UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

"ANÁLISIS JURÍDICO AL ARTÍCULO 63 DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES, EN CUANTO A LA RESPONSABILIDAD DEL 'ENCARGADO'".

T E S I S

PARA OBTER EL TITULO DE:

LICENCIADO EN DERECHO

P R E S E N T A :

CINTHIA LUCERO TELLEZ VALLEJO

ASESOR: LIC. MARTIN LOPEZ VEGA.

NEZAHUALCOYOTL, ESTADO DE MEXICO **2014**

FES Aragón

AGRADECIMIENTOS Y DEDICATORIAS

Agradezco a mis padres que a pesar de todas las adversidades que se han presentado han estado presentes en cada caída y me han tendido la mano para seguir cada día adelante con sus consejos y sus buenos ejemplos.

Agradezco a mi hija Avril Dayana Simón Téllez por ser el motor y energía cada día para seguir adelante inspirándome a ser mejor persona cada día y ser su mayor orgullo.

Agradezco a mi hermano Roberto Téllez Vallejo que me ha ayudado directa e indirectamente con su ejemplo cada día de mi vida para lograr lo que soy hasta este momento.

Agradezco a mi mejor amigo y compañero Gabriel Simón Santos, por haberme dado una hija y ayudarme en todo momento en cada locura, por escucharme y entenderme en mis locuras más grandes.

A mi prima Belén Romero y mi tía Guadalupe Vallejo por estar ahí cuando más las necesito, me escuchan y aconsejan.

Agradezco a mi jefe Arq. Manuel Zarate Sánchez por haberme dado la oportunidad de laborar junto a él desde hace 6 años y a otras personas dentro de la "Asociación Promourb A.C". Que me ha dado tantas enseñanzas y consejos y que gracias a ellos he podido concluir exitosamente mi carrera y lograr un desempeño profesional.

a su vez a mis amigas Blanca Karina, Ariana Chávez, Zulema Jiménez, y a ese grupo de amigas que dentro de la universidad conocí, y que me ayudaron a seguir continuando mis estudios y me inspiraron y ayudaron para terminar el presente trabajo.

Y a todas aquellas personas que estuvieron apoyándome e incitando a seguir adelante cada día y ser mejor.

A nuestra universidad nacional autónoma de México, a la facultad de estudios superiores “Aragón”, por creer en nosotros por darnos un lugar dentro de ella, así como a los profesores que dentro de mi formación aportaron un granito de arena para ser lo que soy ahora.

Dedico esta tesis a mi familia en general en especial a mis padres, hija, hermano y a dios, aunque yo sé que es un logro mío pero sé que es una satisfacción para ustedes por que con esto concluyo su responsabilidad y no habrá más palabras de agradecimiento que exprese, lo que me hacen sentir.

Los perdedores evitan el fracaso, y el fracaso convierte a los perdedores en ganadores. Kiyosaki de su libro "Padre Rico Padre Pobre"

INDICE

INTRODUCCIÓN ---------- I

CAPÍTULO I

ANTECEDENTES DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES.

1.1.- Antecedentes generales de la Ley Federal de Protección de Datos Personales. ---------- 1

1.2.- Antecedentes en México. ---------- 6

1.3.- El Instituto Federal de Acceso a la Información Pública y Protección de Datos. ---------- 9

1.4.- Las Reformas Constitucionales en materia de datos personales. ---------- 14

CAPÍTULO II

BASES DE DATOS, DATOS PERSONALES Y DERECHOS ARCO

2.1.- Los ficheros y bases de datos. ---------- 23

2.2.- Las bases de datos cibernéticas. ---------- 29

2.2.1.- Base de datos en la nube. ---------- 31

2.3.- Datos personales. ---------- 41

2.3.1.- Clasificación de los datos personales. ---------- 45

2.3.2.- Datos personales sensibles. ---------- 49

2.4.- Derechos ARCO. ---------- 52

2.4.1.- Derecho de Acceso. ---------- 52

2.4.2.- Derecho de Rectificación. ---------- 52

2.4.3.- Derecho de Cancelación. ---------- 53

2.4.4.- Derecho de Oposición. ---------- 53

2.5 Principios de los datos personales. ---------- 56

2.6.- De la seguridad de los datos personales. ---------- 58

CAPÍTULO III

CONTENIDO DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES.

3.1.- Aviso de Privacidad. ---------- 60
3.2.- Sujetos contemplados en la LFPDPPP. ---------- 69
3.2.1.- "Titular". ---------- 69
3.2.2.- "Responsable". ---------- 69
3.2.3.- "Encargado" ---------- 70
3.2.4.- "Tercero". ---------- 70
3.3.- Las obligaciones del "Responsable" en torno al Aviso de Privacidad. ---------- 70
3.4.- Las obligaciones del "Encargado" según el Aviso de Privacidad. ---------- 72
3.5.- Relación jurídica entre el "Responsable" y el "Encargado". ---------- 73
3.6.- Contrato de Protección de Datos Personales en Posesión de Particulares. ---------- 74
3.7.- Responsabilidad solidaria entre el "Responsable" y el "Encargado". ---------- 91
3.8.- Sanciones establecidas en la ley para el "Responsable" y el "Encargado". ---------- 96

CAPÍTULO IV

PROPUESTA DE REFORMA A LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES EN CUANTO A LAS SANCIONES.

4.1.- Problemática ante la falta de sanción para el "Encargado". ---------- 99
4.2.- Propuesta de reformas al marco jurídico. ---------- 107

4.3.- Responsabilidad solidaria entre el "Responsable" y el "Encargado" en cuanto a las sanciones. ---------- 110
4.4.- Reforma al artículo 63 de la LFPDPPP. ---------- 112
CONCLUSIONES. ---------- 117
FUENTES CONSULTADAS. ---------- 121

INTRODUCCION

Es un hecho indiscutible que en el mundo de la tecnología, especialmente la informática, ha avanzado vertiginosamente y de manera asombrosa, y que este avance ha impactado de manera importante en el campo de la comunicación y de la información, al permitir el intercambio en línea de la información, eliminando las barreras que los medios físicos (papel) provocaban, haciéndola tardada o engorrosa, y a su vez convirtiéndola a veces en un riesgo para la privacidad de las personas. También se ha hecho evidente que tal desarrollo, desde luego, ha tenido una influencia determinante en el intercambio, comercial, educativo y cultural, así como en otras actividades en las cuales también se proporcionan datos personales; asimismo, se ha advertido que varios países, a fin de evitar un impacto nocivo que pueda generar el avance tecnológico en cuanto a dichos datos, se han visto en la necesidad de legislar o emitir leyes que los protejan.

Con dicho fenómeno y sus posibles impactos, no ha escapado nuestro país, por ello es que se vio en la necesidad de legislar en lo referente a la protección de los datos en personales. En México el derecho a la protección de datos personales soló era reconocido expresamente por la Ley Federal de Transparencia y Acceso a la Administración Pública Gubernamental (sector público).y dentro de la Ley de Protección de Datos Personales del Estado de Colima (sector público y privado); adicionalmente, existían disposiciones sectoriales dentro de la Ley Federal de Protección al Consumidor, Código Penal Federal y Ley General de Salud, entre otras, que reconocían algunos derechos de los titulares de los datos y establecían determinados mecanismos para su protección ; sin embargo ya se señalaba la necesidad de que la materia de protección de datos personales se regulara a nivel Federal.

Por ello, debido el panorama normativo y a que México requería cumplir con sus compromisos internacionales, se consideró necesario expedir una ley en la materia. Debiendo mencionar que se presentaron en el Congreso de la Unión,

diversas iniciativas de ley. Con la finalidad de lograr una regulación a nivel federal con respecto a la recolección, al tratamiento[1] y transmisión de información personal; y fueron reformados el artículo 6°, así como 16 Constitucionales, estableciéndose en este último que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos y a manifestar su oposición, así como a la vez se reformó el artículo 73 Constitucional, agregándose una fracción, en la cual se otorgó facultades al Congreso de la Unión para legislar en materia de datos personales. Y en cumplimiento a tales reformas, este órgano legislativo emitió la Ley Federal de Protección de Datos Personales en Posesión de Particulares, publicada en el Diario Oficial de la Federación (D.O.F.), el 5 de julio de 2010.

Es importante mencionar, que la ley de protección de datos personales en posesión de particulares, tiene como objetivo principal proteger la dignidad y seguridad de la persona, no sólo en sus derechos patrimoniales sino también la moralidad del titular de derechos y obligaciones. Ahora bien, para entender y tener un mayor conocimiento de lo que es esta ley, se realiza en el presente trabajo un análisis general de la misma, así como de su reglamento.

Uno de los motivos de la presente tesis, es el de lograr que la ley que nos ocupa sea conocida y tenga la suficiente trascendencia e importancia para que se realice una verdadera protección de datos y, a su vez, que el titular que somos cada uno de nosotros, tengamos seguridad jurídica a la hora de proporcionar nuestra información personal, y desde luego, una cultura de protección, no sólo a aquellas personas tratantes de los datos en cuestión sino el público en general.

Cabe mencionar que hay personas tanto físicas como morales particulares, que recaban información personal, y que son incapaces de definir que es un dato personal, para que sirve, sus principales derechos y la seguridad adecuada que

[1] Artículo 3o. Para los efectos de esta Ley, se entenderá por... XVIII. Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

se debe de tener no sólo con la información principal sino también con aquella que se considera sensible, la cual en caso de ser divulgada puede traer como resultado la discriminación e incluso se puede llegar a un delito tal como se ha sabido a lo largo de la historia por los principales medios de comunicación.

Un punto importante que se trata en este trabajo, lo constituye la propuesta de que entre el responsable y el encargado del tratamiento de los datos del titular, se efectúe o celebre un contrato de los llamados innominados, para que éste último cuente con una efectiva protección de su información personal, en virtud de que si bien es cierto que en la ley se habla de la elaboración de un documento jurídico entre dichas partes tratantes de datos, también lo es que la misma no especifica a qué clase de documento se refiere en especial.

Basándose en tal disposición cuando se elabora un documento entre el responsable y el encargado de los datos en cuestión, la relación que se da entre ambos, solo se considera de carácter laboral, y en caso de una falta del segundo, al incurrir en mal manejo de los datos del titular, eventualmente podría darse para éste un despido, por no cumplir con los requerimientos y discreción del puesto, que le fue asignado, siendo ésta la única consecuencia que puede sufrir, en virtud de que en la ley no contempla una sanción para el encargado, en el caso de que incurra en alguna conducta que afecte el tratamiento de datos del titular, es decir, cometa una autodeterminación informativa, que lo podemos definir como “conjunto de normas jurídicas destinadas a asegurar a las personas el respeto de sus derechos, especialmente del derecho a la vida privada e intimidad ante el tratamiento automatizado de derechos personales[2]”; debiendo hacer hincapié, en que el encargado es aquella o aquellas personas que por lo general exclusivamente su función es la del manejo y distribución de la información.

[2] NOGUEIRA, Humberto, “Autodeterminación informativa y hábeas data en Chile e información comparativa”, Anuario de Derecho Constitucional Latino- americano, México, 2005, p. 449.

El responsable es aquella persona física o moral de carácter privado, que sólo desempeña funciones meramente administrativas, y que por lo general no tiene un contacto directo con la información de los titulares, aunque según la ley en cuestión, estos tienen el poder de decisión sobre esta información, en la práctica no se desempeña este punto y se le delega la función al encargado, y en caso de una falta o mal manejo de los datos personales por parte de éste, queda en un estado de indefensión el titular por los motivos que se han explicado anteriormente.

También se efectúa en este trabajo una valoración de las obligaciones y sanciones establecidas en dicho ordenamiento (LFDPPPP), para el responsable de datos personales, y con base en tal valoración, se propone que tanto las obligaciones como las sanciones también se deben establecer para el encargado o tratante de los datos en cuestión, por ser éste quien realmente se encarga de su tratamiento.

Por todo ello se realiza un análisis jurídico a la Ley Federal De Protección De Datos Personales en Posesión De Particulares, en cumplimiento a lo dispuesto en su artículo 14, el cual se refiere a la responsabilidad que tiene el nombrado responsable, en cuanto a salvaguardar los datos del titular y procurar el cumplimiento del aviso de privacidad.

Asimismo, se propone en esta tesis adicionar una fracción al artículo 64 de la ley mencionada, de acuerdo a la sanciones que tiene el responsable, ya que no solo él puede caer en el supuesto de la divulgación desmedida de la información, sino se pide la misma sanción en caso de divulgación o transferencia base de datos de forma total o parcial para el encargado, en virtud de que en el mencionado artículo sólo establece sanciones para el responsable, y entra en contradicción de acuerdo con el artículo 58 de ley citada, que nos remite que si el titular podrá ejercer los derechos que estimen pertinentes para su indemnización, dejando poca claridad en lo que pretende decir la ley, si

tendrá algún castigo en caso de violar la ley o si tiene alguna responsabilidad pecuniaria para la indemnización del titular..

Cabe mencionar que en la actualidad según datos registrados en la revista ***b: Secure***, las bases de datos en el mercado negro de la información, pueden variar sus costos que oscilan entre $500.00 y $50,000.00, por un CD ROM con aproximadamente 300,000 datos personales, por ello se considera si el encargado tendrá alguna responsabilidad, ya que sería fácil la divulgación de la información a una cantidad enorme de terceros, si el tratante incurriera en ese supuesto, sin tener consecuencia alguna, o sólo la pérdida de su empleo.

CAPÍTULO I

ANTECEDENTES DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES.

1.1.- Antecedentes generales de la Ley Federal de Protección de Datos.

Aunque para muchas personas, cuando menos en México, la protección de datos personales supone ser un nuevo tema, más no lo es, en otros países como los de la Unión Europea, o Estados Unidos, en donde se desarrolló y llevó a la práctica. Podemos decir, que la evolución de este derecho se debió al gran desarrollo de las tecnologías de la información y comunicación (TICs)[3], que permitieron el intercambio online[4] (en línea) de información, eliminando las barreras que los medios físicos (papel) provocaban, al hacerla tardada y engorrosa, con un riesgo para la privacidad de las personas.

Partiendo de estudios que se han realizado, se podría afirmar que el tema de la protección de datos personales nació a raíz de una jurisprudencia dictada por el Tribunal Constitucional Federal Alemán, precisamente en la sentencia sobre la Ley del Censo. Y que partir de dicha jurisprudencia y otras que le seguirían, organismos de cooperación internacional comenzaron a regular la protección de este derecho; desde luego con el fin y por la urgente necesidad de contener los efectos nocivos de estas nuevas tecnologías (TICs) sobre los derechos fundamentales de las personas.

Con base en investigaciones realizadas, tenemos que en el campo del derecho, y con la finalidad de brindar protección a los datos personales, han surgido nuevas garantías procesales, entre las cuales se puede mencionar el Habeas

---

[3] Son tecnologías de la información y de comunicaciones, constan de equipos de programas informáticos y medios de comunicación para reunir, almacenar, procesar, transmitir y presentar información en cualquier formato es decir voz, datos, textos e imágenes. http://educatics.blogspot.mx/ 03 marzo 2013, 22:06.

[4] Un aparato asociado a un sistema está en línea si se encuentra bajo control directo del mismo, esto es, si se encuentra disponible para su uso inmediato por parte del sistema, sin intervención humana, pero que no puede operar de modo independiente del sistema.

Data[5], así como otros recursos. Citando algunas normatividades internacionales que también protegen este tipo de datos, a continuación se señalan las siguientes:

- 1980- Directrices Relativas a la Protección de la intimidad y de la Circulación Transfronteriza de Datos Personales de la Organización para la Cooperación y el Desarrollo Económico (OCDE).

- 1981- Convenio Nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

- 1990- Directrices para la regulación de los archivos de datos personales informatizados de la Organización de las Naciones Unidas (ONU).

- 1995- Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- 2002- Directiva 2002/58/CE del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

- 2006- Directiva 2006/24/CE, del Parlamento y Consejo Europeo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

[5]"Habeas Data" se refiere al derecho que tiene todo ciudadano a la protección de sus datos personales y a solicitar que sus datos e información sean actualizados, modificado, cancelados o suprimidos, en caso de que la información acerca de su persona vulnere su imagen, honor y privacidad o haya sido comprometida de tal forma que le cause un perjuicio. El Habeas Data es una acción constitucional que se ejerce mediante una petición formal del interesado a los tribunales constitucionales para que verifiquen si los datos de un ciudadano tanto en el ámbito público como privado hayan sido obtenidos lícitamente y conforme al marco legislativo aplicable en la materia..

- 2007- Directrices para la armonización de la protección de datos en la Comunidad Iberoamericana, aprobadas por la Red Iberoamericana de Protección de Datos.

- 2009.- Directiva 2009/136/CE del Parlamento y Consejo Europeo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no 2006/2004 sobre la cooperación en materia de protección de los consumidores.

En el orden internacional destacan como antecedentes de la protección de la intimidad y el honor de la persona en el tratamiento de sus datos:

La Declaración Universal de los Derechos Humanos la cual establece en su artículo 8:

> Artículo 8: "Toda persona tiene derecho a un recurso efectivo, ante los tribunales nacionales, que la ampare contra actos que violen sus derechos fundamentales reconocidos por la Constitución o la ley."
>
> El artículo 12 prescribe: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."[6]

La Declaración Americana de los Derechos y Deberes del Hombre:

> Artículo V declara que "Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar."
>
> Artículo XVIII proclama que "Toda persona puede recurrir a los tribunales para hacer valer sus derechos. Asimismo debe disponer de un procedimiento sencillo y breve por el cual la justicia la ampare

[6] http://www.un.org/es/documents/udhr/, Declaración Universal de los Derechos Humanos, 03 de enero 2013. 17:20.

> contra actos de la autoridad que violen, en perjuicio suyo, alguno de los derechos fundamentales consagrados constitucionalmente."[7]

Proyecto de Convención Americana sobre Autodeterminación Informativa de 1997, el cual contiene 21 artículos, en los cuales se propone una regulación para la protección y movimiento internacional de datos; se abordan en dicho proyecto temas importantes como el derecho a la información en la recolección de los datos, el consentimiento del afectado, la calidad, categorías, seguridad y cesión de los datos, los derechos y las garantías de las personas, el Habeas Data, las sanciones, los recursos, la agencia de protección de datos y el registro de datos.

Alemania el 7 de abril de 1970, el Parlamento del Estado alemán de Hesse, promulga su normativa de protección de datos "*Datenshutz"* convirtiéndose en el primer territorio con una norma dirigida a la protección de datos, posteriormente, el 27 de febrero de 1977, el Parlamento Federal de Alemania aprueba la *Datenshutz* Federal. En estos casos, se crea un Comisario Federal para la Protección de Datos (*Bundesbeauftragter fur den Datenshutz*).

Francia en 1978 se establece la Comisión Nacional de la Informática y de las Libertades, un organismo colegiado que tiene por objeto establecer un registro de bancos de datos de consulta ciudadana.

España desde 1978, la Constitución Española, en su artículo 18, apartado 4, dice: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos..."

Relacionada con esta disposición constitucional, en dicho país se ha publicado la Ley Orgánica 5/1992, de 29 de octubre, que regula el tratamiento automatizado de los datos de carácter personal, y cuyo objeto básico es la protección de la intimidad y el honor de las personas.

---

[7] http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp, 27 enero 2013, 14:25.

Estados Unidos de América el 31 de diciembre de 1974, el Congreso expide el "*PrivacyAct* (literalmente acto de retiro)", con la finalidad de proteger a los individuos en sus libertades y derechos fundamentales frente a la recolección y tratamiento automatizado de datos personales por parte de las agencias federales.

Brasil en el año de 1988 la Constitución Brasileña, en su artículo 5, numeral LXXII, se refiere al "conocimiento de informaciones relativas a la persona de la impetrante..." y a la rectificación de datos.

Aproximadamente 10 años más tarde, en Brasil se expide la Ley número 9.507, de 12 de noviembre de 1997, que reglamenta la citada disposición constitucional, con base en 23 artículos.

Colombia a partir de 1991, el artículo 15 de la Constitución de este país, reconoce al Habeas Data como un derecho fundamental aún no reglamentado.

Paraguay es a partir de 1992, que teniendo como antecedente los registros obrantes en poder de la Policía Nacional, que la Constitución Paraguaya, en su artículo 135, reconoce el derecho de las personas para acceder a la información que le corresponda en archivos públicos y privados, para conocer la finalidad de esos registros y para actualizar, rectificar o destruir los mismos datos.

Perú desde 1993, el artículo 200, inciso 3, de la Constitución, establece de manera expresa el Habeas Data, con el objeto de que el interesado pueda acceder a la información pública, con ciertas limitantes, y evitar la difamación de la persona por la difusión o suministro a terceros de informaciones que afecten la intimidad personal y familiar.

Ecuador el artículo 30 de la Constitución vigente establece el Habeas Data con los objetos de acceder a los registros, bancos o bases de datos, conocer su uso y finalidad, así como para solicitar la rectificación, actualización, eliminación o anulación de los datos, en caso de que estos sean erróneos o afecten

ilegítimamente los derechos de las personas. La Ley de Control Constitucional de 1997 ya ha reglamentado la acción de Habeas Data.

Argentina la nueva Constitución de 1994, en su artículo 43, en su párrafo tercero, establece el Habeas Data como un amparo especial; sin embargo, pese a la gran demanda porque se regulara en ley secundaria el Habeas Data, es hasta el año 2000 que se expide la Ley 25326 de Protección de los Datos Personales, publicada en el Boletín Oficial correspondiente al 2 de noviembre del año mencionado.

En este país Sudamericano, el *Habeas Data* ha tenido gran recepción, y muestra de ello es que en la provincia de Buenos Aires (artículo 20, inciso c de la Constitución Local), Córdoba (artículo 50 de su Constitución), Chubut (artículo 56 de su Ley primaria) y Jujuy (artículo 23, inciso 6, de su Constitución), entre otras, prevén el Habeas Data.

En México, no obstante la gran tradición y entramado constitucional que se posee, no se ha otorgado a los gobernados la garantía procesal del *Habeas Data*. Sin embargo, nuestro país no puede quedarse atrás de los países europeos y latinoamericanos, máxime si se toma en cuenta que algunos de ellos, que ya regulan el Habeas Data, limitan el movimiento internacional de datos con aquellos en los que no brinden condiciones equivalentes de seguridad a las propias, de donde se sigue que México, en alguna medida, se encontraría marginado de este movimiento internacional de datos, en diferentes materias entre las cuales pueden incluirse la comercial y económica.

1.2.- Antecedentes en México.

Podemos decir que aunque en nuestro país la LFPDPPP es relativamente nueva, sin embargo esta ley, a lo largo de su historia tiene varios antecedentes.

En efecto, antes de la expedición de la LFPDPPP, en México, el derecho a la protección de datos sólo era reconocido expresamente por la Ley Federal de

Transparencia y Acceso a la Información Pública Gubernamental (en cuanto al **sector** público) y dentro de la Ley de Protección de Datos Personales del Estado de Colima (sectores público y privado).

Adicionalmente, existían disposiciones sectoriales dentro de la Ley Federal de Protección al Consumidor, Código Penal Federal, y Ley General de Salud, entre otras, que reconocían algunos derechos de los titulares de los datos y establecían determinados mecanismos para su protección.

Entre el 2001 y 2008 se presentaron en el Congreso de la Unión, diversas iniciativas de ley, con la finalidad de que se regulara a nivel federal, la recolección, el tratamiento y la transmisión de información personal entre particulares.

En el año 2007, el presidente Felipe Calderón Hinojosa, en el plan Nacional de Desarrollo 2007-2012, estableció la necesidad de desarrollar una Ley Federal de Protección de datos personales, que regulara la información en poder de los particulares

Debido al panorama normativo y a que el país requería cumplir con sus compromisos internacionales, se consideró necesario expedir una ley en la materia.

En nuestro país, se logró el reconocimiento constitucional del derecho a la protección de datos personales a nivel nacional en el sector privado a través de la reforma al artículo 16 constitucional, en la cual quedó establecido que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición en los términos que fije la ley.

> En efecto, el “Artículo 16 Constitucional, dispone: 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".
>
> (Adicionado mediante decreto publicado en el diario oficial de la federación el 1 de junio de 2009).

Puede afirmarse que como complemento a tal disposición, también se agregó una fracción (XXIX-O) al artículo 73 constitucional, adicionando la materia de protección de datos personales en posesión de particulares, dentro de las materias sobre las cuales tiene facultad para legislar el Congreso de la Unión.

> Y a efecto, el "Artículo 73 Constitucional, establece que: el congreso tiene facultad:
>
> XXIX-O. Para legislar en materia de protección de datos personales en posesión de particulares".
>
> (Adicionado mediante decreto publicado en el diario oficial de la federación el 30 de abril de 2009).

En cumplimiento a los artículos anteriores, el Congreso de la Unión tuvo a bien emitir la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), publicada en el Diario Oficial de la Federación (DOF) el 5 de julio de 2010. Convirtiéndose esta ley en la base del marco regulatorio que vela por la protección de esta clase de datos en el sector privado, teniendo como objetivo principal regular el tratamiento legítimo, controlado e informado de los que se encuentren en posesión de particulares. Dicha ley y los siguientes documentos que a continuación se mencionan, son fundamentales en cuanto se refiere a regulación en materia de Protección de Datos personales:

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

Asimismo, la Secretaria de Economía y el Instituto Federal de Acceso a la Información y Protección de Datos, puso a disposición pública los siguientes documentos:

- Guía Práctica para generar el Aviso de Privacidad.
- Recomendaciones para la designación de la Persona o departamento de datos Personales.

