INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

"PROPUESTA DE UN MODELO DE AUDITORÍA INTEGRAL QUE GARANTICE EL CUMPLIMIENTO DE DISPOSICIONES EN MATERIA DE DATOS PERSONALES Y SEGURIDAD DE LA INFORMACIÓN EN MÉXICO"

SOLUCIÓN ESTRATÉGICA EMPRESARIAL

Que para obtener el grado de MAESTRO EN DERECHO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Presenta:

Federico González Peña

Asesor:

Dra. Olivia Andrea Mendoza Enríquez

Ciudad de México, a 01 de marzo de 2019

AUTORIZACIÓN DE IMPRESIÓN

Ciudad de México, 27 de marzo de 2019

La Gerencia de Capital Humano/ Gerencia de Investigación hacen constar que el proyecto terminal titulado:

"Propuesta de un modelo de auditoría integral que garantice el cumplimiento de disposiciones en materia de datos personales y seguridad de la información en México"

Desarrollada por el alumno

Nombre: **Federico**

Apellido paterno: **González**

Apellido materno: **Peña**

Desarrollado bajo la asesoría del:

Dra. Olivia Andrea Mendoza Enríquez

Ha sido revisado y aprobado por miembro del Núcleo Académico Básico (NAB).

Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención.

Vo. Bo.

Mtra. Gabriela García Acosta
Encargada de la Gerencia de Evaluación de Proyectos

***Anexar a la presente autorización al inicio de la versión impresa del proyecto integrado que ampara la misma.**

Tabla de contenido

Índice de figuras y cuadros

Siglas y abreviaturas

Las siglas y abreviaturas que son utilizadas en el presente documento se muestran a continuación:

Sigla / abreviatura	Significado
APEC	Asia-Pacific Economic Cooperation
CONDUSEF	Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros
CPEUM	Constitución Política de los Estados Unidos Mexicanos
DOF	Diario Oficial de la Federación
ECPA	Electronic Communications Privacy Act
EUA	Estados Unidos de América
IFAI	Instituto Federal de Acceso a la Información y Protección de Datos, hoy INAI
INAI	Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales
OCDE	Organización para la Cooperación y el Desarrollo Económicos
ONU	Organización de las Naciones Unidas
PIPEDA	Personal Information Protection and Electronic Documents Act
PROFECO	Procuraduría Federal del Consumidor
TIC	Tecnologías de la Información y Comunicación

Introducción

El derecho a la protección de los datos de las personas es un derecho fundamental reconocido internacionalmente. Se trata de un derecho subjetivo, autónomo que constituye un instrumento jurídico imprescindible en el desarrollo de una sociedad y que garantiza la libertad del individuo.[1]

El derecho a la protección de datos es reconocido como derecho fundamental en el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea y algunas constituciones de diversos países, entre ellas, México. Dicho derecho ha sido desarrollado en las últimas cuatro décadas de manera paralela al avance informático y tecnológico que ha traído como consecuencia el uso intenso de información. El referido derecho no se acota a reconocer la protección de datos personales dentro de una garantía fundamental y autónoma, sino que, además establece los principios básicos que lo rigen, asimismo, determina la existencia de una autoridad de control independiente encargada de hacer cumplir los extremos de protección de este nuevo derecho.

El avance de las comunicaciones nos obliga a analizar cuándo la tecnología tiene un carácter intrusivo que daña la calidad de vida de las personas, o, por el contrario, cuando sirve para generar beneficios. El hecho es que, derivado de estos avances, el individuo tiene el poder de disponer de su propia información y decidir quién, cómo y cuándo se hará uso de su información. Es así, como en una sociedad donde impera el estado de derecho, se debe garantizar el límite sobre la forma de uso de información y datos personales, tarea que no resulta fácil al considerar la diversidad de medios de comunicación, gobiernos y entidades privadas que acumulan y tratan información, y datos personales para distintos fines, por lo que, los Estados deben tomar medidas preventivas y correctivas que no se limiten al

[1] Peschard Mariscal, Jaqueline. El derecho fundamental de protección de datos personales en México. Tirant Lo Blanch, México, 2013.

ámbito local, sino que trasciendan al ámbito internacional, ya que la protección a la transferencia y flujo de información no queda limitada territorialmente.

Los derechos humanos se presentan como exigencias morales de realización, tanto a nivel personal como comunitario, y que, a partir del desarrollo histórico, se encuentran sustentados por un aparato institucional amplio, así como de un cuerpo normativo en continua expansión.

El derecho a la información y a la protección de datos personales, como derechos nuevos que se conciben actualmente, ofrecen cuestionamientos que llevan a la necesidad de distinguir sobre su naturaleza jurídica y conceptual en el ámbito general de otros derechos. En el caso del contexto europeo, estos derechos son considerados como derechos fundamentales, por tener un reconocimiento como derechos humanos universales, terreno en que esta clase de derechos han adquirido un tratamiento específico y preponderante, en relación con otros países en el mundo. La composición de sus características como ordenamientos jurídicos nuevos trae como consecuencia que a la fecha no existan denominaciones precisas y unívocas sobre su naturaleza jurídica y conceptual. Estas imprecisiones han ocasionado que los derechos objeto de investigación, de manera indistinta, reciban denominaciones como derechos humanos o derechos fundamentales, tanto en instrumentos de derecho internacional como nacional.

Capítulo 1

Orígenes del término "*privacidad*" y su relación con el concepto "*datos personales*".

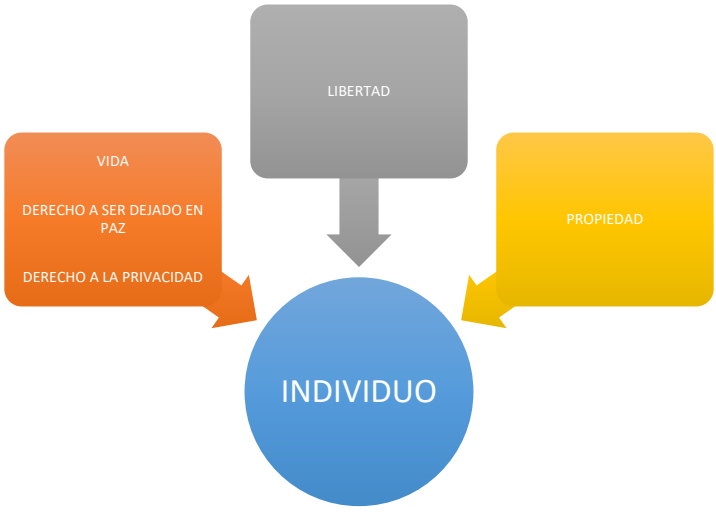
Capítulo 1: Orígenes del término "*privacidad*" y su relación con el concepto "*datos personales*".

Los estudios jurídicos sobre la "*privacidad*" se remontan a finales del siglo XIX con obra "*The Right to Privacy*", de los juristas estadounidenses Samuel Dennis Warren *y* Louis Dembitz Brandeis, documento que se ha convertido en un referente obligado de análisis y estudio en materia del derecho a la privacidad.

Sirve mencionar que Warren y Brandeis rescatan y adoptan la definición de privacidad, entendida como el "derecho a ser dejado en paz (o a solas)" ("*The right to be let alone*")*,* que había sido desarrollado por primera vez en la obra "*The elements of Torts*" del Juez Thomas A. Cooley.[2]

Sin lugar a dudas, la parte fundamental de la obra de Warren y Brandeis es el contraste que hace entre los derechos a la propiedad material e inmaterial, lo que se puede ejemplificar con la representación gráfica que sigue:

Figura 1. Contraste entre los derechos a la propiedad material e inmaterial.



Fuente: Elaboración propia.[3]

Por otro lado, en la tendencia latinoamericana tenemos el concepto "*Habeas*

[2] Warren, Samuel y Brandeis, Louis. El Derecho a la Intimidad. Civitas, Madrid, 1995, p. 13.

[3] *Ídem*.

Data" que etimológicamente significa "*conserva o guarda tu información*". La palabra dato tiene su origen en el latín "*datum*", que, interpretado, desde esta perspectiva, se refiere a la información que forma parte de la vida privada de las personas y que está almacenada en una base de datos.

En cuanto a la naturaleza jurídica del "*habeas data*", notamos que ésta varía dependiendo en el nivel de importancia que le reconoce cada jurisdicción. Por ejemplo, en Argentina y Brasil el "*habeas data*" se reconoce como "*un remedio constitucional*"; en Colombia como un "*derecho autónomo y fundamental"* que permite a un individuo conocer, actualizar y rectificar su información contenida en base de datos".[4]

En México, la percepción del "*habeas data*" es similar a la de Colombia, en el sentido de considerarlo como una garantía constitucional. El jurista mexicano Escobar Fornos, lo reconoce como el "*proceso constitucional que se inicia con la acción que le asiste a toda persona para solicitar a las autoridades judiciales la exhibición de los registros que llevan las autoridades o las personas privadas en los cuales aparecen sus datos personales o los de su grupo familiar o étnico, para enterarse de su exactitud y de la razón de su existencia, y pedir su rectificación, supresión o modificación, si fueren inexactos o encerraren una discriminación*."[5]

No obstante, se considera que la doctrina coincide en que el "*habeas data"* y los "*sistemas de protección de datos*" en las diversas jurisdicciones, son un instrumento que ayuda a proteger la información de las personas, por lo que ambos términos pueden usarse incluso como sinónimos en cuanto a sus efectos jurídicos.

