijo de no existir regulación alguna que les prohíba realizar cualquier procesamiento de datos personales.

Ahora bien, retomando el ejemplo del correo electrónico, los particulares, en la mayor parte del tiempo, violan de manera constante los derechos de terceros, sólo pensemos en la acción del reenvío de un correo electrónico; en la mayoría de las ocasiones nunca borramos los correos de las otras personas que vienen incluidos y de esta manera propagamos información de terceros sin su conocimiento, el problema radica cuando estos datos (por insignificantes que parezcan) llegan a las manos de quien puede darles un uso distinto al planeado por el titular, como veremos más adelante.

3.2.2 Uso para fines comerciales

Los datos personales tienen adquirido un valor de mercado considerable y, por lo tanto, cada vez existen más empresas que se dedican a gestionar la compilación, procesamiento y transmisión de información obtenida de diferentes bases de datos, desde las creadas por las empresas para el control de su personal hasta aquellos obtenidos a partir de una consulta o encuesta.

Con esta información, crean perfiles de gustos, aficiones, gastos, sueldos, para después ofertarlos a terceros que ofrecen bienes o servicios, de ahí que los titulares de los datos reciben llamadas, correos, mensajes o propaganda a su casa u oficina. Como vimos anteriormente, en México la PROFECO y CONDUSEF son las facultadas para llevar un registro de los usuarios que no deseen ser molestados con este tipo de información, sin embargo, la falta de conocimiento por parte de la mayoría, de estas medidas de protección y de los derechos que se tienen en esta

---

los padres de familia por escrito se declararon en contra de la transmisión, por ser violatoria a la intimidad del menor, pero al no existir alguna norma en específico que prohibiera a las autoridades del

materia hace más vulnerables a los titulares de los datos de que su información sea excluida de este tipo de compilaciones.

Asimismo, al realizar estas empresas el procesamiento de la información se abre la puerta a prácticas discriminatorias como el tratar de identificar a los “buenos clientes” de los “malos clientes”, personas con algún tipo de padecimiento o perfil socioeconómico, que tal y como vimos en el capítulo II, en otras legislaciones esto se busca evitar por ser violatorio de Derechos Humanos.

3.2.2.1 Estudios de mercado

Retomando el punto anterior, al realizarse filtrados de información muchas empresas utilizan los resultados de estas consultas para realizar investigaciones que ayuden a las empresas sobre la viabilidad comercial de una actividad económica en específico.

Tal y como hemos visto a lo largo de esta investigación, en muchas ocasiones las personas otorgan información personal sin estar seguros que ésta no será utilizada para fines distintos a los indicados para su recolección, esto es, desde una pequeña encuesta fuera del supermercado, en que le preguntan a las personas cuales son sus preferencias en el uso de un producto hasta la visita de páginas en Internet en las que nos solicitan contestar un cuestionario, pasando por las llamadas telefónicas en que nos ofrecen servicios y además nos solicitan información de conocidos para hacerles las mismas ofertas, con esto, las empresas se hacen llegar de información para conocer el perfil de distintos sectores de la sociedad y saber entonces si un producto puede tener éxito comercial, cuanta producción deberá realizarse, o las modificaciones que deban realizarse para hacerlo comercial, sin que exista una ley en específico que les obligue a informar a los titulares de los datos los fines de la información obtenida y peor aún, que les impida procesar esta información para otros fines.

---

colegio el procesamiento y transmisión de la información, esta fue entregada sin restricciones al GDF.

3.2.2.2 Venta de productos y servicios

En numerosas ocasiones, hemos recibido llamadas telefónicas o correos electrónicos para ofrecernos productos o servicios, sin embargo, el problema no radica en el ofrecimiento de éstos, sino, en como estas empresas obtuvieron nuestros datos para poder comunicarse con nosotros, en los puntos anteriores hemos explicado la forma en que se procesan los datos personales, e inclusive en algunas ocasiones al recibir llamadas telefónicas se nos pregunta si nosotros pudieramos recomendar a alguien, es así como el mismo titular de los datos otorga información de otros titulares a terceros, con el desconocimiento de aquéllos, por lo que de esta forma se acrecenta la información obtenida sin ninguna restricción, ya que estas empresas en este momento, no tienen límite alguno para obtener de los particulares datos de otros particulares y mucho menos la obligación de informar al otorgante de que este simple acto, puede ser violatorio de derechos.

De ahí la importancia de crear una ley que contemple sanciones para los particulares que abusando del desconocimiento de los titulares de los datos obtengan información de terceros, así como también, que sancione a aquellos que no otorgan la información necesaria con el fin de que el titular conozca los fines para los cuales esta otorgando la información y que se le de la opción de consentir su adhesión a una determinada base de datos.

3.2.3 Uso para fines delictivos

En los últimos años, en nuestro país la sociedad civil ha exigido al Gobierno que tome medidas de seguridad mayores, todo esto debido al desencadenamiento de diferentes delitos que han efectado de manera emocional y psicológica a toda la sociedad, es por ello, que se han realizado diferentes reformas a la Constitución y a las leyes con el fin de dar un halo de protección a la sociedad.

Para los fines de esta investigación, entre estas reformas se encuentran la del artículo 16 Constitucional en cuanto a protección de datos personales, la de la ley de telecomunicaciones y la creación del registro de usuarios de telefonía celular, y la creación de la ley general del sistema nacional de seguridad pública (en relación a las bases de datos criminalísticas y de personal[216]) con estas reformas, algunas de sus pretensiones es tener un control de todos los dueños de números celulares, y de los policías y delincuentes a nivel nacional; en todas estas bases de datos propuestas, se tiene previsto obtener de los titulares de los datos desde el nombre hasta las huellas dactilares, por lo que, al contener datos sensibles, se esperaría que se tomaran todas las medidas de seguridad para evitar el mal uso de la información contenida; esto es, para el caso de filtrado de información para el uso de investigaciones criminales, debe asegurarse que esta será utilizada únicamente para una investigación en concreto, por un tiempo determinado y que dicha consulta será destruida una vez terminada la investigación, con el fin de que aquellos titulares de los datos que pudieran estar involucrados en una investigación y al final, no resultaran ser sospechosos, no queden señalados, evitando de esta forma, actos discriminatorios en un futuro; o bien, que existan los controles debidos de seguridad a fin de evitar que la información contenida en estas bases de datos o la obtenida de un procesamiento no sea transferida a terceros.

3.2.3.1 Robo de identidad

Se entiende como robo de identidad al uso ilegal de la información personal de un sujeto, como el nombre, número de seguridad social, licencia de conducir, números de cuenta o tarjetas de crédito y quiénes lo realizan, utilizan esta información para comprar, solicitar créditos o inclusive buscar empleo, con el fin de ligar otros actos delictivos[217].

[216] Art. 5, fracción II de la LGSNSP
[217] http://www.oag.state.ny.us/spanish/bureaus/consumer_frauds/identity_theft.html

Este tipo de delito también es conocido como “phising”, y se presume que alrededor del mundo esta práctica cuesta millones de dolares en pérdidas. En nuestro país no estamos exentos de ello, quizá no es un tema que se de a conocer de manera constante, debido a que en muchas de las ocasiones, el afectado no identifica de manera inmediata que es víctima de este delito, y por otro lado, existe una falta de interés y desconocimiento del tema por parte de autoridades y legisladores ya que el robo de identidad, hoy día, no se encuentra tipificado como delito; de ahí la importancia de crear una ley de protección de datos personales que contemple multas a quienes sin la debida autorización transmiten información a terceros o penas a quien a través de sitios web obtienen datos personales con el fin de cometer actos delictivos, a la vez de realizar las reformas necesarias al código penal federal para su inclusión como delito[218].

3.2.3.2 Secuestro

En la última decada, la población nacional ha exigido al Gobierno mejorar su trabajo en cuestión de seguridad pública, debido a los altos índices delictivos, para ello, se han realizado distintas reformas legales con el fin de dar respuesta a esta solicitud, entre ellas, como ya se había mencionado líneas arriba, estan las reformas a la Ley Federal de Telecomunicaciones y la creación del registro de usuarios de telefonía celular (en adelante RENAUT), con el fin primordial de poder tener un control de quiénes son los usuarios de cada uno de los números de celulares existentes en el país, todo esto debido a que la delincuencia organizada utiliza este medio de comunicación para extorsionar a los familiares de las víctimas, por lo que, al crear el RENAUT, se busca tener un control del 100% de los números existentes, cuestión que hoy día no existe.

Ahora bien, lo importante para este trabajo de investigación no es la persecución de los delitos, si no, los controles que deben crearse con el fin de proteger la

[218] Debido a que la comisión de este delito se realiza con documentos públicos y de que puede suceder en diferentes territorios tanto nacional como internacional, de ahí la importancia que este sea

información personal otorgada, así como también el que existan los medios adecuados para que el titular de los datos pueda acceder a esta información ya sea para actualizarla o eliminarla, de ahí la importancia de contar con los medios legales para resguardar la información con el fin de evitar de que en lugar de servir para identificar a presuntos secuestradores y extorsionadores, sirva a la delincuencia organizada para identificar a posibles víctimas de este tipo de delitos, máxime que la obtención y administración primigenia de esta información será por parte de las compañías de telefonía celular, de ahí, la importancia de crear los controles debidos para evitar que los administradores de las bases de datos lleguen a realizar procesamientos de información distintos a los indicados en las Reglas del Registro Nacional de Usuarios de Telefonía Móvil[219].

Aunado a lo anterior, cabe señalar que en dichas Reglas no se establecieron las obligaciones y posibles sanciones a quien haga uso distinto de la información recabada, así como también, a los concesionarios se les obliga llevar un registro de las llamadas, números marcados y ubicación de cada número telefónico, por lo que, con la información recabada los concesionarios podrían realizar filtros de información y crear perfiles de cada uno de sus usuarios, por lo que, de manera constante violarían la privacidad de los titulares de los datos[220].