1.3.- El Instituto Federal de Acceso a la Información Pública y Protección de Datos.

El Instituto Federal de Acceso a la Información Pública y Protección de Datos (IFAI) es un organismo descentralizado de la Administración Pública Federal y de particulares, no sectorizado que goza de autonomía operativa, presupuestaria y de decisión que se encarga de garantizar los derechos de las personas en cuanto al acceso a la información pública gubernamental, así como el de proteger todos los datos e información de datos personales que se encuentren en manos del Gobierno Federal y en posesión de particulares, también el de resolver las negativas de acceso a la información que las dependencias o entidades del gobierno federal hayan formulado. Por ello es una institución al servicio de la sociedad.

A su vez también lo podemos definir como "un órgano de la Administración Pública Federal, con autonomía operativa, presupuestaria y de decisión, encargado de promover y difundir el ejercicio del derecho de acceso a la información; resolver sobre la negativa a las solicitudes de acceso a la información y proteger los datos personales en poder de las dependencias y entidades[8]."

El instituto pretende:

- Garantizar el derecho de acceso a la información pública gubernamental.

[8] Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, p. 33

- Proteger los datos personales que están en manos del gobierno federal.
- Resolver sobre las negativas de acceso a información que las dependencias o entidades del Gobierno Federal hayan formulado.

A partir de la entrada en vigor de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, más de 250 dependencias y entidades del Gobierno Federal tienen la obligación de atender sus solicitudes de información.

El Instituto Federal de Acceso a la Información y Protección de Datos implementó el sistema electrónico Infomex Gobierno Federal, un mecanismo a través del cual se puede requerir información de manera más rápida y sistematizada a los organismos públicos federales aunque también los requerimientos se pueden hacer por correo certificado o mensajería y acudiendo personalmente ante las Unidades de Enlace de los sujetos obligados; adicionalmente, cabe señalar que a través del referido sistema también se pueden registrar los recursos de revisión interpuestos ante el Instituto Federal de Acceso a la Información y Protección de Datos, es decir, las quejas respecto de las respuestas otorgadas por los sujetos obligados a las solicitudes de acceso. Todas ellas abrirán una Unidad de Enlace para ese fin. Una vez solicitada, un Comité de Información en cada dependencia determinará si la información se otorga o no. En caso de que la decisión sea negativa, el solicitante puede interponer un recurso de revisión ante el IFAI.

Los objetivos principales de INFOMEX son los siguientes:

- Recibir y dar respuesta a las solicitudes de acceso a la información y a datos personales, así como a las correcciones de éstos, que presenten los ciudadanos en forma electrónica.
- Conocer la situación que guardan las solicitudes referidas, mediante los mecanismos de seguimiento del INFOMEX;

- Consultar las más de 500 mil respuestas de la Administración Pública Federal, usando múltiples filtros, como por ejemplo: fecha, estatus y tipo de respuesta otorgada por dependencia y entidad del Gobierno Federal.

Cabe señalar que entre las funciones más importantes del IFAI se encuentran:

- El IFAI sólo interviene en aquellos casos en los cuales, las personas se inconformen e interpongan un recurso de revisión.
- El IFAI elaborará un dictamen en cada caso, abriendo la información o confirmando la decisión de la dependencia.
- En cualquier caso, el IFAI trabajará bajo el principio de publicidad de la información del gobierno.
- El IFAI es un organismo descentralizado de la Administración Pública Federal, no sectorizado, y goza de autonomía operativa, presupuestaria y de decisión.
- El Instituto Federal de Acceso a la Información Pública y Protección de Datos (IFAI) es una institución al servicio de la sociedad.

Competencia del IFAI

Si bien la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental obliga a los Poderes Ejecutivo, Legislativo y Judicial, así como a los organismos constitucionales autónomos (IFE, CNDH, Banco de México), el IFAI tiene facultades para vigilar su cumplimiento y resolver sobre negativas de acceso a la información únicamente respecto a las dependencias y entidades de la Administración Pública Federal (A.P.F.), incluidas la Presidencia y la Procuraduría General de la República.

Conforme a la misma Ley, tanto los Poderes Legislativo y Judicial, como los organismos constitucionales autónomos, deben expedir sus propios

reglamentos para garantizar la exacta observancia y aplicación de las disposiciones.

El Pleno del IFAI

Es el órgano máximo de dirección está integrado por cinco comisionados, cuyo nombramiento corresponde al titular del Poder Ejecutivo Federal, sin la objeción de la Cámara de Senadores. Los comisionados duran en su encargo siete años sin posibilidad de reelección, y sólo podrán ser removidos cuando trasgredan en forma grave o reiterada las disposiciones contenidas en la Constitución Federal o en la LFTAIPG[9]; cuando sus actos u omisiones afecten las atribuciones del Instituto, o cuando hayan sido sentenciados por un delito grave que merezca pena corporal; gozan de garantías de independencia y de plena autonomía para la conducción del Instituto y el ejercicio de sus atribuciones, entre las cuales destaca la expedición de lineamientos y criterios en materia de clasificación de la información gubernamental y protección de datos personales, así como en la resolución de los recursos de revisión que las personas interpongan en contra de negativas de acceso a la información.

El IFAI es presidido por un Comisionado, elegido por sus colegas por un período de dos años, con posibilidad de una reelección. El Comisionado Presidente, además de sus funciones propias como miembro del Pleno del Instituto, ejerce la representación legal del Instituto y constituye el enlace entre el órgano de dirección y la estructura ejecutiva del IFAI, con el fin de coordinar la ejecución y el desarrollo de las políticas y los programas institucionales.

Estructura de Apoyo al Pleno

La estructura de apoyo al pleno está constituida por dos Secretarías: La Secretaría de Acuerdos y la Secretaría Ejecutiva.

[9] LEY Federal de Transparencia y Acceso a la Información Pública Gubernamental

La Secretaría de Acuerdos tiene la función de apoyar al Pleno y a los Comisionados en la definición y expedición de los lineamientos y criterios de clasificación y desclasificación de la información gubernamental; en la sustanciación y elaboración de los proyectos de resolución de los recursos que sean interpuestos ante el Instituto ante negativas de acceso a la información; y en materia de protección de datos personales; en la gestión de los asuntos jurídicos del IFAI, y en la elaboración de los estudios que sirvan de apoyo al Pleno para el desempeño de sus atribuciones. Para ello, tiene adscritas tres direcciones generales: Asuntos Jurídicos, Clasificación y Datos Personales y Estudios e Investigación.

La Secretaría Ejecutiva, por su parte, tiene la función de apoyar al Pleno en la coordinación y vigilancia de las dependencias y entidades de la Administración Pública Federal respecto al cumplimiento de las obligaciones que la Ley les impone; en el diseño y desarrollo de los programas de capacitación a los servidores públicos del gobierno federal; en la atención y orientación a la sociedad para el ejercicio del derecho de acceso a la información, así como en la ejecución de las políticas y los programas de planeación y administración del IFAI, informática y sistemas, relaciones institucionales con los Poderes Legislativo y Judicial, organismos constitucionales autónomos, gobiernos locales y municipales. Para ello, tiene adscritas seis direcciones generales: Administración; Atención a la Sociedad y Relaciones Institucionales; Comunicación Social; Coordinación y Vigilancia de la A.P.F.; Informática y Sistemas y Vinculación con Estados y Municipios.

Servir para presentar solicitudes de información o solicitudes de acceso o corrección a datos personales ante dependencias y entidades del Poder Ejecutivo Federal.

Ofrecer asesoría para conocer cuáles organismos de gobierno han establecido sus propios procedimientos de acceso a información -como los poderes

Legislativo y Judicial y los organismos con autonomía como el IFE, la Comisión Nacional de Derechos Humanos, el Banco de México y la UNAM.

Ayudar a un recurso de revisión ante el IFAI cuando una dependencia o entidad te ha negado acceso a información gubernamental o solicitudes de acceso o corrección a datos personales.

Defender el derecho de acceso a la información, a través de la revisión y eventual modificación de las negativas de acceso de las dependencias y entidades.

Brindarte información actualizada y especializada sobre el acceso a la información en México y la protección a los datos personales.

1.4.- las Reformas Constitucionales en materia de datos personales.

En México se han promulgado leyes de “libertad de información”, de “acceso a la información” y de “protección de datos personales” entre las que podemos citar la Ley Federal de Transparencia y Acceso a la Información Pública, del 2002 (legislación Federal) y Leyes Estatales (32 entidades federativas). Ley de Protección de Datos Personales, Estado de Colima, 2003, Distrito Federal 2009, etc. También, se encuentran de forma dispersa en documentos de diversa naturaleza, existiendo un conjunto de disposiciones en materia de Protección de Datos tales como:

- Reglamento de la Ley Federal de Transparencia y Acceso a la Información Pública.
- Lineamientos que deberán observar las dependencias y entidades de la Administración Pública Federal en la recepción, procesamiento, trámite, resolución y notificación de las solicitudes de corrección de datos personales que formulen los particulares.

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

Leyes que se encuentran diseñadas para posibilitar a los individuos el examen de la información pública y que con ello puedan obtener información sobre las acciones de sus gobiernos en sus tres niveles federal, estatal y local. Con todo ello, deben equilibrar la apertura de la información pública con la protección de la información personal y confidencial que el Estado, en sus tres niveles, posee sobre los ciudadanos. Debiendo hacer hincapié en que el derecho a la privacidad es un derecho fundamental que se encuentra establecido en la Constitución Política de los Estados Unidos Mexicanos (C.P.E.U.M.), la dificultad se denota cuando se trata de establecer una división entre lo que es información pública e información privada. La Suprema Corte de Justicia de la Nación (SJCN) estableció en una tesis jurisprudencial que, “para determinar lo que es vida privada, se puede recurrir al método de exclusión y sostener que la vida privada es todo aquello que no constituya la vida pública[10]”.

[10] DADA ESCALANTE, Paola, "Información contra privacidad", México entra en la era de la transparencia, México,

La reforma al artículo 6º Constitucional

Como primer antecedente podemos decir que se encuentra en la reforma realizada en 2007 artículo 6º constitucional, el cual se adiciona un párrafo segundo a este numeral, sentando las bases respecto al derecho a la información (transparencia), y que se incluye la protección de datos personales por parte de las entidades públicas, dando reconocimiento a los derechos de acceso y rectificación, en el que literalmente nos dice:

> Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, los derechos de tercero, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley.
>
> El derecho a la información será garantizado por el Estado. Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:
>
> I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.
> II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.

Reforma al artículo 16 Constitucional

“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”.

Este articulo a lo largo de la carrera de la abogacía es sumamente sonado e importante no sólo para los estudiantes y los litigantes sino para todos los mexicanos ya que nos señala un derecho fundamental de protección, ya que si

---

Instituto Federal de Acceso a la Información Pública, 2004. 4

alguna autoridad pretende un acto en contra de alguien y no cuenta con un documento fundamentado por alguna ley y motivado con argumentos fehacientes y apegados a derecho se da la violación a las garantías individuales, y con tal enunciado comienza el texto del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. Reiterando de nueva vez contra tal declaración, que se puede argumentar que solamente por medio de un mandato escrito y que suscriba una autoridad competente, es posible "molestar a una persona" siempre y cuando dicha autoridad funde y motive, legalmente, su proceder.

Las pretensiones necesarias de puntualizar son que el sentido del artículo 16º, Constitucional es el de proteger a los individuos de cualquier perturbación que puedan sufrir principalmente en su persona, familia, propiedades, documentos etc., sin que exista de por medio, mandato legal alguno, es decir, excluir de todos aquellos que sin ser autoridades con mandato, la posibilidad de molestar a un individuo. Esa molestia puede realizarse a través de diferentes actos entre los que se pueden encontrar atentados contra la Intimidad.

Sin embargo, aún cuando el artículo 16 constitucional protege los derechos de los ciudadanos a la privacidad de sus hogares, de la información y las comunicaciones, dejan lagunas sobre la protección del concepto moderno de datos personales, razón por la cual es de fundamental relevancia la adición de un segundo párrafo al artículo indicado, lo cual tuvo lugar el 1 de junio del 2009, 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 proceda 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".

La adición de un párrafo segundo al artículo 16 constitucional, establece que toda persona tiene derecho a la protección de sus datos personales y a ejercer los derechos denominados "ARCO" (acceso, rectificación, cancelación y oposición); el derecho referido sólo podrá limitarse por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. Cabe señalar que la LFPDPPP por su parte, acopla estos supuestos dentro de su artículo 4.

Es importante resaltar que el Derecho de Protección de Datos Personales se encuentra consagrado internacionalmente en el artículo 12 de la Declaración Universal de los Derechos Humanos de 1948, en el artículo 17 puntos 1 y 2 del Pacto Internacional de Derechos Civiles y Políticos de 1966; así como en el numeral 11 puntos 2 y 3 de la Convención Americana de Derechos Humanos de 1969, entre otros. Otro punto importante de no perder de vista lo apuntado por el presidente del Tribunal Europeo de Derechos Humanos en el discurso de apertura de la XIII Conferencia de Comisarios de Protección de Datos: "aunque hablamos de protección de datos, de legislación de protección de datos y de Autoridades de protección de datos, no deben existir dudas respecto a la verdadera naturaleza del objetivo que motiva la creación de las normas de protección de datos o de las instituciones que garantizan el cumplimiento de las mismas. Su finalidad real no es tanto la protección de datos sino la protección de las personas: más precisamente aún, es la protección de la vida privada de las personas en una nueva era que impone la recogida y almacenamiento de más y más datos sobre sus vidas privadas y hace aumentar las posibilidades de manipulación y mal uso de tales datos[11]" .

La reforma al artículo 73 Constitucional

[11] RYSDALL, R, Protección de datos y el Convenio Europeo de los Derechos Humanos. Discurso de apertura dela XIII Conferencia de Comisarios de Protección de Datos, Novatica, marzo de 1992, citado por Campuzano Tomé, Herminia, Vida Privada y Datos Personales, su protección frente a la sociedad de la información, Tecnos, Madrid, España, 2000. p. 56

México al estar establecido como una República representativa, democrática y federal, en la que los Estados que la integran son libres y soberanos en cuanto a su régimen interior, si bien unidos por el Pacto federal, encontrábamos que los asuntos informáticos que inciden en el ámbito del Derecho Civil o Penal, podían hasta la presente reforma, ser regulados por cada una de las Entidades Federativas a su libre y mejor parecer.

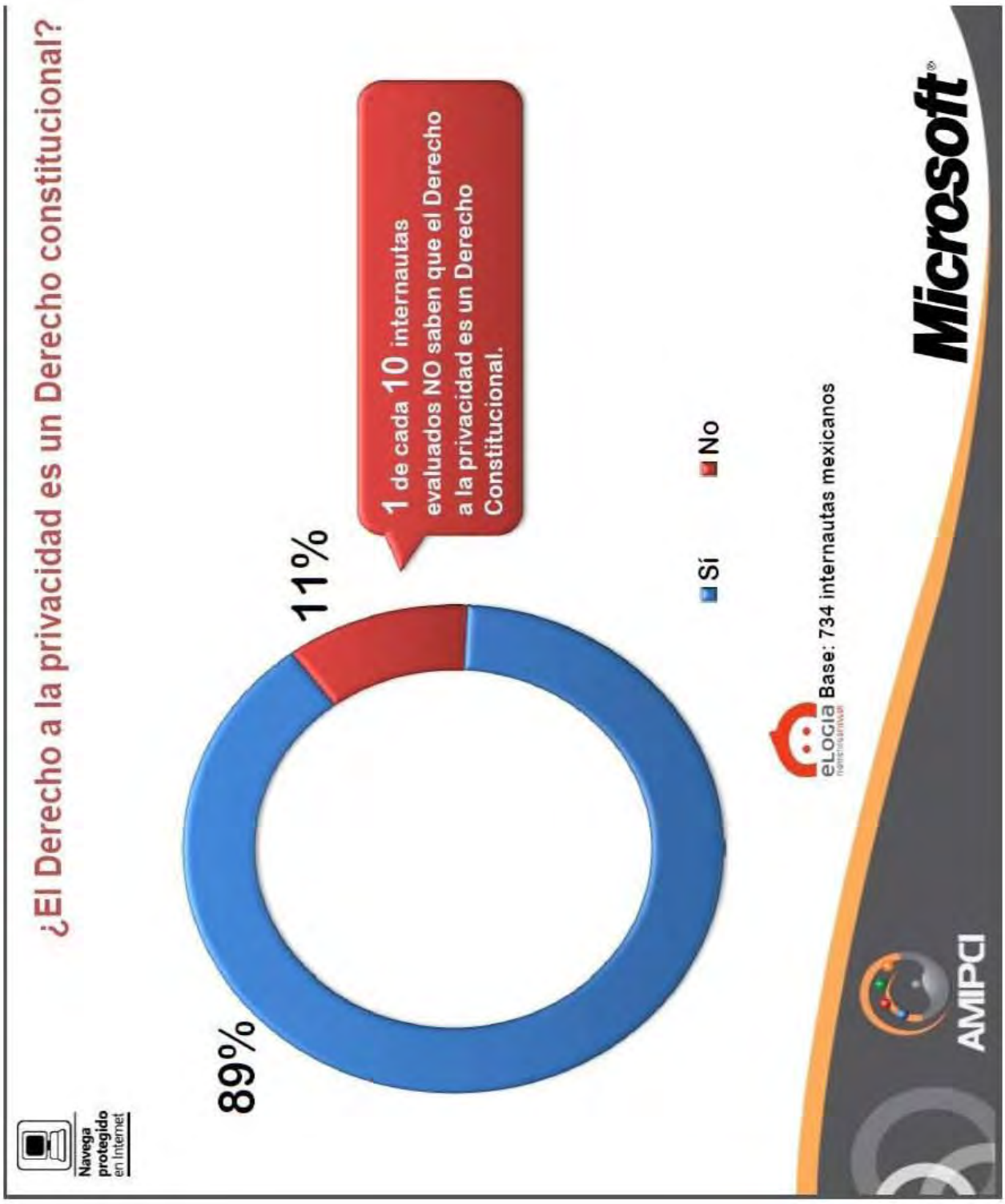
El Congreso Federal, constitucionalmente, tenía ya, facultades exclusivas para legislar sobre: hidrocarburos, minería, industria cinematográfica, comercio, juegos con apuestas y sorteos, intermediación y servicios financieros, energía eléctrica y nuclear, derecho marítimo, ciudadanía, migración, vías generales de comunicación, correos, aguas, moneda, delitos federales, coordinación en materia de seguridad pública, fiscalización superior de la federación, leyes del trabajo reglamentarias del artículo 123 Constitucional, nacionalidad y extranjería, migración, salubridad, coordinación de la educación, generación, difusión y aplicación de conocimientos científicos y tecnológicos, entre otras. situaciones en donde se puede llegar a transgredir la Intimidad —como regla general— y en especial la Intimidad genética, comprendida como datos relativos a la salud, tales como se sustenta con las legislaciones siguientes:

- Reglamento de la Ley General de Salud en materia de Investigación para la Salud, "Artículo 13.
- Reglamento de Servicios Médicos del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado, Artículo 57;
- Ley Reglamentaria del Artículo 5o. Constitucional, relativo al Ejercicio de las Profesiones en el Distrito Federal, Artículo 36;
- Código Civil para el Distrito Federal, Artículo 1912;
- Código Penal para el Distrito Federal; Artículo 213;
- Norma Oficial Mexicana NOM- 168-SSA1-1998, relativa al Expediente Clínico.

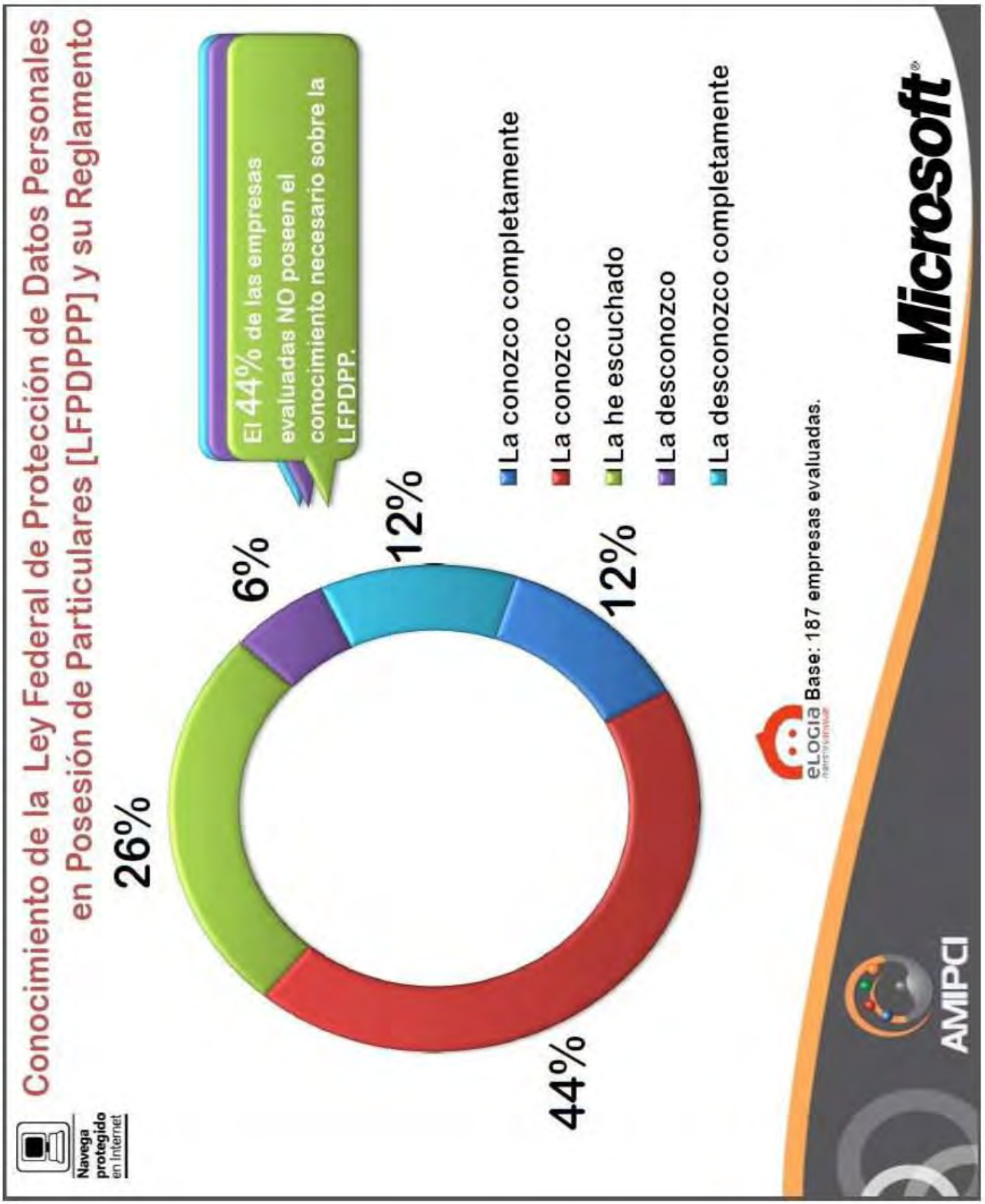
La reciente reforma del pasado 30 de abril del 2009 al Art. 73 Construccional, adiciona la fracción XXIX-O, en la que se otorga facultades exclusivas al H. Congreso de la Federación para legislar en materia de Protección de Datos en posesión de particulares.

Considero que, dada la importancia, la trascendencia, el carácter global e internacional de la Internet, de las Tecnologías de Información y Comunicación y de las herramientas tecnológicas que pueden afectar las relaciones económicas y sociales, lo ideal u óptimo es que se eleve a nivel federal la materia informática, sea cual sea su ámbito de aplicación o la rama del Derecho en la que incida. En consecuencia, considero que la reforma de la Constitución Política de los Estados Unidos Mexicanos en su artículo 73 es un acto de transcendental importancia, aunque cada una de las reformas establecidas en la Constitución nos da puntos importantes para la creación de la ley en estudio.

La Asociación Mexicana de Internet (AMIPCI) fue fundada en 1999; integra a las empresas que representan una verdadera influencia en el desarrollo de la Industria de Internet en México. Esta imagen nos hace referencia sobre una encuesta realizada por AMIPCI sobre la si la privacidad es un derecho constitucional.



Esta imagen nos hace referencia sobre una encuesta realizada por AMIPCI sobre el conocimiento de esta ley y su reglamento con los ciudadanos.



CAPÍTULO II

BASES DE DATOS, DATOS PERSONALES Y DERECHOS ARCO

2.1.- Los ficheros y bases de datos.

Se le conoce a un fichero como un conjunto de información clasificada y almacenada de diversas formas para su conservación y fácil acceso en cualquier momento.

Un fichero puede ser un sistema de archivos físicos contenidos en cajas u otros elementos de almacenamiento que forman parte de un conjunto mayor como una biblioteca o archivo público o privado. A menudo, el fichero utiliza una taxonomía o sistema de clasificación común para todos sus contenidos que permiten la búsqueda de datos específicos de forma rápida y sencilla. El más común es el orden alfabético por concepto o autor, pero también puede clasificarse la información según áreas temáticas, por orden cronológico u otros criterios dependiendo de la información contenida en el fichero.

En informática, un archivo o fichero también es un conjunto de información que se almacena en forma virtual para ser leído y/o accedido por medio de una computadora, las posibilidades de almacenamiento y clasificación son mucho más ricas en un sistema informático, ya que la información no ocupa un espacio físico y, por ende, es posible conservar millones de datos en un dispositivo muy pequeño. Inclusive, se puede guardar información de texto, audio o video en un mismo lugar sin inconveniente alguno.