---

[4] Coronel Carcelén, Felipe Francisco. La protección del derecho a la vida privada en internet y otros medios de comunicación electrónicos. Borrador de tesis. Pontificia Universidad Católica de Chile, p. 35. Disponible en: http://www.alfa-redi.org/sites/default/files/articles/files/coronel.pdf [Fecha de consulta: 01 de septiembre de 2018]

[5] Escobar Fornos, Iván. Introducción al derecho procesal constitucional. Porrúa, México, 2005, pp. 300 y 301.

1.1. Evolución del derecho a la privacidad y protección de datos personales como derechos humanos

Los conceptos del “derecho a la información” y “protección de datos personales” no han tenido una definición reconocida universalmente, ya que varía en función de la legislación de cada país, no obstante, existen principios y normas de carácter internacional que los reconocen y conceptualizan.[6]

En la Declaración Universal de los Derechos del Hombre se les reconoce como derechos y libertades fundamentales del hombre, derechos que se encuentran establecidos en los artículos 12 y 19. El primero de los citados, se refiere al derecho a la vida privada:

> *Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques*.

Y el segundo de ellos, sobre el derecho a la información señala:

> *Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección*.

---

[6] Araujo Carranza, Ernesto. El derecho a la información y la protección de datos personales en el contexto general y su construcción teórica y jurídica. IUS Revista del Instituto de Ciencias Jurídicas de Puebla, A.C., núm. 23, 2009, pp. 174-213. Instituto de Ciencias Jurídicas de Puebla, A. C. Puebla, México, p. 202. Disponible en: https://www.redalyc.org/pdf/2932/293222963009.pdf [Fecha de consulta: 05 de septiembre de 2018]

En relación a la legislación internacional aplicable a los países del continente americano, la Carta de la Organización de los Estados Americanos del 30 de abril de 1948 precisa en su preámbulo "*que la misión histórica de América es ofrecer al hombre una tierra de libertad y un ámbito favorable para el desarrollo de su personalidad y la realización de sus justas aspiraciones*"*.*

La Convención Americana sobre Derechos Humanos, suscrita en la Conferencia Especializada Interamericana sobre Derechos Humanos o Pacto de San José, celebrada del 7 al 22 de noviembre de 1969, establece el objetivo de consolidar un régimen de libertad personal y de justicia social fundado en el respeto de los derechos esenciales del hombre, los cuales no nacen del hecho de ser nacional de determinado Estado, sino en el atributo de ser un persona, razón por la cual justifica la protección internacional.

Ambos instrumentos internacionales coinciden en que los derechos que nos ocupan son "*derechos esenciales del hombre*".

1.2. Derecho a la intimidad

Históricamente, la necesidad de regular la protección de información y datos personales surge después de la segunda guerra mundial con la devastadora experiencia de ver agredidos todo tipo de derechos, especialmente los relacionados con la vida y con la dignidad humana. Al inicio, países europeos optaron por homogeneizar los derechos y garantías inherentes al hombre en un contexto internacional en aras de obtener su reconocimiento y protección universal. Posteriormente, esta tendencia se dio en el resto del mundo.

El derecho a la privacidad ha ido evolucionando hasta encontrarse plasmado en tratados y criterios especializados sobre la protección de los datos personales, cuyos lineamientos han tomado en consideración los fenómenos derivados del tratamiento de información y datos a través de dispositivos digitales, teniendo así, un cercano seguimiento a la materia conocida como Tecnologías de la Información y Comunicación (TIC).

En México, como es sabido, una vez que los tratados internacionales han

sido ratificados por el Senado adquieren un rango constitucional,[7] por lo que, vale la pena hacer mención de los tratados internacionales relativos a la protección de la vida privada y a la protección de datos personales.

1.2.1. Declaración Universal de los Derechos Humanos, ONU, 10 de diciembre de 1948

En la Declaración Universal de los Derechos Humanos, de diciembre de 1948, en el artículo 12 se estableció lo siguiente:

> *Artículo 12.- Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*[8]

1.2.2. Pacto Internacional de Derechos Civiles y Políticos, ONU, 16 de diciembre de 1966

En 1966, el derecho a la privacidad fue incluido en el Pacto Internacional de Derechos Civiles y Políticos, cuyo artículo 17 señala:

> *1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.*
>
> *2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.*

1.2.3. Convención Americana sobre Derechos Humanos de 1969

El llamado "*Pacto de San José*" refiere en su artículo 11:

---

[7] Cfr. Artículo 133 de la CPEUM.

[8] Artículo 12 de la Declaración Universal de los Derechos Humanos. Véase en: Declaración Universal de los Derechos Humanos, ONU, Francia, 10 de diciembre de 1948. Disponible en: http://www.un.org/es/universal-declaration-human-rights/ [Fecha de consulta: 05 de febrero de 2018]

> […] *que toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad y que por tanto no deberá ser objeto de injerencias arbitrarias o abusivas en su vida privada, familia, domicilio, correspondencia, ni deberá sufrir ataques ilegales a su honra o reputación.*[9]

Además, el artículo 13 de este mismo ordenamiento establece que las libertades de pensamiento y expresión determinadas, no podrán existir previa censura, pero que el ejercicio de esos derechos estará sujeto a responsabilidades ulteriores, mismas que tendrán que estar expresamente fijadas por la ley y que deberán tender a asegurar, entre otras cuestiones, el respeto a los derechos o a la reputación de los demás.

1.2.4. Declaración Americana de los Derechos y Deberes del Hombre

Esta declaración, la primera redactada en este siglo en materia de derechos humanos señala en su artículo 5, que "*toda persona tiene derecho a la protección de la Ley contra ataques abusivos a su honra, a su reputación y a su vida privada y familiar*"; y en su artículo 10, indica que "*toda persona tiene derecho a la inviolabilidad y circulación de su correspondencia*".

1.2.5. Convención sobre los Derechos del Niño de 1989

Por último, conviene agregar la Convención sobre los Derechos del Niño de 1989, la cual menciona en su artículo 16, que "*ningún niño será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra o a su reputación"*; en todo caso, el niño tiene derecho también a la protección de la ley contra esas injerencias y ataques.

---

[9] Artículo 11 del Pacto de San José, Convención Americana sobre Derechos Humanos. Véase en: Convención Americana sobre Derechos Humanos, OEA, Costa Rica, 22 de noviembre de 1969. Disponible en: https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm [Fecha de consulta: 05 de febrero de 2018]

De acuerdo a esta Convención se entiende por niño "*todo ser humano menor de dieciocho años de edad, salvo que, en virtud de la ley que le sea aplicable, haya alcanzado antes la mayoría de edad*".

Se considera niño o niña a toda persona desde su nacimiento hasta los doce años, inclusive; y adolescente, a toda persona desde los trece años hasta alcanzar la mayoría de edad.

1.2.6. Unión Europea

Actualmente, los 27 Estados de la Unión Europea cuentan con regulaciones sobre protección de datos, las cuales se encuentran homogeneizadas y adaptadas a las directrices que al efecto ha promulgado el parlamento de la Unión Europea. En este apartado se presentará la evolución del marco jurídico europeo que ha sido referencia para legislaciones nacionales de todo el mundo.

En 2009, durante la 31ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad en Madrid, se gestó una propuesta conjunta para la redacción de "*Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal*". Gracias al consenso de casi 50 países, se logró integrar las legislaciones de los cinco continentes, en donde se enfatiza la universalidad de los principios y garantías que configuran este derecho y, además, se reafirma la necesidad y viabilidad de avanzar hacia un marco internacional de carácter vinculante, que "*contribuya a una mayor protección de los derechos y libertades individuales en un mundo globalizado, y por ello, caracterizado por las transferencias internacionales de información*".[10]

[10] Estándares Internacionales sobre Protección de Datos Personales y Privacidad (Resolución de Madrid). 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, 5 de noviembre de 2009, Madrid. Disponible en: https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf [Fecha de consulta: 01 de marzo de 2018]

1.2.7. Convención Europea de Derechos Humanos

La Convención Europea de Derechos Humanos, firmada el 4 de noviembre de 1950 y con entrada en vigor a partir del 3 de septiembre de 1953, se caracteriza por haber marcado la pauta para importantes ordenamientos y disposiciones, siendo relevante el estudio del apartado 8; 8.1:

> *Artículo 8: 8.1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia; 8.2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto y en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.*[11]

Del apartado transcrito se advierte la importancia que se le ha dado al derecho a la privacidad, es decir, a la vida privada, supuesto que coincide con la materia de protección de la Organización de los Estados Americanos en relación a la privacidad de las personas.

1.3. Derecho a la protección de los datos personales

1.3.1. Resolución 509 del Consejo de Europa de 1968 sobre protección de datos

Para abordar el tema, se considera conveniente identificar como antecedente la Resolución 509/1968 de la Asamblea del Consejo de Europa sobre "*los derechos humanos y los nuevos logros científicos y técnicos*".

[11] Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (Convención o Convenio Europeo de Derechos Humanos). Consejo de Europa, 4 de noviembre de 1950, Roma. Disponible en: https://www.echr.coe.int/Documents/Convention_SPA.pdf [Fecha de consulta: 06 de febrero de 2018]

El Consejo de Europa vio la necesidad de estudiar las tecnologías de la información y su potencial invasión en los derechos de las personas, de ahí que creo una comisión consultiva encargada del análisis de los posibles impactos. En dicha resolución se emitieron directrices y criterios de protección de información y datos personales destacando la necesidad de generar elementos de protección frente al uso inevitable de la tecnología en el manejo de datos masivos.