3.2.3.3 Fraude electrónico

Este delito se encuentra ligado con el robo de identidad, debido a que el delincuente busca conseguir los datos confidenciales de usuarios como contraseñas o claves de acceso a cuentas bancarias principalmente, los medios más utilizados son el correo electrónico o mensajes de texto por teléfono celular, en estos mensajes generalmente se indica al usuario que acceda a alguna página web conocida (por lo

reconocido primeramente a nivel federal para su inclusión posterior a nivel estatal.

[219] Emitidas por el Pleno de la Comisión Federal de Telecomunicaciones y publicadas en el DOF el 15 de mayo de 2009.

[220] Numeral 10 de las Reglas.

regular son copias idénticas de páginas visitadas con regularidad por la persona), donde deberá completar información sobre sus datos personales.

El problema radica en el primer acercamiento que tiene el delincuente con la información, generalmente obtenida por correos electrónicos enviados masivamente o la inclusión de la persona en distintas bases de datos (redes sociales, revistas electrónicas, servicios bancarios, etcétera) sin que observe las medidas adecuadas para proteger su información, ya que a partir de este primer acercamiento es que entonces el delincuente puede observar los movimientos que dentro de internet realiza la persona. Debido a esto, es que en caso de existir una Ley de Protección de Datos Personales, podría obligarse a todas las páginas web hospedadas en servidores nacionales a certificar las medidas de seguridad e informar a sus usuarios de cómo proteger su información, así como también, podría entonces firmar convenios de colaboración a nivel internacional en el que se pueda crear una red de investigación y protección de datos personales, tal y como en otros países se ha hecho[221].

3.2.4 Para fines políticos

Cuando en 2006, se dudó de la legitimidad de las elecciones, por el margen tan estrecho de votos, el Poder Legislativo realizó distintas reformas a la Constitución y al Código Federal de Instituciones y Procedimientos Electorales (en adelante COFIPE), con el fin de hacer más equitativas las elecciones. Entre estas modificaciones se establecieron límites a los tiempos oficiales en radio y televisión por parte de candidatos y partidos políticos, sin embargo, olvidaron que existen otros medios como el teléfono, internet, correo electrónico que pueden ser utilizados por estos y sin limitación alguna[222].

[221] Hay que recordar que en las legislaciones estudiadas en el capítulo II, uno de los requerimientos señalados para la transmisión transfronteriza de datos personales, es que el receptor radique en un país en el que se dictaminen las normas necesarias a fin de crear las medidas necesarias para proteger la información.
[222] Art. 345, 1, inciso b) del COFIPE

Por otro lado, el Registro Federal de Electores, que es el encargado de administrar la base de datos de todos los ciudadanos, entre sus funciones y obligaciones se encuentra el acceso a esta por parte de la ciudadanía, funcionarios y partidos políticos, tal y como se establece en diversos artículos del COFIPE:

> *Artículo 171 (…)*
> *4. Los miembros de los Consejos General, Locales y Distritales, así como de las comisiones de vigilancia, tendrán acceso a la información que conforma el padrón electoral, exclusivamente para el cumplimiento de sus funciones y no podrán darle o destinarla a finalidad u objeto distinto al de la revisión del padrón electoral y las listas nominales.*
> *(…)*
> *Artículo 192*
> *1. En cada Junta Distrital, de manera permanente, el Instituto pondrá a disposición de los ciudadanos los medios para consulta electrónica de su inscripción en el padrón electoral y en las correspondientes listas nominales, conforme a los procedimientos que determine la Dirección Ejecutiva del Registro Federal de Electores.*
>
> *2. Los partidos políticos tendrán acceso en forma permanente a la base de datos del padrón electoral y las listas nominales, exclusivamente para su revisión, y no podrán usar dicha información para fines distintos.*
>
> *Artículo 321 (…)*
> *1. Los partidos políticos, a través de sus representantes en la Comisión Nacional de Vigilancia, tendrán derecho a verificar las listas nominales de electores residentes en el extranjero, a que se refiere el inciso b) del párrafo 2 del artículo anterior, a través de los medios electrónicos con que cuente la Dirección Ejecutiva del Registro Federal de Electores.*
> *(…)*

Tal y como se puede observar, en los numerales que hacen referencia a partidos políticos se establece que estos tendrán acceso permanente al padrón electoral y si bien, se plasma la prohibición de usar esta información con fines distintos, dentro del COFIPE no existe algún tipo de sanción para el caso en que estos la utilicen con otros fines; por lo que, es necesario implementar las medidas necesarias para evitar que partidos políticos (o miembros de estos) puedan utilizar esta base de datos con objetivos distintos a los establecidos debido a las lagunas de ley existentes.

Ahora bien, si relacionamos este acceso permanente a la base de datos del padrón, con el acceso a los medios de comunicación que no fueron limitados en la actual legislación, y a que las restricciones establecidas por la PROFECO y la CONDUSEF para que los titulares de los datos no sean molestados en su domicilio, en donde la restricción no será aplicada a partidos políticos, es como podemos entender que estos puedan enviar correos electrónicos, mensajes a celular y llamadas a domicilio para dar a conocer a los electores sus plataformas políticas, lo cual, en realidad esta violando el derecho a la intimidad de las personas, aunado a que sus datos personales en realidad están siendo utilizados para fines distintos para los cuales fueron recabados, de ahí la importancia de la creación de una ley de protección de datos que contemple los cuatro fundamentos de protección: Acceso, Rectificación, Cancelación y Oposición, donde este último sea el que permita al Titular de los datos a decidir si quiere recibir información de los partidos políticos y que sus datos personales pertenezcan a la base de datos de “posibles” electores que forman estos.

3.2.4.1 Preferencias políticas

Alrededor del mundo en tiempos electorales, se realizan encuestas de opinión para conocer las preferencias de los electores, con esta información, los partidos políticos y candidatos modifican sus estrategias para hacerse llegar de votos y tratar de ganar la contienda política.

En muchas ocasiones, en este tipo de encuestas al realizarse no sólo se cuestiona sobre la preferencia política de la persona, si no también llegan a solicitarse datos personales, sin que al titular de estos, se le indique el fin que se persigue, esto es, al igual que existen agencias dedicadas a recabar información para hacer estudios de mercado, también hay las que se dedican a informar y encontrar posibles electores, lo que ayuda a los partidos políticos a conocer las posibilidades para ganar una elección o encontrar nuevos miembros de partido, de ahí la importancia de que se ofrezca al ciudadano la información necesaria para decidir si en la realización de una encuesta desea otorgar sus datos personales.

Por otro lado, tal y como se estudió en otros países la preferencia política de las personas es considerado un dato sensible para evitar restricciones o discriminación, por lo que, en nuestro caso, al crear una ley de protección de datos esta debiera considerar ý reconocer esta información como dato sensible, lo cual conllevaría a evitar el mal uso de esta información en el momento de aplicar programas gubernamentales.

3.2.4.2 Estrategia electoral

Aunado al punto anterior, en los últimos años alrededor del mundo candidatos y partidos políticos han utilizado los medios antes señalados para dar a conocer sus plataformas políticas y de esta forma ampliar el número de posibles electores, cabe recordar que en las pasadas elecciones de Estados Unidos, los candidatos abrieron perfiles en redes sociales, las cuales les sirvieron para conocer de primera mano las principales necesidades y percepciones de la ciudadanía, lo que les ayudó a “mercantilizar” su imagen y de esta forma, ganar más votos.

De la misma forma, en nuestro país, en las pasadas elecciones de julio, los distintos partidos políticos ofrecieron a través de sus páginas de internet, redes sociales, mensajes en páginas de correo electrónico, o llamadas telefónicas, la oferta política de sus candidatos, sin que esto pudiera ser monitoreado, ya que quedaba fuera de

las facultades del IFE, por lo que, sin considerar los gastos producidos, la ciudadanía vio invadida su privacidad con esta propaganda, al recibir correos, mensajes o anuncios en las páginas que se saben son las más visitadas, por lo que, al crearse una ley de protección de datos, esta podría incluir la opción de que los electores decidan si quieren recibir esta información y de esta manera vigilar también si los partidos políticos hacen un uso distinto de los datos personales que tienen a su alcance.

3.2.4.3 Fraude electoral

Este es un delito controversial y que se presta a la polémica por la dificultad de probar su existencia debido a los intereses políticos que existen en torno a este; para fines de este trabajo de investigación, uno de los actos que se realizan para cometer este delito, es la suplantación de personas o bien asumiendo identidades, esto es, a través del conocimiento del padrón electoral se crean documentos personales que servirán para identificarse en el momento de emitir el voto.

Debido a lo anterior, es por ello que se hace necesario tener un control más estricto del manejo de la información, y de todos los procesamientos y filtros de información posibles a realizar para evitar la suplantación o robo de identidad, por lo que, es necesario la coordinación real entre los distintos entes de gobierno que manejan datos personales tales como el control de población por medio de la CONAPO, el padrón electoral por medio del IFE y la posible creación de la cédula de identidad nacional que contendrá datos biométricos, lo cual serviría para cruzar información, validar la real existencia de alguien e identificar la posible duplicidad o robo de identidades, así como también, en cuanto se registrará el fallecimiento de una persona, automáticamente la información podría darse de baja en todas estas bases de datos con el fin de evitar que los “muertos” voten, compren o realicen cualquier otro tipo de actividad ilícita.

3.3 Defensa del particular frente al uso indiscriminado de la información de otros particulares.

A lo largo de esta investigación hemos podido revisar diferentes formas de violación a la intimidad y datos personales, y como también distintos países han legislado para proteger estos derechos, sin embargo, falta analizar las opciones existentes que podrían ser utilizadas para establecer un procedimiento para que el particular pueda hacer valer estos derechos.

Actualmente, existen procedimientos establecidos para que los titulares de los datos puedan acceder a su información personal y solicitar su modificación, rectificación o cancelación ante organismos gubernamentales; falta entonces la creación o ajustes debidos a estos procedimientos para su funcionamiento entre particulares.