El sistema suele organizar taxonómicamente la información en forma automática, permitiendo que el usuario la encuentre con sólo ingresar palabras clave en un buscador específico, lo cual supone una operación rápida y útil cuando la información almacenada es múltiple. A su vez, los sistemas informáticos suelen replicar los ficheros físicos y, así, organizar el contenido en carpetas y subcarpetas creadas y administradas por el usuario que son

ubicadas en el disco interno y que pueden ser abiertas mediante accesos directos dispuestos en el escritorio virtual del ordenador.

Los sistemas de ficheros surgieron al informatizar el manejo de los archivadores manuales para proporcionar un acceso más eficiente a los datos almacenados en los mismos. Un sistema de ficheros sigue un modelo descentralizado, en el que cada departamento de la empresa almacena y gestiona sus propios datos mediante una serie de programas de aplicación escritos especialmente para él.

Estos programas son totalmente independientes entre un departamento y otro, y se utilizan para introducir datos, mantener los ficheros y generar los informes que cada departamento necesita. Es importante destacar que en los sistemas de ficheros, tanto la estructura física de los ficheros de datos como la de sus registros, están definidas dentro de los programas de aplicación.

Cuando en una empresa se trabaja con un sistema de ficheros, los departamentos no comparten información ni aplicaciones, por lo que los datos comunes deben estar duplicados en cada uno de ellos. Esto puede originar inconsistencias en los datos. Se produce una inconsistencia cuando copias de los mismos datos no coinciden: dos copias del domicilio de un cliente pueden no coincidir si sólo uno de los departamentos que lo almacenan ha sido informado de que el domicilio ha cambiado.

Otro inconveniente que plantean los sistemas de ficheros es que cuando los datos se separan en distintos ficheros, es más complicado acceder a ellos, ya que el programador de aplicaciones debe sincronizar el procesamiento de los distintos ficheros implicados para garantizar que se extraen los datos correctos.

La rápida evolución que la tecnología de bases de datos ha experimentado en la última década, así como la variedad de nuevos caminos abiertos, han conducido a investigadores y asociaciones interesadas, a reflexionar sobre el futuro de esta tecnología. Estas reflexiones quedan recogidas en numerosos

debates y manifiestos que intentan poner orden en un campo en continua expansión.

Esta imagen nos hace referencia sobre las bases de datos y la facilidad de transferir información.

Bases de datos

Un paquete manejador de bases de datos es más conveniente cuando se esta trabajando con bases de datos, y un administrador de archivos se usa más cuando sólo se está buscando un archivo desde un procesador de textos.

El cambio que opera la informática es que multiplica para cualquier organización o persona la posibilidad de realizar un tratamiento automático y racional de la información. Ésta se encuentra recogida en archivos informáticos llamados "bases de datos", que sustituyen a los antiguos ficheros de papel. Estos archivos informáticos, las bases de datos, son también ficheros, lo único que cambia es el formato: son ficheros (archivos) informáticos.

“La mayor potencia de los ordenadores sobre el papel a la hora de "tratar" la información que suministran las bases de datos, y la generalización de su uso por cualquiera que tenga un PC, ha obligado a los gobiernos a publicar normas

jurídicas que regulen el tratamiento de la información" (Gonzalo Gallo Ruiz, 2003).

Una base de datos es un conjunto de datos almacenados en memoria externa que están organizados mediante una estructura de datos. Cada base de datos ha sido diseñada para satisfacer los requisitos de información de empresas u otro tipo de organización, como por ejemplo, una universidad o un hospital.

Los tipos de datos que pueden introducirse en una Base de Datos, se dividen en:

- Numéricos: se pueden introducir números para identificar partes del archivo, esto identifica la parte que numera al archivo o lo distingue de alguna manera.
- Texto: el texto es un nombre que identifica al campo, ya sea el nombre del autor
- Etiquetas: son los títulos con los que cada campo es designado.
- Fórmulas: son datos que aparecen como numéricos pero fueron hechos por medio de fórmulas.

Las Bases de Datos son programas que administran información y hacen más ordenada la información, aparte de hacerla fácil de buscar, entre sus usos principales facilitan el almacenaje de información, así como lograr una búsqueda más rápida y eficiente de la misma, se puede tener una mayor organización y estructuracion.

Sus características son ventajosas o desventajosas: pueden ayudarnos para almacenar, organizar, recuperar, comunicar y manejar información en formas que serían imposibles sin la tecnología con la que contamos hoy en día, tales como los programas computacionales especializados para dicho manejo, pero también son desventajosas ya que se cuenta con grandes cantidades de información en bases de datos de las que no se tiene control del acceso ni

protección alguna para salvaguardar dicha información sin riesgo de que un tercero pueda hacer un uso distinto al destinado.

Un paquete manejador de bases de datos es más conveniente cuando se está trabajando con bases de datos, y un administrador de archivos se usa más cuando sólo se está buscando un archivo desde un procesador de textos.

Los sistemas de bases de datos presentan numerosas ventajas gracias, fundamentalmente, a la integración de datos y a la interfaz común que proporciona el SGBD[12]. Estas ventajas se describen a continuación.

Los sistemas de ficheros almacenan varias copias de los mismos datos en ficheros distintos. Esto hace que se desperdicie espacio de almacenamiento, además de provocar faltas de consistencia de datos (copias que no coinciden). En los sistemas de bases de datos todos estos ficheros están integrados, por lo que no se almacenan varias copias de los mismos datos. Sin embargo, en una base de datos no se puede eliminar la redundancia completamente, ya que en ocasiones es necesaria para modelar las relaciones entre los datos, o bienes necesarios para mejorar las prestaciones.

Eliminando o controlando las redundancias de datos se reduce en gran medida el riesgo de que haya inconsistencias. Si un dato está almacenado una sola vez, cualquier actualización se debe realizar sólo una vez, y está disponible para todos los usuarios inmediatamente. Si un dato está duplicado y el sistema conoce esta redundancia, el propio sistema puede encargarse de garantizar que todas las copias se mantengan consistentes. Desgraciadamente, no todos los SGBD de hoy en día se encargan de mantener automáticamente la consistencia.

En los sistemas de ficheros, los ficheros pertenecen a los departamentos que los utilizan, pero en los sistemas de bases de datos, la base de datos pertenece a la empresa y puede ser compartida por todos los usuarios que estén

12 Sistema de Gestión de Base de Datos.

autorizados. Además, las nuevas aplicaciones que se vayan creando pueden utilizar los datos de la base de datos existente.

La integridad de la base de datos, se refiere a la validez de los datos almacenados. Normalmente, la integridad se expresa mediante restricciones o reglas que no se pueden violar. Estas restricciones se pueden aplicar tanto a los datos, como a sus relaciones, y es el SGBD quien se encargará de mantenerlas.

La seguridad de la base de datos, consiste en la protección de datos frente a usuarios no autorizados. Sin unas buenas medidas de seguridad, la integración de datos en los sistemas de bases de datos hace que éstos sean más vulnerables que en los sistemas de ficheros. Sin embargo, el SGBD permite mantener la seguridad mediante el establecimiento de claves para identificar al personal autorizado a utilizar la base de datos. Las autorizaciones se pueden realizar a nivel de operaciones, de modo que un usuario puede estar autorizado a consultar ciertos datos pero no a actualizarlos, por ejemplo.

Mejora en la accesibilidad a los datos. Muchos SGBD proporcionan lenguajes de consulta o generadores de informes que permiten al usuario hacer cualquier tipo de consulta sobre los datos, sin que sea necesario que un programador escriba una aplicación que realice tal tarea.

Mejora en la productividad. El SGBD proporciona muchas de las funciones estándar que el programador necesita escribir en un sistema de ficheros. A nivel básico, el SGBD (Sistema de Gestión de Base de Datos) proporciona todas las rutinas de manejo de ficheros típicas de los programas de aplicación. El hecho de disponer de estas funciones permite al programador centrarse mejor en la función específica requerida por los usuarios, sin tener que preocuparse de los detalles de implementación de bajo nivel. Muchos SGBD también proporcionan un entorno de cuarta generación consistente en un conjunto de herramientas que simplifican, en gran medida, el desarrollo de las aplicaciones que acceden

a la base de datos. Gracias a estas herramientas, el programador puede ofrecer una mayor productividad en un tiempo menor.

2.2.- Las bases de datos cibernéticas.

Primero que nada la cibernética es una disciplina íntimamente vinculada con la teoría general de sistemas, al grado en que muchos la consideran inseparable de esta, y se ocupa del estudio del mando, el control, las regulaciones y el gobierno de los sistemas. El propósito de la cibernética es desarrollar un lenguaje y técnicas que nos permitan atacar los problemas de control y comunicación en general.

La cibernética es una ciencia, nacida hacia 1948 e impulsada inicialmente por Norbert Weiner que tiene como objeto “el control y comunicación en el animal y en la máquina” o “desarrollar un lenguaje y técnicas que nos permitirán abordar el problema del control y la comunicación en general” Mucha gente asocia la cibernética con la robótica, los robots y el concepto de *cyborg*[13] debido al uso que se le ha dado en algunas obras de ciencia y ficción, pero desde un punto de vista estrictamente científico, la cibernética trata acerca de sistemas de control basados en la retroalimentación.

Lo que estabiliza y coordina el funcionamiento de los sistemas complejos como los seres vivos o las sociedades y les permite hacer frente a las variaciones del ambiente y presentar un comportamiento más o menos complejo es el control, que le permite al sistema seleccionar los ingresos *(inputs)* para obtener ciertos egresos *(outputs)* predefinidos. La regulación está constituida por los mecanismos que permiten al sistema mantener su equilibrio dinámico y alcanzar o mantener un estado.

Ciertas aplicaciones de la cibernética pueden presentar algunas desventajas por ejemplo:

[13] Acrónimo en inglés cyborg: cyber (cibernético) + organism (organismo), (organismo cibernético) se utiliza para designar una criatura compuesta de elementos orgánicos y dispositivos cibernéticos generalmente con la intención de mejorar las capacidades de la parte orgánica mediante el uso de tecnología.

- La Falta de empleo a la población, a causa de que las máquinas realizarían un mejor trabajo que un humano. Pobreza global,

Esta opinión es muy subjetiva ya que desde mi punto de vista una maquina no trabaja igual que el ingenio, instinto y autodeterminación de una persona, aunque a lo largo de los días podemos denotar que un barrendero no trabaja igual que una maquina de limpieza, refiriéndonos a esto con la agilidad, rapidez y eficacia de ésta, dándose con ello, el reemplazo de mano de obra humana por mano de obra robótica.

Algunas ventajas son:

La reducción de las jornadas laborales, los trabajos complejos o rutinarios pasarían a ser de las máquinas. Además, la cibernética brinda un gran aporte al campo medicinal.

Un conocimiento mayor de como funcionan los sistemas complejos pudiera llevar a la solución de problemas también complejos como la criminalidad en las grandes ciudades.

Con toda esta explicación nos vamos a las bases de datos cibernéticas y con ello podemos decir que a la hora de la recopilación de la información de datos de las personas en medios electrónicos entendiéndose estos como computadoras (discos duros, CD ROM, memorias, etc. Y con ellas programas especializados en la recopilación, almacenamiento y acomodo y demás de la información, siendo los mas conocidos en un sistema operativo Windows y un programa de arranque Office, el programa de Microsoft Excel y Access) o las ya muy conocidas nubes, existe mas agilidad, mas capacidad y a la hora de la búsqueda de la información más rapidez y precisión para la localización de información.

Por ello podríamos definir las bases de datos cibernéticas, como aquella recopilación de gran cantidad de información establecida como caracteres,

almacenada en dispositivos de almacenamiento y que con ello facilitan la búsqueda de la información.

2.2.1.- Base de datos en la nube.

Nuevamente para entender que son las bases de datos en nubes, primero debemos de entender que son las nubes a nivel cibernético.

En este tipo de computación (nubes), todo lo que puede ofrecer un sistema informático se ofrece como servicio, de modo que los usuarios puedan acceder a los servicios disponibles "en la nube de Internet" sin conocimientos (o, al menos sin ser expertos) en la gestión de los recursos que usan. Según el IEEE *Computer Society*[14], es un paradigma en el que la información se almacena de manera permanente en servidores de Internet y se envía a cachés[15] temporales de cliente, lo que incluye equipos de escritorio, centros de ocio, portátiles, etc.

La computación en la nube, son servidores desde internet encargados de atender las peticiones en cualquier momento. Se puede tener acceso a su información o servicio, mediante una conexión a internet desde cualquier dispositivo móvil o fijo, ubicado en cualquier lugar. Sirven a sus usuarios desde varios proveedores de alojamiento repartidos frecuentemente por todo el mundo. Esta medida reduce los costos, garantizando un mejor tiempo de actividad y que los sitios web sean invulnerables a los *hackers*, a los gobiernos locales y a sus redadas policiales.

"Cloud computing" es un nuevo modelo de prestación de servicios de negocio y tecnología, que permite incluso al usuario acceder a un catálogo de servicios estandarizados y responder con ellos a las necesidades de su negocio, de forma flexible y adaptativa, en caso de demandas no previsibles o de picos de

[14] corresponde a las siglas de (Institute of Electrical and Electronics Engineers) en español Instituto de Ingenieros Eléctricos y Electrónicos

[15] En informática, el caché de CPU, es un área especial de memoria que poseen los ordenadores. Funciona de una manera similar a como lo hace la memoria principal (RAM), pero es de menor tamaño y de acceso más rápido. Es usado por la unidad central de procesamiento para reducir el tiempo de acceso a datos ubicados en la memoria principal que se utilizan con más frecuencia.

trabajo, pagando únicamente por el consumo efectuado, o incluso gratuitamente en caso de proveedores que se financian mediante publicidad o de organizaciones sin ánimo de lucro.

El cambio que ofrece la computación desde la nube es que permite aumentar el número de servicios basados en la red. Esto genera beneficios tanto para los proveedores, que pueden ofrecer, de forma más rápida y eficiente, un mayor número de servicios, como para los usuarios que tienen la posibilidad de acceder a ellos, disfrutando de la 'transparencia' e inmediatez del sistema y de un modelo de pago por consumo. Así mismo, el consumidor ahorra los costos salariales o los costos en inversión económica (locales, material especializado, etc).

Computación en nube consigue aportar estas ventajas, apoyándose sobre una infraestructura tecnológica dinámica que se caracteriza, entre otros factores, por un alto grado de automatización, una rápida movilización de los recursos, una elevada capacidad de adaptación para atender a una demanda variable, así como virtualización avanzada y un precio flexible en función del consumo realizado, evitando además el uso fraudulento del software y la piratería.

La computación en nube es un concepto que incorpora el software como servicio, como en la Web 2.0 [16]y otros conceptos recientes, también conocidos como tendencias tecnológicas, que tienen en común el que confían en Internet para satisfacer las necesidades de cómputo de los usuarios.

Beneficios

Integración probada de servicios Red. Por su naturaleza, la tecnología de *cloud computing* se puede integrar con mucha mayor facilidad y rapidez con el resto de las aplicaciones empresariales (tanto software tradicional como Cloud

[16] Un sitio Web 2.0 permite a los usuarios interactuar y colaborar entre sí como creadores de contenido generado por usuarios en una comunidad virtual.

Computing basado en infraestructuras), ya sean desarrolladas de manera interna o externa.

Prestación de servicios a nivel mundial. Las infraestructuras de *cloud computing* proporcionan mayor capacidad de adaptación, recuperación completa de pérdida de datos (con copias de seguridad) y reducción al mínimo de los tiempos de inactividad.

Una infraestructura 100% de *cloud computing* permite al proveedor de contenidos o servicios en la nube prescindir de instalar cualquier tipo de *hardware*, ya que éste es provisto por el proveedor de la infraestructura o la plataforma en la nube. Un gran beneficio del *cloud computing* es la simplicidad y el hecho de que requiere mucha menor inversión para empezar a trabajar.

Implementación más rápida y con menos riesgos, ya que se comienza a trabajar más rápido y no es necesaria una gran inversión. Las aplicaciones del cloud computing suelen estar disponibles en cuestión de días u horas en lugar de semanas o meses, incluso con un nivel considerable de personalización o integración.

Actualizaciones automáticas que no afectan negativamente a los recursos de TI[17]. Al actualizar a la última versión de las aplicaciones, el usuario se ve obligado a dedicar tiempo y recursos para volver a personalizar e integrar la aplicación. Con el *cloud computing* no hay que decidir entre actualizar y conservar el trabajo, dado que esas personalizaciones e integraciones se conservan automáticamente durante la actualización.

Contribuye al uso eficiente de la energía. En este caso, a la energía requerida para el funcionamiento de la infraestructura. En los *datacenters*[18] tradicionales, los servidores consumen mucha más energía de la requerida realmente.

[17] Recursos de TI son las Personas, Infraestructura, Aplicaciones e Información.

[18] Se denomina centro de procesamiento de datos a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

En cambio, en las nubes, la energía consumida es sólo la necesaria, reduciendo notablemente el desperdicio.

Desventajas

Podemos encontrar en este tipo de servicios una serie de desventajas tales como:

- La centralización de las aplicaciones y el almacenamiento de los datos origina una interdependencia de los proveedores de servicios.
- La disponibilidad de las aplicaciones está ligada a la disponibilidad de acceso a Internet.
- Los datos "sensibles" del negocio no residen en las instalaciones de las empresas, lo que podría generar un contexto de alta vulnerabilidad para la sustracción o robo de información.
- La confiabilidad de los servicios depende de la "salud" tecnológica y financiera de los proveedores de servicios en nube. Empresas emergentes o alianzas entre empresas podrían crear un ambiente propicio para el monopolio y el crecimiento exagerado en los servicios.
- La disponibilidad de servicios altamente especializados podría tardar meses o incluso años para que sean factibles de ser desplegados en la red.
- La madurez funcional de las aplicaciones hace que continuamente estén modificando sus interfaces, por lo cual la curva de aprendizaje en empresas de orientación no tecnológica tenga unas pendientes significativas, así como su consumo automático por aplicaciones.
- Seguridad. La información de la empresa debe recorrer diferentes nodos para llegar a su destino, cada uno de ellos (y sus canales) son un foco de

inseguridad. Si se utilizan protocolos seguros, HTTPS[19] por ejemplo, la velocidad total disminuye debido a la sobrecarga que éstos requieren.

- Escalabilidad a largo plazo. A medida que más usuarios empiecen a compartir la infraestructura de la nube, la sobrecarga en los servidores de los proveedores aumentará, si la empresa no posee un esquema de crecimiento óptimo puede llevar a degradaciones en el servicio o altos niveles de *jitter*.[20]

Infraestructura como servicio

La infraestructura como servicio, también llamado en algunos casos *hardware as* a *service, HaaS,* se encuentra en la capa inferior y es un medio de entregar almacenamiento básico y capacidades de cómputo como servicios estandarizados en la red. Servidores, sistemas de almacenamiento, conexiones, enrutadores, y otros sistemas se concentran (por ejemplo a través de la tecnología de virtualización), para manejar tipos específicos de cargas de trabajo desde el procesamiento en lotes ("*batch*") hasta aumento de servidor/almacenamiento durante las cargas pico. El ejemplo comercial mejor conocido es Amazon Web *Services*[21], cuyos servicios EC2 y S3 ofrecen cómputo y servicios de almacenamiento esenciales (respectivamente). Otro ejemplo es *Joyent,* cuyo producto principal es una línea de servidores virtualizados, que proveen una infraestructura en-demanda altamente escalable para manejar sitios *Web*, incluyendo aplicaciones *Web* complejas escritas en *Python, Ruby, PHP, y Java*.

[19] Hypertext Transfer Protocol Secure (HTTPS) es un protocolo de comunicaciones para la comunicación segura a través de una red informática, con especial despliegue en toda la Internet.
[20] El jitter suele considerarse como una señal de ruido no deseada. En general se denomina jitter a un cambio indeseado y abrupto de la propiedad de una señal.
[21] un conjunto completo de servicios de infraestructuras y aplicaciones que le permiten ejecutar prácticamente todo en la nube, desde aplicaciones empresariales y proyectos de grandes datos hasta juegos sociales y aplicaciones móviles.

Tipos de nubes

- Una nube pública es una nube computacional mantenida y gestionada por terceras personas no vinculadas con la organización. En este tipo de nubes tanto los datos como los procesos de varios clientes se mezclan en los servidores, sistemas de almacenamiento y otras infraestructuras de la nube. Los usuarios finales de la nube no conocen que trabajos de otros clientes pueden estar corriendo en el mismo servidor, red, sistemas de almacenamiento, etc. Aplicaciones, almacenamiento y otros recursos están disponibles al público a través del proveedor de servicios que es propietario de toda la infraestructura en sus centros de datos; el acceso a los servicios sólo se ofrece de manera remota, normalmente a través de Internet.
- Las nubes privadas son una buena opción para las compañías que necesitan alta protección de datos y ediciones a nivel de servicio. Las nubes privadas están en una infraestructura en demanda manejada por un solo cliente que controla qué aplicaciones debe correr y dónde. Son propietarios del servidor, red, y disco y pueden decidir qué usuarios están autorizados a utilizar la infraestructura.
- Las nubes híbridas combinan los modelos de nubes públicas y privadas. Usted es propietario de unas partes y comparte otras, aunque de una manera controlada. Las nubes híbridas ofrecen la promesa del escalado aprovisionada externamente, en-demanda, pero añaden la complejidad de determinar cómo distribuir las aplicaciones a través de estos ambientes diferentes. Las empresas pueden sentir cierta atracción por la promesa de una nube híbrida, pero esta opción, al menos inicialmente, estará probablemente reservada a aplicaciones simples sin condicionantes, que no requieran de ninguna sincronización o necesiten bases de datos complejas.

Una base de datos en la nube, es una base de datos que se ejecuta en la nube. Hay dos modelos de implementación: los usuarios pueden ejecutar la base de datos en la nube de forma independiente, utilizando una imagen de máquina virtual, o pueden comprar el acceso a un servicio de base de datos, gestionada por un proveedor de base de datos en nube. De las bases de datos disponibles en la nube, algunas son basadas en *SQL*[22] y algunos utilizan un modelo de datos *NoSQL*.

Existen dos métodos principales para ejecutar una base de datos en la nube:

- Imagen de máquina virtual: Las plataformas en la nube permiten a los usuarios comprar instancias de máquinas virtuales por un tiempo limitado. Es posible ejecutar una base de datos en estas máquinas virtuales. Los usuarios pueden subir su imagen propia con una base de datos instalada en ella, o utilizar imágenes prefabricadas de máquinas que ya incluyen una instalación optimizada de una base de datos. Por ejemplo Oracle provee una imagen prefabricada con una instalación de *Oracle Database 11g Enterprise Edition on Amazon EC2*[23].
- Base de datos como servicio: Algunas plataformas en la nube ofrecen opciones para el uso de bases de datos como servicio, sin lanzar físicamente una instancia de máquina virtual para la base de datos. En esta configuración, los propietarios de aplicaciones no tienen que instalar y mantener la base de datos por su cuenta. En cambio, el proveedor de servicios de base de datos se encarga de la instalación y el mantenimiento de la base de datos, y los propietarios de aplicaciones pagan de acuerdo a su uso. Por ejemplo, Amazon Web Services, provee dos servicios de base de datos como parte de su oferta en la nube, Simple DB que almacena pares llave-valor en formato *NoSql y Amazon*

[22] El lenguaje de consulta estructurado o *SQL* (por sus siglas en inglés *Structured Query Language* ,es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ellas. Una de sus características es el manejo del álgebra y el cálculo relacional que permiten efectuar consultas con el fin de recuperar de forma sencilla información de interés de bases de datos, así como hacer cambios en ella.

[23] Amazon Elastic Compute Cloud (Amazon EC2) es una parte central de la plataforma de cómputo en la nube de la empresa Amazon.com

Relational Database Service que está basado en *SQL* con una interfaz *MySql.*

- Una tercera opción, es administrar el alojamiento de una base de datos en la nube, donde la base de datos no se ofrece como un servicio, pero el proveedor de la nube aloja la base de datos y administra en nombre del propietario de la aplicación. Por ejemplo, el servicio en la nube de *Rackspace* ofrece alojamiento gestionado para bases de datos *MySQL*[24].

La mayoría de los servicios de bases de datos ofrecen consolas web, que el usuario final puede utilizar para aprovisionar y configurar las instancias de la base de datos. Por ejemplo, la consola web de Amazon Web Services permite a los usuarios lanzar instancias de bases de datos, crear instantáneas (similar a las copias de seguridad) de bases de datos y realizar un seguimiento de las estadísticas de la base de datos.

Los servicios de las bases de datos consisten en un componente de administración que controla las instancias de cada base de datos subyacente utilizando una *API*[25] de servicios, la cual se expone al usuario final, y permite a los usuarios realizar operaciones de mantenimiento y ampliar sus instancias de la base de datos. Por ejemplo, el servicio de *Amazon Relational Database,* provee una *API* que permite crear una instancia de una base de datos, modificar los recursos disponibles de cada instancia, eliminar una instancia, la creación de una instantánea (similar a una copia de seguridad) de una base de datos y restauración de una base de datos a partir de una instantánea.

Los servicios de las bases de datos mantienen la pila del software subyacente, transparente al usuario la pila, normalmente incluye el sistema operativo, base de datos y el software de terceros utilizado por la base de datos. El proveedor de servicios, es responsable de la instalación, parches y actualización de la pila de software subyacente.

---

[24] *MySQL* es un sistema de gestión de bases de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones.