1.3.2. Carta de los Derechos Fundamentales de la Unión Europea de 2000

Otro avance en la materia se da en el año 2000, al reconocerse el derecho a la protección de datos como un derecho fundamental y autónomo, distinto al derecho a la intimidad y a la privacidad de las personas en la Carta de Derechos Fundamentales de la Unión Europea proclamada en Niza el 07 de diciembre del año 2000. En este instrumento se precisa que los datos podrán recabarse mediante consentimiento de la persona, que los datos tendrán un fin específico, que las personas tendrán derecho a cancelar el tratamiento de su información, y que existirá una autoridad encargada de velar la garantía del derecho.

1.3.3. Convenio número 108 del Consejo de Europa para la protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal de 1981

Este acuerdo se caracteriza por hacer una llamada de atención a los países para que modificaran su legislación para proteger adecuadamente el derecho de los individuos en relación a la vida privada, toda vez que el desarrollo de las tecnologías informáticas deviene intrusivo y sin control.[12]

El Comité creado para el análisis respectivo emitió dos resoluciones, la 73/22 y la 74/29, ambas para proteger la vida privada de las personas ante la operación de bases de datos electrónicas. Estos documentos son un interesante referente ya que logran el primer consenso para definir las "*pautas de conducta*" en el manejo

[12]Recomendación 509, celebrada en la 3° parte de la XIX cesión, 1968. Ver también la obra de Novo Monreal, Eduardo. Derecho a la vida privada y libertad de información. Siglo XXI Editores, México, cuarta edición, 1989, p. 3.

de datos por parte de los Estados.[13]

1.3.4. Resolución 45/95 de la Asamblea General de la ONU de 1990

Un gran avance en la materia se da en la ONU mediante la Resolución 45/95 de la Asamblea General del 14 de diciembre de 1990, por la que se establecen las directrices de protección de datos. En este instrumento se establecen las garantías mínimas que deben prever las legislaciones nacionales en cuanto a la protección de los datos personales como un derecho humano, dando como resultado los siguientes principios:

Principios de licitud y lealtad; de exactitud, de especificación de la finalidad; de acceso de la persona interesada; de no discriminación; de limitación de facultad para hacer excepciones; de seguridad; de supervisión y sanciones; reglas para el flujo transfronterizo; así como de tratamiento de archivos informatizados públicos y privados.

En este sentido, en dicha resolución y en el Convenio 108 del Consejo de Europa fueron un primer avance para homologar las garantías mínimas del derecho a la protección de datos personales, y, por su parte, en los lineamientos dictados en la Directiva 95/46/CE del 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y su libre circulación, se precisan las obligaciones y prerrogativas y se amplía el ámbito de protección.

1.3.5. Sentencia del Tribunal Alemán de 1983

No podemos dejar de citar la Sentencia del Tribunal Constitucional Federal de Alemania de 1983, dentro del juicio emitido sobre la ley del censo, el cual dio origen al estudio y alcances del derecho a la intimidad, conceptualizándolo como la expresión de un derecho a la autodeterminación informativa. Mismo principio que

[13] Coronel Carcelén, Felipe Francisco. *Op cit,* p. 43.

hoy recoge nuestra Ley Federal de Protección de Datos Personales en Posesión de los Particulares.[14]

La resolución de referencia hace un interesante planteamiento, primero definiendo el derecho de la personalidad como la "*facultad del individuo, derivada de la idea de autodeterminación de decidir básicamente por sí mismo cuándo y dentro de qué límites procede a revelar situaciones referentes a su propia vida".*[15]

Posteriormente, la sentencia de mérito explica el término "*autodeterminación informativa*" como un derecho a la protección de información de una persona ante un tratamiento automatizado, siendo necesario el consentimiento del individuo para disponer sobre la revelación y uso de sus datos.

1.3.6. Directiva 95/46/CE sobre la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos datos de 1995

[14] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, artículo 1: "La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas." Publicada en el DOF el 05 de julio de 2010. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

[15] Herrán Ortiz, Ana Isabel. El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales. Dykinson, España, 2002, p. 65. Disponible en: https://books.google.com.mx/books?id=CCVT48egc5MC&pg=PA65&lpg=PA65&dq=facultad+del+individuo,+derivada+de+la+idea+de+autodeterminaci%C3%B3n+de+decidir+b%C3%A1sicamente+por+s%C3%AD+mismo+cu%C3%A1ndo+y&source=bl&ots=qUSLJdbUFo&sig=zT5ZLp0ZTqELO_R_jjY6W2L4vHA&hl=es&sa=X&ved=2ahUKEwjv3o3T7OvfAhUm0YMKHWyTDukQ6AEwAXoECAgQAQ#v=onepage&q&f=false

La Directiva 95/46/CE se caracteriza por tratar de impedir la libre circulación de información personal dentro de un contexto comercial en la Comunidad Europea, evitando que la defensa de los derechos fundamentales obstaculice los objetivos de la integración económica.[16]

Así, conviene citar:

> *1. Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.*
>
> *2. Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1.*

Es, por tanto, que esta Directiva se encarga principalmente de establecer los principios para la protección de la privacidad a nivel regional (Europa), los cuales deben incorporarse a la legislación de cada Estado miembro. Este instrumento prohíbe la transferencia de datos personales desde la Comunidad a cualquier Estado no miembro que no tenga leyes de protección de datos "*adecuadas*" es decir, con los mismos estándares.[17]

---

[16] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Parlamento Europeo y Consejo de la Unión Europea. Luxemburgo. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML

[17] De conformidad con el artículo 25 principio número 2, "el carácter adecuado del nivel de protección que ofrece un tercer país se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o

Otra de las grandes novedades que aportó esta Directiva fue la de proponer la creación de una o más autoridades públicas que se encarguen de velar por la debida aplicación de las normas propuestas, con el objeto de que actúen con "*completa independencia*", con "*poderes efectivos de investigación*" en el procesamiento.[18]

Así mismo, la Directiva ordena alentar la elaboración de códigos de conducta, de acuerdo a las particularidades de cada sector.

Por último, la Directiva propone la creación de un Grupo de Trabajo ("*Working Party*") que emana por disposición del artículo 29, titulado "*Grupo de protección de las personas en lo que respecta al tratamiento de datos personales*", con naturaleza consultiva e independiente. Al respecto señala:

> *2. El Grupo estará compuesto por un representante de la autoridad o de las autoridades de control designadas por cada Estado miembro, por un representante de la autoridad o autoridades creadas por las instituciones y organismos comunitarios, y por un representante de la Comisión. Cada miembro del Grupo será designado por la institución, autoridad o autoridades a que represente.*

1.3.7. Directiva 97/66/CE del Parlamento Europeo y del Consejo sobre procesamiento de datos en el sector de las telecomunicaciones dentro de la Comunidad, del 15 de diciembre de 1997

---

sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países". El artículo 25, principio número 6 declara que la Comisión puede decidir que un tercer país "asegure un nivel adecuado de protección (...), a la vista de su legislación o de los compromisos internacionales que ha asumido especialmente al término de las negociaciones [que ha mantenido con la Comisión]". Ambos artículos de la Directiva 95/46/CE.

[18] Artículo 28 de la Directiva 95/46/CE.

Este instrumento se identifica como el elemento que complementa a la directiva 95/46/CE antes citada, enfocándose en el tratamiento de datos a través de las telecomunicaciones. A continuación, la parte relevante de dicha directiva:[19]

> *1. La presente Directiva establece la armonización de las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y de los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las telecomunicaciones, así como la libre circulación de tales datos y de los equipos y servicios de telecomunicación en la Comunidad.*
>
> *2. A los efectos mencionados en el apartado 1, las disposiciones de la presente Directiva especificarán y completarán la Directiva 95/46/CE. Además, protegerán los intereses legítimos de los abonados que sean personas jurídicas.*
>
> *3. La presente Directiva no se aplicará a las actividades no comprendidas en el ámbito de aplicación del Derecho comunitario, como las previstas por las disposiciones de los títulos y VI del Tratado de la Unión Europea y, en cualquier caso, a las actividades que tengan por objeto la seguridad pública, la defensa, la seguridad del Estado (incluido el bienestar económico del Estado cuando dichas actividades estén relacionadas con la seguridad del Estado) y a las actividades del Estado en materia penal.*

Esta Directiva se aplica únicamente al tratamiento de datos personales en relación con la prestación de servicios públicos de telecomunicaciones en las redes públicas de telecomunicaciones en la Comunidad Europea y, especialmente, a través de la red digital de servicios integrados (RDSI) y las redes móviles digitales

[19] Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. Parlamento Europeo y Consejo de la Unión Europea. Bruselas. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:ES:HTML

públicas.

Asimismo, y de manera importante, establece como obligación para el proveedor de un servicio público de telecomunicaciones la adopción de las medidas técnicas y de gestión para preservar la seguridad de sus servicios, incluyendo la confidencialidad de las comunicaciones personales.

1.3.8. Estados Unidos y Canadá

Las legislaciones de EUA y Canadá cuentan con una amplia protección en el ámbito del derecho a la privacidad, desde la salvaguarda constitucional del derecho a la vida privada hasta leyes federales sobre la protección de datos personales en el sector público y privado, que se encuentran adecuadas a los avances tecnológicos. Según las necesidades de esta investigación, solo se hará referencia a las siguientes: "*Privacy Act*" (1974) y "*Electronic Communications Privacy Act*" (1986), ambas de EUA; y respecto a Canadá, se revisará la ley especializada, "*Personal Information Protection and Electronic Documents Act*" (1990), junto con el análisis de un caso jurisprudencial (case law) de gran relevancia en el tema de privacidad y protección de datos personales.