En Argentina por ejemplo, existe el *habeas data* con el cual, el particular puede iniciar un procedimiento ante tribunales para hacer valer sus derechos ya sea frente a los entes de gobierno o particulares, en dicho procedimiento se reconoce el derecho de los titulares de los datos y la posible reparación del daño por el mal uso del que hubiese sido objeto y los tribunales pueden llegar a establecer desde multas hasta suspensión en el uso de las bases de datos para aquellos particulares que violen los derechos de terceros[223], por lo tanto, supone una garantía sobre el adecuado manejo de la información personal que se encuentra bajo poder de terceros, lo cual permite evitar los abusos y subsanar los errores involuntarios en la administración y publicación de datos personales.

Por lo que, el establecimiento de un procedimiento parecido en nuestro país, garantizaría a todos los habitantes que su información personal sería procesada bajo estrictos controles de seguridad y con los fines para los cuales fueron otorgados, ya que de lo contrario quien hiciera un uso inadecuado de la información contenida en las bases de datos se haría acreedor de sanciones cuantificadas de acuerdo al daño

[223] *Vid Supra,* 2.3 Ley Argentina. Pag. 105 a 139

ocasionado, por lo que, con esto se otorgaría seguridad jurídica a cualquier titular de datos lo que daría como resultado la protección y respeto a su privacidad.

CAPÍTULO IV. INSTRUMENTOS DE PROTECCIÓN A LA INTIMIDAD Y DATOS PERSONALES ENTRE PARTICULARES

Como se ha estudiado a lo largo de esta investigación, en nuestro país es importante contar con un instrumento que proteja y otorgue los medios jurídicos necesarios para que los titulares de los datos puedan ejercer sus derechos.

En este último capítulo presentaremos la propuesta de creación de una Ley de Protección de Datos Personales que contemple tanto a los entes de gobierno como a los particulares, ya que como hemos visto, la violación del derecho a la intimidad y protección de datos puede darse casi por cualquier individuo.

4.1 Diseño Constitucional

4.1.1 Propuesta de Reforma

Tal y como se vio en el capítulo anterior, el pasado primero de junio de 2009, se promulgó una reforma al artículo 16 de la Constitución, adicionándose un segundo párrafo en el que se reconoce y se eleva a rango constitucional la protección de datos personales.[224]

Sin embargo, a nuestro parecer la adición de este párrafo no debió realizarse en el artículo 16, si no en el 6, para lo cual, expondremos a continuación, nuestro punto de vista.

Si bien es cierto, que el artículo 16 en su primer párrafo, reconoce el derecho a la privacidad de los individuos, también lo es, que todo el artículo esta directamente relacionado con la actuación del Estado hacia estos y sin ninguna ampliación hacia el actuar de los particulares en contra de otros particulares.

---

[224] *Vid Supra* 3.1.1. Constitución Política de los Estados Unidos Mexicanos, pag. 157

Esto es, este artículo nos recuerda que la actuación del Estado se encuentra limitada por el derecho, con el fin de que la persona, familia, posesiones, bienes y derechos de los gobernados encuentren protección ante injerencias arbitrarias por parte de las autoridades, por lo que el principio de legalidad inscrito en este artículo, es una especie de "poder vedado", en donde el Estado puede intervenir únicamente cuando se cumplen ciertos requisitos de orden constitucional y que de acuerdo a sus orígenes, en el pensamiento jurídico y filosófico de la ilustración, se cumple con la obligatoriedad que tienen las autoridades de someterse a las leyes, que al fin al cabo son provenientes de la voluntad y la razón del pueblo[225]; por lo que, al insertar la protección de datos personales en este artículo y quedar relacionado con esta obligación del Estado de motivar y fundamentar conforme a derecho cualquier actuación, podría llegar a interpretarse que una ley emanada de este párrafo no debe necesariamente contemplar a los particulares. De ahí que el Congreso se vio obligado a insertar la fracción XXIX-O al artículo 73 de la Constitución, *"Para legislar en materia de protección de datos personales en posesión de particulares."*[226].

Es así, que si damos una segunda lectura a los párrafos primero y segundo de este artículo es que podremos darnos cuenta que guardan tres principios que desde su origen ha mantenido el artículo 16: a) acto de molestia emanado de autoridad competente, b) garantía de mandamiento escrito, en el que se funde y motive la causa legal para ejecutar un acto de molestia en contra de un particular, c) garantía de detención por orden judicial:

> *"Art. 16.- Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.*

[225] Este pensamiento quedó plasmado en el artículo 6° de la Declaración de los derechos del hombre y del ciudadano de 1789, que a la letra establece: "La ley es la expresión de la voluntad general. Todos los ciudadanos tienen derecho a participar en su elaboración, personalmente o por medio de sus representantes. La ley debe ser igual para todos, tanto para proteger como para castigar. Puesto que todos lo ciudadanos son iguales ante la ley, cada cual puede aspirar a todas las dignidades, puestos y cargos públicos, según su capacidad y sin más distinción que la de sus virtudes y talentos."

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

Debido a lo anterior, bien pudiera interpretarse entonces que los titulares de los datos sólo podrán ejercer el derecho de protección ante el Estado y no ante otros particulares, ya que de querer ejercer una acción en contra de otro particular, probablemente, daría pie al Juicio de Amparo en contra de alguna resolución, por parte de quien se encontrara en este supuesto.

Ahora bien, con respecto a la propuesta inicial de este trabajo de investigación, de incluir en el articulo 6 constitucional el derecho a la protección de datos personales, se debía a tres puntos principalmente:

1. El derecho a la protección de datos personales, se encuentra ligado al derecho de la información, que tal y como se vió en el primer capítulo, es el derecho que toda persona tiene para crear, investigar, conocer y difundir **cualquier** tipo de información, y en la actualidad, muchas de las veces en que se ejerce este derecho ante los entes de gobierno, se solicita información sobre datos personales, de ahí la importancia de limitar el acceso con el fin de salvaguardar la privacidad de la información.

2. Actualmente, el artículo 6 en sus fracciones II y III, contempla la protección de datos personales y a la vida privada en posesión de los entes de gobierno, por

[226] *Vid Supra,* capítulo III. Pag. 159

lo que a nuestro parecer, para reconocer ampliamente este derecho fundamental con todos los derechos que conlleva (acceso, rectificación, cancelación y oposición) solo debió realizarse una ampliación a este artículo y establecer la obligación de los particulares a respetar este derecho.

3. La LFTAIPG, tal y como se vió en el capítulo anterior, contempla la protección de datos y el IFAI es el encargado de crear los instrumentos para controlar la información relativa a estos, debido a ello, con la modificación al artículo 6, habría sido más sencillo desprender tanto del artículo como de la citada ley, este derecho y volverlo independiente al Derecho de la Información, que tal y como lo mencionamos en el capítulo anterior, estos dos derechos no deberían ser vigilados por el mismo organismo[227].

De esta manera, el Congreso no se habría visto en la necesidad de ampliar sus facultades para poder legislar en materia de protección de datos personales en manos de particulares, ademas de que con la reforma actual, se corre con el peligro de que este derecho es protegido sólo en cuanto a actos de molestia por parte del Estado.

Por último, después de este análisis, nosotros proponemos que podría realizarse entonces, en el segundo párrafo del artículo 16, una reforma en el que se agregara la obligación de los particulares de respetar y proteger los datos personales en su posesión, por lo que, el citado segundo párrafo de este artículo podría quedar de la siguiente manera:

> *"Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley,* ***el Estado y las personas físicas y morales estarán obligadas a su observancia y se***

[227] *Vid Supra* 3.1.2. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Pag.160

> ***establecerán*** *los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros"*

4.2 Ley de Protección de Datos Personales entre Particulares

Esta ley deberá ser de observancia general en toda la República y tendrá por objeto regular el derecho a la autodeterminación informativa de las personas atendiendo a los cuatro principios de este derecho: Acceso, Rectificación, Corrección y Oposición, que permita, por un lado el legítimo, controlado e informado procesamiento de datos personales y la protección a la privacidad, y por otro lado, deberá regular el tratamiento de los datos personales por parte de los sujetos obligados.

4.2.1 Preámbulo

Como hemos visto, la creación de una ley de protección de datos personales adquiere particular relevancia no sólo porque los datos circulan indiscriminadamente sino porque en ocasiones, éstos pueden ser conocidos y utilizados por personas con fines ilícitos, para la comisión de delitos, o simplemente de formas no autorizadas, que eventualmente causan molestia o perjuicios a los titulares y por otra parte, nos enfrentamos a la realidad de que los datos personales son necesarios para una infinidad de operaciones comerciales o de muy diversas índoles en beneficio de sus titulares y, en general, del comercio y la economía nacional; es decir, no es dable pensar que las múltiples relaciones que se plantean entre las personas, incluso entre una jurisdicción y otra, puedan llevarse a cabo sin diversos grados de manifestación y uso de datos personales.

Debido a lo anterior, proponemos que esta ley, deberá ser reglamentaria del segundo párrafo del artículo 16 Constitucional con el fin de atender a la protección de este

derecho y establecer los mecanismos necesarios para que los titulares de los datos puedan ejercer su derecho de acceso, rectificación, cancelación y oposición.

4.2.2 Ámbito de aplicación

Al tratarse de información relativa a la población y que el Estado forma los registros públicos y documentos para llevar su control, y de que a partir de éstos se van creando las diferentes bases de datos personales, deberá ser de observancia federal.

Aunado a lo anterior, es importante recordar los diferentes tratados internacionales suscritos por México que dan pie a la protección de la privacidad y datos personales, por lo que esta ley deberá contemplar las obligaciones signadas por nuestro país, de ahí la importancia de garantizar la protección de datos a nivel federal para que sirva de columna vertebral a las leyes locales que pudieran desprenderse de esta.