[25] Interfaz de programación de aplicaciones (IPA) o *API* (del inglés *Application Programming Interface).*

Los servicios de las bases de datos cuidan la escalabilidad y la alta disponibilidad de éstos. Características de escalabilidad difieren entre los proveedores - algunos ofrecen auto-escala, mientras que otros permiten al usuario ampliar mediante una API, pero no escalar automáticamente. Normalmente hay un compromiso para un cierto nivel de alta disponibilidad (por ejemplo, 99,9% o 99,99%).

Modelo de datos

También es importante diferenciar entre bases de datos en la nube que son relacionales en oposición a las no relacionales (*NoSQL*):

• Bases de datos SQL, son un tipo de base de datos que se puede ejecutar en la nube (ya sea como una imagen de máquina virtual o como un servicio, dependiendo del proveedor). Las bases de datos SQL poseen baja escalabilidad, ya que no fueron nativamente diseñadas para entornos en la nube, aunque los servicios en la nube de base de datos basado en SQL están tratando de hacer frente a este desafío.

• Bases de datos *NoSQL*, son otro tipo de base de datos que puede ejecutarse en la nube. Las bases de datos *NoSQL* están diseñados para servir cargas pesadas de lecto-escritura y son capaces de escalar hacia arriba y hacia abajo con facilidad. Y por lo tanto son más adecuadas para funcionar de forma nativa en la nube. Sin embargo, la mayoría de las aplicaciones actuales se construyen en torno a un modelo de datos SQL, así que trabajar con bases de datos NoSQL con frecuencia requiere una reescritura completa del código de la aplicación.

Cabe señalar que el tratamiento de datos personales en el denominado cómputo en la nube se encuentra contenido en el artículo 52 del reglamento de la ley en estudio.

> **Artículo 52.** Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en la nube, en los que el responsable se adhiera a los mismos mediante

> condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:
> **I.** Cumpla, al menos, con lo siguiente:
> **a)** Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el presente Reglamento;
> **b)** Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio;
> **c)** Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y
> **d)** Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio, y
> **II.** Cuente con mecanismos, al menos, para:
> **a)** Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta;
> **b)** Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio;
> **c)** Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio;
> **d)** Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y
> **e)** Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable.
> En cualquier caso, el responsable no podrá adherirse a servicios que no garanticen la debida protección de los datos personales.
> Para fines del presente Reglamento, por cómputo en la nube se entenderá al modelo de provisión externa de servicios de cómputo bajo demanda, que implica el suministro de infraestructura, plataforma o software, que se distribuyen de modo flexible, mediante procedimientos de virtualización, en recursos compartidos dinámicamente.
> Las dependencias reguladoras, en el ámbito de sus competencias, en coadyuvancia con el Instituto, emitirán criterios para el debido tratamiento de datos personales en el denominado cómputo en la nube."

Tal y como señala el artículo anterior el computo en el computo en la nube se tienen que acatar las medidas de seguridad establecidas por la ley y observar aún más la seguridad en este tipo de base de datos, además tampoco violan los derechos ARCO para el titular de los datos personales.

En lo particular con el avance de las tecnologías este método en un futuro próximo será la base de datos de las empresas ya que proporcionan un servicio rápido y eficáz y con las medidas de seguridad adecuadas proporcionaran un servicio de difícil sustracción de información.

2.3.- Datos personales.

En la actualidad, la tecnología ha llegado a niveles que hace unos diez años, no se imaginaba o se consideraba un cambio muy lejano, a la vez, en la actualidad el avance de la era de las comunicaciones, el manejo e intercambio de datos y la utilización de *software* en la vida diaria, se ha convertido en una práctica habitual, tanto para la personas comunes, como para el sector público y para las empresas, las cuales los utilizan para el desarrollo de sus actividades cotidianas, tales como:

- Venta de bienes (libros, automóviles, casas, electrodomésticos, etc).
- Contratación de servicios (de telecomunicaciones, prestación de servicios análisis clínicos, un seguro de vida o la inscripción a una escuela).
- Oferta de empleo (al presentar el currículum o llenar una solicitud laboral)
- Aspectos bancarios y bursátiles (trasferencias, pagos, cotizaciones, negociaciones etc).
- Comunicación (a través de las redes sociales*, Facebook, twiter, hi5*, etc)
- Otros (Ideología, afiliación política, religión, origen étnico, preferencia sexual, etc...)

El artículo 16 de nuestra Constitución, así como varias legislaciones en nuestro país, reconoce ya el derecho fundamental a que los datos personales sean protegidos. Y por ello, todas las personas físicas o morales que cuenten con bases de datos (escuelas, hospitales, médicos, aseguradoras, empresas, etc.,),

están obligadas a seguir ciertas reglas que garanticen su uso adecuado y seguro.

Por ello para tener un mayor entendimiento del tema tenemos que definir que es un Dato, del "latín *datum*: lo que se da. S XVIII - Referencia, informe[26]" y con ello podemos decir que es una representación simbólica (numérica, alfabética, algorítmica, etc), que nos proporciona un atributo o característica de identificación. Los datos describen hechos empíricos, sucesos y entidades, pero un dato en si no constituye información específica, es el procesamiento sistematizado de los datos, lo que nos proporciona información o entendimiento. En términos de tecnología computacional se podría definir como cualquier Información que una computadora registra y almacena[27]; por ello de acuerdo a la unión de estos elementos podríamos decir que es cualquier elemento que se proporcione ya sea a nivel técnico o cibernético que nos proporcione algún tipo de información detallada para ser analizada.

Y a su vez al definir Persona: se deriva del latín, mascara de actor, de *per*: a través, y *sonare*: sonar s. XII- individuo hombre o mujer[28], al unir diremos que es aquella referencia de la persona hombre o mujer, en un sentido general.

En estricto sentido se diría que los datos personales son cualquier información concerniente a una persona física identificada o identificable, tal y como nos lo señala el artículo 3° de la ley de la materia; con esto podemos concluir que se consideran datos personales a aquellos que son los inherentes a una persona, que sólo a esta le corresponden, tales como:

Nombre y apellidos (filiación). estado civil (soltero, casado, viudo o separado, etc.). domicilio (tipos de domicilio legal convencional fiscal etc.), datos bancarios (número de cuenta; hipoteca, préstamos, etc., así como su cuantía); creencias religiosas, Ideas políticas (a no ser que se declaren voluntariamente),

26 CORRIPIO Fernando, Diccionario Etimológico General de la Lengua Castellana, Editorial BRUGUERA, Segunda edición, septiembre de 1977, España.

27 Op. cit

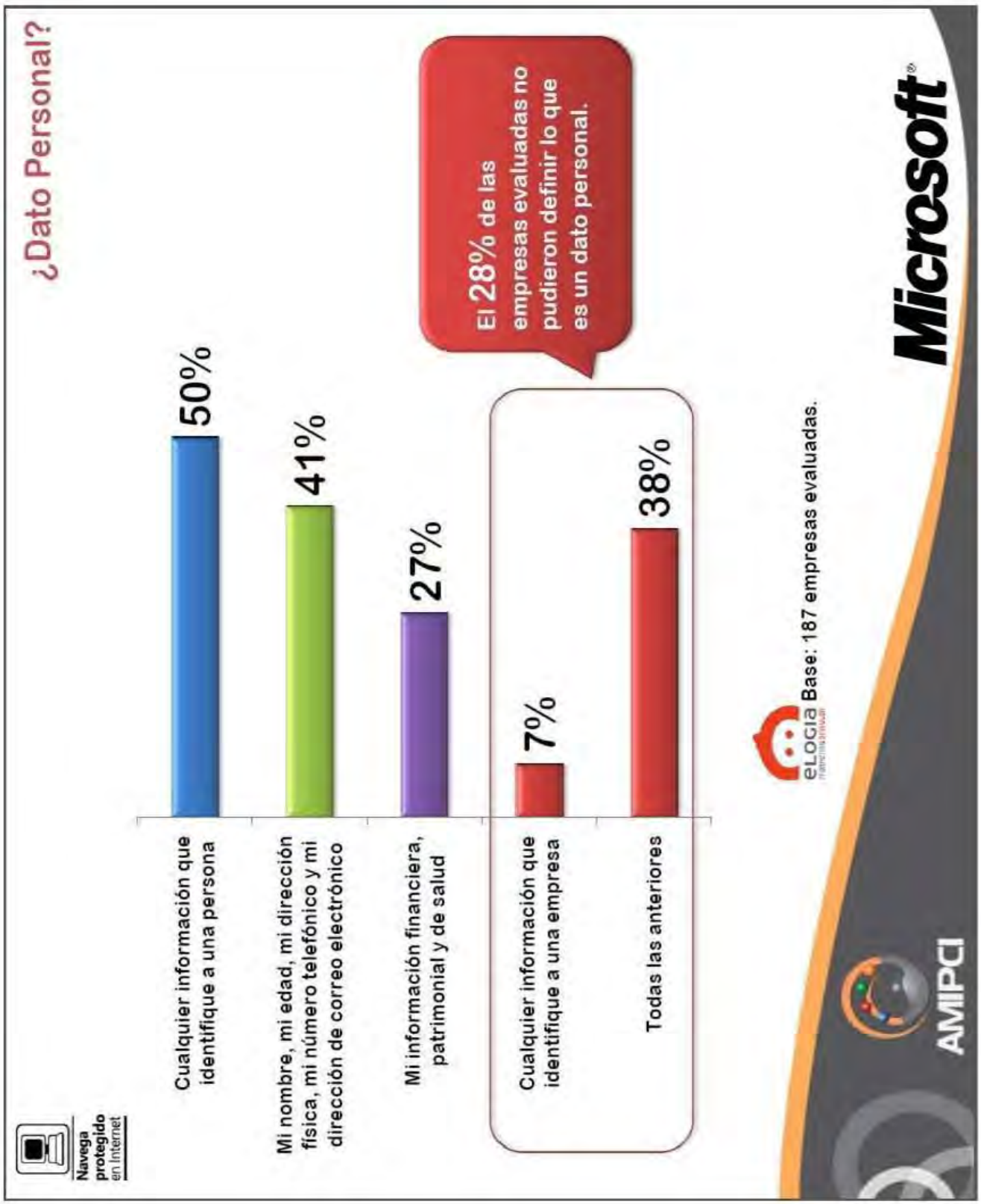
28 Ibídem, CORRIPIO Fernando.

orientación sexual (de la índole que sea); datos laborales (cargo: si no es público; ingresos fijos o por cheques regalo, etc.); informes médicos (radiografías, análisis, etc.), derecho a la propia imagen (excepto si se cede).

El *blog* del **INSTITUTO FEDERAL DE ACCESO A LA INFORMACION Y PROTECCION DE DATOS**, nos proporciona el siguiente concepto de datos personales "Es cualquier información relacionada contigo, por ejemplo, tu nombre, teléfono, domicilio, fotografía o huellas dactilares, así como cualquier otro dato que pueda servir para identificarte. Este tipo de datos te permiten además, interactuar con otras personas, o con una o más organizaciones, así como que puedas ser sujeto de derechos[29] **"**.

29 http://blog.derecho-informatico.org/faqs/datos-personales/ 23 08/12 23:33

Esta imagen nos hace referencia sobre una encuesta realizada por AMIPCI y dándonos a denotar la falta de conocimiento sobre la materia..



2.3.1.- Clasificación de los datos personales.

Conocido lo que es un dato personal, es conveniente señalar en este punto que, legalmente, hay varios tipos de datos personales, y la clasificación se puede llevar a cabo según dos criterios:

- Según su importancia.
- Según su seguridad.

El primer criterio (según su importancia), clasifica a los datos personales en función de la relación que tienen esos datos con el derecho a la intimidad. Hay datos personales especialmente protegidos o también llamados "Datos personales sensibles, que la ley en L.F.P.D.P.P.P nos define como: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas preferencia sexual. ".

La relación de cuáles son esos datos sensibles, está en el artículo 3 de la ley L.F.P.D.P.P.P. Son precisamente a los que nos referíamos hace un instante, es decir, son los datos que tienen mayor relación con los aspectos más importantes del derecho a la intimidad. Para diferenciarlos, se puede decir que los "datos personales" son toda aquella información básica que no están especialmente protegidos. Y "datos personales SENSIBLES" son los referidos a la ideología, religión, creencias, afiliación sindical, salud, vida sexual, origen racial o étnico y comisión de infracciones penales o administrativas y que su mala utilización dañaría la moralidad del titular.

El segundo criterio de clasificación de los datos personales (según su seguridad), está basado en las medidas de seguridad que se deben cumplir cuando se posea datos personales.

Estas medidas de seguridad se encuentran previstas en el articulo 19 de la L.F.P.D.P.P.P. y se deben desarrollar medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, medidas las cuales se desarrollarán posteriormente realizando una exposición más detenida, porque tiene una gran importancia práctica.

Otras formas de clasificación son las siguientes:

Datos de nivel básico: Son aquellos datos personales que no se clasifiquen como de nivel medio atenuado, de nivel medio o de nivel alto. Datos de nivel medio atenuado: aquellos datos personales que permitan obtener una evaluación de la personalidad de individuo.

Datos de nivel medio: Aquellos datos personales relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y prestación de servicios de información sobre solvencia patrimonial y crédito.

Datos de nivel alto: Aquellos datos personales relativos a la ideología, religión, creencias, origen racial, salud, vida sexual y datos recabados para fines policiales sin consentimiento del interesado.

Es importante saber que los datos personales están altamente protegidos por la Ley. La utilización, no ya abusiva o fraudulenta, sino incluso negligente, de dichos datos, es sancionable administrativamente con importantes multas y otro tipo de sanciones y está castigada como delito.

A su vez también se encuentra de acuerdo a la denominación que a través de la lectura de una serie de avisos de privacidad en el Distrito Federal la siguiente clasificación:

Datos de identificación y contacto

Nombre
Estado Civil
Registro Federal de Contribuyentes(RFC)
Clave única de Registro de Población (CURP)
Lugar de nacimiento
Fecha de nacimiento
Nacionalidad
Domicilio
Teléfono particular
Teléfono celular
Correo electrónico
Firma autógrafa
Firma electrónica
Edad
Fotografía

Datos sobre características físicas

Color de la piel
Color del iris
Color del cabello
Señas particulares
Estatura
Peso
Cicatrices
Tipo de sangre

Datos biométricos

Imagen del iris

Huella dactilar

Palma de la mano

Datos laborales

Puesto o cargo que desempeña

Domicilio de trabajo

Correo electrónico institucional

Teléfono institucional

Referencias laborales

Información generada durante los procesos de reclutamiento, selección y Contratación

Capacitación laboral

Datos académicos

Trayectoria educativa

Títulos

Cédula profesional

Certificados

Reconocimientos

Datos migratorios

Entradas al país

Salidas del país

Tiempo de permanencia en el país

Calidad migratoria

Derechos de residencia

Aseguramiento

Repatriación

Datos patrimoniales y/o financieros

Bienes muebles

Bienes inmuebles

Información fiscal

Historial crediticio

Ingresos

Egresos

Cuentas bancarias

Número de tarjetas de crédito

Seguros

Afores

Datos sobre pasatiempos, entretenimiento y diversión

Pasatiempos

Aficiones

Deportes que practica

Juegos de su interés

2.3.2.- datos personales sensibles

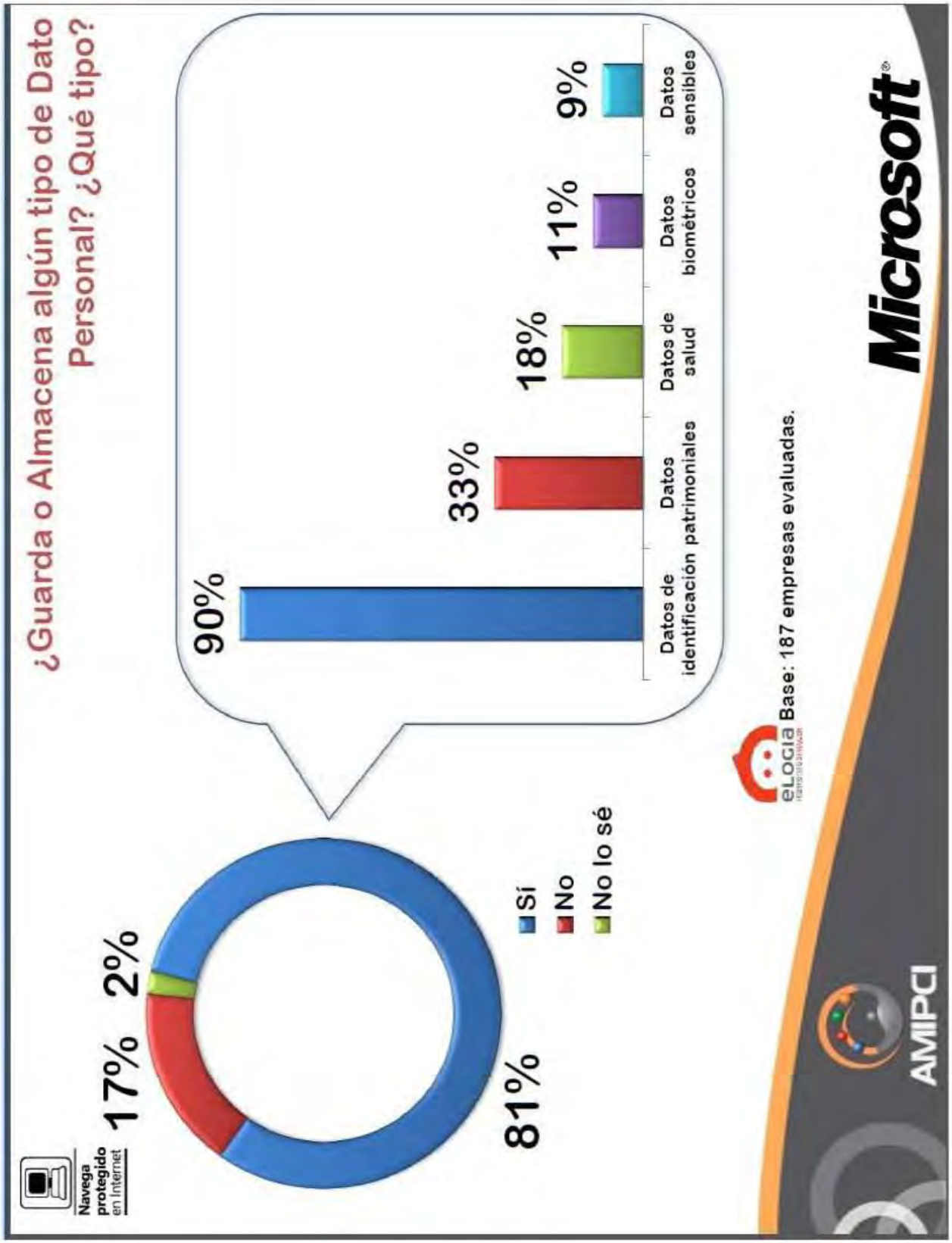
Como ya se ha definido con anterioridad este tipo de datos son aquellos que, de divulgarse de manera indebida, afectarían la esfera más íntima del ser humano. Ejemplos de este tipo de datos son: el origen racial o étnico, el estado de salud, la información genética, las creencias religiosas, filosóficas y morales, la afiliación sindical, las opiniones políticas y las preferencias sexuales. Estos datos requieren mayor protección y la Ley establece un tratamiento especial, que se encuentra contemplado en el artículo noveno:

> **Artículo 9.** Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.
>
> No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para

finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado.

La siguiente imagen nos refiere, a que en la actualidad en nuestra información genética se pueden encontrar datos personales sensibles que pueden vulnerar al titular de estos en su persona o esfera social, entre otras.

Esta imagen nos hace referencia la encuesta realizada por AMIPCI y a las empresas que tipo de datos recaban.



2.4.- DERECHOS ARCO

Derechos ARCO: derechos de Acceso, Rectificación, Cancelación y Oposición.

2.4.1 Derecho de Acceso

El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos.

- Justificación: no es necesaria, salvo si se ha ejercitado el derecho en los últimos doce meses.
- Plazos: El responsable del fichero resolverá sobre la solicitud de acceso en el plazo máximo de un mes a contar desde la recepción de la solicitud. El acceso podrá hacerse efectivo durante 10 días hábiles tras la comunicación de la resolución.
- Denegación: Son motivos de denegación que el derecho ya se haya ejercitado en los doce meses anteriores a la solicitud (salvo que se acredite un interés legítimo al efecto) y que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de sus datos.

2.4.2 Derecho de Rectificación

Derecho del afectado a que se modifiquen los datos que resulten ser inexactos o incompletos.

- Justificación: debe indicarse a qué datos se refiere y la corrección que haya de realizarse aportando documentación.
- Plazo: 10 días hábiles.

- Denegación: debe motivarse y procede indicar que cabe invocar la tutela de la AEPD.

2.4.3 Derecho de Cancelación

Derecho del afectado a que se supriman los datos que resulten ser inadecuados o excesivos.

- Justificación: debe indicarse el dato a cancelar y la causa que lo justifica, aportando documentación.
- Plazo: 10 días hábiles.
- Denegación: debe motivarse y procede indicar que cabe invocar la tutela de la AEPD. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado, que justificaron el tratamiento de los datos.

4.4.4 Derecho de Oposición

Derecho del afectado a que no se lleve a cabo el tratamiento de sus datos de carácter personal o se cese en el mismo en los supuestos en que no sea necesario su consentimiento para el tratamiento, que se trata de ficheros de prospección comercial o que tengan la finalidad de adoptar decisiones referidas al interesado y basadas únicamente en el tiraje automatizado de sus datos.

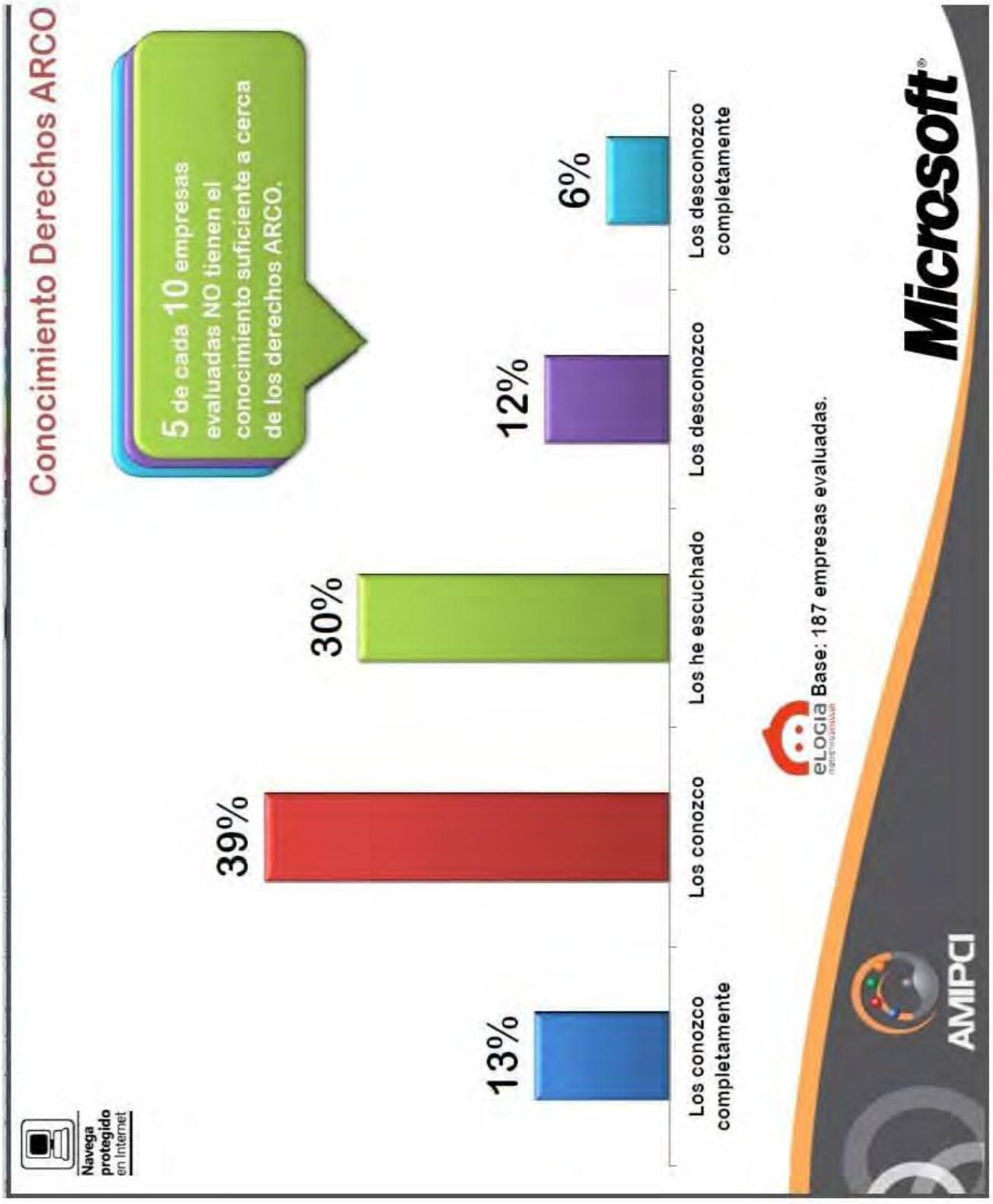
- Justificación: concurrencia de motivos fundados y legítimos relativos a su concreta situación personal.
- Plazo : 10 días hábiles.
- Denegación: debe motivarse e indicar que cabe invocar la tutela de la AEPD.