1.3.9. Ley de Privacidad (Privacy Act)

La Ley de Privacidad de EUA fue promulgada el 31 de diciembre 1974, ésta es de índole federal, establece un código de prácticas justas respecto a la información personal y regula el almacenamiento, tratamiento, uso y transmisión de la información de identificación personal que se mantienen en los sistemas de registros de los organismos federales. La Ley de Privacidad prohíbe la divulgación de información de un sistema de registros sin consentimiento escrito del titular, a menos que la divulgación sea exceptuada.

Este ordenamiento estipula salvaguardias contra la invasión de la privacidad personal por el mal uso de los registros por parte de las agencias federales. Los documentos pueden estar protegidos contra liberación de conformidad con una o más exenciones previstas en la Ley de Privacidad. De conformidad con la misma, estos documentos pueden no darse a conocer, incluso a la persona a que se refieren los registros, es decir, al titular de los datos, a menos que la Ley de Libertad

de Información exija su revelación. Enseguida, se mencionarán algunas de sus características principales:

- La Ley de Privacidad se ocupa fundamentalmente de los documentos contenidos en un sistema de registros que pueden recuperarse mediante el nombre de la persona o un identificador personal.
- Para hacer una solicitud de registros protegidos por la Ley de Privacidad, es necesario ser ciudadano estadounidense o extranjero, admitido legalmente para residencia permanente en EUA.
- La ley permite solicitar registros relativos a otra persona con la autorización por escrito de la misma. Este tipo de solicitud se llama "*solicitud de información de terceros*".
- Aquellos que no sean ciudadanos estadounidenses, podrán solicitar los registros que se relacionan con ellos, pero su solicitud se procesará de conformidad con la Ley de Libertad de Información y no conforme a la Ley de Privacidad.

1.3.10. Electronic Communications Privacy Act

Según Thomas J. Smedinghoff en el libro "*Online Law*", el Congreso de EUA expresó que el objeto de la ECPA es regular "*el creciente problema del acceso y uso, por personas no autorizadas, a las comunicaciones electrónicas que no deben estar disponibles al público*."[20]

La ECPA protege la privacidad de todas las formas de comunicación electrónica en cuanto a:

- Comunicación telefónica de voz ("*voice mail*");

[20] Smedinghof, Thomas J. Online law: The legal guide to doing business on the internet. Addison-Wesley, EUA, 1996, p. 2000.

- Comunicaciones digitales de computadora a computadora, v.g. correo electrónico (“*e-mails*”), mensajes almacenados en boletines electrónicos, entre otros, y
- Comunicaciones de los teléfonos portátiles.

Se trata de una ley aplicable tanto al sector público como al privado, que provee penalidades civiles y criminales por intercepción intencional y no autorizada de las comunicaciones electrónicas. Algunos de los derechos que busca ampliar son la libertad de expresión y el derecho a la seguridad de documentos, pertenencias contra registros y allanamientos no razonables.

Principalmente, la ECPA prohíbe a los entes públicos y privados, tales como los proveedores de Internet, operadores de redes privadas, administradores de sistemas de boletines electrónicos, por mencionar algunos, lo siguiente:

- Intercepción y revelación del contenido de cualquier comunicación electrónica;
- Acceso ilegal a las comunicaciones electrónicas almacenadas en computadoras, y
- Divulgar el contenido de cualquier comunicación electrónica almacenada.

Asimismo, busca aumentar la confianza de la sociedad en las leyes que protegen la privacidad en las comunicaciones electrónicas, obligando a los responsables del tratamiento de las bases de datos a:

- Conocer las leyes que impactan las comunicaciones electrónicas;
- Conocer que, por ley, para que el gobierno pueda interceptar esas comunicaciones, debe mediar una orden de la corte;
- Conocer que, por ley, para que el gobierno pueda acceder a comunicación almacenada, debe mediar una orden de cateo;
- Establecer la política y procedimiento de la compañía en cuanto a la entrega de información de comunicaciones electrónicas, y

- Asegurarse que existan mecanismos para evitar y detectar la intercepción intencional de las comunicaciones electrónicas.

A raíz del ataque del 11 de septiembre de 2001 a las torres gemelas en Nueva York, la ley fue enmendada por las secciones 209-212 de la "*USA Patriot Act*", de donde se destaca lo siguiente:

- Antes de la enmienda, el gobierno de EUA necesitaba solicitar una orden ("*Title III Wiretap*") para poder abrir un "*voicemail*", no obstante, ahora, luego de ésta, el gobierno podrá acceder a éstos con solo solicitar una búsqueda ordinaria.
- La ECPA especifica que el proveedor de un servicio de comunicación electrónica (ISP) debe de suministrar registros electrónicos cuando el gobierno de EUA los solicite. Antes de la enmienda, un proveedor de comunicaciones electrónicas no podía divulgar registros de comunicaciones a terceros. Sin embargo, luego de ésta, el proveedor de comunicaciones electrónicas puede divulgar información, siempre y cuando considere razonable este hecho y la decisión se sustente en la posibilidad de alguna emergencia, ya sea porque peligre de muerte o de lesión física cualquier persona, o porque pueda estar en peligro la seguridad nacional. La enmienda no clarifica qué se debe considerar por "razonablemente".

1.3.11. Personal Information Protection and Electronic Documents Act

En 2010, mientras México celebraba la adopción de su nueva Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Canadá ya celebraba el décimo aniversario de su propia ley, la Ley de Protección de la Información Personal y los Documentos Electrónicos (PIPEDA por su nombre en inglés), y la oficina canadiense ya contaba con veinte años de existencia velando por el respeto de su ley en materia de protección de datos personales, primero en el sector público y luego en el privado.

PIPEDA emplea el concepto de actividad comercial de manera que solo se aplica con motivo de una transacción; al respecto, el artículo 2.1 de la ley define la

actividad comercial como: cualquier actividad habitual o cualquier acto aislado que tiene carácter comercial por su naturaleza, incluyendo la venta, el trueque o el alquiler de listas de donantes, de afiliados o de recaudación de fondos. Este concepto, fundamental para la interpretación del campo de aplicación de la ley, se basa en la naturaleza de la actividad en cuestión.

De este modo, todas las actividades de una organización activa en el mundo de los negocios, que recoge, use o comunique datos personales con motivo de sus actividades de negocio, deberían atenerse a la ley. Sin embargo, una organización sin afán de lucro, como una universidad o un organismo benéfico, no estaría sujeta a la ley, a menos que dicha entidad venda ocasionalmente listas de datos de donantes actuales o anteriores.

Por otro lado, no distingue entre los datos personales y los datos personales confidenciales. Sin embargo, en su primer año de implementación no se sabía demasiado bien lo que se entendía por dato personal. Por ejemplo, varias empresas se apresuraron a argumentar que algunos de los datos atribuidos a los clientes —concretamente sus números de cuenta o de tarjeta de crédito— pertenecían en realidad a la empresa y no al cliente, ya que estos datos habían sido producidos por la empresa y no proporcionados por los clientes.

El artículo 2º de PIPEDA sólo refiere que un dato personal es "*cualquier dato relativo a una persona identificable*", sin embargo, dicho artículo no establece que la información debe provenir de una persona o ser proporcionada por ella, ni tampoco habla del titular de la información, la disposición se limita a afirmar que para que un dato sea considerado personal, debe guardar relación con una persona identificable.

Los diez principios para el tratamiento de la información en los que se basa PIPEDA son:

1. Responsabilidad.
2. Definición de los fines de la recopilación de datos.
3. Consentimiento.

4. Limitación de la recopilación.
5. Limitación del uso, comunicación y conservación.
6. Exactitud.
7. Medidas de seguridad.
8. Transparencia.
9. Acceso a los datos personales, y
10. Posibilidad de denunciar el incumplimiento de los principios.

En específico, PIPEDA contiene disposiciones concretas sobre la circulación transfronteriza de los datos, lo anterior en razón del vertiginoso auge que han ido tomando las actividades en línea, pues, aunque simplemente se trate de actividades económicas o sociales, éstas conllevan a la circulación de datos sin precedentes entre territorios de diversa competencia.

Para mayor abundamiento, se recomienda ampliamente la lectura contenida en el "*VIII Encuentro de Autoridades Iberoamericanas sobre Protección de Datos"* publicado por la Oficina del Comisionado de Privacidad de Canadá, el cual contiene las palabras de Chantal Bernier, Comisionado adjunto para la protección de la intimidad en Canadá, llevado a cabo el 29 de septiembre de 2010, en la Ciudad de México.

1.3.12. Memorándum de Montevideo (Región Iberoamericana)

En julio de 2009, la Oficina de Privacidad de Canadá realizó un cuidadoso estudio de las políticas de privacidad de "*Facebook*", así como del manejo de los datos personales de los usuarios. Ante las estadísticas obtenidas (90% de los jóvenes de entre 12 y 17 años están en línea) y ante la incidencia creciente de intrusiones, ya sea con fines comerciales o criminales, se hizo evidente -y urgente- la necesidad de convocar a un grupo multidisciplinario y multinacional de expertos a efecto de revisar el marco jurídico existente en materia de protección de datos personales.

De ahí, la elaboración del *Memorándum de Montevideo,*[21] el cual es un marco que responde a la realidad social, cultural y jurídica de la región Iberoamericana.

En el Memorándum impera el principio del interés superior del niño y funda sus recomendaciones en cinco ejes que se sólo se podrán lograr con la participación conjunta de autoridades y sociedad civil:

1) Recomendaciones en materia de prevención y educación de niñas, niños y adolescentes

Este instrumento fomenta el uso responsable y seguro de Internet y de las redes sociales digitales, lo que se traduce en la atención que se debe tener en las políticas de privacidad, seguridad y alertas sobre las distintas redes. Para ello, se pidió reforzar el sistema educativo con una marcada visión preventiva, por lo que se obliga a incluir en los planes educativos de todos los niveles, una agenda relativa al uso informado de Internet.