4.2.3 Sujetos obligados

A lo largo de esta investigación se ha reconocido que en la actualidad los entes de gobierno son los únicos obligados a proteger los datos personales en su posesión, por lo que además de contemplarlos en esta ley, será de suma importancia incluir a los particulares, los cuales como hemos visto anteriormente, son los que tienen mayor posibilidad de hacerse llegar de información personal debido al constante movimiento que los titulares de datos llegan a realizar por sus diversas actividades, por lo que, proponemos los siguientes sujetos:

1. El Poder Ejecutivo, Legislativo y Judicial
2. La administración publica centralizada
3. Las empresas paraestatales
4. Organismos autónomos
5. Organismos descentralizados

6. Instituciones de crédito
7. Asociaciones religiosas
8. Sindicatos y asociaciones profesionales
9. Partidos políticos
10. Personas físicas y morales de carácter privado que lleven a cabo el tratamiento y procesamiento de datos personales

4.2.4 Regulación de la captura de datos

Es importante incluir un capítulo dedicado a la regulación del procesamiento de los datos personales, ya que este es el objeto toral de la ley, la protección de la información, así como el respeto a los derechos que el titular de los datos tiene con respecto al tratamiento de estos, para lo cual proponemos que deberá contemplarse:

a) Deberá crearse una comisión encargada de vigilar el cumplimiento de la ley, así como también de emitir las opiniones y criterios con respecto a la protección y procesamiento de datos personales.

b) Todos los sujetos obligados deberán registrar las bases de datos en su posesión, ante la comisión encargada, y cada registro deberá contener: el objeto y fin de la base de datos, período de conservación de la información, procedimientos para la actualización, rectificación o cancelación de la información por parte de los titulares de los datos, las medidas de seguridad para proteger la información, nombre del encargado del tratamiento de la información y procedimientos a seguir para el procesamiento de datos.

c) En caso de que el procesamiento de datos de cómo resultado la transmisión de estos a terceros, deberá existir un acuerdo de voluntades en el que se plasmará la obligación de ambas partes de informar al titular de los datos de dicha transmisión, así como también

se deberá indicar a quien serán transmitidos, el objeto de la transmisión y la prohibición de su retransmisión.

d) Para el caso de transmisión internacional de información, esta sólo podrá realizarse a los países que reconozcan el derecho a la privacidad y protección de datos personales y ofrezcan las medidas de seguridad debidas para su transmisión y conservación.

e) Deberá contemplarse todas las bases de datos personales que se encuentren en cualquier soporte: electrónico, documental, de imagen, biométrico, etcétera.

f) En el proceso de recolección, al titular de los datos se le deberá informar el objeto y fin que se persigue con esta, si existe la posibilidad de la transmisión de la información, el derecho de oponerse a su inclusión en la base de datos, salvo que los datos sean disociados, tenga como objeto la seguridad nacional, o el manejo estadístico o histórico de la información.

g) Los datos obtenidos deberán ser verificados para su autenticación y solicitarle al titular, en caso de ser necesario, la actualización de la información.

h) Deberá señalarse al titular de los datos de manera sencilla, cual es el procedimiento a seguir en caso de actualización, corrección o cancelación.

4.2.5 Obligaciones del receptor de datos

Este capítulo describirá las obligaciones que el receptor de datos personales deberá observar hacía el manejo de la información en su posesión, entre los cuales proponemos:

a) Manejarse en apego a la ley.
b) Guardar secrecía en torno al procesamiento de la información, aún y después de terminado el objeto de la base de datos personales.
c) Establecer las medidas de seguridad con el fin de evitar el robo o pérdida de la información.
d) Permitir el acceso al titular de los datos con el fin de corregir, actualizar o cancelar la información.
e) Dar aviso a la comisión reguladora de la fecha de término del procesamiento de información, y en caso de haberse realizado alguna transmisión, a quien fue realizada.
f) En caso de ser necesaria la conservación de la información con fines estadísticos o históricos, disociar la información a modo tal de que no pueda ser relacionada con el titular de los datos.
g) En los casos que tengan que ver con la seguridad nacional, la obligación de transmitir la información a la autoridad solicitante y dar aviso a la comisión reguladora.

4.2.6 Comisión de vigilancia y protección

En las iniciativas de ley que se han presentado ante el Congreso, existen dos opiniones sobre la manera en que deberá vigilarse el cumplimiento de la protección de datos personales, la primera propone que el IFAI sea el regulador de esta protección, para lo cual expresamos en el capítulo anterior esta no sería la mejor alternativa debido a que si se amplían facultades al Instituto, este podría quedar

rebasado, sus facultades podrían resultar contradictorias ya que por un lado vigilaría a los entes de gobierno que otorguen información y por otro lado, también tendría la facultad de vigilar a los particulares para el cumplimiento y protección de datos personales, por lo que el instituto correría el peligro, en el momento de emitir criterios, dejar a alguno de estos derechos mermados en su protección.

La segunda opinión, se inclina por la existencia de un organismo regulador en la protección de este derecho, a nuestro parecer esta es la más viable, ya que este organismo bien podría tener la facultad de emitir opiniones y vigilar tanto a los entes de gobierno como particulares en el cumplimiento de la ley, máxime que como hemos visto, en algunas ocasiones las bases de datos personales pueden llegar a relacionarse entre sí, tomemos como ejemplo el RENAUT, la información es recabada y procesada por particulares y posteriormente transmitida a la Secretaría de Gobernación, por lo que un organismo con las facultades para vigilar a ambos sectores podrá revisar que los datos personales procesados cumplan con la función para lo cual fueron obtenidos.

Por otro lado, este organismo podría contar con la infraestructura necesaria para llevar un registro y control de las bases de datos personales, a modo tal de revisar que el encargado del procesamiento de datos cumpla con los objetivos y procedimientos establecidos para la creación de las bases de datos[228]. Asimismo, al tratarse de medios tan especializados para el manejo de la información, será importante contar con especialistas en diversas ramas tanto tecnológicas como sociales a modo tal de entender de manera amplia el tratamiento de la información.

Debido a lo anterior, para este capítulo de la ley, proponemos:

a) Creación de una comisión autónoma para vigilar el cumplimiento de esta ley.
b) Objeto de la comisión

[228] Este control deberá estar relacionado con el registro de la base de datos descrito en el inciso b), del punto 4.2.4 Regulación de la captura de datos. Pag. 7

c) Estructura, en el que invariablemente deberá contar con especialistas en el área jurídica, tecnologías de la información, documentalistas y archivistas.
d) Organización, compuesta por: un presidente, consejos regionales, registro nacional de bases de datos personales, visitadurías y órgano de control.
e) Facultad para vigilar y realizar visitas de inspección a los encargados del procesamiento de datos.
f) Obligación de emitir opiniones y criterios con respecto a los casos que se presenten ante la comisión.
g) Dar seguimiento a los procedimientos iniciados por los titulares de los datos y los encargados del procesamiento de datos.
h) Girar oficios de conocimientos a las autoridades correspondientes en los casos en que amerite su actuación.

4.2.7 Sanciones

Con el fin de evitar violaciones a lo establecido en esta ley y de homologar las sanciones en esta materia previstas en otras leyes, se deberán preveer las sanciones correspondientes, las cuales deberán ir desde amonestaciones hasta la cancelación de la base de datos dependiendo del daño, las cuales también deberán incluir sanciones económicas y físicas. Para ello, proponemos sanciones por los siguientes conceptos:

a) No registrar la base de datos antes de su inicio de operaciones ante la comisión reguladora.
b) No informar oportunamente al titular de los datos de sus derechos.
c) Negar el acceso, rectificación, cancelación u oposición del titular de los datos.
d) No aplicar medidas de seguridad para la protección de la información.
e) Transmisión de la información a terceros sin el conocimiento del titular de los datos y de la comisión.
f) Pérdida de la información.

g) Negarse a transmitir información solicitada para los casos de seguridad nacional.

Para la aplicación de estas, deberán considerarse si los actos que dieron pie a la sanción fueron ejecutados por:

1. Particulares que tengan en su posesión bases de datos personales.
2. Servidores públicos que tengan entre sus funciones el procesamiento de datos personales.
3. Particulares o servidores públicos que no tengan entre sus funciones el procesamiento de bases de datos personales y hayan violado las medidas de seguridad por hacer mal uso de la información.

Por último, también deberá considerarse la reparación del daño a los titulares de datos, que por estas acciones hayan sufrido menoscabo en su honor, privacidad o patrimonio, para lo cual, lo conveniente sería que un porcentaje de las multas aplicadas tengan como destino al titular de los datos que haya sufrido la violación a sus derechos; por lo que, las violaciones a esta ley, deberan ser clasificadas y cuantificadas de acuerdo al daño causado.

4.2.8 Recursos legales

Para el último capítulo de esta ley, proponemos la creación de un procedimiento de *habeas data*, en el que el titular de los datos tenga la oportunidad de hacer valer sus derechos. Dicho procedimiento no deberá limitar los recursos e instancias a las que el titular pueda acceder en busca de la administración de justicia.

Asimismo, se debe contemplar que para el ejercicio de este derecho, pueden converger otros de tipo civil o penal, para lo cual, será necesario considerar como leyes supletorias o complementarias para la resolución de conflictos, el Código Civil Federal y el Código Penal Federal, por lo que se deberán realizar las respectivas

reformas a estos códigos que integren delitos en contra de la protección de datos, robo de identidad, fraudes electrónicos o faltas como daño al honor, invasión a la vida privada, etcétera; de esta manera, al resolverse el conflicto, el órgano jurisdiccional podrá condenar a quien haya violentado estos derechos y por lo tanto, se podrá imponer la sanción o multa correspondiente, de la cual, un porcentaje deberá ser destinado a la reparación del daño que haya sufrido el titular de los datos, por lo que en estos casos no solo la ley serviría como previsora de violación de derechos si no también, las sanciones impuestas servirán como medidas coercitivas a modo tal de evitar futuras violaciones.

CONCLUSIONES.