Exclusivamente en los siguientes casos puede la empresa negarse total o parcialmente a ejercitar los derechos ARCO:

- Cuando el solicitante no sea el titular de los datos personales, o el representante no esté debidamente acreditado.
- Cuando la persona física o empresa no tenga en su posesión los datos personales.
- Cuando se lesionen datos personales de un tercero.
- Cuando exista algún impedimento legal o resolución de autoridad competente que restrinja el ejercicio de alguno de los derechos ARCO.
- Cuando la rectificación, cancelación y oposición solicitada haya sido previamente realizada.

La empresa deberá comunicar y justificar cuando se actualice alguno de los anteriores supuestos y no pueda llevar a cabo la acción que le fue solicitada.

Esta imagen nos hace referencia la encuesta realizada por AMIPCI y si los usuarios conocen los Derechos ARCO.



2.5.-Principios de los datos personales.

Los principios de protección de datos, pueden definirse como una serie de reglas mínimas que deben observar las empresas o entes privados que tratan datos personales (personas físicas o morales), garantizando con ello un uso adecuado de la información personal. Estos principios son: licitud, consentimiento, calidad, información, proporcionalidad y responsabilidad.

Principio de Licitud - Se refiere al compromiso que deben asumir los entes privados (personas físicas o morales), que traten tu información cuando solicitas la prestación de un bien o servicio, respetando en todo momento la confianza que depositas en ellos para el buen uso que le darán a los datos.

Principio de Consentimiento - Al ser tú el dueño de los datos, este principio te permite decidir de manera informada, libre, inequívoca y específica, si quieres compartir tu información con otras personas. Para las empresas que la posean, implica el deber de solicitar tu autorización o consentimiento para que pueda tratar la información que te concierne, sobre todo cuando se trata de datos sensibles que afectan tu esfera más íntima. La Ley exige a las empresas soliciten tu consentimiento de manera expresa y por escrito. Adicionalmente,

deberán implementar medidas de seguridad muy estrictas que eviten quebrantar la confidencialidad, integridad y disponibilidad de esos datos.

Principio de Calidad - Los datos personales en posesión de empresas deben estar actualizados y reflejar con veracidad la realidad de la información, de tal manera que cualquier inexactitud no te afecte. Asimismo, implica que el tiempo que esa empresa conserve tus datos no debe exceder más allá de lo necesario, para el cumplimiento de los fines que justificaron su tratamiento. Cuando se cumpla íntegramente la finalidad para la cual se proporcionaron los datos, el tratamiento deja de ser necesario y, por lo tanto, las empresas deben cancelarlos.

Principio de Información - Se refiere a la potestad que te otorga la Ley de conocer previamente las características esenciales del tratamiento a que serán sometidos los datos personales que proporciones a un ente privado o empresa. En un lenguaje comprensible, las empresas y las personas físicas deben dar a conocer esas características a través del "Aviso de Privacidad".

Principio de Proporcionalidad - Las empresas sólo podrán recabar los datos estrictamente necesarios e indispensables para la finalidad que se persigue y que justifica su tratamiento.

Principio de Responsabilidad - Quienes traten datos personales deben asegurar que ya sea dentro o fuera de nuestro país, se cumpla con los principios esenciales de protección de datos personales, comprometiéndose a velar siempre por el cumplimiento de estos principios y a rendir cuentas en caso de incumplimiento[30].

30 Op cit http://blog.derecho-informatico.org/faqs/datos-personales/ 23 08/12 23:33

2.6.- De la seguridad de los datos personales.

Cabe señalar, que la seguridad de los datos personales debe resguardarse mediante los mecanismos suficientes para una verdadera protección, como ya se mencionó con anterioridad en el cuerpo de este trabajo la seguridad debe ser primordial, por ello se toman en cuenta los siguientes tipos.

Física, allegándose de todos los elementos necesarios para proteger el resguardo de los datos, aunque se puede pensar que los datos pueden ser sustraídos por Hackers o dañados por virus, pero la seguridad de estos será nula si no se ha previsto como combatir un incendio o algún otro desastre, ya sea causado por el hombre o la naturaleza.

La Seguridad Física, la definimos como la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial"[31]. Son los controles, mecanismos de seguridad y procedimientos dentro y alrededor para la protección de la base de datos, así como los medios de acceso remoto al y desde el mismo; implementados para la protección de hardwares y medios de almacenamiento de datos.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas, tanto por el hombre como por la naturaleza del medio físico en que se encuentran ubicados la información de los titulares, también se debe tomar en cuenta que tipo de edificación se tiene para saber que tipo de protección se debe utilizar y en que ecosistema nos encontramos.

Las principales amenazas que se prevén en la seguridad física son: desastres naturales, incendios accidentales tormentas e inundaciones, así como

---

[31] *HUERTA, Antonio Villalón. "Seguridad en Unix y Redes". Versión 1.2 Digital - Open Publication License v.10 o Later. 2 de Octubre de 2000. http://www.kriptopolis.org*

Amenazas ocasionadas por el hombre, Disturbios, sabotajes internos y externos deliberados.

Cabe señalar que tan simple como recurrir al sentido común, para darse cuenta que cerrar una puerta con llave o cortar la electricidad en ciertas áreas siguen siendo técnicas válidas en cualquier entorno.

Tecnica, en esta seguridad podremos señalar como peligros mas latentes el robo o la sustracción electrónica de la base de datos, tomando medidas como el de capacitar personal especialista tales como, técnicos, programadores o simplemente adquirir una licencia de uso de algún antivirus, o la implementación de claves para el acceso a equipos de computo.

Administrativa, podemos basarla en políticas y normas que se deben de implantar y seguir. Las políticas proporcionan las reglas que gobiernan el cómo deberían ser configurados los sistemas y cómo deberían actuar los empleados de una organización en circunstancias normales y cómo deberían reaccionar si se presentan circunstancias inusuales. Define lo que debería de ser la seguridad dentro de la organización y pone a todos en la misma situación, de modo que todo el mundo entienda lo que se espera de ellos, tales como seguridad privada o veladores, así como podemos señalar que otra persona encargada del resguardo y protección y que podemos señalar en este punto es el responsable o la persona que trata los datos, señalando como posible protección el punto de acceso a dicha información.

Jurídica, esta seguridad no va encaminada a un principio del derecho, en este caso la definimos como aquella protección que se hará allegándose de los instrumentos jurídicos necesarios para los sujetos que surgen con esta relación jurídica. Se considera como un elemento jurídico que contempla la ley al aviso de privacidad, porque con este, tanto el responsable como el titular, están teniendo la confianza de que ambos estarán de acuerdo con el tratamiento en general de los datos.

CAPÍTULO III

CONTENIDO DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES.

3.1.- Aviso de Privacidad.

Es aquel "Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales, de conformidad con el artículo 15 de la presente Ley".

Con dicho documento se pretende contestar las siguientes preguntas.

1. Quién recopila los datos?
2. Qué datos recopila (sensibles o no);
3. Con qué finalidad los recopila;
4. Cómo limitar su uso o divulgación;
5. Cómo revocar su uso;
6. Cuál es el procedimiento que tiene el titular para ejercer sus derechos de acceso, rectificación, corrección y oposición (mejor conocidos como Derechos ARCO):
7. La forma en la que se comunican cambios al Aviso de Privacidad; y
8. La aceptación o negativa para autorizar la transferencia de datos a terceros.

El aviso de privacidad, pretende que la persona tratante de datos informe al titular de los datos personales todo lo que le acontece a dicha información, por ello es una declaración que informa al titular de los datos personales>

- quién recaba (responsable),
- qué recaba (información que se recaba)

- para qué recaba (las finalidades del tratamiento)
- cómo limitar el alcance (uso o divulgación)
- cómo revocar consentimiento
- cómo ejercer derechos ARCO (medios)
- cómo comunica cambios al aviso (procedimiento y medio) [32]

Por Ley, el Aviso de Privacidad debió ponerse a disposición de los interesados (hacerse público y difundirse) desde el 6 de julio de 2011, tal y como lo señala el Transitorio Tercero de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (*publicación 6 de julio de 2010*).

Las modalidades del Aviso de Privacidad

Aviso de Privacidad completo

Este aviso deberá incluir todos los elementos informativos citados en el apartado anterior (artículos 8, 15, 16 y 36 de la Ley).

Esta modalidad de aviso deberá incluir, al menos, la información que refiere a identidad y domicilio del responsable y las finalidades del tratamiento (artículo 17 de la Ley). Asimismo, este aviso deberá proveer los mecanismos para que el titular conozca el aviso de privacidad completo.

Un ejemplo de un aviso de privacidad:

AVISO PRIVACIDAD.

ASOCIACION PROMOURB A.C., representado por el Arq. Manuel Zarate Sánchez , con domicilio en calle Rosas MZ 04 LT 16, colonia las flores, ciudad México, municipio Tecámac, C.P. 55760, Estado de

32 GUÍA PRÁCTICA PARA GENERAR EL AVISO DE PRIVACIDAD IFAI.

México , señalando como e-mail zaquisa2010@hotmail.com , es el responsable del uso y protección de sus datos personales, y al respecto le informamos lo siguiente:

¿Para qué fines utilizaremos sus datos personales?

Los datos personales que recabamos de usted, los utilizaremos para las siguientes finalidades, que son necesarias para el servicio que solicita:

Elaboración de documentación

Llamadas telefónicas urgentes

De manera adicional, utilizaremos su información personal para las siguientes finalidades secundarias que no son necesarias para el servicio solicitado, pero que nos permiten y facilitan brindarle una mejor atención:

Prospección comercial

En caso de que no desee que sus datos personales se utilicen para estos fines secundarios, indíquelo a continuación:

No consiento que mis datos personales se utilicen para los siguientes fines:

[ ] Prospección comercial

La negativa para el uso de sus datos personales para estas finalidades no podrá ser un motivo para que le neguemos los servicios y productos que solicita o contrata con nosotros.

¿Qué datos personales utilizaremos para estos fines?

Para llevar a cabo las finalidades descritas en el presente aviso de privacidad, utilizaremos los siguientes datos personales:

Nombre

Estado Civil

Registro Federal de Contribuyentes (RFC)

Clave única de Registro de Población (CURP)

Lugar de nacimiento

Fecha de nacimiento

Nacionalidad

Domicilio

Teléfono particular

Teléfono celular

Correo electrónico

Firma autógrafa

Edad

Puesto o cargo que desempeña

Trayectoria educativa

Calidad migratoria

¿Cómo puede acceder, rectificar o cancelar sus datos personales, u oponerse a su uso?

Usted tiene derecho a conocer qué datos personales tenemos de usted, para qué los utilizamos y las condiciones del uso que les damos (Acceso). Asimismo, es su derecho solicitar la corrección de su información personal en caso de que esté desactualizada, sea inexacta o incompleta (Rectificación); que la eliminemos de nuestros registros o bases de datos cuando considere que la misma no está siendo utilizada adecuadamente (Cancelación); así como oponerse al uso de sus datos personales para fines específicos (Oposición). Estos derechos se conocen como derechos ARCO.

Para el ejercicio de cualquiera de los derechos ARCO, usted deberá presentar la solicitud respectiva por escrito, mediante correo electrónico o directamente en las oficinas.

Con relación al procedimiento y requisitos para el ejercicio de sus derechos ARCO, le informamos lo siguiente:

a) ¿A través de qué medios pueden acreditar su identidad el titular y, en su caso, su representante, así como la personalidad este último?

“IFE, licencia manejo o pasaporte”

b) ¿Qué información y/o documentación deberá contener la solicitud?

Nombre, dirección y el derecho que se pretende modificar.

c) ¿En cuántos días le daremos respuesta a su solicitud?

20 días hábiles

d) ¿Por qué medio le comunicaremos la respuesta a su solicitud?

Vía E-mail o por escrito en la dirección señalada para oír y recibir notificaciones.

e) ¿En qué medios se pueden reproducir los datos personales que, en su caso, solicite?

CD ROM.

Los datos de contacto de la persona o departamento de datos personales, que está a cargo de dar trámite a las solicitudes de derechos ARCO, son los siguientes:

a) Nombre de la persona o departamento de datos personales: Cinthia Lucero Téllez Vallejo

b) Domicilio: calle Rosas MZ 04 LT 16, colonia Las flores, ciudad México, municipio o delegación Tecámac, C.P. 55760, en la entidad de México, país México.

c) Correo electrónico: lucero0072000@gmail.com

d) Número telefónico: 5559351456 y 5536202919

Usted puede revocar su consentimiento para el uso de sus datos personales

Usted puede revocar el consentimiento que, en su caso, nos haya otorgado para el tratamiento de sus datos personales. Sin embargo, es importante que tenga en cuenta que no en todos los casos podremos atender su solicitud o concluir el uso de forma inmediata, ya que es posible que por alguna obligación legal requiramos seguir tratando sus datos personales. Asimismo, usted deberá considerar

que para ciertos fines, la revocación de su consentimiento implicará que no le podamos seguir prestando el servicio que nos solicitó, o la conclusión de su relación con nosotros.

Para revocar su consentimiento deberá presentar su solicitud a través del siguiente medio:

Escrito en oficinas o e-mail

Con relación al procedimiento y requisitos para la revocación de su consentimiento, le informamos lo siguiente:

a) ¿A través de qué medios pueden acreditar su identidad el titular y, en su caso, su representante, así como la personalidad este último?

IFE, licencia de manejo, pasaporte.

b) ¿Qué información y/o documentación deberá contener la solicitud?

Documento identificación y asunto.

c) ¿En cuántos días le daremos respuesta a su solicitud?

20 días hábiles.

d) ¿Por qué medio le comunicaremos la respuesta a su solicitud?

Vía e-mail o por escrito en la dirección señalada para oír y recibir notificaciones.

¿Cómo puede limitar el uso o divulgación de su información personal?

Con objeto de que usted pueda limitar el uso y divulgación de su información personal, le ofrecemos los siguientes medios:

E- mail y oficina.

De manera adicional, le informamos que contamos con los siguientes listados de exclusión, en los cuales podrá registrarse para que sus datos personales no sean tratados para ciertos fines:

Nombre del listado Finalidad para las que aplica Medio para obtener mayor información

Lista de afiliados, número de afiliados y oficinas

El uso de tecnologías de rastreo en nuestro portal de internet

Le informamos que en nuestra página de internet utilizamos *cookies*[33], *web beacons* u otras tecnologías, a través de las cuales es posible monitorear su comportamiento como usuario de internet, así como brindarle un mejor servicio y experiencia al navegar en nuestra página. Los datos personales que recabamos a través de estas tecnologías, los utilizaremos para los siguientes fines:

Comerciales

Los datos personales que obtenemos de estas tecnologías de rastreo son los siguientes:

Identificadores, nombre de usuario y contraseñas de una sesión

Idioma preferido por el usuario

Región en la que se encuentra el usuario

[33] cookie (o galleta informática) es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.

Tipo de navegador del usuario

Tipo de sistema operativo del usuario

Fecha y hora del inicio y final de una sesión de un usuario

Estas tecnologías podrán deshabilitarse asistiendo a la oficina.

¿Cómo puede conocer los cambios en este aviso de privacidad?

El presente aviso de privacidad puede sufrir modificaciones, cambios o actualizaciones derivadas de nuevos requerimientos legales; de nuestras propias necesidades por los productos o servicios que ofrecemos; de nuestras prácticas de privacidad; de cambios en nuestro modelo de negocio, o por otras causas.

Nos comprometemos a mantenerlo informado sobre los cambios que pueda sufrir el presente aviso de privacidad, a través de: oficina o vía e mail.

El procedimiento a través del cual se llevarán a cabo las notificaciones sobre cambios o actualizaciones al presente aviso de privacidad es el siguiente:

Escrito

Su consentimiento para el tratamiento de sus datos personales

Consiento que mis datos personales sean tratados de conformidad con los términos y condiciones informados en el presente aviso de privacidad. [ ]

Nombre y firma del titular:

_____

3.2.- Sujetos contemplados en la LFPDPPP.

Todas las personas físicas y morales que recaben datos personales para fines comerciales o de divulgación; entre los negocios que pueden ser identificados como sujetos obligados por esta Ley están, desde los grandes bancos, aseguradoras, telefónicas, medios de comunicación, tiendas departamentales y de autoservicio, laboratorios, inmobiliarias, líneas aéreas, hasta escuelas, tintorerías, médicos, dentistas, talleres mecánicos y pizzerías. Es decir, la legislación contempla a todos aquellos giros que recaban datos personales de sus clientes, sin importar su tamaño. (Comunicado IFAI 30 jun 2011, Diario Reforma)

3.2.1.- "Titular".

La persona física a quien corresponden los datos personales, tal y como lo cita el articuló 3º de la L.F.P.D.P.P.P. También podríamos decir que es aquella persona que tiene un título o documento que la identifica y que, por lo tanto, tiene ciertos derechos y obligaciones. Podemos decir que somos cada uno de nosotros, los usuarios de servicios proporcionados por el responsable, y que en el titular debe caber la cultura de privacidad, ya que es sobre éste donde recae el daño en caso de que su información sea trasmitida a terceros no viables o no facultados por éste, para el tratamiento de sus datos, es quien resulta directamente afectado.

3.2.2.- "Responsable".

Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales; con ello podríamos decir que es aquella persona que se encarga de recabar datos, tratarlos y protegerlos a nombre y representación.

El responsable de los datos personales tiene una serie de facultades de las cuales hablaremos más adelante, pero este sujeto es importante que ponga atención a las actividades que realiza el “encargado” conforme a la ley el

“responsable” es el único sancionado y afectado por ser éste en quien recaen todos los efectos jurídicos.

3.2.3.-. "Encargado”.

La persona física o jurídica que junto con el responsable se encarga del tratamiento de datos personales, como consecuencia de una relación jurídica, esto quiere decir que es aquella persona que se le remite la información del titular de datos.

El encargado debe tener una preparación adecuada para la protección de los datos, dado que el es quien maneja la información y al no hacerlo puede incurrir en errores cuyas consecuencias repercutan en el responsable o el titular.

3.2.4.- "Tercero".

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

El tercero lo podemos definir como aquella persona que no es encargado, responsable o titular, y que puede estar facultado ya sea por un documento firmado y motivado por la autoridad competente, o puede ser reconocido por el titular para que a su vez también se encargue del tratamiento de los datos personales, cambiando su denominación a responsable o encargado según sea el caso.

3.3.- Las obligaciones del "Responsable" en torno al Aviso de Privacidad.

El artículo 15 de la Ley establece que el responsable deberá informar a los titulares de los datos personales la información que recaba de ellos y con qué fines, a través del aviso de privacidad.

Pero no solo el artículo 15 contempla las obligaciones para el responsable, también a lo largo del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Artículo	Obligación
8	Su consentimiento tácito para el tratamiento de sus datos personales, salvo en los casos en los que se requiera el consentimiento expreso.
8	Establecer mecanismos y procedimientos en el aviso de privacidad para que, en cualquier momento, el titular pueda revocar el consentimiento para el tratamiento de sus datos personales.
12	Limitar el tratamiento de los datos personales a las finalidades previstas en el aviso de privacidad.
14	Garantizar que el aviso de privacidad dado a conocer al titular sea respetado, en todo momento, por él o por terceros con los que guarde alguna relación jurídica.
16	Informar en el aviso de privacidad al menos los elementos que establece el artículo 16 de la Ley.
17 y 18	Dar a conocer el aviso de privacidad en los momentos y formas que establecen los artículos 17 y 18 de la Ley.
23	Dar a conocer al titular el aviso de privacidad al que está sujeto el tratamiento de sus datos personales.
36	Comunicar el aviso de privacidad a terceros a quienes transfiera los datos personales.
36	Incluir una cláusula en el aviso de privacidad, que indique si el titular acepta o no la transferencia de sus datos personales.
Tercero transitorio	Expedir los avisos de privacidad a más tardar el 6 de julio de 2011 (un año después de la entrada en vigor de la Ley).

Así pues como ya se estableció con anterioridad, el responsable de los datos personales tiene una serie de obligaciones con respecto del titular, pero que pasaría en caso de que no cumpliese con estas obligaciones, las sanciones se encuentran contenidas en el artículo 63 LFPDPPP,

3.4.- Las obligaciones del "Encargado" según el Aviso de Privacidad.

En el artículo 49 del reglamento de la ley en comento nos señala:

> **“Artículo 49.** El encargado es la persona física o moral, pública o privada, ajena a la organización del responsable, que sola o conjuntamente con otras, trata datos personales por cuenta del responsable, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio".

En esta definición, el reglamento explica y detalla más la figura del encargado, dando a entender que es una persona diferente al responsable y que como ya se mencionó con anterioridad, debe haber un instrumento jurídico que nos da hincapié para hablar acerca del contrato de protección de datos personales innominado o atípico.

De conformidad como lo que dispone La Ley en referencia las obligaciones del encargado son las siguientes:

Obligaciones del encargado

> **“Artículo 50.** El encargado tendrá las siguientes obligaciones respecto del tratamiento que realice por cuenta del responsable:
>
> **I.** Tratar únicamente los datos personales conforme a las instrucciones del responsable;
>
> **II.** Abstenerse de tratar los datos personales para finalidades distintas a las instruidas por el responsable;
>
> **III.** Implementar las medidas de seguridad conforme a la Ley, el Reglamento y las demás disposiciones aplicables;
>
> **IV.** Guardar confidencialidad respecto de los datos personales tratados;

> Miércoles 21 de diciembre de 2011 DIARIO OFICIAL (Tercera Sección) 11
>
> **V.** Suprimir los datos personales objeto de tratamiento una vez cumplida la relación jurídica con el responsable o por instrucciones del responsable, siempre y cuando no exista una previsión legal que exija la conservación de los datos personales, y
>
> **VI.** Abstenerse de transferir los datos personales salvo en el caso de que el responsable así lo determine, la comunicación derive de una subcontratación, o cuando así lo requiera la autoridad competente. Los acuerdos entre el responsable y el encargado relacionados con el tratamiento deberán estar acordes con el aviso de privacidad correspondiente".

Como se advierte las obligaciones son por cuenta del responsable, mas no se habla acerca de que sucedería si no fuese por cuenta del responsable, si fuese por autodeterminación del tratante y así cometer un delito o una sanción de las que establece el articulo 63 de la LFPDPPP, sanciones que solo están previstas para el responsable mas no para el tratante.

3.5.- Relación jurídica entre el "Responsable" y el "Encargado".

Del análisis jurídico de los artículos principales que regulan al encargado y al responsable, destaca el que a continuación se transcribe

> **“Artículo 51.** La relación entre el responsable y el encargado deberá estar establecida mediante cláusulas contractuales u otro instrumento jurídico que decida el responsable, que permita acreditar su existencia, alcance y contenido".

Como más adelante se expone, debe existir un documento jurídico que avale la relación jurídica entre ambos sujetos, y aunque el artículo anterior no nos hace mención del contrato de protección de datos personales, se le ha denominado así, por los especialistas en la materia.

3.6.- Contrato de Protección de Datos Personales en Posesión de Particulares.

En la actualidad las empresas o personas físicas responsables del manejo de datos personales, pretenden avalar la relación jurídica entre el responsable y el encargado, elaborando una serie de documentos que acreditan dicha relación.

Al respecto cabe resaltar el hecho de que en el caso de las empresas, quien funge como tratante o encargado del manejo de datos personales, la mayoría de las veces, es su propio personal, en quien delegan las obligaciones que en ese rubro le corresponden al responsable, pese a que por lo general no cuenta con ninguna capacitación, ni mucho menos se la dan, para que esté en condiciones y pueda brindar o proporcionar a los titulares un adecuado manejo y protección de sus datos.

Siendo esas circunstancias, bajo las cuales las empresas que manejan datos personales elaboran los documentos a que nos hemos referido, habiéndose observado que tal actitud obedece al hecho de que a las mismas solo les interesa la relación laboral que tienen con su personal, así como el de economizar, teniendo menos trabajadores y departamentos especializados para encargarse del manejo de los datos en cuestión, no interesándoles de ninguna manera llevar a cabo la celebración de algún contrato que garantice la seguridad y protección de los datos del titular, lo que desde luego es lesivo para los derechos e intereses de éste, motivo por el que es de suma importancia que para lograr una efectiva regulación que garantice la protección y seguridad de los datos en cuestión, es conveniente que el responsable, dígase personas físicas o morales, al delegar al encargado la obligación relativa al tratamiento de datos personales, celebre con éste un contrato, el cual debe ajustarse a los requerimientos que exige la ley, para que de esta forma quede garantizada la protección y seguridad de los datos del titular.

Es decir, se cree un instrumento o acuerdo, el cual cumpla con los requisitos que exige la ley para que los contratos sean válidos, como son los de existencia

y validez, así como de formalidad, a que nos hemos referido, mismos que exige el Código Civil para que un acuerdo de esta naturaleza tenga validez y obligue a los que lo celebran a cumplirlo; y en el caso que nos ocupa, quede garantizado también, de alguna forma, que el titular de los datos personales no sufra daños o perjuicios de ninguna clase.

En este sentido se propone que en dicho acuerdo de voluntades, las partes contratantes puedan incluir también, cláusulas en las que se convenga la toma de cursos de capacitación para el personal que la empresa asigne, para el manejo de los datos, los cuales no van a resultar gravosos, ya que en su mayoría los ofrece el IFAI.

Obviamente, la propuesta que se formula es porque los documentos que elaboran o utilizan las empresas y personas físicas con los encargados del tratamiento de datos del titular, no cumplen con los requisitos y formalidades exigidas para un contrato; lo que desde luego podría acarrear varias consecuencias, pues en caso de un ilícito por parte de una persona física o moral encargada del tratamiento de datos personales, colocaría al titular en desventaja, al privarlo de la posibilidad de demandar o exigir de quien también se encarga del manejo de sus datos, la satisfacción de alguna pretensión.