Se recomienda usar seudónimos, siempre que estos no sirvan para engañar o confundir sobre la identidad real, por tal motivo es menester informar sobre los riesgos de ser engañados en relación a la identidad de la otra persona y los robos o la suplantación de identidad.

Se hace un breve paréntesis para profundizar en el tema de la identidad de los usuarios, específicamente por el uso de seudónimos y por el común anonimato bajo el cual navegan un sinnúmero de usuarios, por ello se reproduce una importante reflexión que hace el jurista Carlos Gregorio:

> *Dado que la causa principal de la mayoría de los riesgos es el anonimato —y la sensación de impunidad que se deriva de él— muchos piensan que es necesario incrementar los sistemas de identificación de los usuarios.*

[21] Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes. Seminario Derechos, Adolescentes y Redes Sociales en Internet, Montevideo, 27 y 28 de julio de 2009. Disponible en: http://www.iijusticia.org/Memo.htm

En primer lugar, puede decirse que el anonimato irreversible, es una ilusión. Es posible si una persona crea una cuenta de correo electrónico en un cibercafé, y a partir de ella crea una cuenta en una red social o hace un comentario a una nota en un periódico; si tiene un cuidado extremo en que su opinión esté escrita en un lenguaje neutro, sea tan sucinta como pueda ser, y además realice todo esto por única vez... probablemente que su anonimato sea irreversible. Pero la dirección IP ya lo ubica geográficamente, el idioma utilizado y el tema abordado reducen el círculo; y su estilo de lenguaje aporta más información. Pero Internet tiene sus reglas de negocios, y la libertad de expresión -en particular la expresión anónima- no es un buen negocio.[22]

2) Recomendaciones para los Estados sobre el marco legal

Primordialmente, exige la existencia de una normativa que asegure la protección de los datos personales y la aplicación efectiva de los mecanismos, dando prioridad a los niños, niñas y adolescentes (México, desde 2010, cuenta con la normatividad relativa).

Establece un principio llamado "*espejo*", en donde toda acción u omisión considerada ilegal en el mundo "*real*", debe tener el mismo tratamiento en el mundo "*virtual*".

3) Recomendaciones para la aplicación de las leyes por parte del Estado

Se valora la labor del sistema judicial para asegurar el buen uso de Internet y las redes sociales, puesto que toda resolución judicial además de restaurar los derechos vulnerados, es la mejor forma de enviar un mensaje claro a ciudadanos y empresas sobre la voluntad de aplicar las normas y los principios.

[22] Gregorio, Carlos G. Impacto y evolución de las redes sociales digitales: libertades y derechos, en Gregorio, Carlos G. y Ornelas, Lina (Comp.). Protección de datos personales en las redes sociales digitales: en particular de niños y adolescentes. Memorándum de Montevideo. IFAI/ IIJusticia, México, 2011, pp. 66 y 67.

En este sentido, se debe garantizar que los procesos judiciales y administrativos sean sencillos, ágiles, de fácil acceso y tramitados con prioridad por parte de los tribunales y autoridades responsables.

Además, pide fortalecer el uso de la responsabilidad civil extracontractual objetiva, como mecanismo regulatorio para garantizar que el uso de las aplicaciones no vulnere los derechos fundamentales en la sociedad de la información y conocimiento, internet y redes sociales digitales.

4) Recomendaciones en materia de políticas públicas.

Especialmente, sugiere establecer mecanismos de respuesta, sistemas de información y asesoría para las víctimas; crear mecanismos (nacionales e internacionales) para compartir y procesar información reportada sobre los eventos denunciados, con la intención de establecer formas de protección temprana con base en los riesgos detectados; promover la sensibilización y divulgación de información pública sobre estos temas; impulsar el desarrollo de un conocimiento especializado en la materia y de investigación para formular políticas adecuadas.

5) Recomendaciones para la industria

Se reconoce el rol fundamental de la industria (proveedores de acceso a Internet, desarrolladores de aplicaciones y de redes sociales) y urge a su participación en las medidas de prevención y protección, en conjunto con las autoridades, especialmente, en el campo de manejo y protección de datos personales.

Capítulo 2

Antecedentes internacionales y marco jurídico de protección de datos personales.

Capítulo 2: Antecedentes internacionales y marco jurídico de protección de datos personales.

2.1. Normas emitidas por organismos internacionales

2.1.1. Lineamientos de la OCDE

México forma parte de la OCDE, organización que formó el Grupo de Expertos sobre Bancos de Datos ("*Data Bank Panel*"), que analizó y estudió diferentes aspectos de la privacidad llegando al consenso que los países miembros deben asumir un compromiso de adopción de principios generales para la protección de datos personales.

En 1978, la OCDE creó un nuevo grupo internacional denominado "*Grupo de Expertos sobre Barras Transfronterizas de Información y Protección de Privacidad*", cuya labor fue desarrollar lineamientos de consenso general para el flujo transfronterizo de datos y la protección de datos personales.

Los resultados de los trabajos de la OCDE concluyeron con la promulgación en 1980 de los Lineamientos sobre la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales –Lineamientos de la OCDE-.[23] Estos Lineamientos fueron adoptados el 23 de septiembre de 1980 como una recomendación del Consejo de la OCDE los cuales aplican a datos personales en poder del sector público y privado que, debido a la forma en que se procesan, a su naturaleza o al contexto en que se usan, suponen un riego para la privacidad y las libertades individuales. Dichos lineamientos establecen en los capítulos dos y tres, los siguientes ocho principios básicos:

1) Principio de limitación de recogida. Este principio implica que deben existir límites al recabar los datos personales y cualquiera de estos datos deberán obtenerse con medios legales y justos.

---

[23] Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OCDE, 23 de septiembre de 1980. Disponible en: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html [Fecha de consulta: 07 de febrero de 2018]

2) Principio de calidad de los datos. Establece que los datos personales deberán ser relevantes para el propósito de su uso.

3) Principio de especificación del propósito. El propósito de recabar datos –finalidad- se deberá especificar a más tardar en el momento en que se produce dicha recogida.

4) Principio de limitación de uso. No se deberá divulgar, poner a disposición o usar los datos personales excepto si se tiene el consentimiento del sujeto implicado.

5) Principio de salvaguardia de la seguridad. Se emplearán medidas razonables de seguridad para proteger los datos personales contra riesgos.

6) Principio de transparencia. Deberá existir una política general sobre transparencia en cuanto a evolución, prácticas y políticas relativas a datos personales.

7) Principio de participación individual. Todo individuo tendrá derecho a:

   -Que el controlador de datos le confirme que tiene datos sobre su persona;

   -Que se le comuniquen los datos relativos a su persona en un tiempo razonable, y

   -Que se le expliquen las razones por las que una petición suya haya sido denegada.

8) Principio de responsabilidad. La responsabilidad del cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

En resumen, estos Lineamientos ofrecen garantías para la protección de datos personales a través de sus principios mismos que comparten la intención de protección de los instrumentos internacionales analizados en capítulos anteriores, con las siguientes excepciones:

- El presente modelo no tiene como centro la protección del individuo (sujeto de un derecho fundamental), sino que gira en torno al valor económico de los datos en cuanto al flujo internacional de la información para cubrir, con

determinada protección, la necesidad de las economías de transmitir y tratar datos personales para la consecución de sus negocios, y

- Se prevé un esquema más flexible en cuanto a la implantación de la política pública pues no exige una autoridad garante independiente y promueve el esquema de autorregulación por parte de las empresas y sectores involucrados, a través de códigos de conducta, sellos de confianza entre otros.

2.1.2. Marco de privacidad del APEC

El Marco de privacidad de APEC[24] es una herramienta de protección que busca un equilibrio entre la seguridad de la información personal y el libre flujo de información en la región Asia-Pacífico para asegurar sus fines comerciales.

El artículo 5 de dicho ordenamiento, establece que este documento concuerda con los valores básicos de los Lineamientos de Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de 1980 de la OCDE, que su objetivo es promover el comercio electrónico en toda la región Asia-Pacífico y reafirmar el valor de la privacidad para los individuos y para la sociedad de información. El artículo 8 establece que este Marco fue desarrollado reconociendo la importancia de:

- Desarrollar protecciones apropiadas para la información personal.
- Reconocer el libre flujo de información como algo esencial para economías de mercado desarrolladas y en desarrollo.
- Posibilitar organizaciones globales que recopilen, accedan, usen o procesen información en economías de APEC.
- Posibilitar agencias de seguridad para cumplir con su mandato de proteger la privacidad de la información, y

[24] Marco de Privacidad de APEC. APEC, diciembre de 2005. Disponible en: https://sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf

- Presentar mecanismos internacionales para promover y hacer cumplir la privacidad de la información.

En resumen, el objetivo de este Marco es mantener un equilibrio entre la necesidad de las economías de transmitir y tratar datos personales para la consecución de sus negocios y la debida protección de dichos datos de conformidad con principios básicos.

Los principios básicos de protección están contenidos en los artículos 14 al 25 y son:

1) Prevención del daño.
2) Aviso: El que recolecta la información personal está obligado a proporcionar al individuo declaraciones claras.
3) Limitación de recolección.
4) Usos de la información personal.
5) Elección.
6) Integración de la información personal.
7) Medidas de seguridad.
8) Acceso y Corrección, y
9) Responsabilidad.