Primera. En este trabajo de investigación hemos estudiado diferentes frentes relacionados al derecho a la intimidad y a la protección de datos personales, y lo que implicaría para el Estado garantizar estos derechos tan desconocidos hoy día en nuestro país.

Segunda. Los avances científicos y tecnológicos han revolucionado la vida del hombre a lo largo de la historia, por lo que, hoy día, la vida misma no puede entenderse sin el uso de estas herramientas, debido a ello, el Estado debe crear las normas necesarias para regular su uso, aplicación y límites.

Tercera. La finalidad del Derecho es regular la vida del hombre en sociedad en cualquiera de sus aspectos, lo que da como resultado el adecuado disfrute y protección de los derechos de los gobernados, como también el establecimiento de los límites de éstos con respecto de los de otra persona.

Cuarta. La protección de los derechos humanos, ha evolucionado de la misma forma en que la sociedad lo ha hecho, por ejemplo, en sus inicios durante la Revolución Francesa, se buscó y exigió reconocer la igualdad del hombre y en la actualidad, se exige el respeto a la individualidad de cada persona, o lo que es lo mismo, en las primeras generaciones de los derechos humanos, se hace referencia a este como miembro de la sociedad y a partir de la tercera generación, el reconocimiento del hombre, como ser único e irrepetible.

Quinta. En la actualidad se reconoce que la tecnología ha llegado a marcar una diferencia en el desarrollo de los pueblos, por lo que el acceso a esta es considerado parte de sus derechos.

Sexta. Con las diferentes revoluciones liberales en el siglo XIX, surge la idea de que la difusión de la información es un derecho del hombre y una libertad que debe configurarse como fundamento de los Derechos Humanos.

Séptima. El derecho a la información es entendido como aquel que tiene el ser humano a crear, investigar, acceder y difundir información, por cualquier medio de comunicación, reconocido políticamente como la obligación del Estado de dar a conocer al gobernado todas sus actividades.

Octava. A finales del siglo XIX Warren y Brandeis en su artículo “The Right of Privacy”, señalaron los alcances a la invasión de la privacidad si no se limitaba el acceso a la información confidencial de las personas, cuestionando cosas tan simples como el hecho de fotografiar a alguien en la calle y publicar la fotografía en un periódico, hasta la lectura de una carta y su publicación, por lo que muchos opositores señalan que estas observaciones van en contra del derecho a la información o inclusive la libertad de prensa.

Novena. El desarrollo de las nuevas tecnologías en la adquisición y difusión de la información representan una amenaza a la intimidad y esta debe ser considerada importante para las personas y el bienestar en consecuencia, de la sociedad, debido a que la invasión a la privacidad puede llegar a ocasionar lesiones y daños tan graves que se reflejen tanto de forma física como patrimonial, por lo que la ley debiera alistarse para impedir este tipo de comportamientos de la misma manera que se utiliza para prevenir otros que quizá son más tangibles.

Décima. El derecho a la intimidad debe entenderse como aquella información que el individuo se reserva así mismo, tales como sus pensamientos o sentimientos, y estos a su vez, se encuentran conectados a hechos o personas de su alrededor como la familia, costumbres o conocimientos los que derivan en otros como datos de domicilio, lugar de trabajo o capacidad económica.

Décima primera. El derecho a la intimidad debe ser respetado y protegido, siendo el Estado el obligado a realizar esta tutela y exigir su protección frente a cualquier otra persona, ya sea física o moral, para que el individuo sepa que la sociedad tiene límites de acercamientos hacía su persona y por ende, su vida privada le pertenece y sólo en caso necesario y por medio de su voluntad, esa información pueda darse a conocer.

Décima Segunda. La protección de datos personales concede derechos a los individuos respecto a su información y que es suceptible de tratamiento automatizado, con el fin de evitar que sea vulnerada su libertad y dignidad.

Décima Tercera. Este derecho busca imponer obligaciones a todos aquellos que controlan y tienen acceso a las bases de datos personales como el de permitir el acceso de esta información a los titulares y decidir sobre el manejo que de esta se de, lo cual significa que los sujetos tengan la libertad de elección sobre la revelación y transmisión de la información.

Décima Cuarta. El estudio de la experiencia de otros países al afrontar la evolución de la sociedad y la forma en que esta debe ser organizada, que deriva en la creación de marcos jurídicos afines, es de suma importancia para que en nuestro país se consideren los aspectos debidos para la regulación en el manejo de datos personales; es así como hemos visto que en otros países se buscó proteger a las personas en cuanto al uso de las nuevas tecnologías que pudieran repercutir en daño y como tenemos aspectos protegidos de manera más radical en Europa que en América, quizá todo esto debido a los distintos acontecimientos históricos en ambas partes del mundo.

Décima Quinta. Francia conoció la invasión Alemana y como su gobierno utilizó los datos personales para identificar a judíos, familiares y demás personas relacionadas a ellos con el fin de eliminarlos, y en el presente, al enfrentarse a las nuevas tecnologías reconoció que si bien estas podrían ser un instrumento para facilitar las

actividades cotidianas, también podrían ser usadas no sólo para identificar a las personas, si no también llegar a ser violatoria del derecho a la intimidad de las personas, estos fueron los primeros aspectos que la sociedad francesa se cuestionó cuando en los setenta se comenzó a debatir sobre la protección de datos, dando como resultado en la primera legislación en esta materia y tomada como base para la creación de los lineamientos europeos, en ella se protege la privacidad de la información de las personas y establece parámetros para el uso de las nuevas tecnologías en el procesamiento de la información.

Décima Sexta. La privacidad de las personas y de sus familias, es un derecho que debe ser protegido por parte del Estado, por lo que España ha sido más radical en la reglamentación en el uso de los datos personales, a modo tal, de contemplar aspectos que van desde el nombre, hasta la silueta de las personas en una fotografía.

Décima Séptima. Estados Unidos de América por un lado reconoce que el Estado debe garantizar la protección de los derechos de sus ciudadanos, y por el otro, no le interesa poner barreras en la transmisión de la información, que pudieran repercutir en la actividad mercantil, de ahí que exija que las empresas deban llevar un control de sus clientes y respetar su derecho de inclusión o exclusión en el tratamiento y procesamiento de la información.

Décima Octava. Argentina trató de crear una ley que pudiera cumplir con las exigencias establecidas por la Unión Europea y las Estadounidenses, a modo tal, de brindar protección a los titulares de los datos y crear las medidas de seguridad necesarias en la transmisión de la información.

Décima Novena. En la actualidad la legislación existente en nuestro país solo obliga a los entes de gobierno a establecer criterios y lineamientos de protección de datos personales, por lo que los particulares pueden hacer uso indiscriminado de la información contenida en sus bases de datos personales.

Vigésima. La reforma al artículo 16 Constitucional a nuestro parecer debió realizarse en el artículo 6º, ya que como se estudió a lo largo de este trabajo de investigación, el derecho a la protección de datos esta mas vinculado al derecho a la información que a la garantía de seguridad jurídica establecida en este artículo.

Vigésima Primera. Con la legislación actual, el titular de los datos esta expuesto a que su información pueda ser utilizada con fines distintos a los que dieron origen a su recolección, por lo que no existen límites en la transmisión de la información a otros particulares.

Vigésima Segunda. No existe reconocido dentro de nuestra legislación, el delito de robo de identidad, por lo que es necesario su inclusión, dada la facilidad con la que hoy día puede ser robada la información de los usuarios de las nuevas tecnologías.

Vigésima Tercera. La creación de controles tanto de las polícias del país como de números telefónicos coadyuvarán en la persecución de delitos tales como secuestro o extorsión, pero deberá asegurarse la protección de la información con el fin de evitar su mal uso o transmisión.

Vigésima Cuarta. Actualmente, la legislación permite que los partidos políticos puedan acceder a bases de datos personales, lo que si bien por un lado significa la revisión de información y el asegurarse de evitar fraudes electorales, por otro lado, llega a significar el acceso libre a información confidencial de los electores que puede resultar en el uso inadecuado de la información, por lo que el elector debe tener el derecho de oponerse a que los partidos políticos usen su información personal.

Vigésima Quinta. La necesidad y oportunidad de establecer una regulación específica sobre la protección de datos personales en México está más que justificada desde diversos puntos de vista, entre los que puede destacarse, en primer lugar, la garantía de un derecho de los ciudadanos como es el derecho a la

privacidad y, en segundo lugar, los beneficios que ello reporta tanto al sector privado como al público, en cuanto que esta garantía, en caso de que cumpla con unos determinados requisitos, determina que se facilite la realización de transacciones comerciales y de otro tipo a nivel internacional, buscando así además el reconocimiento de un nivel adecuado de protección de datos por parte de otros países que en su legislación lo exigen, lo que supondría la libre realización de transferencias internacionales de datos con destino a México[229].

Vigésima Sexta. La creación de una ley de protección de datos personales, deberá garantizar por parte del Estado la reparación del daño sufrido por el titular de los datos, cuando otro particular violente sus derechos.

Vigésima Séptima. Una ley de protección de datos personales debe garantizar la capacidad del individuo para comunicarse y participar socialmente sin menoscabo de sus derechos, por lo que su régimen jurídico y previsión deberán ser acordes y determinantes para una mejor función y existencia de una sociedad democrática.