Es más, se ha observado que los documentos que en la actualidad celebran entre el responsable y el encargado, respecto al manejo de datos personales, se les quiere dar el carácter de contrato, no obstante de que en los mismos se omite cumplir con los requisitos que requiere un contrato para que sea válido, dichos documentos no se encuentran ni siquiera nominados por la ley, ni hay una cláusula para ellos. Sólo se habla en la misma de que las partes celebran un documento jurídico.

Desde luego la propuesta de que entre el responsable y el encargado se celebre un contrato de la naturaleza a que nos hemos referido, es decir que cubra los requisitos que la ley señala para la validez del mismo, no demerita al aviso de privacidad, ya que se busca que éste auxilie al contrato propuesto, por

tratarse de un documento que, de acuerdo a la ley, y realidad social es importante e indispensable para el titular y le sirve como respaldo en lo referente al tratamiento y protección de sus datos personales

La sustentante, propone la celebración de un instrumento jurídico, al cual podría denominarse contrato de protección de datos personales en posesión de particulares, y qué como se ha señalado, debe celebrarse entre el responsable y el encargado de los datos en cuestión, para que en caso de un mal manejo o un tratamiento inadecuado de los datos del titular, ambos asuman la responsabilidad ante el mismo.

La propuesta de celebrar tal contrato, estaría además acorde a la ley, en virtud de que si la misma reconoce la existencia de ambas partes (responsable y encargado), como sujetos, en cuanto a protección de datos, también las debe considerar en un plano de igualdad por lo que se refiere a responsabilidad, cuando incurran en el incumplimiento de la obligación de velar por la protección y seguridad de aquellos cuya custodia y tratamiento se les ha confiado; esto en virtud de que como se puede advertir, la ley solo descarga responsabilidades y obligaciones, incluso sanciones únicamente para el responsable, jamás se solidariza con éstas al tratante, omisión que de alguna manera podría ocasionar consecuencias negativas para el titular de los datos, lo que se puede evitar con la celebración del contrato en cuestión.

Cabe destacar al respecto, que en la práctica por cuanto hace al responsable y el encargado o tratante, es éste último quien muchas veces incurre en más responsabilidad, ya que es quien realmente maneja los datos del titular, y aunque no en todos los casos, pero es el que tiene conocimiento total de todo lo relacionado con su tratamiento..

En este orden de ideas, y para adecuar el marco jurídico en el cual puede situarse al contrato propuesto, es necesario referirnos a las clasificaciones de los contratos, por lo cual es de primordial importancia definir qué se entiende por contrato y convenio.

Etimológicamente el término contrato tiene un origen latino en el vocablo "*Contractus"* que significa pacto, ajuste o convenio que crea una obligación entre las personas que lo hacen o consumen. Rojina Villegas, lo define, contrato como: "Un acuerdo de voluntades para crear o transmitir derechos y obligaciones[34]."

A su vez Pothier Robert nos define que, "un contrato es un convenio formal entre dos o más personas sobre cualquier objeto, en cuanto a Derecho comparado se refiere[35]", algo parecido nos dice el art. 1101 del Cód. Francés es "una convención, por la cual una o varias personas se obligan, hacia una o varias otras, a dar, hacer o no hacer alguna cosa",

De acuerdo con el Código Civil Mexicano de 1928, el convenio (en sentido amplio) es un acuerdo de voluntades para crear (producir), transferir, modificar o extinguir derechos y obligaciones.

El contrato es un acuerdo de voluntades para crear o transferir derechos y obligaciones.

De manera que los contratos son actos jurídicos y los actos jurídicos son especies de hechos jurídicos (en sentido amplio)[36].

El convenio *latu sensu*, es decir en sentido general, es el acuerdo de dos o más voluntades manifestado en forma exterior para crear, trasmitir, modificar o extinguir derechos y obligaciones[37].

El convenio en sentido especial es el acuerdo que modifica o extingue derechos y obligaciones[38].

---

[34] ROJINA VILLEGAS, Rafael. "Contratos". Ed. Porrúa. México DF.
[35] POTHIER, Robert Joseph. "Tratado de las Obligaciones". Pág. 10 Tribunal Superior de Justicia del Distrito Federal y la Dirección General de Anales de Jurisprudencia y Boletín Judicial, invierno 2002-2003.
[36] FIGUEROA Luis Mauricio , Contratos Civiles, Editorial Porrúa , México 2007
[37] CASTILLO CHIRINO Joel, Contratos, Editorial Porrúa , México 2007
[38] BORJA SORIANO Manuel, Teoría General delas Obligaciones, Editorial Porrúa, México 1962.

El código Civil Federal nos define el convenio como

Artículo 1792.- Convenio es el acuerdo de dos o más personas para crear, transferir, modificar o extinguir obligaciones.

Artículo 1793.-Los convenios que producen o transfieren las obligaciones y derechos, toman el nombre de contratos.

De lo anterior podemos concluir que un contrato es un acuerdo que pueden celebrar dos o más personas, ya sea físicas o morales, sobre un objeto o un servicio, siempre y cuando sea licito que y no sea contrario a la ley o las buenas costumbres que cree o transmita derechos y obligaciones.

Los elementos del contrato son de dos clases: los de existencia (articulo 1794) y de validez (articulo 1795) según el Código Civil Federal:

Elementos de existencia:

- Consentimiento
- Objeto que pueda ser materia de contrato

Elementos de validez:

- Capacidad
- Falta de vicios de la voluntad
- Licitud en el objeto, motivo o fin
- Forma

El problema del código es que los enuncia los elementos de validez de manera negativa, aunque hay doctrinas que los enuncian de manera positiva, pero consideramos que los elementos mencionados son los más importantes.

El consentimiento:

Podríamos definirlo ampliamente, pero lo fundamental, es entender que es a lo que se refiere. En estricto sentido puede entenderse de dos diversas formas: como voluntad del deudor de obligarse o como un acuerdo de voluntades; pero su esencia radica en el hecho de que los sujetos que intervienen en la celebración de un contrato, deben conocerlo, entender sus alcances, pero fundamentalmente es que están plenamente convencidos de aceptar lo que firman.

El objeto:

Según el objeto, se puede clasificar a los contratos de varias formas, como lo hace el maestro de derecho Borja Soriano, quien establece las clasificaciones siguientes:

“Clasificación de los contratos según sus funciones. De acuerdo a sus funciones específicas, éstos se clasifican en las siguientes categorías:

a) Por la interdependencia de las obligaciones: Bilaterales y Unilaterales;
b) Por la valoración económica de las prestaciones: Onerosos y Gratuitos;
c) Por la precisión de los efectos económicos entre las partes: Contratos conmutativos y aleatorios;
d) Por la entrega física del objeto: Contratos reales;
e) En cuanto a su función jurídica relacionada con otros actos jurídicos en: Contratos principales y Contratos accesorios;
f) En cuanto a su ámbito de temporalidad: Contratos instantáneos y Contratos de tracto sucesivo;

g) En cuanto a su nacimiento y validez: Consensuales, Formales, Solemnes[39]".

En atención a su delimitación legal, aquellos contratos que no se encuentran expresamente regulados por la ley se les conoce como Innominados. Refiriéndose a este tipo de contratos, los tratadistas jurídicos como Alessanrdri y Somarriva, señalan: "las partes pueden celebrarlos en virtud de la autonomía de la voluntad, que autoriza para pactar cualquier contrato, cualquiera sea su naturaleza, siempre que se respete la ley, el orden público y las buena costumbres[40]."

Al respecto el tratadista Manuel Osorio, nos dice:

"….. Son aquellos que la ley no designa con denominación especial, no son objeto de una reglamentación que los individualice y lo distinga de los demás, contrario a lo que sucede con los contratos nominados[41]"

Podemos decir, que son acuerdos que se rigen por las reglas que gobiernan los actos y declaraciones de voluntad; reglas que son de carácter general, y que vienen siendo aplicables a todo tipo de actos y manifestaciones de voluntad, cualquiera sea su naturaleza.

Por las propias estipulaciones de las partes.

Finalmente cabe señalar, que en este tipo de contratos (innominados), se aplican por analogía las reglas de los contratos nominados más semejantes, siempre que las modalidades especiales de los que se toman como modelo permitan la aplicación de esas reglas; mismas que como hemos mencionado, son de carácter doctrinario y no vinculantes u obligatorias de aplicar.

---

[39] BORJA Soriano M. Ob. Cit.
[40] ALESSANDRI R, Arturo y Somarriva U, Manuel. "Curso de Derecho Civil, Fuentes de las Obligaciones"
[41] OSORIO, Manuel. "Diccionario de C.C. Jurídicas" Editorial Helestica, Pág. 17

Ahora bien, aplicando a la materia de protección de datos personales lo que anteriormente se expuso con relación a los contratos, en lo concerniente a los requisitos de existencia y validez, a sus clasificaciones, y en especial a aquella que los diferencia entre nominados e innominados, podemos decir, lo siguiente:

Si bien es cierto que entre las personas físicas y morales que manejan datos personales, o bien entre el responsable y el encargado, muchas veces existe alguna relación, la cual formalizan a través de un documento que elaboran, también lo es, que dicha relación solo tiene el carácter de laboral, y que si llegan a celebrar algún documento jurídico, relacionado con la protección de datos, este documento no se ajusta a los requerimientos de un contrato.

En efecto, actualmente, la mayoría de los responsables que celebran algún contrato con los trabajadores, a quienes asignan como tratante o encargado de datos personales, como ya se ha mencionado, generalmente se concretan a formular un documento al que solo le dan apariencia de contrato, dicho documento en realidad solo respalda su relación laboral con esos trabajadores, más no su responsabilidad con la trata de datos personales.

Elaboran tales documentos tomando algunos requisitos de los contratos, logrando formar si acaso, aquellos que se les conoce como innominados o atípicos. Es decir, el responsable y el encargado, elaboran documentos a los que les tratan de un viso de contratos de protección de datos personales, los cuales no se encuentran contemplados en la ley.

Por ello, una de las propuestas que se hacen en la presente tesis, es, que el contrato que celebren el responsable y encargado de datos personales, se individualice y regule en la ley de manera especial, para que de esta manera el titular tenga la seguridad de que sus datos van a estar garantizados en cuanto a su tratamiento (uso, divulgación, almacenamiento, transferencia, etc.) y que en caso de un mal manejo de estos, el titular pueda ejercitar las acciones correspondientes en contra de ambas partes, y de cierta forma tenga la seguridad de que se le pueda cubrir alguna prestación que reclame, ya sea de

carácter económico o moral, ocasionada por el ilícito en que hayan incurrido las personas involucradas en el tratamiento de sus datos.

A continuación se ejemplifica a grandes rasgos como debe ser un contrato de protección:

CONTRATO DE CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS

[NOMBRE DE LA EMPRESA] (a quien de ahora en adelante se le denominará “RESPONSABLE” con domicilio en [DOMICILIO COMPLETO], con R.F.C. [COLOCAR RFC],representada por el C. [NOMBRE DEL REPRESENTANTE], mayor de edad, con Documento Nacional de Identidad [COLOCAR DOCUMENTACION EN CASO DE SER NECESARIO], y que cuenta con poderes suficientes en virtud de la escritura pública otorgada el día [FECHA DEL INSTRUMENTO] ante el Notario de [NOMBRE DEL NOTARIO Y NUMERO DE NOTARIA] [NUMERO DE PROTOCOLO] de su protocolo. Y de otra parte, [NOMBRE DEL ENCARGADO] que de ahora en adelante se le denominara “ENCARGADO” con domicilio en [DOMICILIO COMPLETO], con R.F.C. [COLOCAR RFC],representada por el C. [NOMBRE DEL REPRESENTANTE, EN CASO DE EXISTIR], mayor de edad, con Documento Nacional de Identidad [COLOCAR DOCUMENTACION EN CASO DE SER NECESARIO], y que cuenta con poderes suficientes en virtud de la escritura pública otorgada el día [FECHA DEL INSTRUMENTO] ante el Notario de [NOMBRE DEL NOTARIO Y NUMERO DE NOTARIA] [NUMERO DE PROTOCOLO] de su protocolo.

En adelante, denominadas individual o conjuntamente como la “Parte” o las “Partes”.

DECLARAN

PRIMERO.- Que [RESPONSABLE] desea [OBJETO CONTRATO]. Para ello, necesita contar con la colaboración técnica de [ENCARGADO], a fin de que la misma [NOMBRE DE LA EMPRESA] ejecute el tratamiento de los siguientes

datos (SEÑALAR LOS DATOS PERSONALES A TRATAR)

SEGUNDO.- Que, como consecuencia de la relación existente entre [EMPRESA1] y [EMPRESA2 O ENCARGADO], ésta última necesita acceder a información de carácter confidencial y a datos de carácter personal incluidos en ficheros titularidad de [EMPRESA1].

TERCERO.- Que, como consecuencia de lo anterior, las Partes desean definir los términos y condiciones bajo los cuales se regulará el acceso, por [EMPRESA2 O ENCARGADO], a la información confidencial de [EMPRESA1] y a datos de carácter personal incluidos en Ficheros pertenecientes a la misma.

En virtud de lo anterior, las Partes, reconociéndose mutuamente capacidad suficiente para el otorgamiento de este acto, formalizan el presente Acuerdo de Confidencialidad y protección de datos (el “Acuerdo”) con sujeción a las siguientes

CLAUSULAS

1.- OBJETO Constituye el objeto del presente Acuerdo regular las condiciones en las que [EMPRESA2 O ENCARGADO] accederá a la información suministrada por [EMPRESA1], necesaria para la implementación del tratamiento de los datos personales.

2.- CONFIDENCIALIDAD A los efectos previstos en este Acuerdo por “Información Confidencial” se entenderá toda aquella información, ya sea técnica, financiera, comercial o de cualquier otro carácter, que sea suministrada y/o comunicada por [EMPRESA1] a [EMPRESA2 O ENCARGADO] en relación con el PROYECTO, mediante palabra, por escrito o por cualquier otro medio o soporte, tangible o intangible, actualmente conocido o que posibilite el estado de la técnica en el futuro.

En el supuesto de que, previamente a la celebración de este Acuerdo, [EMPRESA2 O ENCARGADO] hubiera tenido acceso a información de

[EMPRESA1] aquélla será considerada, para los efectos previstos en el presente documento, como Información Confidencial, salvo aquella que expresamente sea calificada por [EMPRESA1] como información de libre uso y/o divulgación.

Obligaciones

A) [EMPRESA2 O ENCARGADO], acusará recibo de cualquier Información Confidencial que le suministre [EMPRESA1], tan pronto como la reciba.

B) [EMPRESA2 O ENCARGADO] dará cumplimiento a todas y cada una de las siguientes clausulas en lo que respecta a la Información Confidencial suministrada por [EMPRESA1] en relación con el PROYECTO:

PRIMERA.- Tan pronto como [EMPRESA2 O ENCARGADO] reciba o genere información confidencial se obligará a:

1. Mantenerla, con sujeción a la más estricta confidencialidad,

2. Utilizarla solamente en relación con lo señalado por la [EMPRESA1], con apego a su aviso de privacidad, así como el consentimiento de los titulares de los datos personales.,

3. No revelarla a una tercera parte sin el previo consentimiento escrito de [EMPRESA1] o de su titular.,

4. Revelar dicha Información únicamente a los empleados de su compañía que tengan necesidad expresa de conocerla en relación con el desarrollo de tareas del tratamiento.

SEGUNDA.- [EMPRESA2 O ENCARGADO] adoptará las medidas de seguridad oportunas que aseguren el cumplimiento, por los empleados o terceros, que, en su caso, tengan acceso a la Información Confidencial, de todos los términos y condiciones establecidos en el presente Acuerdo.

TERCERA.- En caso de desistimiento en el proceso de contratación por cualquiera de las Partes o si esta no se lleva a cabo dentro del plazo de validez de la oferta o en todo caso a los 6 (SEIS) meses de emitida la oferta, [EMPRESA2 O ENCARGADO] devolverá a [EMPRESA1] la Información Confidencial suministrada y borrará o destruirá cualquier copia de la misma que hubiese sido realizada, certificando dicho extremo a [EMPRESA1], de acuerdo con la solicitud expresa que esta última le realice.

CUARTA.- En caso de que las negociaciones mencionadas en el Expositivo Primero culminaran en la formalización de un contrato entre las partes, a la finalización del mismo, [EMPRESA2 O ENCARGADO] devolverá a [EMPRESA1] la Información Confidencial suministrada y borrará o destruirá cualquier copia de la misma, certificando dicho extremo a [EMPRESA1], de acuerdo con la solicitud expresa que esta última le realice.

QUINTA.- [EMPRESA2 O ENCARGADO] devolverá a [EMPRESA1] toda la Información Confidencial y toda copia de ella en el plazo de 30 días a partir de la recepción de una petición por escrito procedente de [EMPRESA1].

Exclusiones

Lo establecido en esta cláusula no será de aplicación a ninguna información sobre la que [EMPRESA2 O ENCARGADO] pudiera demostrar:

a) Que fuera del dominio público en el momento de haberle sido revelada.

b) Que, después de haberle sido revelada, fuera publicada o de otra forma pasara a ser de dominio público, sin quebrantamiento de la obligación de confidencialidad por la parte que recibiera dicha información.

c) Que, en el momento de haberle sido revelada, la parte que la recibiera ya estuviera en posesión de la misma por medios lícitos o tuviera derecho legalmente a acceder a la misma.

d) Que tuviera consentimiento escrito previo de la otra parte para revelar la información.

e) Que haya sido solicitada, conforme a la normativa vigente, por Autoridades Administrativas o Judiciales competentes que deban pronunciarse sobre aspectos totales o parciales de la misma, en cuyo caso, la parte que tenga que realizar la presentación deberá comunicárselo a la otra con carácter previo a que dicha presentación tenga lugar.

3.- DATOS DE CARÁCTER PERSONAL:

Si, debido a la naturaleza de las negociaciones o de la realización del Proyecto objeto del presente Acuerdo, [EMPRESA2 O ENCARGADO] tuviese que acceder a datos de carácter personal incluidos en ficheros titularidad de [EMPRESA1], deberá cumplir lo dispuesto EN LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES. En cualquier caso, será [EMPRESA1], como titular de los ficheros, quien decidirá sobre la finalidad, contenido y uso del tratamiento de los datos, limitándose [EMPRESA2 O ENCARGADO] a utilizar dichos datos, única y exclusivamente, para los fines que figuren en el Contrato.

El acceso a los datos de carácter personal incluidos en Ficheros titularidad de [EMPRESA1], a los que pudiese tener acceso [EMPRESA2 O ENCARGADO], no tiene la consideración legal de comunicación o cesión de datos, sino de simple acceso a los mismos, como elemento necesario para llevar a cabo las negociaciones reguladas en el presente Acuerdo.

Los ficheros que contengan datos de carácter personal a los que pudiese acceder [EMPRESA2 O ENCARGADO] como consecuencia de este Acuerdo, son propiedad exclusiva de [EMPRESA1], extendiéndose también esta titularidad a cuantas elaboraciones, evaluaciones, segmentaciones o procesos similares que, en relación con los mismos, pudiese realizar [EMPRESA2 O ENCARGADO], de acuerdo con los servicios que se pactan en el presente

Acuerdo o en futuros Contratos, declarando [EMPRESA1] que los mismos son confidenciales a todos los efectos, sujetos, en consecuencia, al más estricto secreto profesional, incluso una vez finalizada la validez del presente Acuerdo.

En su calidad de encargado de tratamiento, [EMPRESA2 O ENCARGADO] queda obligado al cumplimiento de lo establecido en la Ley FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES, se compromete específicamente a:

A) Custodiar los datos de carácter personal a los que pudiesen tener acceso como consecuencia de este Acuerdo, adoptando las medidas de índole técnica y organizativas necesarias, y en especial las establecidas por LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES y demás disposiciones de desarrollo, para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos suministrados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

B) Utilizar o aplicar los datos personales, exclusivamente, para la realización de los servicios que se pactan y, en su caso, de acuerdo con las instrucciones impartida por el titular de los ficheros que contengan los datos.

C) No comunicarlos, ni siquiera para su conservación a otras personas, ni tampoco las elaboraciones, evaluaciones o procesos similares citados anteriormente, ni duplicar o reproducir toda o parte de la información, resultados o relaciones sobre los mismos.

D) Asegurarse que los datos de carácter personal a los que pudieran tener acceso sean manejados únicamente por aquellos empleados cuya intervención sea precisa para la finalidad establecida y que, únicamente en el supuesto que tal posibilidad esté autorizada expresamente y con carácter previo por la Parte titular de los ficheros, cualesquiera terceros a los que les sea revelada cualquier

información, estén vinculados a guardar la confidencialidad debida de conformidad con lo prevenido en esta cláusula.

E) Admitir controles y auditorias que, de forma razonable, pretenda realizar [EMPRESA1], a los efectos de cumplimiento de lo aquí establecido, así como que pueda añadir, a los datos personales facilitados, unos registros de control.

F) Una vez finalizada la prestación contractual, destruirlos, certificando esta circunstancia a [EMPRESA1] o, si ésta última así lo indica, devolvérselos a la misma así como también los soportes o documentos en que consten, sin conservar copia alguna.

En el supuesto de incumplimiento por [EMPRESA2 O ENCARGADO], incluidos sus empleados, de sus obligaciones según lo establecido en la presente cláusula o de las derivadas de la legislación aplicable en materia de protección de datos, la misma será considerada responsable del tratamiento, y de forma específica asumirá la total responsabilidad que pudiera derivarse al titular de los ficheros como consecuencia de cualquier tipo de sanciones administrativas impuestas por procedimientos judiciales o extrajudiciales contra el titular.

4.- DERECHOS DE PROPIEDAD

Este Acuerdo no supone la concesión, expresa o implícita, a favor de [EMPRESA2 O ENCARGADO] de derecho alguno sobre la Información Confidencial objeto del mismo.

En consecuencia, el suministro, generación o uso de dicha Información no podrá entenderse, en ningún caso, como concesión de patente, licencia o derecho de autor alguno a favor de [EMPRESA2 O ENCARGADO], considerándose que aquella permanecerá en todo momento en el ámbito de propiedad de [EMPRESA1] o del tercero a quien pertenezca.

5.- COMUNICACIONES

Todas las notificaciones que deban realizarse por medio escrito, incluidas en las disposiciones del presente acuerdo, se realizarán, enviando por correo certificado a la parte anunciada en su sede social o en el domicilio indicado para estos efectos por la parte notificada, a la atención de los designados más abajo. Se considerará como fecha de notificación el día siguiente al que se trasmitió o entregó a Correos.

A los efectos previstos en el presente Acuerdo, las Partes designan a las siguientes personas como interlocutores a través de los cuales deberán canalizarse todas las comunicaciones:

Por [EMPRESA1]:

•Attn: [EMPRESA1/INTERLOCUTOR/NOMBRE]

•Tfno.: [EMPRESA1/INTERLOCUTOR/TELÉFONO]

Por: [EMPRESA2]:

•Attn.: [EMPRESA2/INTERLOCUTOR/NOMBRE]

•Teléfono: [EMPRESA2/INTERLOCUTOR/TELÉFONO]

La sustitución de cualquiera de los anteriores interlocutores del Proyecto, deberá ser comunicada por escrito a la otra Parte con la debida antelación.

6.- ENTRADA EN VIGOR

Este Acuerdo entrará en vigor en la fecha de firma por los representantes autorizados de las partes.

7.- DURACIÓN

Las disposiciones del presente acuerdo permanecerán en vigor de forma indefinida pese a la eventual terminación de las negociaciones entre las partes o la formalización del contrato.

8.- PUBLICIDAD

El presente Acuerdo no dará derecho alguno a ninguna de las Partes a realizar campañas de publicidad o acciones de marketing relacionadas con el mismo o con las negociaciones entre las Partes sin autorización expresa de la otra.

Respecto a las notas de prensa se acuerda que sean coordinadas entre los gabinetes o departamentos correspondientes, debiendo existir un acuerdo expreso, mutuo y escrito, en su caso.

9.- DAÑOS Y PERJUICIOS

Ambas partes acuerdan que el pago de los daños y perjuicios puede no constituir remedio suficiente en caso de incumplimiento real de las disposiciones del presente Acuerdo, y ninguna de las partes se opondrá al otorgamiento de compensaciones equitativas, incluso la ejecución forzosa.

10.- INTRANSFERIBILIDAD

El presente acuerdo es personal entre las dos Partes, y no podrá transferirse total o parcialmente sin la autorización previa por escrito de la otra Parte.

11.- LEGISLACIÓN Y JURISDICCIÓN APLICABLE

Este Acuerdo se interpretará de conformidad con las leyes MEXICANAS.

En caso de litigio o controversia entre las Partes en relación con la interpretación, ejecución, incumplimiento, resolución o nulidad de parte o de la totalidad del presente Acuerdo, las Partes, renunciando al fuero que pudiera

corresponderles, se someten a la jurisdicción de los Juzgados y Tribunales del Distrito Federal.

12.- VARIOS

Este Acuerdo se limita a regular el tratamiento de la Información Confidencial y Protección de Datos de Carácter Personal, sin que ello obligue en modo alguno a [EMPRESA1] a suministrar o divulgar más Información que aquella que, en cada momento, ésta estime oportuna. El acuerdo no implica compromiso alguno por parte de [EMPRESA1] que pueda entenderse como el establecimiento de un encargo formal para la realización de trabajos onerosos.

Y en virtud de lo anterior, las Partes firman el presente Acuerdo, en [PONER LUGAR Y FECHA].