Los principios de la OCDE y APEC son muy parecidos ya que su fin principal es buscar un equilibrio entre el flujo de datos personales que implica el intercambio comercial y la protección de los mismos.

Como ejemplo de países que siguen la normatividad de APEC tenemos a Canadá en donde se aplican leyes de protección de datos personales en el orden federal y provincial. Su sistema se rige por dos leyes federales, a saber, la "*Privacy Act*", relativa a la información que tiene el gobierno y la PIPEDA.[25]

[25] PIPEDA. Disponible en: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/ [Fecha de consulta: 10 de febrero de 2018]

Otro modelo de protección de datos personales es el de EUA, regido por dos ordenamientos: "*Privacy Act*" de 1974 y el "*Freedom of Information Act*". En este sistema jurídico el garante principal es el Departamento de Justicia a través de la Oficina de Información y Privacidad. No obstante, lo anterior, otras dependencias cuentan con lineamientos específicos, tal es el caso de los sectores salud y comercio. Ahora bien, es importante señalar que el régimen estadounidense se caracteriza por la aplicación de regulaciones sectoriales de privacidad mediante un mecanismo denominado Acuerdo de Puerto Seguro (Safe Harbor) en donde no se reconoce el derecho a la protección de datos personales como tal.

-Acuerdo del Puerto Seguro (Safe Harbor)

La aplicación del Acuerdo de Puerto Seguro tiene sus orígenes en la negociación mantenida durante más de dos años entre el Departamento de Comercio de EUA y la Comisión Europea, partiendo de los diferentes enfoques y niveles de protección que cada uno da a la vida privada de sus ciudadanos y considerando que EUA se basa en la autorregulación del sector privado.

Mediante la aplicación de dicho acuerdo, las entidades de EUA que voluntariamente deciden adherirse a los principios contenidos en el mismo, pueden recibir datos personales de responsables establecidos en alguno de los Estados miembros de la Unión Europea, pues con dicha adhesión se entiende que esas entidades proporcionan una protección suficiente.

El Acuerdo de Puerto Seguro funciona desde el 1 de noviembre de 2000, cuando el Departamento de Comercio de EUA inició el proceso de auto certificación en línea de las entidades de EUA que desearan adherirse a los principios de Puerto Seguro. El Departamento de Comercio publica una lista anual en la que aparecen las entidades que han certificado su adhesión a los principios.[26]

Las empresas que deciden no adherirse al Puerto Seguro deben cumplir con garantías de protección de otro tipo para poder transferir datos con la Unión Europea, un instrumento utilizado para estos fines son los "*contratos tipo*" en los

[26] Listado disponible en: https://safeharbor.export.gov/list.aspx

que se contienen cláusulas con el mínimo de protección establecido en los siguientes principios del Puerto Seguro:

1) Notificación.
2) Opción.
3) Transferencia ulterior
4) Seguridad
5) Integridad de los datos
6) Acceso, y
7) Aplicación

Al comparar el Acuerdo del Puerto Seguro con el Marco de la APEC y el marco que regula a la Comunidad Europea, se podrá notar que el primero es menos estricto en cuanto a la forma en la que se deben cumplir los principios, ya que la adhesión de las entidades es un régimen voluntario que se produce mediante la auto certificación dirigida al Departamento de Comercio de EUA. Lo anterior significa que son las propias empresas las que manifiestan que cumplen con los principios.

Este esquema utilizado en EUA es el prototipo de la auto regulación por empresa o sector, contrario a lo que sucede en la Comunidad Europea, en donde la normatividad es obligatoria para el sector público y privado, se aplica de manera homogénea para todos los países que la conforman e implica una autoridad independiente que garantiza el cumplimiento de los principios con facultades de sanción.[27]

2.1.3. Marco de la comunidad europea

El instrumento de referencia que regula la protección de datos en la Comunidad Europea es la Directiva 95/46/CE de 24 de octubre de 1995, relativa a la Protección

[27] Al respecto debe hacerse notar que el Grupo del Artículo 29 ha cuestionado el carácter adecuado de los principios de Puerto Seguro de EUA no por su naturaleza

de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre circulación de estos Datos.[28]

Este es un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea, tal como lo hace la normatividad de la OCDE y de APEC. Sin embargo, este instrumento fija límites mucho más estrictos para la recogida y utilización de los datos personales y prevé de manera obligatoria la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos.

Existen en el mundo dos principales vertientes entorno a la protección de información y los datos personales: el modelo europeo que busca proteger la información y su propiedad con la intención de conservar la integridad y honor de la persona aun y cuando el individuo hubiese fallecido. La razón de protección de este modelo son los derechos humanos de los individuos.

Por otra parte, tenemos el modelo estadounidense el cual pretende proteger la información de las personas bajo el concepto del derecho a la privacidad, el cual puede extinguirse con la muerte del sujeto. Este modelo surge derivado de motivos comerciales, ya que las empresas utilizaban de manera indiscriminada esa información.

2.1.4. Otras regulaciones en materia de datos personales

Diversos países y organismos han promulgado leyes y directrices de protección de datos personales y en cada país se ha buscado adaptar, a sus propias condiciones

---

auto reguladora, sino por su falta de efectividad. Al respecto véase el informe preparado el 19 de abril de 2004 en el contexto de la revisión de los principios de Puerto Seguro titulado "*Safe Harbour Decision Implementation Study*", disponible en:
http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/07_etude_safe-harbour-2004_/07_etude_safe-harbour-2004_en.pdf, el cual fue solicitado por la Comisión Europea.

[28] Directiva 95/46/CE, op cit.

culturales, económicas y políticas las bases de alguno de los dos modelos de protección de datos personales existentes. A continuación, se mencionan algunos casos relevantes sobre las leyes de protección de datos personales de distintos países, organizaciones y regiones del mundo:

1. **ONU**. En 1948, adopta la Declaración Universal de Derechos Humanos, en la que su artículo 12 señala que las personas tienen derecho a la protección de la ley de sus datos personales.

2. **Alemania**. En 1970 fue aprobada la primera ley de protección de datos (Datenschutz). En 1977, el Parlamento Federal Alemán aprueba la Ley Federal Bundesdatenschutzgesetz. Estas leyes impiden la transmisión o transferencia de cualquier dato personal sin la autorización de la persona interesada.

Como se mencionó, la Sentencia del Tribunal Constitucional Federal (Bundesverfassungsgericht) de la República Federal de Alemania del 15 de septiembre de 1983 ha servido como referente para que la gran mayoría de los países reconozcan una protección a los datos personales de cada individuo. Dicha sentencia configura el derecho a la intimidad como expresión de un derecho a la autodeterminación informativa.

3. **Suecia**. En 1973 fue publicada la que fue una de las primeras leyes de protección de datos en el mundo, cuyo principal objetivo fue el resguardo en el manejo de información personal.

4. **EUA**. La protección de datos tiene base en la "*Privacy Act*" de 1974, cuyo origen se mencionó, es la protección de la integridad de la persona.

5. **Unión Europea.** El primer convenio internacional de protección de datos fue firmado en 1981 por Alemania, Francia, Dinamarca, Austria y Luxemburgo. Es conocido como "Convenio 108" o "Convenio de Estrasburgo". En los 90's, se establece una norma común que se denominó Directiva 95/46/CE. La directiva es

referente a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

6. **España**. La ley Orgánica 15 de 1999, establece la protección de datos de carácter personal. Está ley ha sido importante para Latinoamérica porque se ha utilizado como firme referente del modelo europeo.

En el contexto del territorio español, la necesidad y convivencia del reconocimiento de un derecho fundamental a la protección de datos se encuentra apoyada sobre la base de tres principios esenciales: primero, los debates parlamentarios en torno al artículo 18.4 de la CE; segundo, la tradicional concepción pre-informativa del derecho a la intimidad no ofrece respuesta eficaz a la exigencia de tutela de la persona en la sociedad informática, y tercero, la especial naturaleza y significación de los bienes jurídicos implicados en el desarrollo de las nuevas formas de comunicación para dar respuesta a los nuevos fenómenos tecnológicos.[29]

Así, en el ámbito español, de manera expresa e independiente se garantiza la protección del derecho a la intimidad,[30] así como el pleno ejercicio de los demás derechos fundamentales frente a los eventuales abusos informáticos, por lo que en su artículo 18.4 de la Constitución Española se puede leer lo siguiente: “La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”.

---

[29] *Cfr*. Herrán Ortiz, Ana Isabel, *op cit*. pp. 19-110, y su diverso cuaderno titulado: El derecho a la protección de datos personales en la sociedad de la información., Universidad de Deusto, Cuadernos Deusto de Derechos Humanos, núm. 26, España, pp. 16-18. Disponible en: http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf [Fecha de consulta: 01 de marzo de 2018]

[30] Artículo 18.1. Constitución Española: "Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen".

Dicho artículo constitucional ha sido desarrollado por la Ley Orgánica 15/1999 del 13 de diciembre de Protección de Datos de Carácter Personal.[31] Sin embargo, ha sido el Tribunal Constitucional Español quien ha dado respuesta al reconocimiento de un nuevo derecho fundamental a la protección de datos.

7. **Latinoamérica**. En América Latina las leyes de protección de datos personales surgen como una necesidad derivada del incremento del uso de las TIC y el aumento de las vulnerabilidades asociadas. En su mayoría, estas leyes se asemejan al modelo europeo: en Argentina la Ley 25.326 (2000), Chile (1999), Panamá (2002), Brasil (1997), Paraguay (2000), y Uruguay (2008).

8. **Rusia**. En el año 2006 fue aprobada una exhaustiva ley de protección de datos personales.