[229] Estudio sobre protección de datos a nivel internacional. – Instituto Federal de Acceso a la Información: México, 2004. p.9

BIBLIOGRAFÍA

- BAZÁN, Victor. El Habeas Data, el derecho a la autodeterminación informativa y la superación del concepto preinformático de la intimidad. UNAM, Instituto de Investigaciones Jurídicas, México, En: Boletín Mexicano de Derecho Comparado, Nueva Serie Año XXXI, número 94, ene.-abr., 1999, pp. 13-76
- BRU CUADRADA, Elisenda. La protección de datos en España y la Unión Europea: Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad. Universitat Oberta de Catalunya, España, 2007, En: IDP. Revista de Internet, Derecho y Política, número 5, pp.78-92
- DE PINA, Rafael y DE PINA VARA, Rafael. Diccionario de Derecho. Porrúa, México, 2003, 525 p.
- Derecho a la Información y Derechos Humanos: Estudios en homenaje al maestro Mario de la Cueva / coords. CARPIZO MCGREGOR, Jorge; CARBONELL, Miguel. UNAM, Instituto de Investigaciones Jurídicas, México, 2000, 522 p.
- Diccionario de Informática. 2ª. Ed., Ediciones Díaz de Santos, México,1993, 758 p.
- FLORES MENDOZA, Imer Benjamín. La concepción del Derecho en las corrientes de la filosofía jurídica. UNAM, Instituto de Investigaciones Jurídicas, México, En: Boletín Mexicano de Derecho Comparado, Nueva Serie, Año XXX, número 90, sept.-dic., 1997, pp.1001-1036.
- GARCÍA-GONZÁLEZ, Aristeo. La protección de datos personales: Derecho fundamental del siglo XXI. Un estudio comparado. UNAM, Instituto de Investigaciones Jurídicas, México, En: Boletín Mexicano de Derecho Comparado, Nueva Serie, Año XL, número 120, sept.-dic., 2007, pp.743-778
- GÓMEZ-ROBLEDO VERDUZCO, Alonso; ORNELAS NÚÑEZ, Lina. Protección de datos personales en México: El caso del Poder Ejecutivo Federal. UNAM, Instituto de Investigaciones Jurídicas, México, 2006, p. 29.
- HOBBES, Thomas. Leviatán. Tomo I, Clásicos Ciencia Política, Número 13, quinta edición, Gernika, México, 2005, 377 p.

- Informe UNESCO 19 c/93, 16 de agosto de 1976.
- Instrucción 1/2006, de la Agencia Española de Protección de Datos sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras.
- KAPLAN, Marcos. Ciencia, Estado y Derecho en las primeras revoluciones industriales. UNAM, Instituto de Investigaciones Jurídicas, México, 2000, 246 p.
- MENDEL, Toby. Consideraciones sobre el estado de las cosas a nivel mundial en materia de acceso a la información. UNAM, Instituto de Investigaciones Jurídicas, México, En: Derecho Comparado de la Información, jul.-dic., 2006, pp. 3-15.
- MICHEL, Víctor Hugo. Cibernautas soslayan las advertencias del peligro. En: Milenio: Diario, año 9, número 3174, 8: sept., 2008, p.39.
- OTÓN SIDOU, J.M. Las nuevas figuras del derecho procesal constitucional brasileño: mandado de injuncao y habeas data. UNAM, Instituto de Investigaciones Jurídicas, México, En: Boletín Mexicano de Derecho Comparado, Nueva Serie Año XXIV, número 70, ene.-abr., 1991, pp.169-187.
- PICHARDO PAGAZA, Ignacio. Modernización administrativa: Propuesta para una reforma inaplazable. El Colegio Mexiquense, UNAM, Facultad de Ciencias Políticas y Sociales, México, 2004, 391 p.
- SALDAÑA, Javier. ¿Derechos morales o derechos naturales?: Un análisis conceptual desde la teoría jurídica de Ronald Dworkin. UNAM, Instituto de Investigaciones Jurídicas, México, En: Boletín Mexicano de Derecho Comparado, Nueva Serie, Año XXX, número 90, sept.-dic., 1997. pp. 1207-1226.
- Sentencia 292/2000 del Tribunal Constitucional Español.
- TÉLLEZ VALDEZ, Julio. Derecho Informático. UNAM, Instituto de Investigaciones Jurídicas, México, 1991, 98 p.
- VELASCO SAN MARTÍN, Cristos. Privacidad y protección de datos personales en Internet ¿Es necesario contar con una regulación específica en

México?. Instituto Nacional de Estadística Geografía e Informática, México, En: Boletín de Política Informática, número 1, 2003, pp.1-12

- VILLANUEVA, Ernesto. Temas selectos de derecho de la información. UNAM, Instituto de Investigaciones Jurídicas, México, 2004, 238 p.
- VILLAR, Rafael; Díaz de León, Alejandro y GIL HUBERT, Johanna. Regulación de Protección de Datos y de Sociedades de Información: Una comparación de países seleccionados de América Latina, los Estados Unidos, Canadá y la Unión Europea. Banco de México, México, 2001, En: Documento de Investigación, número 2001-07, 161 p.

PÁGINAS EN INTERNET.

- ¿Censo o Publicidad?. -- En: El País, 02, octubre, 2002, http://www.elpais.com/articulo/opinion/Censo/publicidad/elpepiopi/20021002elpepiopi_4/Tes : 07/01/2009: 13:20 hrs.
- Agencia Española de Protección de Datos. https://www.agpd.es/
- Diccionario de la Real Academia Española. http://www.rae.es/rae.html: 28/08/2008: 15:05 hrs.
- Dictamen que presenta la Comisión de Administración Pública Local por el que se crea la Ley de Protección de Datos Personales del Distrito Federal. -- http://seguridad2008.politicadigital.com.mx/lectura.html 05/12/2008: 14:28 hrs.
- Dirección Nacional de Protección de Datos Personales de Argentina (http://www.jus.gov.ar/dnpdpnew/ : 09/02/2009: 22:35 hrs.
- GOLIN KRAMMES, Alexandre. Sistemas Jurídicos e Tecnología : Evoluções e influências. http://www.alfa-redi.org/rdi-articulo.shtml?x=9334: 05/06/08: 22:28 hrs.
- GRANERO, Horacio R. El impacto de las nuevas tecnologías en el Derecho. Universidad del Salvador, Instituto de Informática Jurídica, http://www.salvador.edu.ar/ua1-4-hg.htm : 30/07/08 : 14:59 hrs.
- http://caselaw.lp.findlaw.com/data2/circs/dc/071312p.pdf : 05/03/2009:19:49 hrs.
- http://dublincore.org/ : 11/06/08: 22:27 hrs.

- http://es.wikipedia.org :04/09/08: 21:45 hrs.
- http://europa.eu/scadplus/leg/es/lvb/l14012.htm : 12/11/2008: 13:40 hrs.
- http://lared.wordpress.com/2005/12/10/derechos-delitos-y-libertades-en-internet/ : 21/09/2008: 17:37 hrs.
- http://lared.wordpress.com/2005/12/10/derechos-delitos-y-libertades-en-internet/ : 21/09/2008: 17:37 p.m
- http://noticias.juridicas.com/base_datos/Admin/constitucion.t1.html#c2s1 :10/11/08: 11:06 hrs.
- http://noticias.juridicas.com/base_datos/Admin/lo15-1999.t1.html :10/11/2008: 15:19 hrs.
- http://seguridad2008.politicadigital.com.mx/lectura.html :05/12/2008: 14:28 hrs.
- http://www.aaba.org.ar/bi130019.htm; 27/01/08 : 09:47 hrs.
- http://www.alegsa.com.ar/Diccionario/categorias.php : 16/06/08: 20:26 hrs.
- http://www.article19.org/ : 30/07/08 : 22:23 hrs.
- http://www.cnil.fr : 21/09/2008: 21:49 hrs.
- http://www.export.gov/safeharbor/eu/sh_en_docs1.asp : 01/04/2009: 23:30 hrs.
- http://www.lopd-proteccion-datos.com/ley-proteccion-datos.php :02/10/2008: 14:19 hrs.
- http://www.monografias.com/trabajos14/datos/datos.shtml : 09/06/08: 23:53 hrs.
- http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html : 29/08/2008: 11:28 hrs.
- http://www.scjn.gob.mx/NR/rdonlyres/A8070BE8-07B2-45E3-A53C-036F1CD07D46/0/Principales_Criterios_CAI_06_06_2008.pdf : 08/09/2008 :11:10 hrs..
- http://www.txitua.org/index.php/datos-personales/ : 16/09/2008: 21:15 hrs.
- http://www.uasnet.mx/derecho/info3.html : 28/08/08: 09:18 hrs.
- http://www.uasnet.mx/derecho/info3.html 28/08/08: 09:18 hrs.
- http://www.ugr.es/~redce/REDCE7/articulos/16sentenciasupremoamericano.htm#12bis : 19/03/2009: 21:36 hrs.

- http://www.uslaw.ibls.com/uslaw/home.htm :06/03/2009: 22:46 hrs.
- http://www4.law.cornell.edu/uscode/15/ch41schIII.html : 01/04/2009: 23:16 hrs.
- INSTITUTO FEDERAL DE ACCESO A LA INFORMACIÓN PÚBLICA. Marco teórico metodológico. IFAI, México, 2003, 113 p., En: http://www.ifai.org.mx/TemasTransparencia/#publicaciones :30/09/08: 0:45 hrs.
- La CNIL en bref. En: www.cnil.fr : 18/09/2008: 21:06 hrs.
- NAVARRO, Fidela. Derecho a la información y Democracia en México. En: http://www.mexicanadecomunicacion.com.mx/Tables/RMC/rmc87/derecho.html : 01/07/08 : 12:30 hrs.
- NOGUEIRA, Charo. El INE venderá datos del censo electoral si la persona no se opone por escrito. – En: El País, 2, octubre, 2002, http://www.elpais.com/articulo/sociedad/INE/vendera/datos/censo/electoral/persona/opone/escrito/elpepisoc/20021002elpepisoc_2/Tes : 07/01/2009: 13:36 hrs.
- PUENTE DE LA MORA, Ximena. Privacidad de la información personal y su protección legal en Estados Unidos. España: Alfa Redi, Revista de Derecho Informático. Núm. 096, agosto de 2006. En: http://www.alfa-redi.org/rdi-articulo.shtml?x=6956 : 26/03/2009: 20:24 hrs.
- TANÚS, Gustavo Daniel. Protección de datos personales. Principios generales, derechos, deberes y obligaciones. Argentina: Revista Jurídica El Derecho, 19 de julio de 2002. En: http://www.protecciondedatos.com.ar/ 16/01/2009 : 22:01 hrs.
- WARREN, Samuel D. y BRANDEIS, Louis D. The right to privacy. En: Harvard Law Review, Vol. IV, no. 5, December 15, 1890, http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html; 20/08/08: 11:54 hrs.