3.7.- Responsabilidad solidaria entre el "Responsable" y el "Encargado".

Como se ha mencionado, los sujetos más importantes, en lo concerniente al tratamiento de datos de carácter personal, independientemente de las precauciones y la cultura de protección que debe tener el titular, son los responsables y los encargados. Estos sujetos constituyen las figuras más importantes en dicho rubro, ya que son quienes se encargan de gestionar los datos en cuestión. Sin embargo, como ya se ha dicho, pese a que en los hechos ambos comparten tal responsabilidad, al único a quien se imponen obligaciones y establecen sanciones en la ley es al responsable. Tal y como se advierte de lo dispuesto en los artículos 63 y 64 de la ley en comento. En efecto, en cuanto a las obligaciones del responsable, el artículo 63 establece:

> **Artículo 63.-** Constituyen infracciones a esta Ley, las siguientes conductas llevadas a cabo por el responsable:
>
> I. No cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición al tratamiento de sus datos personales, sin razón fundada, en los términos previstos en esta Ley;

II. Actuar con negligencia o dolo en la tramitación y respuesta de solicitudes de acceso, rectificación, cancelación u oposición de datos personales;

III. Declarar dolosamente la inexistencia de datos personales, cuando exista total o parcialmente en las bases de datos del responsable;

IV. Dar tratamiento a los datos personales en contravención a los principios establecidos en la presente Ley;

V. Omitir en el aviso de privacidad, alguno o todos los elementos a que se refiere el artículo 16 de esta Ley;

VI. Mantener datos personales inexactos cuando resulte imputable al responsable, o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de los titulares;

VII. No cumplir con el apercibimiento a que se refiere la fracción I del artículo 64;

VIII. Incumplir el deber de confidencialidad establecido en el artículo 21 de esta Ley;

IX. Cambiar sustancialmente la finalidad originaria del tratamiento de los datos, sin observar lo dispuesto por el artículo 12;

X. Transferir datos a terceros sin comunicar a éstos el aviso de privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos;

XI. Vulnerar la seguridad de bases de datos, locales, programas o equipos, cuando resulte imputable al responsable;

XII. Llevar a cabo la transferencia o cesión de los datos personales, fuera de los casos en que esté permitida por la Ley;

XIII. Recabar o transferir datos personales sin el consentimiento expreso del titular, en los casos en que éste sea exigible;

XIV. Obstruir los actos de verificación de la autoridad;

XV. Recabar datos en forma engañosa y fraudulenta;

XVI. Continuar con el uso ilegítimo de los datos personales cuando se ha solicitado el cese del mismo por el Instituto o los titulares;

> XVII. Tratar los datos personales de manera que se afecte o impida el ejercicio de los derechos de acceso, rectificación, cancelación y oposición establecidos en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos;
>
> XVIII. Crear bases de datos en contravención a lo dispuesto por el artículo 9, segundo párrafo de esta Ley, y
>
> XIX. Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la presente Ley.

Como se puede advertir, en todas y cada una de las fracciones del numeral aludido, por cuanto hace a manejo de los datos personales, únicamente se establecen una serie de obligaciones para el responsable, pero jamás para el encargado. Deberían señalarse obligaciones también a éste último, para que en caso de incumplimiento con las mismas, ambas partes (responsable y tratante), respondan solidariamente.

En cuanto a las sanciones, el artículo 64 de la ley multicitada, establece.

> Artículo 64.- Las infracciones a la presente Ley serán sancionadas por el Instituto con:
>
> I. El apercibimiento para que el responsable lleve a cabo los actos solicitados por el titular, en los términos previstos por esta Ley, tratándose de los supuestos previstos en la fracción I del artículo anterior;
>
> II. Multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones II a VII del artículo anterior;
>
> III. Multa de 200 a 320,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones VIII a XVIII del artículo anterior, y
>
> IV. En caso de que de manera reiterada persistan las infracciones citadas en los incisos anteriores, se impondrá una multa adicional que irá de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. En tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.

Como se desprende de lo dispuesto por dicho artículo, las sanciones que se establecen, van dirigidas únicamente para el responsable del manejo de los datos personales del titular, nunca para el encargado.

Las sanciones indicadas también deberían dirigirse también al encargado, ya que éste, como se ha mencionado en líneas anteriores, es quien en los hechos realmente trata los datos del titular.

Por lo tanto, las sanciones que se contemplan en el artículo 64 de la ley en comento, deberían establecerse también para el encargado o tratante de datos personales, para que en caso de incurrir en infracciones en el tratamiento de los mismos, o que genere un ilícito, responda ante el titular.

Ahora, si bien es cierto se ha hablado de responsabilidad solidaria, y este concepto o idea es aplicable en materia civil para los acreedores o deudores, sin embargo, saliendo del campo de obligaciones civiles o mercantiles, también podría ser aplicable en el laboral, y se hablaría entonces de la existencia de una responsabilidad solidaria, valiendo la redundancia, entre el responsable, que es patrón y tratante, que sería el trabajador, para que respondan sobre su conducta ante el titular de datos personales. O bien, si ajustamos la conducta de dichos sujetos, la cual no puede ir contra la moral, el derecho y las buenas costumbres, es decir, que no pueden ni deben divulgar la información que corre dentro de la empresa o que debemos tener una cláusula de protección de datos personales (esta cláusula se debe contemplar en el contrato de protección de datos personales), para que el encargado no divulgue o traspase la información a algún tercero y que en caso de que ocurra este hecho sean sancionadas ambas partes, por la falta de probidad de el tratante.

Es decir, que haya sanciones para ambos en caso de filtro de información a algún tercero no autorizado.

Respecto a lo anterior, resulta aplicable la siguiente tesis, a la letra dice:

Novena Época
Instancia: Tribunales Colegiados de Circuito
Fuente: Semanario Judicial de la Federación y su Gaceta
XXVI, Noviembre de 2007
Página: 751
Tesis: V.1o.C.T.89 L
Tesis Aislada
Materia(s): laboral

PATRÓN SOLIDARIO. NO TIENE DICHO CARÁCTER LA PERSONA FÍSICA O MORAL QUE RECIBE LOS TRABAJOS DE UN GUARDIA DE SEGURIDAD PROPORCIONADO POR UNA EMPRESA PRESTADORA DE SERVICIOS, SI AQUÉL TIENE COMO FIN VIGILAR, SALVAGUARDAR O PROTEGER LOS BIENES DE LA CONTRATANTE, CON ELEMENTOS PROPIOS DE LA PRESTADORA Y BAJO SU ORDEN Y DEPENDENCIA.

En aquellos casos en que el patrón directo de un trabajador es una empresa prestadora de servicios a diversos clientes, la relación laboral se da entre la parte trabajadora y aquella empresa, y para determinar si quien recibe el servicio tiene el carácter de patrón solidario, debe tomarse en cuenta lo siguiente: a) si la empresa prestadora de servicios que contrató al trabajador ejecuta los trabajos con elementos propios; b) si cuenta con recursos suficientes para cumplir con las obligaciones que deriven de la relación laboral; y, c) si la empresa, persona física o moral a quien se le atribuye la responsabilidad solidaria, se benefició de manera exclusiva o principal con los trabajos desempeñados. Ahora bien, si en el caso concreto el servicio prestado consiste en el de guardia de seguridad, de acuerdo con la naturaleza de esa función no es posible considerar a las empresas receptoras del servicio como patrones solidarios, en primer término, porque para tenerlas con tal carácter es necesario que la prestación del servicio se proporcione en forma exclusiva o principal; y, en segundo, porque el trabajador es enviado por la prestadora del servicio a ejecutar sus labores bajo su orden y dependencia a un número variable de empresas receptoras, y utilizando los elementos que aquélla le proporciona. Consecuentemente, no es factible admitir que basta que una persona física o moral haya recibido los servicios personales del trabajador como guardia de seguridad para tener por comprobada la responsabilidad solidaria en la relación jurídica de trabajo, ya que tal servicio tiene como fin vigilar, salvaguardar o proteger los bienes o derechos de las empresas contratantes del servicio, en los lugares requeridos por éstas de forma eventual, transitoria o temporal.

PRIMER TRIBUNAL COLEGIADO EN MATERIAS CIVIL Y DE TRABAJO DEL QUINTO CIRCUITO.

> Amparo directo 829/2006. Carlos Fornes Tirado. 4 de mayo de 2007. Unanimidad de votos. Ponente: Eugenio Gustavo Núñez Rivera. Secretaria: Raquel Nieblas Germán.

Analizando la tesis transcrita, y adecuándola al caso de la protección de datos, el trabajador, en este caso el encargado, pide deslindarse de la responsabilidad por mandato del patrón, en nuestro caso del responsable; pero que pasaría si por cuenta propia el encargado incurriera en un error, y transfiriera la información a persona no autorizada; de acuerdo a la legislación de protección de datos personales, quien tendría que responder por dicha conducta sería el responsable, valiendo la redundancia; en tanto que el encargado quedaría exento de la misma. Por tal motivo, es que se propone que exista una responsabilidad solidaria para ambos sujetos (responsable y encargado). Pues puede ocurrir que el encargado haya trasferido la información a persona no autorizada, y de esta forma incurriría en una falta de probidad.

3.8.- Sanciones establecidas en la ley para el "Responsable" y el "Encargado".

Como ya hemos comentado existen sanciones para los responsables, estas sanciones se encuentran contenidas en la ley en comento en el CAPÍTULO X De las Infracciones y Sanciones, que nos hace alusión desde el artículo 63 sobre las conductas llevadas a cabo por el encargado y con ello las infracciones en las que puede incurrir, entre ellas se contemplan las siguientes:

- incumplir con la solicitud de los derechos ARCO, sin razón fundada, así como negligencia y dolo en la tramitación;
- Declarar la inexistencia de datos personales;
- Dar mal tratamiento a los datos personales;
- Omisión en el aviso de privacidad;
- Exista error en los datos personales y como consecuencia afecten los derechos de los titulares;

- Cambiar la finalidad del tratamiento de los datos sin autorización del titular, así como la transferencia de estos a un tercero no facultado y el recabar la información sin consentimiento del titular.
- Obstrucción a los actos de verificación de la autoridad;
- Cualquier incumplimiento del responsable a las obligaciones establecidas a su cargo en términos de lo previsto en la presente Ley.

Las infracciones a la Ley serán sancionadas por el Instituto, apercibiendo al responsable para que lleve a cabo los actos solicitados por el titular, así como multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones II a VII del artículo 63; multa de 200 a 320,000 días de salario mínimo vigente en el Distrito Federal, en los casos previstos en las fracciones VIII a XVIII del artículo en mención.

En caso de que de manera reiterada persistan las infracciones citadas, se impondrá una multa adicional de 100 a 320,000 días de salario mínimo vigente en el Distrito Federal. En tratándose de infracciones cometidas en el tratamiento de datos sensibles, las sanciones podrán incrementarse hasta por dos veces, los montos establecidos.

El Instituto fundará y motivará sus resoluciones, considerando:

- La naturaleza del dato;
- La notoria improcedencia de la negativa del responsable, para realizar los actos solicitados por el titular;
- El carácter intencional o no, de la acción u omisión constitutiva de la infracción;
- La capacidad económica del responsable, y
- La reincidencia.

Las sanciones que se señalan se impondrán sin perjuicio de la responsabilidad civil o penal que resultase.

A su vez también el responsable puede incurrir en delitos que el artículo 67 de la LFPDPPP nos señala de la siguiente manera:

> **Artículo 67.-** Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.
>
> **Artículo 68.-** Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.
>
> **Artículo 69.-** Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.

Del contenido de dicho artículo, se desprende que las penas a que se refiere van destinadas al responsable, como persona autorizada para tratamiento de datos, pero como se ha señalado, jamás se habla del encargado, como sujeto de dichas penas.

CAPÍTULO IV

PROPUESTA DE REFORMA A LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE PARTICULARES EN CUANTO A LAS SANCIONES.

4.1.- Problemática ante la falta de sanción para el "Encargado".

Un pilar básico y fundamental de un efectivo sistema de protección de datos personales es la garantía de la seguridad de la información, entendida ésta como la implementación de medidas administrativas, físicas y técnicas eficaces para garantizar y velar por la integridad, confidencialidad y disponibilidad de tus datos personales. Ello contribuye a minimizar los riesgos de acciones en contra de tu información personal como robo, alteración o modificación, pérdida total o parcial, transmisiones indebidas o ilícitas, accesos no autorizados y robo de identidad, entre otras, que pueden lesionar los derechos o libertades fundamentales.

A lo largo de la historia se han sabido una serie de situaciones en las que se ve envuelto el patrón y el trabajador, este tipo de situaciones en muchas ocasiones se debe a negligencia por parte del trabajador, ya sea de manera voluntaria o accidental, esto es, que el encargado o tratante, distribuya datos personales vulnerando al titular en cuanto a su seguridad e integridad.

Ubicándonos en un contexto más apegado a la ley que nos ocupa, el encargado de la protección de datos personales, tiene la obligación de capacitarse, para realizar esta función; también debe de estar consciente de que sobre él recae la seguridad de proteger los datos de que trata; así mismo, debe de cumplir con una serie de requisitos para que le sea delegada la obligación de ser el responsable, y pueda llevar un tratamiento adecuado de la información que se le encarga, garantizando de esta manera un buen manejo para evitar el mal tratamiento de datos personales.

Podríamos definir el mal tratamiento de los datos personales, como aquella conducta que produce un menoscabo a la información de este tipo de datos o un daño a su seguridad.

Otro aspecto importante del tema en cuestión, tiene que ver con la protección de los datos personales en Internet o en software informáticos. Este campo de estudio le ha correspondido al derecho informático o al derecho de la informática, también incluye a la biotecnología, a la ingeniería genética, a la electrónica y a las telecomunicaciones en su espectro más amplio. A partir de las reformas al Código de Comercio, a la Ley Federal de Protección al Consumidor, Código Civil y Código de Procedimientos Civiles, en nuestro país se regula el comercio electrónico. La novedosa forma de intercambio comercial por medios electrónicos, compras en Internet o intercambio de datos e información entre los usuarios, dan cuenta de la importancia de proteger los derechos de la privacidad e intimidad de las personas.

Ahora bien, ahondando sobre el tema que nos ocupa en este apartado, referente a la existencia de sanciones en la ley en comento, primero que nada es conveniente puntualizar que en ella, como ya se ha señalado, no existen sanciones para el encargado de el tratamiento de los datos personales, ya que la única persona en quien recaen aquellas, es en el “responsable”, esto se puede constatar tanto en el contenido de la LFPDPPP como en su reglamento. Esta ausencia de sanciones para el encargado, en apariencia no crea una problemática, ya que para muchas personas, con el hecho de que se repare el daño que se ocasiona al titular de los datos, es más que suficiente; sin embargo no es tan sencillo, puesto que con las reformas que se proponen a la ley. Por ello es necesario establecer obligaciones así como sanciones para el tratante a efecto que responda también ante el titular, en caso de que incurra en un ilícito relacionado con el tratamiento de los datos de éste.

La problemática de la inseguridad sobre protección de datos personales, en opinión de la sustentante, también se puede ver desde el punto de vista de un

conocimiento general. Se ha observado que cuando se asiste a un lugar donde se proporcionarán datos personales, nos dicen ¿ya conocen nuestro aviso de privacidad? o simplemente nos presentan un documento lleno con pequeñas letras, el cual por comodidad se prefiere firmar, sin informarse de su contenido; tomémoslo como punto inicial la cultura de protección, ya que muy pocos usuarios de servicios o personas tienen este tipo de cultura, la cultura de privacidad la cual podemos entender como aquella prudencia que deben de tener todas aquellas personas que proporcionen sus datos personales, con ello se quiere decir el cuidado que debe tener al proporcionar información, ya sea personal o íntima (datos personales sensibles). y el hecho de que las personas no tengan cultura de protección, favorece que se le realicen hechos que pueden resultar en su perjuicio, en el caso de los datos personales sensibles, el daño de la intimidad personal, como ya hemos mencionado este tipo de información es aquella que a nadie le gustaría que se anduviera divulgando, como es el caso de una enfermedad, que provocase burla o discriminación, o bien de una tendencia sexual, familia etc.

Por ejemplo.

Cada día se escucha decir a los padres frases a sus hijos, como: “no platiques con extraños” “no te subas a carros que no conozcas” “cuida tus cosas” etc.

Pero actualmente con las tecnologías de la información, tal y como las redes sociales, no se toma esa clase de precauciones, definiendo más el ejemplo, dirijámonos a *facebook*, una red social mundial muy famosa, en la que interactúan personas de todo tipo y en la que con solo tener una cuenta de correo electrónico, misma que la puede crear cualquier persona con información falsa, se crea un famoso llamado “perfil”; en el cual al crear tu cuenta, se desglosan una serie de documentos, de supuesta privacidad, a los cuales poca gente les toma atención y tienden a darle clic en siguiente, o si acepto, sin darse cuenta que en ese tipo de documentos le ocultan a un servidor, para que este pueda jugar a su modo con la información recabada, ya que dentro de

este tipo de servidores se encuentra una clausula con los términos y condiciones de uso, que otorgan la facultad para utilizar cualquier información que se encuentre dentro del perfil de la persona como decidan dichos servidores.

También no se toma en consideración que este tipo de páginas, conocidas mayormente como redes sociales, son internacionales, y que al momento que un usuario sube información a la red, regala su información, ya que es de dominio público y no se puede detener tan fácilmente el flujo de su información, independientemente que se borre el perfil o la cuenta, su información quedará disponible en caso que decidan regresar y de nuevo subir su información en línea.

Posteriormente se pide información tal y como, lugar de residencia, edad, estado civil, creencias religiosas, gustos en cuanto a la recreación, la lectura, series favoritas, ideología etc. Después se pide información acerca de la gente que conoces y tu relación con la misma.

También tiene una aplicación[42], que permite a través de el teléfono móvil o por la dirección del IP[43], u otros medios, el proporcionar la ubicación con exactitud del lugar en el cual te encuentras; por si fuera poco, pide subir una imágen en la cual te identifiquen tus contactos, como la persona que dices ser.

Y así sucesivamente a través de la navegación, con el tiempo proporcionas más información como más interés, que lugares frecuentas, donde has estado, en que hoteles, restaurantes, plazas has acudido, cursos, talleres etc. Esto es, darle a conocer la intimidad general del usuario a las personas.

---

[42] es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos. Suele resultar una solución informática para la automatización de ciertas tareas complicadas como pueden ser la contabilidad, la redacción de documentos, o la gestión de un almacén.

[43] dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del Modelo OSI.

Con lo anterior se da lugar a que los menores o gente que no tiene una cultura de protección, publique toda clase de información acerca de si mismos; y sin saber proteger su información dentro de este servidor, otorgan información de todo tipo a toda clase de gente.

Y aunque se lleven a cabo campañas de concientización y más información, nos damos cuenta, que tanto en el ciudadano, como en el gobierno, no hay un freno a este tipo de ordenadores extranjeros, ni mucho menos se tiene conocimiento a nivel general de quien es el responsable y el encargado de este tipo de tratamiento.

Como segundo punto haremos mención de las gentes que si tienen conciencia de protección, y si se preocupan de leer el aviso de privacidad de cualquier empresa o ente particular a la cual le proporcionan información.

Supongamos que se logra que la mayoría de las personas tenga cultura de privacidad, pero ¿realmente tenemos seguridad jurídica en el manejo de la información personal?,

Que pasa a nivel empresa si el responsable no tiene el cuidado de capacitar al encargado, o el encargado no tiene el cuidado adecuado de la información, se recaería de nuevo en un paraíso de datos como *Facebook*, pero a nivel personal, a nivel del encargado, y no solo *Facebook* también entre este tipo de servidores podemos englobar a *Hotmail*. Una página que proporciona correos electrónicos para el envío de información, que se enlaza a otros servidores, en lo general, la red. Es un flujo de información, en la que si no se encuentra la cultura de protección en el usuario, es muy difícil evitar la divulgación de la misma.

Pongamos otro ejemplo.

Una empresa, digamos, una constructora, que compra un bien inmueble, por decir un terreno, pero que a la hora de realizar el contrato de compraventa

respectivo se proporciona información, tal y como el nombre del comprador, su dirección, estado civil, RFC, CURP, lugar de nacimiento, oficio o arte, teléfono, referencias, entre otras cosas un beneficiario y su relación de parentesco con este.

Como se puede observar, se proporciona información exacta, por lo regular, del núcleo familiar. Ahora bien, supongamos que en esta constructora, no se toman las medidas necesarias para que exista una persona encargada capacitada en el manejo de datos personales; el responsable puede que cumpla con sus funciones al proteger y salvaguardarlos bajo todas las medidas de seguridad ya citadas con anterioridad, pero el encargado es una persona que tiene un cumulo de información importante en sus manos y de muchas personas, compradoras de terrenos.

El encargado, al no tener una sanción establecida por la ley, aunque el responsable se encargue del pago de los daños y perjuicios causados, solo peligraría su trabajo, ya que no existe una sanción como tal mas que la responsabilidad si se logra comprobar que en el caso de que ocurriera una fuga de información y se suscitara un delito en el cual el encargado participase directamente podría fincarse a este una responsabilidad penal.

Pero en este mismo supuesto, que pasaría si el titular se da cuenta que su información fue proporcionada y ha sido filtrada, antes de que se cause cualquier otro percance, que podría hacer el titular al encargado del tratamiento de su información, o en el mejor de los casos de que no se cometiera algún acto delictivo o se viera el titular acosado o molestado, por partidos políticos, instituciones de crédito o terceras personas quienes no deberían de tener esta clase de información.

¿Realmente con la reparación del daño que a veces es una precaria cantidad, reparan la tranquilidad, la libertad y la seguridad entre otras?

No solo basándonos en la seguridad de los datos, también en la procuración del respeto a los derechos ARCO, ya que a su vez que el responsable tiene que cumplir con la solicitud del titular, el encargado también debe de hacerlo y velar por los intereses del mismo, siendo esta una obligación; y así al encargarse del tratamiento, en caso de una solicitud de acceso a su información por parte del titular, procurar que se atienda pronto, así como por lo que respecta a los demás derechos como son los de rectificación, oposición o cancelación. Tomando en consideración lo anterior, ponemos el siguiente caso:

Qué ocurriría si el encargado no procurara que el titular tuviere pronto su información en caso de que este llegara a necesitar datos que son difíciles de memorizar, o en su defecto, al momento no estén a su disposición, o que se encuentren erróneos, la persona titular no podrá corregir la información falsa para así tener una validez jurídica, en el caso de que nos mantengamos en el ejemplo de la constructora, se puedan realizar las escrituras con la información correcta, o que el comprador quisiera cancelar su contrato de compraventa o cambiar la información de su beneficiario etc.

También a la hora de la cancelación, él prefiere que no se guarde total o parcialmente su información, el encargado tiene que realizar la cancelación de la información para futuros problemas que pudiese tener el titular por el resguardo indebido de la información; no debe incurrir en el engaño al titular de la información al afirmar que los datos proporcionados han sido eliminados, cuando no se ha hecho; debe apegarse a los principios establecidos por la ley, procurando que el aviso de privacidad esté completamente a la vista, o proporcionar información para despejar las dudas que surgieran en las personas que no se encuentran familiarizadas con este concepto; así mismo el encargado debe cumplir principalmente con el deber de confidencialidad, (establecido en el artículo 21 de la Ley en comento), y procurar que el manejo de la información lo realice el personalmente para evitar el flujo de la misma a cualquier otro tercero no autorizado, a efecto de cumplir la finalidad exclusiva

por la cual fueron proporcionados los datos, y sobre cualquier otra cosa, procurar la seguridad de la información que le es confiada.

En resumen el encargado debe, procurar proteger la información tal y como lo haría el responsable, y ello solo se lograría estableciendo obligaciones solidarias para ambos sujetos.

La propuesta de la sustentante, es que se establezca en la ley una sanción, para que ambas partes tanto el responsable como el encargado respondan de forma solidaria

Esta medida propositiva es con el fin de que tanto la persona responsable como el titular de la información tomen precauciones y tengan una seguridad como un equipo; el propietario de los datos, al proporcionar información, quien la recibe, o sea el responsable, para emplear a personas que cubran con el perfil requerido, y que tendrán una sanción por su negligencia o falta de honradez.

Podemos decir que el encargado tiene las funciones del responsable, que le otorga tanto la ley como el reglamento, y al no tener una sanción existe la posibilidad de que pueda divulgar la información del titular, sin tener que enfrentar problemas serios, y en cambio obtener beneficios económicos o personales.

La sociedad informatizada afronta nuevos riesgos y el Derecho “debe” estar a la altura de las circunstancias. No se trata de plantear la cuestión en términos de una lucha entre la sociedad cibernética y los derechos fundamentales. Juzgamos superada la etapa en que el problema discurría como una tensión dialéctica entre “vida privada vs. Computadoras”, pues el presente estado de la evolución de la normativa furtiva de la información personal constituye una síntesis de los intereses sociales e individuales en juego[44].

[44] BATTO, Hilda. “Informática, Libertad y Derechos Humanos”, en Derecho Informático, Edit. Depalma,

4.2.- Propuesta de reformas al marco jurídico.

Es un hecho, como ya se ha señalado, que en el mundo se ha dado un significativo avance de la tecnología, principalmente en el campo de las comunicaciones, especialmente en el área de la informática, la cual se ha venido desarrollando de una manera muy dinámica; obviamente tal acontecimiento ha impactado de manera determinante a varias actividades como el comercio, las educativas, culturales, financieras y otras más en las que se da el intercambio de datos personales y pone de manifiesto el efecto nocivo que muchas veces ha ocasionado en estos el desarrollo de la tecnología.