9. **Perú**. La ley 29.733 del 2 de julio de 2011, al igual que México, es una de las leyes más recientes de protección de datos personales en Latinoamérica.

10. **México**. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares fue publicada en el DOF el 5 de julio de 2010, entró en vigor un día después y tiene efectos a partir de enero del año 2012.

Esta ley pretende salvaguardar el respeto a la privacidad, dignidad e información de las personas, en ella se establecen cuatro derechos fundamentales que tienen los individuos sobre su información en posesión de cualquier persona física o empresa particular (aseguradoras, bancos, tiendas departamentales, telefónicas, hospitales, laboratorios, universidades, etc.), son los denominados derechos ARCO: Acceso, Rectificación, Corrección y Oposición.

[31] Ley que vendría a modificar la antigua Ley Orgánica 5/1992 de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal. Publicada el 31 de octubre en el Boletín Oficial del Estado Español. Disponible en: https://www.boe.es/boe/dias/1992/10/31/pdfs/A37037-37045.pdf [Fecha de consulta: 10 de marzo de 2018]

2.1.5. Sentencia C-362/14 del Tribunal de Justicia de la Unión Europea

El 26 de octubre de 2015, el Tribunal de Justicia de la Unión Europea emitió una sentencia por la cual considera que, los países miembros de la Unión no se encuentran limitados o restringidos de realizar sus funciones en materia de investigación e implementación de medidas de control de transferencias de datos personales a países terceros, aun cuando la Comisión Europea haya declarado que el tercer país garantiza un nivel adecuado de protección adecuado de los datos personales trasferidos.

Esta decisión se dio en el marco de la denuncia presentada por el activista austriaco Maximilian Schrems, quien como usuario de "*Facebook*" (que almacena todos los datos de sus afiliados en Irlanda, y son transmitidos a los servidores de la red social en EUA), en la que reclamó las trasferencias de los datos personales realizadas por "*Facebook*", toda vez que, a la luz del caso Snowden, "*Estados Unidos no garantiza una protección suficiente de los datos transferidos a ese país frente a las actividades de vigilancia por las autoridades públicas*".

La autoridad irlandesa desestimó la denuncia de Schrems con fundamento en la decisión de 26 de julio de 2000, por la cual la Comisión Europea había declarado que los EUA garantizaban un nivel adecuado de protección de datos, en el marco del régimen de "safe harbor".

Sin embargo, el Tribunal Supremo Irlandés, quien ahora conoce del asunto, sometió una consulta al Tribunal de Justicia Europeo a efecto de saber los alcances de la referida decisión, limitaban las facultades de las autoridades nacionales en el sentido de controlar las transferencias de datos personales a particulares en terceros países que hayan sido objeto de una decisión de la Comisión.

Esta sentencia supone que un Tribunal local no puede declarar que un país determinado garantiza un nivel de protección similar al de la Unión Europea en la transferencia de información y datos personales, si no se ha realizado una revisión exhaustiva de la legislación de ese país, determinando que no es suficiente analizar

un régimen o esquema de protección determinado, como en este caso "*régimen de puerto seguro*" o "*safe harbor*."

2.2. Marco jurídico nacional en materia de protección de datos personales

2.2.1. Evolución del derecho a la privacidad y protección de datos en México

Es incuestionable la importancia de la mercadotecnia y la publicidad en sus diversas actividades y giros en nuestra sociedad. Hoy día no sólo el comercio y la industria dependen de sus campañas y creatividad, sino también los gobiernos para dar a conocer logros o retos, los políticos para destacar su imagen, los partidos políticos publicitar sus propuestas y, sobre todo, para dar a conocer el producto o servicio cuyo mensaje interesa hacer llegar al consumidor o destinatario.

Es por tanto que, resultó imperante la conveniencia de contar con un instrumento legal que disuadiera hechos delictivos por los que se pudo constatar la venta de base de datos con información relativa a las personas en poder tanto del sector público como privado.

2.2.2. La necesidad de protección de información y datos personales como derecho fundamental en México

México era considerado como un paraíso en el manejo de datos personales en donde la falta de una regulación tanto preventiva como sancionatoria, así como de una autoridad independiente, propiciaba operaciones ilícitas y la generación de negocios en un mercado negro a partir de la información personal.

Todo país que viva un estado de derecho debe garantizar no solo su actuación transparente, sino la forma en que toma decisiones y ejerce los recursos públicos, además de garantizar la esfera privada de los individuos que conforman la sociedad, con la intención de evitar injerencias arbitrarias e ilegales.

La marcha imparable de una nueva vida tecnológica en la nueva sociedad conlleva la preocupación de la invasión a la vida privada que puede suscitarse por el flujo dinámico de información de un país a otro para ser utilizada de diversas formas, siendo la más importante, la base de publicidad con objetivo de comercialización.

Durante los últimos diez años, se ha recopilado el conocimiento generado por la humanidad en los últimos cinco siglos, siendo lo más impactante, que dicha información puede ser obtenida desde un dispositivo como un teléfono o una tableta.

Existen otros adelantos tecnológicos de similar importancia, tales como el ancho de banda, la capacidad de almacenamiento de datos, el acceso inalámbrico a Internet desde un dispositivo móvil, aplicaciones que permiten el intercambio de audio y video de alta calidad en forma instantánea. De igual forma, se ha revolucionado la manera en que los usuarios se comunican y generan información en plataformas como redes sociales y aplicaciones "*peer to peer*", lo cual habilita el libre intercambio de información en tiempo real y sin restricción alguna.

En el sector de la comercialización de productos o servicios, México también presenta una evolución al parecer incontrolable; la disposición de productos en línea y la minería de datos facilitan la plataforma idónea de intercambio de información sobre personas con un perfil comercial predeterminado objeto de una segmentación del mercado.

Las empresas de mercadotecnia y, en general, todo el empresariado nacional, se auxilian en sus actividades de mercadotecnia y administrativas mediante la recopilación de datos de los particulares que las TIC permiten procesar y almacenar en grandes bases de datos para su posterior tratamiento.

Consecuentemente, se llegó al consenso de que el objetivo era contar con un ordenamiento que estableciera derechos innegables de protección y tratamiento de información y datos personales que debieran ser adecuadamente tutelados buscando un sano equilibrio entre su protección y uso.

2.2.3. Orígenes y principios de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares en México

Si bien México cuenta con leyes que regulan el acceso a la información pública tanto a nivel federal como en las entidades federativas desde el año 2012 e, incluso, cuenta con una reforma constitucional en dicho tema del año 2007, el legislador tenía en la agenda pendiente complementar el esquema jurídico en materia de

protección de datos personales al dotar de contenido a este nuevo derecho, así como para establecer las obligaciones de los particulares en el debido tratamiento de información de toda persona.[32]

A partir de la década de los 90's diversos legisladores promovieron iniciativas de ley básicamente inspiradas en la legislación europea en esta materia. Sin embargo, dichas leyes quedaron estancadas, dado que el Congreso de la Unión no contaba con facultades expresas para legislar sobre el tema de la protección de información y datos personales.

Posteriormente, se promovió una reforma no sólo para corregir la insuficiencia legislativa sino también elevar a rango constitucional como garantía individual el derecho de protección a la información y datos personales. Una vez superado lo anterior y después de diversos esfuerzos se aprobó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, misma que fue publicada en el DOF el 05 de julio de 2010.

Podemos considerar que esta ley se constituye como un marco general que contempla reglas, requisitos, condiciones y obligaciones mínimas para garantizar un adecuado tratamiento de los datos personales por parte de los particulares sin obstaculizar el flujo de los mismos que se traduzcan en la imposición de barreras, es decir, esta ley establece una serie de prohibiciones orientadas a lograr un equilibrio entre la protección de la información personal y la libre circulación de la misma.

Esta nueva ley encomendó como autoridad reguladora al extinto IFAI, siendo un ente de carácter autónomo que tuvo por objeto, de acuerdo a su ley orgánica el obligar a las diversas dependencias del Estado a poner a disposición de los gobernados las fuentes y archivos para transparentar la información gubernamental dentro de un nuevo marco de democracia. Consecuentemente, se concentran en

[32] Ornelas Núñez, Lina y Pinar Mañas, José Luis. La protección de datos personales en México. Tirant Lo Blanch, México, 2013, p. 101.

un solo órgano, tanto la protección de la información y datos de los ciudadanos en posesión del gobierno, como aquellos que resultan en poder de los particulares.

Uno de los objetivos fundamentales de la referida ley es proteger la información y datos de las personas físicas de manera que se regule 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, en términos de la referida ley.

El otro principio fundamental de la ley es dotar a la persona del derecho al respeto de su información personal, toda vez que para cualquier acción de tratamiento tiene que obtenerse previamente el consentimiento ya sea expreso o tácito.

2.2.4. Marco jurídico nacional en materia de privacidad y protección de datos personales

En lo concerniente a México entre el 2001 y el 2009 se presentaron iniciativas en materia de protección de datos personales, sin embargo, ninguna propuesta integraba los intereses de todos los actores involucrados.

Aunque previamente a la expedición de la ley existían diversas regulaciones que preveían mecanismos de protección de datos tales como las normas para el tratamiento de datos de solvencia patrimonial y crediticia, y con fines de prospección comercial o publicitaria.

El primer antecedente a la ley fue la iniciativa de Ley Federal de Protección de Datos Personales presentada por el Senador Antonio García Torres en el 2001. Dicha iniciativa tenía por objeto asegurar que el tratamiento de datos personales se realizara con respeto a las garantías de las personas físicas y en lo conducente a los datos de las personas jurídicas; esta iniciativa no prospero.