LEGISLACIÓN.

- Acuerdo por el que se establecen las Reglas de Operación y funcionamiento del Registro Publico de Consumidores. Texto vigente

- Acuerdo por el que se establecen las reglas de operación y funcionamiento del Registro Público de Consumidores. Texto vigente
- Constitución Política de los Estados Unidos Mexicanos. Texto vigente
- Instrucción 1/2006, de la Agencia Española de Protección de Datos sobre el Tratamiento de Datos Personales con fines de vigilancia a través de Sistemas de Cámaras o Videocámaras.
- Ley 25.326. Protección de los Datos Personales. Texto vigente.
- Ley de Protección y defensa de los usuarios de servicios financieros. Texto vigente
- Ley de Transparencia y Acceso a la Información del Distrito Federal. Texto vigente
- Ley Federal de Transparencia y Acceso a la Información. Texto vigente
- Ley n°78-17 del 6 de enero de 1978, “Ley de Informática, ficheros y libertades”. Texto vigente
- Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal. Texto vigente.
- Lineamientos de Protección de Datos Personales del Instituto Federal de Acceso a la Información Pública. Texto vigente.
- Semanario Judicial de la Federación.

ANEXO 1

De las Comisiones Unidas de Puntos Constitucionales; y de Estudios Legislativos, el que contiene proyecto de decreto que adiciona un párrafo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos[230].

INTERVINO EL SEN. RICARDO GARCÍA CERVANTES, POR LAS COMISIONES, PARA FUNDAMENTAR EL DICTAMEN FUE APROBADO POR 97 VOTOS; 1 ABSTENCIÓN. SE TURNÓ A LA CÁMARA DE DIPUTADOS.

Dictamen de las Comisiones Unidas de Puntos Constitucionales y de Estudios Legislativos que contiene Proyecto de Decreto que adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

HONORABLE ASAMBLEA

A las comisiones que suscriben, les fue turnada para su estudio y elaboración del dictamen correspondiente la Iniciativa con Proyecto de Decreto que adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

De conformidad con el artículo 72 de la Constitución Política de los Estados Unidos Mexicanos, y con los artículos 85, 86 y 94 de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos, así como en los artículos 56, 60, 87 y 88 del Reglamento para el Gobierno Interior del Congreso General de los Estados Unidos Mexicanos, se somete a consideración de esta Honorable Cámara de Senadores el presente dictamen al tenor de los siguientes:

I. ANTECEDENTES

En sesión ordinaria celebrada por la Cámara de Senadores el día 25 de noviembre de 2008, los Senadores Santiago Creel Miranda y Alejandro González Alcocer integrantes del Grupo Parlamentario del PAN; Pablo Gómez Álvarez integrante del Grupo Parlamentario del PRD y Pedro Joaquín Coldwell integrante del Grupo Parlamentario del PRI, presentaron la Iniciativa con Proyecto de Decreto que adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos.

En la misma fecha, la Mesa Directiva acordó turnar esta iniciativa a las Comisiones Unidas de Puntos Constitucionales y de Estudios Legislativos para su estudio, análisis y elaboración del dictamen correspondiente.

[230] Discutida ante la Cámara de Senadores el 4 de diciembre de 2008.

II. MATERIA DE LA INICIATIVA

La Iniciativa con Proyecto de Decreto, materia del presente dictamen, tiene por objeto desarrollar en el máximo nivel de nuestra normatividad el derecho a la protección de datos personales.

Esta reforma establece una nueva garantía constitucional: la protección de los datos personales y los correlativos derechos al acceso, rectificación, cancelación u oposición en torno al manejo de los mismos por parte de cualquier entidad o persona, pública o privada, que tenga acceso o disponga de los datos personales de los individuos. Con ello se asegura el derecho a la protección de datos personales a nivel nacional, extendiendo su aplicación a todos los niveles y sectores en dos ámbitos fundamentales:

Los datos personales en posesión de los entes públicos.

Los datos personales en poder del sector privado.

Asimismo, la iniciativa propone establecer los supuestos de excepción a esta nueva garantía, mismos que deberán precisarse en la ley, bajo criterios y razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros.

Lo anterior se propone adicionando un párrafo segundo al artículo 16 constitucional en los siguientes términos:

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

III. CONSIDERACIONES

Desde 1917, nuestra Carta Magna estableció en las garantías individuales, los derechos relativos a la libertad individual, de entre los que destacan la inviolabilidad de correspondencia y domicilio, y más adelante, el secreto a las comunicaciones privadas. Derechos vinculados con la intimidad y privacía de la persona, porque protegen ciertas áreas o espacios relativos a todo ser humano. Sin embargo, hoy, con el reconocimiento de un catálogo abierto de derechos y con el creciente avance tecnológico, ha sido necesario dar respuesta a las nuevas pretensiones individuales, consecuencia de los cambios sociales que la globalización y los avances tecnológicos han ido introduciendo, dando lugar a lo que ya se conoce como la "sociedad de la información, por lo que México no debe mostrarse ajeno a ello.

Como en el caso de otros derechos humanos, en nuestro país el derecho a la protección de datos personales ha pasado por diversas fases.

El primer paso se dio con la aprobación de la Ley Federal de Transparencia y Acceso a la Información Pública en 2002, al establecer en la fracción II de su artículo 3, lo siguiente:

"*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*";

El segundo paso concluyó el 20 de julio de 2007 con la publicación en el Diario Oficial de la Federación de la reforma al artículo 6º constitucional, en el que por primera ocasión se hace referencia expresa al derecho a la protección de datos en la Constitución Política, como un derecho distinto al derecho de acceso a la información pública; protección limitada a la información en poder delas autoridades, entidades, órganos y organismos de los tres órdenes de gobierno.

Un tercer paso, fue la aprobación de la Minuta con Proyecto de Decreto por el que se adicionan un segundo y tercer párrafos, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política.

Sobre el particular, cabe señalar el origen de la misma:

El 5 de abril de 2006, el entonces Senador Antonio García Torres (PRI) presentó iniciativa de adición al artículo 16 constitucional, la cual fue dictaminada y aprobada en el Senado el 18 de abril del mismo año.

El 19 de abril de 2006 la minuta fue recibida en la Cámara de Diputados y el dictamen respectivo fue aprobado por el Pleno el 20 de septiembre de 2007, mismo que presentó dos modificaciones, por lo que fue devuelta al Senado de la República.

El 25 de septiembre de 2007 la minuta fue turnada a las comisiones respectivas en la Cámara de Senadores.

TEXTO MINUTA **SENADO DE LA REPÚBLICA** **(CÁMARA DE ORIGEN)** **19 abril 2006**	**TEXTO MINUTA** **CÁMARA DE DIPUTADOS** **20 septiembre 2007**
Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. Toda persona tiene derecho a la protección de sus datos personales, así como al derecho de acceder a los mismos y, en su caso, obtener su rectificación, cancelación o destrucción en los términos que fijen las leyes. La ley puede establecer supuestos de excepción a los principios que rigen el tratamiento de datos, por razones de seguridad nacional, de orden público, seguridad, salud o para proteger los derechos de tercero. No podrá librarse (...)	**Artículo 16.** Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal de procedimiento. **Toda persona tiene derecho a la protección de sus datos personales, así como al derecho de acceder a los mismos, y en su caso, obtener su rectificación, cancelación y manifestar su oposición en los términos que fijen las leyes.** **La Ley puede establecer supuestos de excepción a los principios que rigen el tratamiento de datos, por razones de seguridad nacional, de orden, seguridad y salud públicos o para proteger los derechos de tercero.** No podrá librarse (...)

Sobre el particular, es importante señalar que en reunión de trabajo de la Comisión de Puntos Constitucionales del Senado de la República, al analizar la minuta en comento, en términos generales se estuvo de acuerdo con las modificaciones propuestas por la Colegisladora, mismas que se circunscriben a dos cuestiones:

En el primer párrafo, se suprimen las palabras "o destrucción" y se agrega la expresión "y manifestar su oposición".

En el segundo párrafo, se cambió la posición del término "público" con el fin de calificar no sólo a la palabra "orden", sino también a las voces "seguridad" y "salud".

No obstante lo anterior, en una lectura y análisis detallado de la nueva disposición constitucional contenida en la minuta analizada, se encontró que existían algunos problemas de redacción y sintaxis que podrían ser superados con una nueva redacción de la reforma propuesta, que inclusive podría expresarse de manera más clara y sencilla en un solo párrafo. Por lo anterior, y toda vez que el artículo 72 constitucional inciso e) limita la capacidad de revisión por parte de la Cámara de Origen a una diversa modificación o reforma realizada por la Cámara Revisora a la minuta originalmente enviada, en aras de lograr la mejor expresión respecto de este

nuevo derecho de toda persona a proteger sus datos personales, es que fue presentada la iniciativa analizada en el presente dictamen, a fin de que, de ser aprobada tanto por la Cámara de Origen como por la Revisora, resolver en su oportunidad el trámite procedente a la minuta devuelta por la Cámara de Diputados.

Lo anterior, no sin antes considerar que la aprobación del presente dictamen con proyecto decreto sería el paso definitivo para alcanzar la consolidación de este derecho. Es importante mencionar que los autores de la iniciativa en estudio coinciden en lo esencial con el texto modificado por la Colegisladora al reconocer la necesidad que existe de incluir entre los derechos fundamentales previstos en la Carta Magna, el de la protección de datos personales, a efecto de dotar al gobernado de un poder de disposición y control sobre los datos personales que le conciernan.