Tales circunstancias han hecho patente la necesidad de tomar medidas, para lograr una debida protección y seguridad de los datos en cuestión; debiendo señalar que también se ha hecho urgente tal necesidad, debido a que, paralelo al avance de la tecnología, igualmente ha crecido la inseguridad, misma que es ocasionada por individuos o grupos delictuosos quienes por cualquier medio obtienen información personal, y a través de la intimidación u otros mecanismos afectan a su titular, obteniendo determinadas sumas de dinero.

A tales vicisitudes no ha sido ajeno nuestro país, por lo que con el objeto de proporcionar una adecuada protección y seguridad a las personas que proporcionan datos de carácter personal, fue que se creó la LFPDPPP; pero aunque esta ley fue publicada en el 2011, hasta la fecha no hay la certeza de que haya funcionado. Si bien hay encuestas que nos dicen que si se ha aplicado a las empresas, así como de cuantos particulares ya cuentan con el aviso de privacidad, mas no existe ninguna que nos permita evaluar si efectivamente esta legislación ha cumplido en lo general con la finalidad para la que fue creada o simplemente será un documento más como muchas otras leyes promulgadas.

Buenos Aires, Argentina, 1987, p. 249; cit. por Travieso, Juan Antonio, Derechos Humanos y Derecho Internacional, Edit. Heliasta S.R.L., Buenos Aires, Argentina, 1990, p. 354.

Todo lo analizado en el cuerpo de este trabajo nos lleva a concluir que la ley en cuestión no ha tenido el impacto ni la importancia que debiera. Y si esto sucede a nivel de la metrópoli, en provincia es mayor el desconocimiento de la misma, pues cabe señalar, que en cuestionamientos realizados a personas del estado de Hidalgo, principalmente en Pachuca, nos responden que no saben de dicho ordenamiento, siendo que el mismo es una Ley Federal, lo cual podría significar, que el Gobierno no le ha dado la importancia debida, ni mucho menos el órgano encargado de ésta, el IFAI.

Por ello, uno de los motivos que se persiguen con el presente trabajo de investigación, es el divulgar información sobre la ley que nos ocupa, es decir, dar a conocer lo qué es la misma, cuál es su contenido, a quienes va dirigida, que es lo que se pretende con ella, y enfatizar que tiene como objetivo principal dar seguridad y protección a los ciudadanos como titulares de datos personales, además darles información de que en la misma existen sanciones para las personas que hacen mal tratamiento de los datos en cuestión, y sobre todo para que dicha información les proporcione una cultura, para que cuando se vean en la necesidad de aportar sus datos, sepan que como titulares o propietarios de los mismos, también tienen derechos para exigir de las personas involucradas en el tratamiento de estos, una responsabilidad, en el caso de que los usen, den a conocer, o bien los transfieran sin su consentimiento, por no estar permitido en la ley, so pena de ser sancionados en alguna de las formas que establece la misma, y que de tomarse en cuenta las propuestas hechas en esta tesis, en un caso dado puedan ser resarcidos de daños y perjuicios.

Por tanto, si las personas titulares de datos personales no saben acerca de la ley, tampoco sabrán de las sanciones que contempla la misma cuando son violados dichos datos, por ello se considera que a medida que sean establecidas de forma solidaria obligaciones y sanciones para los tratantes de los multicitados datos, y no solo para el responsable, estamos seguros que dicha ley tendrá eficacia y por lo mismo será conocida de forma íntegra por la ciudadanía aportante de datos.

Pues es del conocimiento general, que una persona sabe acerca de que el robo es un delito, en virtud de que dicho ilícito se encuentra tipificado como tal en el Código Penal. Asimismo, las personas conocen acerca del incumplimiento de contrato, porque esta figura jurídica se encuentra establecida en la legislación Civil, y es por tales consideraciones también que se proponen a la ley que nos ocupa las reformas a que nos hemos referido:

Se propone reformar el artículo 63 de la LFPDPPP, para que exista una responsabilidad solidaria entre el responsable y el encargado, en lo que respecta a sus obligaciones, en consecuencia las sanciones tanto pecuniarias como penales deben ser para ambos, para evitar el flujo de información, así como la comisión de delitos contra los titulares de datos; por lo tanto en los artículos del apartado de sanciones de la ley en cuestión debe establecerse expresamente que los mismos son aplicables para ambos (responsable y encargado).

> Artículo 67. Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.
>
> Artículo 68. Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.
>
> Artículo 69. Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.

Así mismo se propone reformar el Código Civil Federal, para establecer la regulación de un contrato de protección de datos personales en posesión de particulares, el cual quedaría reglamentado en la, PARTE SEGUNDA, de las Diversas Especies de Contratos, TITULO DECIMOSÉPTIMO, del ordenamiento sustantivo indicado.

Esto es, para que exista un contrato entre el responsable y el encargado para tener una mayor seguridad jurídica todos los sujetos contemplados en la Ley

Federal de Protección de Datos Personales, y el contrato se encuentre expresamente regulado para la realización del mismo, el hecho de que la ley principal lo contemple creará que este tipo de regulaciones sean importantes.

4.3.- Responsabilidad solidaria entre el "Responsable" y el "Encargado" en cuanto a las sanciones.

El tema de que trata en este apartado es una de las propuestas más importantes que se formulan en este trabajo, porque el objetivo del mismo es precisamente que se logre una efectiva protección y seguridad de los datos del titular y garantice que en un caso dado a éste se le pueda resarcir de las consecuencias que arroje alguna conducta que lesione su patrimonio cometida por quienes manejan sus datos.

Por ello y para entender más sobre dicha propuesta, se hace necesario mencionar que como lo hemos señalado, los sujetos más importantes, en cuanto al tratamiento de datos de carácter personal, son los responsables y los encargados. Estos sujetos constituyen las figuras más importantes en dicho rubro, ya que son quienes se encargan de la gestión de los datos en cuestión.

Asimismo, se ha resaltado el hecho de que en el caso de las empresas, a quien asignan éstas, la mayoría de las veces, como tratante o encargado del manejo de datos personales, es a su propio personal, y es en quien delegan las obligaciones que en ese rubro le corresponden al responsable, a pesar de que por lo general no cuenta con ninguna capacitación, ni mucho menos se la dan, para que esté en condiciones de poder brindar o proporcionar a los titulares un adecuado manejo y protección de sus datos.

Sin embargo, como también lo hemos mencionado, pese a que en los hechos tanto el responsable como el encargado o tratante de datos personales comparten la responsabilidad de ver y velar por la protección y seguridad de los datos personales del titular, al único a quien se imponen obligaciones y establecen sanciones en la ley es al responsable, tal y como se advierte de lo

dispuesto en los artículos 63 y 64 de la ley en comento, pero jamás se establecen para el encargado.

Es en este marco que se propone una responsabilidad solidaria del encargado en relación con el responsable, puesto que como ya se ha mencionado, en la ley solo existen tanto obligaciones y sanciones para el responsable, más no para el encargado o tratante de datos personales, por tal razón se propone que las mismas también se establezcan para éste último, para que una vez que exista una responsabilidad solidaria entre ambos, se solucionen varios problemas, entre otros robo, alteración o modificación, pérdida total o parcial, transmisiones indebidas o ilícitas, accesos no autorizados y robo de identidad, que pueden lesionar los derechos o libertades fundamentales del titular, en los que se ve envuelto el patrón y el trabajador, es decir responsable y encargado, y que en muchas ocasiones se deben a negligencia por parte de éste último, ya sea de manera voluntaria o accidental,

Conductas como las anteriores, que se podrían evitar con la propuesta que se formula, ya que teniendo obligaciones y sanciones el encargado, procuraría tener más precaución o cuidado al manejar los datos de la persona titular de los mismos, y con ello no solo ofrecería una seguridad a éste, sino que al responsable también, además de que el encargado tendrá el derecho de exigir al responsable medidas para procurar la seguridad de los datos, y éste a su vez también se vería, para evitarse problemas como los señalados, en la necesidad de escoger mejor al personal que va a designar para el tratamiento de los datos y darle una buena capacitación tanto técnica como científica para que en lo más mínimo cometa algún error, pues se debe recordar que el encargado de la protección de datos personales, tiene la obligación de capacitarse, para realizar esta función; y estar consciente de que sobre él recae la seguridad de proteger los datos de que trata; así mismo, debe de cumplir con una serie de requisitos para que le sea delegada la obligación de ser el responsable, y pueda llevar un tratamiento adecuado de la información que se le encarga, garantizando de

esta manera un buen manejo para evitar el mal tratamiento de datos personales.

Además, de adoptarse tal propuesta, la misma complementaría a la que se formula respecto a la celebración entre el responsable y el encargado del contrato que hemos llamado de protección de datos personales, ya que ambos compartirían una responsabilidad; así mismo el encargado podría requerir al responsable para que cumpla con su obligación contractual y estaría en aptitud o tendría el derecho de exigir al responsable medidas para procurar la seguridad de los datos; el responsable a su vez se vería, para evitarse problemas como los señalados, en la necesidad de darle al encargado una buena capacitación tanto técnica como científica para que en lo más mínimo cometa algún error, y cumplir de esta manera con el deber de brindad al titular de los datos una buena protección y seguridad de los mismos.

4.4.- Reforma al artículo 63 de la LFPDPPP.

Las infracciones que contempla la Ley por el incumplimiento de las obligaciones relacionadas con el Aviso de Privacidad son:

Infracción: Omitir en el Aviso de Privacidad alguno o todos los elementos que se refiere el artículo 16 de la Ley.

Multa: De 100 a 160,000 días de salario mínimo vigente en el DF. Art. 64 de la LFPDPPP.

Infracción: Transferir datos a terceros sin comunicar a éstos el Aviso de Privacidad que contiene las limitaciones a que el titular sujetó la divulgación de los mismos.

Multa: De 200 a 320,000 días de salario mínimo vigente en el DF. Art. 64 de la LFPDPPP.

En consecuencia, el principal beneficio de adecuarse la propuesta de la sustentante, es que al momento en que el titular del dato requiera a una empresa el ejercicio de alguno de sus derechos de acceso, rectificación, cancelación u oposición, o se requiera transferir o recibir bases de datos a nivel nacional o internacional, la empresa sabrá cómo responder a este requerimiento en forma eficiente, práctica y conforme a la Ley, con lo cual se evitarán las sanciones, que pueden llegar a $9,571,200 pesos y que pueden duplicarse a $19,142,400 pesos, en caso de datos sensibles, independientemente de las sanciones en caso de reincidencia.

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

Uno de los principales objetivos de la ley, es el de desincentivar conductas contrarias a lo establecido por la misma, y al tratarse de un derecho fundamental reconocido a nivel constitucional, debe garantizarse al ciudadano en tal virtud, una vez que ha sido violado su derecho, habrá una consecuencia para el responsable que actuó con negligencia o dolo (mas no para el encargado) en el debido tratamiento de su información, máxime cuando ésta fuere respecto a datos sensibles. Es importante destacar que para efectos de sus resoluciones, el IFAI no está subordinado a autoridad alguna, ya que es un organismo descentralizado de la Administración Pública Federal, no sectorizado, por lo que goza de autonomía operativa, presupuestaria y de decisión. Es una institución al servicio de la sociedad[45].

[45] https://www.infomex.org.mx/gobiernofederal/home.action, 20 septiembre 2013, 10:38.

Como se ha resaltado con anterioridad, los sujetos más importantes, en cuanto al tratamiento de datos personales del titular, son el responsable y el encargado. Ambos sujetos son determinantes en dicho rubro, ya que son quienes se encargan de la gestión de los datos en cuestión.

Sin embargo, como también lo hemos mencionado, pese a que en los hechos tanto el responsable como el encargado o tratante de datos personales comparten la función de velar por la protección y seguridad de los datos personales de titular, al único a quien se imponen obligaciones y establecen sanciones en la ley es al responsable, tal y como se advierte de lo dispuesto en los artículos 63 y 64 de la ley en comento, pero jamás se establecen para el encargado.

Tal omisión de no establecer obligación o sanción alguna en la ley para el tratante o encargado, en un caso dado redunda en perjuicio del titular, ya que si a éste se le causara algún daño o menoscabo en su patrimonio, por incurrir en un mal manejo de sus datos, el mismo quedaría en estado de indefensión, al no poder hacer efectiva alguna acción, por no contemplar la ley obligación ni sanción alguna para el tratante. Es decir, que el propietario de los datos de ninguna manera podría ser resarcido de los daños o perjuicios que le causara el encargado, ya que el responsable solo estaría limitado a las sanciones que le impone la ley; siendo por tal razón que se propone que además de las obligaciones y sanciones establecidas para el responsable se impongan también para el encargado o tratante, por ser la persona que realmente tiene a su cargo el uso, distribución almacenamiento y difusión de los datos en cuestión, y es precisamente quien, en caso de un mal manejo de dichos datos, quedaría sin ninguna responsabilidad, por lo mismo de que en la ley no se contempla obligación alguna para él. Un ejemplo de las sanciones que se aplican a los responsables, es la impuesta a Banamex, el día 28 de agosto de 2013, donde el Pleno del IFAI resolvió, por unanimidad, imponer cuatro multas, que en total suman 9 millones 848 mil 140 pesos:

Multan a Banamex por dar datos personales

El Instituto Federal de Acceso a la Información multó con más de nueve millones de pesos a la sociedad financiera Banamex por revelar datos de un particular.

La firma Tarjetas Banamex S.A. de C.V. fue multada por el Instituto Federal de Acceso a la Información (IFAI) por más de nueve millones de pesos por haber revelado los datos personales de un particular para cobrar un adeudo.

A través de un comunicado, el IFAI informó que en junio del año pasado un particular presentó una denuncia ante el organismo en la que expuso que Banamex entregó sus datos personales sin su autorización a un despacho jurídico que le reclamó adeudos de una persona ajena a él.

"El particular sostuvo que el banco se había comprometido, en dos ocasiones y por escrito, a cesar las llamadas telefónicas de cobranza. Sin embargo, no cumplió", expresó el organismo de transparencia.

Debido a esto, se le solicitó a la firma financiera que emitiera un reporte detallado con la queja y, al no ser atendido, el instituto ordenó un procedimiento de verificación.

El pasado mes de marzo se elaboró una resolución en la que se expuso que la empresa financiera incurrió en diversas infracciones a la Ley Federal de Protección de Datos Personales, por lo que comenzó el procedimiento para imponer sanciones.

Por su parte, Banamex compareció en abril de este año para defender sus derechos ante el IFAI, pero no logró desarticular o evadir las infracciones impuestas.

El IFAI informó que Banamex no respetó los principios de consentimiento de calidad y de responsabilidad, mantuvo datos inexactos del titular y no llevó a cabo la rectificación de los datos[46].

Lo anterior nos demuestra que si una empresa tiene fallas o vulnerabilidad debido a que su personal no está capacitado o no le toman la importancia debida a este tipo de información, el IFAI, como ya lo hemos señalado con anterioridad, tiene las facultades para sancionar cuando se haga mal uso de los datos personales, facultades que le otorga la LFPDPPP.

[46] http://www.eluniversal.com.mx/nacion-mexico/2013/multa-ifai-a-tarjetas-banamex-por-dar-datos-personales-948500.html, 13 septiembre 12:30 am.

Por ello se señala que la actuación de un encargado, incluso, en caso de incurrir en un mal tratamiento de los datos que le hayan sido asignados para su resguardo y protección, podría ocasionar un perjuicio mayor al titular , al saber que la ley no establece ninguna obligación para él. Siendo por las anteriores consideraciones que en el presente trabajo se propone que sea adicionado el artículo en comento (artículo 63 LPDPPP), agregando algún párrafo en el cual se contemplen obligaciones para el encargado o tratante de datos; y también se le impongan sanciones para el caso de que incurra en un mal tratamiento de los datos del titular, esto es, que les dé un mal uso, los difunda, divulgue, o bien, los trasfiera a personas ajenas o terceros, no estando autorizado por el titular, y le cause a este daños y perjuicios, tanto en su patrimonio como en su persona, en el caso de que se vean afectados sus datos sensibles, esto es, que se den a conocer aspectos de raza, religión, sexo, creencia, salud etc.

Con la reforma propuesta al artículo citado, el propietario de los datos personales tendría una garantía de que estos serán respetados, en virtud de que al establecerse obligaciones, responsabilidades y sanciones para el encargado, ante el establecimiento de tales medidas, el mismo adoptaría los cuidados necesarios para no incurrir en alguna responsabilidad al manejar los datos del titular.

CONCLUSIONES:

PRIMERA.- En el mundo, la tecnología ha avanzado de manera vertiginosa, y en especial en el campo de la informática; este avance, lo que, ha venido a influir de manera determinante en el área de las comunicaciones e información, afectando por consiguiente las relaciones sociales, principalmente la privacidad de las personas, porque con base al intercambio comercial, educativo, cultural así como de otras actividades, sus datos personales han ido perdiendo esa privacidad.

SEGUNDA.- Era imperiosa la necesidad el crear una legislación que se encargara de la protección de los datos de carácter personal, y en especial de regular la actividad de aquellas personas particulares que se encargan de recabar tal información y su tratamiento; por ello es el acierto en la promulgación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, ordenamiento con el cual se protegen tanto los registros médicos, financieros, educativos y de otra índole que tienen los titulares, con la finalidad de que sean tratados y protegidos de manera adecuada. Esta Ley recoge compendios de los modelos general y sectorial, y se erige como una herramienta legal necesaria para proteger la privacidad de las personas respecto al tratamiento que puedan dar otros particulares respecto a su información personal.

TERCERA.- En países vecinos al nuestro, la cultura de protección de datos personales se ha dado ya desde años atrás, sin embargo en México, a pesar de que desde el año 2010 existe una ley sobre esta materia, la introducción de esta cultura ha sido lenta; es por lo que en este trabajo se hace especial énfasis en la intensificación de este tema, no solo para que conozcan de ella las personas adultas sino también las jóvenes, que generalmente son quienes día a día se encargan de trasmitir información a través de redes informáticas.

CUARTA.- La legislación ha creado la necesidad de comprender ¿Cómo? ¿Cuándo? ¿Dónde? y ¿Por qué? se recaba la información de los titulares, lo

que nos permite, conocer las bases de datos donde se almacena la información, es por tal motivo que en el presente trabajo se hace especial énfasis, en la cultura de protección de datos que deben ir asimilando las personas usuarias de los servicios, en virtud de que no existe mayor seguridad que el conocimiento, que muchas veces se traduce en la precaución que se debe tomar en todas las actividades que se realizan día con día, y especial cuando se aportan datos de carácter personal a un particular o a una empresa, de tal manera que si no se pone atención y no se toman precauciones, quien los aporta resulta afectado, ya sea en su persona o en su patrimonio.

QUINTA.- Respecto de las empresas particulares, se hace hincapié en que, deben considerar la asignación de presupuesto para **seguridad** de Tecnologías de la Información y hacer de la protección de información una práctica común en la operación del giro de la empresa o la persona física. Con frecuencia la responsabilidad de asegurar el cumplimiento de las regulaciones recae en los profesionales de Tecnologías de la Información, sin embargo, para que estas sean adecuadas tienen que estar involucrados los diversos representantes de la empresa, empezando por los dueños del negocio, el área legal, Recursos Humanos, Sistemas y Tecnologías de la Información. No hay que olvidar que la falla en este sentido puede traer serias consecuencias, incluyendo multas sustanciales y demandas legales que afectarán directamente la situación financiera de la empresa.

SEXTA.- Como usuarios, debemos comprometernos a percibir con claridad los derechos a los que tenemos acceso a través de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, En La medida que entendamos esos derechos, comprenderemos la responsabilidad que asumimos al relacionarnos con los datos personales de otra persona, es Importante conocer la ley indicada a fin de estar en posibilidades de atender oportunamente los compromisos requeridos por esta legislación, así como los procesos en los que se tratan datos personales. El estudio de la ley en la materia permite conocer que es un aviso de privacidad, entender para que sirve día a día a los titulares

les proporcionará seguridad tanto para ellos como para sus familias, y tendrán también conocimiento de los derechos ARCO (acceso rectificación cancelación y oposición).

SEPTIMA.- Con la necesidad de que se capacite al personal que colabora con el particular, o bien al de una empresa, al que se le asigna el tratamiento de datos de carácter personal, para garantizar de alguna manera una adecuada protección y seguridad de los datos en cuestión; igualmente se debe crear un documento que jurídicamente sustente la responsabilidad solidaria entre el responsable y el encargado, para una mayor seguridad jurídica de todos los sujetos definidos en la Ley, esto es la existencia de un contrato en el que existan que cumpla con todos los elementos para los de su clase; con el objeto de que las partes contratantes se encuentren comprometidas con los intereses del titular, en cuanto a velar por la seguridad y protección de los datos de éste, y que en dicho documento consten las actividades específicas del encargado y la responsabilidad que este tiene para con los titulares y el responsable.

OCTAVA.- Se deben establecer en los artículos 63 y 64 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, obligaciones y sanciones respectivamente para el encargado o tratante de los datos en comento; para efectos de que junto con el responsable tenga una responsabilidad solidaría ante el titular de datos en cuestión, y éste igualmente quede protegido ante la comisión de algún ilícito por parte de dicho encargado, que le pudiera afectar en su persona o bien en su patrimonio, al causarle algún daño o perjuicio.

NOVENA.- Aunque en teoría tanto el responsable como el tratante o encargado asumen una responsabilidad en cuanto al tratamiento de datos personales, en la práctica el que realmente se encarga del tratamiento de los mismos, es el último de los mencionados, quien muchas veces, por no tener una capacitación adecuada para el correcto manejo de los datos personales, cuya custodia se le asigna, incurre en algún error o en algún ilícito, ya sea proporcionando a un

tercero los datos del titular sin el consentimiento de este, ocasionándole algún daño o perjuicio o bien una afectación en la esfera de sus derechos íntimos (raza, religión, orientación sexual, inclinación política, salud etc.); y toda vez que en la ley de la materia no se le impone ni obligación ni sanción alguna no puede imputársele alguna responsabilidad por tal conducta, por ello es de suma importancia la modificación de los artículos 63 y 64 de la citada ley.

FUENTES CONSULTADAS:

LIBROS

- NOGUEIRA, Humberto, "Autodeterminación informativa y hábeas data en Chile e información comparativa", Anuario de Derecho Constitucional Latino- americano, México, 2005, p. 449.

- GALLO RUIZ, Gonzalo, Iñigo Coello de Portugal Martínez del Peral, Fernando Parrondo García, Héctor Sánchez Montenegro. La Protección de Datos Personales: Soluciones en Entornos Microsoft®, Madrid, 2003.

- CORRIPIO Fernando, Diccionario Etimológico General de la Lengua Castellana, Editorial BRUGUERA, Segunda edición, septiembre de 1977, España

- *HUERTA VILLALÓN, Antonio. "Seguridad en Unix y Redes". Versión 1.2 Digital - Open Publication License v.10 o Later. 2 de Octubre de 2000.*

- ROJINA VILLEGAS, Rafael. "Contratos". Ed. Porrúa. México DF.

- POTHIER, Robert Joseph. "Tratado de las Obligaciones". Pág. 10 Tribunal Superior de Justicia del Distrito Federal y la Dirección General de Anales de Jurisprudencia y Boletín Judicial, invierno 2002-2003.

- FIGUEROA Luis Mauricio, Contratos Civiles, Editorial Porrúa, México 2007.

- CASTILLO CHIRINO Joel, Contratos, Editorial Porrúa, México 2007.

- BORJA SORIANO Manuel, Teoría General delas Obligaciones, Editorial Porrúa, México 1962.

- ALESSANDRI R, Arturo y Somarriva U, Manuel. "Curso de Derecho Civil, Fuentes de las Obligaciones".

- OSORIO, Manuel. "Diccionario de C.C. Jurídicas" Editorial Helestica, Pág. 17.

- BATTO, Hilda. "Informática, Libertad y Derechos Humanos", en Derecho Informático, Edit. Depalma, Buenos Aires, Argentina, 1987, p. 249; cit. por Travieso, Juan Antonio, Derechos Humanos y Derecho Internacional, Edit. Heliasta S.R.L., Buenos Aires, Argentina, 1990, p. 354.

- SALMERÓN CASTRO, Alicia, ¿Cómo formular un proyecto de tesis? : guía para estructurar una propuesta de investigación desde el oficio de la historia, México, D.F. Trillas, 2013.

- WITKER VELÁSQUEZ Jorge Alberto, La investigación jurídica, México : UNAM, Instituto de Investigaciones Jurídicas, 2011.

- ORTIZ CASTRO José Iván, Aproximación metodológica a los niveles jurídico-políticos de la investigación social, Medellín, Colombia: Universidad de Medellín, 2005. archivo electrónico.

FUENTES ELECTRONICAS

- http://www.un.org/es/documents/udhr/, Declaración Universal de los Derechos Humanos, 03 de enero 2013. 17:20.
- http://www.oas.org/es/cidh/mandato/Basicos/declaracion.asp, 27 enero 2013, 14:25.
- http://blog.derecho-informatico.org/faqs/datos-personales/ 23 08/12 23:33

- https://www.infomex.org.mx/gobiernofederal/home.action, 20 septiembre 2013, 10:38.
- Mhttp://www.eluniversal.com.mx/nacion-mexico/2013/multa-ifai-a-tarjetas-banamex-por-dar-datos-personales-948500.html, 13 septiembre 12:30 am.

LEGISLACION

- Constitución Política de los Estados Unidos Mexicanos

- Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

- Guía Práctica Para Generar El Aviso De Privacidad IFAI.

- Ley Federal De Protección De Datos Personales.