Por lo que esta iniciativa se basa en la propuesta de la minuta en comento, sin embargo, como consecuencia de una revisión constitucional, sistémica, lingüística y de técnica legislativa, y con el ánimo de enriquecer la reforma que ahora se dictamina, es que se propone con otra redacción, misma que se considera más concisa y ordenada. La cual, respeta el espíritu de la reforma contenida en la minuta.

La nueva redacción de la iniciativa en estudio incluye de un modo explícito y preciso el derecho que toda persona tiene a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley. Asimismo, contempla que dicha legislación establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, los cuales, como ya se ha mencionado, serán por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas, o para proteger los derechos de terceros.

Una vez hechas las precisiones anteriores, cabe señalar que le objetivo de la iniciativa en estudio es consolidar el derecho de protección a la persona en relación con el uso que se dé a su información personal, tanto por entes públicos como privados, es decir, desarrollando su ámbito de aplicación a todos los niveles y sectores.

Es importante considerar que si bien es cierto que las disposiciones establecidas en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y la reforma al artículo 6º constitucional publicada el 20 de julio de 2006, en torno al derecho a la protección de datos personales, han servido como referente para impulsar la reforma que hoy se analiza, también lo es que sigue presente la necesidad de dotar de contenido a este derecho en cuanto a los principios que deben regir todo tratamiento de datos personales, los derechos de que gozan los titulares de los datos, así como las excepciones a los principios en la materia.

En cuanto a la primera parte del párrafo que se propone adicionar, que a la letra dice:

"*Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, ...*"

Esta propuesta se estima procedente, toda vez que se reconocen y quedan protegidos los derechos de acceso, rectificación, cancelación y oposición, conocidos por su acrónimo como derechos **ARCO**, reconocidos en la Directiva Europea 95/46 CE del 24 de octubre de1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de sus datos y a la libre circulación de estos datos.

Con esta reforma quedarían establecidos derechos internacionalmente reconocidos con los que debe contar el gobernado para verdaderamente dotarlo de un poder de disposición sobre sus datos personales.

Es importante considerar que los derechos fundamentales han pasado por varias generaciones, una primera, en la cual se reconocen los derechos individuales, clasificados en civiles y políticos; una segunda, en la cual se reconocen los derechos económicos, sociales y culturales, y una tercera, en la cual se reconocen derechos para incentivar el progreso social y elevar los niveles de vida de la población y atienden a los nuevos fenómenos de la vida social, entre ellos, los avances de las ciencias y la tecnología y el libre desarrollo de la personalidad.

En la primera generación, la de los derechos civiles y políticos, se reconocen, entre otros, el derecho fundamental a la intimidad, a la privacidad, a la libertad, a no ser molestado en la vida privada, personal y familiar.

En este derecho fundamental no se engloba al derecho a la protección de los datos personales, ya que éste descansa más bien en una idea de autonomía de la persona, en el derecho al control sobre los datos que nos conciernen, a que nadie los conozca, los recoja, los trate, informatizadamente o no, a que no se cedan a terceros sin consentimiento propio, libre e informado y a que nuestros datos, en todo caso, correspondan a nuestra realidad, conforme a los principios jurídicos de la materia.

Por lo que resulta necesario reconocer un derecho a la protección de los datos personales y que este reconocimiento se incorpore en el texto constitucional, pues de esta manera se generaría una certeza indiscutible del derecho, le brindaría seguridad y estabilidad.

El derecho fundamental de la protección de datos personales comprende otros derechos que corresponden a los gobernados, como acceder a los mismos y, en su caso, obtener su rectificación, cancelación u oposición en los términos que fijen las leyes.

El derecho de oposición, que tiene sus antecedentes en el derecho francés[231], fue incorporado en la citada Directiva Europea con el objeto de facultar a los ciudadanos a manifestar su conformidad en torno al tratamiento de datos que han sido obtenidos de fuentes accesibles al público para fines de publicidad.

Otra de las razones que justifica la existencia del derecho de oposición es su posible utilización para impugnar los efectos jurídicos de las denominadas "decisiones individuales automatizadas"[232]. En esa tesitura, el derecho de oposición se emplea como una herramienta para combatir determinaciones basadas únicamente en un tratamiento automatizado de datos destinado a evaluar ciertos aspectos relativos a la personalidad, como el rendimiento laboral, fiabilidad, conducta, entre otros.

El derecho de oposición permitirá a los particulares ejercer de manera más amplia y efectiva su derecho a disponer de los datos personales que le conciernen.

Por otra parte, cabe destacar que con mecanismos como el que se propone no se interfiere con la dinámica del comercio, al permitir la posibilidad de que el consentimiento sea otorgado de manera tácita, hasta en tanto no haya manifestación de voluntad en contrario y conforme a los esquemas que al efecto se establezcan en su momento por el legislador ordinario.

Respecto a la segunda parte del párrafo que se adiciona con la propuesta de la iniciativa en estudio, que establece:

"....*la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros."*

Estas comisiones unidas la consideran adecuada, ya que la protección de datos personales puede estar sujeta a excepciones bajo ciertos supuestos y condiciones, esto es sólo en los casos en los que por su trascendencia este derecho se encuentre en contraposición con otros derechos y amerite una ponderación de la autoridad teniendo presente el bien común, como es el caso de la seguridad nacional, disposiciones de orden público**,** seguridad y salud públicas o para proteger los derechos de tercero. Puesto que la categoría de un derecho fundamental no puede ser un derecho superior a cualesquier otro o bien a intereses sociales o públicos.

En ese tenor, se estima admisible que los derechos relativos a los datos personales puedan estar sujetos a excepciones bajo ciertos supuestos y condiciones:

Seguridad nacional.- toda vez que es indispensable mantener la integridad, estabilidad y permanencia del Estado mexicano.

---

[231] ARENAS RAMIRO, Mónica. *El derecho fundamental a la protección de datos personales en Europa*, Valencia, Tirant lo Blanch, p.499

[232] Artículo 15 de la Directiva 95/46 CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de sus datos y a la libre circulación de estos

Disposiciones de orden público.- ya que el orden público tiene un sentido de equidad que rebasa los intereses particulares, privados, individuales, porque en realidad el orden público representa el núcleo íntegro de la sociedad[233].

Seguridad pública.-por ser una función a cargo de la Federación, las entidades federativas y los municipios, que comprende la prevención, investigación y persecución de los delitos, así como la sanción de las infracciones administrativas.

Salud pública.- en virtud de que ésta también es responsabilidad del Estado, a quien corresponde controlar o erradicar enfermedades, así como prevenir los riesgos que afectan a la salud del conjunto de la población y promocionar hábitos de vida saludables.

Con lo anterior, se establece con toda claridad que el derecho a la protección de datos personales, como todo derecho, encuentra límites frente a otros intereses jurídicos.

Conviene recordar que al adquirir el derecho a la protección de datos personales el carácter de un derecho fundamental, resulta indispensable que las excepciones a la aplicación de los principios que rigen la materia sean establecidas al mismo nivel jerárquico, es decir, en la Ley Fundamental, a efecto de que en virtud del principio de supremacía constitucional, previsto en el artículo 133 de la Carta Magna, se asegure desde el máximo nivel normativo cuáles son los límites a los que se pueden someter los citados principios, así como los parámetros en función de los que deberá desarrollarse cualquier instrumento normativo. En el caso que nos ocupa queda claro además que existe una reserva de ley en la materia, es decir, que el desarrollo de los supuestos de excepción establecidos en la Constitución deberán ser desarrollados únicamente en instrumentos de rango legislativo.

Asimismo, estas comisiones dictaminadoras estiman importante hacer referencia a que en la actualidad el derecho a la privacidad, y el de los datos personales, están seriamente amenazado por la que se ha querido llamar "sociedad de la información", que es un paradigma que está produciendo grandes cambios en el mundo en este siglo, cambios impulsados principalmente por los nuevos medios disponibles para crear y divulgar información a través de tecnologías digitales.

El empleo de nuevas tecnologías y el desarrollo de la informática permiten acumular una cantidad enorme de información que es ordenada y clasificada automáticamente y que puede ser almacenada en espacios muy reducidos. La información puede ser recogida en cualquier lugar del mundo y quedar almacenada y clasificada de

[233] Ponencia presentada en el Congreso Internacional de Derecho de Familia, en el Instituto de Investigaciones Jurídicas de la UNAM (IIJ-UNAM), "El orden público en el Derecho Familiar Mexicano", Güitrón Fuentecilla Julián, 22, 23 y 24 de noviembre de 2005. www.juridicas.unam.mx/sisjur/familia/pdf/15-147s.pdf

inmediato mediante conexiones telefónicas o a través de Internet y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos.

Por ello, ante este creciente avance tecnológico ha sido necesario dar respuesta a los nuevos retos que debe enfrentar la libertad de las personas como consecuencia de los cambios que la tecnología ha ido introduciendo. México debe así adecuar su marco constitucional para otorgar a toda persona una protección adecuada contra el posible mal uso de su información.

Por las razones anteriormente expuestas, se considera procedente incorporar en el texto constitucional la propuesta de la iniciativa en estudio, por lo que las comisiones dictaminadoras sometemos a la consideración de esta Soberanía el siguiente

PROYECTO DE DECRETO QUE ADICIONA UN PÁRRAFO AL ARTÍCULO 16 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS

Artículo Único: Se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:

"Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento.

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

No podrá librarse orden de aprehensión sino por la autoridad judicial y sin que preceda denuncia o querella de un hecho que la ley señale como delito, sancionado con pena privativa de libertad y obren datos que establezcan que se ha cometido ese hecho y que exista la probabilidad de que el indiciado lo cometió o participó en su comisión.

(...)
(...)
(...)"

ARTÍCULO TRANSITORIO

Artículo único. El presente decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.
Salón de Sesiones de la Cámara de Senadores del Honorable Congreso de la Unión de los Estados Unidos Mexicanos, a los veintisiete días del mes de noviembre de dos mil ocho.

COMISIÓN DE PUNTOS CONSTITUCIONALES COMISIÓN DE ESTUDIOS