El segundo antecedente es la iniciativa de Ley de Protección de Datos personales presentada por el diputado Luis Miguel Barbosa Huerta en el 2001, la cual tenía por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos.

En el 2005, el diputado Jesús Martínez Álvarez presento la iniciativa de Ley Federal de Protección de Datos personales la cual tenía por objeto garantizar la protección de los datos personales que se encontraban contenidos en documentos, archivos, registros, bancos de datos u otros medios tecnológicos de procesamiento de datos a efecto de proteger y garantizar la identidad personal, la privacidad de la imagen y el honor.

En el 2006, el Senador Antonia García Torres presentó de nueva cuenta la iniciativa de Ley Federal de Protección de Datos Personales la cual tenía por objeto tutelar el derecho de las personas a la protección de sus datos personales en el ámbito privado, siguiendo el modelo europeo.

Ese mismo año, el diputado David Hernández Pérez presento la iniciativa de Ley Federal de Protección de Datos personales la cual tenía por objeto proteger los datos personales de los titulares y regular su tratamiento en posesión de personas físicas o morales de carácter privado.

Posteriormente, la diputada Sheyla Fabiola Aragón Cortés presentó la iniciativa de Ley Federal de Protección de Datos Personales, la cual tenía por objeto proteger los datos personales, así como regular el tratamiento que de los mismos realizarán las entidades del sector privado.

En el 2008 fue presentada la iniciativa de Ley de Protección de Datos Personales en Posesión de Particulares por el diputado Luis Gustavo Parra Noriega la cual tenía por objeto la protección de los datos personales contenidos en bases de datos en posesión de particulares, con la finalidad de garantizar el derecho al honor, imagen y vida privada de las personas. Esta iniciativa tuvo un papel preponderante en la actual ley de datos personales para el sector privado.

2.2.5. Constitución Política de los Estados Unidos Mexicanos

En el ámbito nacional, la tutela de la vida privada se desprende del contenido de los artículos 6°, 7°, 14º y 16º constitucionales. Los artículos 6 y 7 refieren que la vida privada, la moral y la paz pública son límites a la libertad de expresión y a la libertad de imprenta, respectivamente. Por su parte, el artículo 14, en su párrafo segundo, de la CPEUM señala que "*nadie podrá ser privado de la vida, de la libertad*

o de sus propiedades, posesiones o derechos, sino mediante juicio seguido ante los tribunales previamente establecidos [...]".

Pero es el artículo 16 el que tutela completamente el derecho a la privacidad y a la protección de datos personales, al establecer:

> *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.*

Dicho artículo también establece la inviolabilidad del domicilio, así como la inviolabilidad de las comunicaciones privadas y de la correspondencia.

2.2.6. Ley Federal de Acceso a la Información Pública Gubernamental

El primer instrumento normativo en materia de protección de datos personales en México, fue la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental[33] -Ley Federal de Transparencia-, publicada en el DOF el 11 de junio de 2002.

Esta ley tuvo como finalidad garantizar a toda persona el acceso a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos, o con autonomía legal, y a cualquier otra entidad federal. La Ley

[33] Dicha ley fue abrogada mediante el "Decreto por el que se abroga la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y se expide la Ley Federal de Transparencia y Acceso a la Información Pública". Publicado en el DOF el 9 de mayo de 2016. El texto abrogado se encuentra disponible en*:* http://www.diputados.gob.mx/LeyesBiblio/abro/lftaipg/LFTAIPG_abro.pdf, por su parte la ley vigente se encuentra disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf

Federal de Transparencia parte de la premisa de que toda la información que generen los entes públicos federales en ejercicio de sus funciones, debe ser accesible a toda persona que lo solicite, a través de los mecanismos o procedimientos previamente establecidos para ello.

Sin embargo, esta premisa de máxima publicidad de la información gubernamental tiene límites o excepciones, las cuales se consagran en los artículos 13, 14 y 18 de este instrumento jurídico. Los artículos 13 y 14 enumeran una serie de supuestos en los que cierta información puede ser clasificada con el carácter de reservada. Por su parte, el artículo 18 señala los supuestos en que determinada información puede ser clasificada con el carácter de confidencial.

Entre las hipótesis normativas previstas en el artículo 18 de la Ley Federal de Transparencia, se establece que serán considerados como información confidencial los datos personales que requieran el consentimiento de los individuos para su difusión, distribución o comercialización en los términos señalados en la misma.

Por otra parte, la citada ley contempla un capítulo de protección de datos personales. En particular, el capítulo IV estableció los principios generales que deben regir el tratamiento de datos personales en posesión de los entes públicos, tales como consentimiento, información, seguridad, calidad, entre otros, así como disposiciones generales que dan vida a los derechos de acceso y rectificación.

A través de la Ley Federal de Transparencia se delinearon los primeros matices y disposiciones del derecho a la protección de datos en México. Un importante acontecimiento en el desarrollo de este derecho fue la aprobación del decreto por el cual se adicionó un segundo párrafo (Apartado A), con siete fracciones, al artículo 6 de la Constitución Política de los Estados Unidos Mexicanos.[34] Dicha reforma fue publicada en el DOF el 20 de julio de 2007.

[34] Decreto por el que se adiciona un segundo párrafo con siete fracciones al Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos. Publicado en el DOF

En materia de protección de datos personales, las fracciones II y III tienen la virtud de ser las primeras menciones constitucionales expresas que hacen un reconocimiento del derecho a la protección de datos personales, dando continuidad a la labor iniciada por el legislador ordinario a través de la Ley Federal de Transparencia. La reforma también señaló la necesidad de contar con un dispositivo legal que regule este derecho.

De manera trascendental los años 2008 y 2009 se distinguen por la concreción de tres acontecimientos relevantes, relacionados con la evolución y consolidación del derecho a la protección de datos en México: las reformas a los artículos 16 y 73 de la CPEUM; y la emisión del dictamen correspondiente de la Comisión de Gobernación de la Cámara de Diputados de la iniciativa de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

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

Publicada en el DOF el 5 de julio de 2010, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares es una ley[35] reglamentaria que, en el segundo párrafo del artículo 16 constitucional, llena un vacío legal a nivel federal (anteriormente, sólo los Estados de Jalisco, Colima y Morelos tenían regulación al respecto) cuya premisa es la "autodeterminación informativa". A un año de su publicación y entrada en vigor, obliga a todos los responsables del tratamiento de datos personales a otorgar un "*aviso de privacidad*" a los titulares de los mismos, y a tener dentro de la organización a un encargado (ya sea una sola persona o un grupo colegiado) para el manejo de este tema.

El objetivo de la ley, su reglamento y demás disposiciones, es salvaguardar y regular el tratamiento legítimo, controlado e informado de las bases de datos que

---

el 20 de julio de 2007. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=4994148&fecha=20/07/2007

[35] Disponible para su consulta en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

contengan datos personales, para así garantizar la privacidad y el derecho a la autodeterminación informativa, y el acceso, rectificación y cancelación de los mismos.

Como se ha referido, los sujetos regulados por la ley son las personas físicas o morales que para sus actividades cotidianas recaben, manejen, utilicen o traten información personal, con excepción de las sociedades de información crediticia y las personas que recolectan y almacenan datos personales para uso exclusivamente personal o doméstico

Prevé mecanismos ágiles, expeditos y sencillos para que los ciudadanos puedan ejercer sus derechos ante los responsables de las bases de datos. Para tal efecto, se conciben como autoridades competentes a la Secretaría de Economía y al extinto IFAI, hoy INAI. Este último se encargará de promover y difundir el ejercicio del derecho a la información, además de resolver en caso de negativa a las solicitudes de acceso a la información, y proteger los datos personales en poder de las dependencias y entidades.

Contra las resoluciones del Instituto, los particulares podrán promover Juicio de Nulidad ante la autoridad competente (en este caso el Tribunal Federal de Justicia Fiscal y Administrativa). Asimismo, los gobernados que consideren que han sufrido un daño o lesión en sus bienes o derechos, como consecuencia del incumplimiento a lo dispuesto en la Ley, podrán ejercer las acciones necesarias a efecto de que proceda la indemnización correspondiente, por lo que tendrán que recurrir a la vía civil.

Al respecto, cabe resaltar que la ley es omisa en cuanto a si, para ejercer la acción de indemnización, se requiere o no como prerrequisito la declaratoria de infracción por parte del Instituto, en cuyo caso, se prolongaría el plazo para la reparación del daño. Lo anterior tendrá que ser esclarecido en la práctica por los tribunales.

Por su parte, este ordenamiento otorga una importante protección a los llamados “*datos sensibles*”, relacionados con las preferencias sexuales, origen étnico, racial o estado de salud, que podrían ser mal utilizados para discriminar o

excluir a una persona, de suerte que en caso de que sean violentados, las penas se duplicarán.

Los responsables de las bases de datos están limitados en cuanto al uso de los datos personales, pues estos sólo pueden ser utilizados según los fines por los que fueron recabados. Asimismo, son necesarias las medidas de seguridad que eviten su pérdida, robo o acceso no autorizado, de lo contrario se sancionará, de tres meses a tres años de prisión, a quien con fines de lucro vulnere la seguridad de las bases de datos que estén bajo su custodia; y de seis a cinco años, a quien mediante engaños trate de aprovecharse del error en que se encuentre el titular o persona autorizada a transmitir la información personal.

Entre las principales infracciones administrativas cabe citar a las siguientes:

1) tratamiento de datos personales en contravención de la Ley;

2) omitir aviso de privacidad;

3) uso o transferencia de datos personales sin consentimiento de titular;

4) uso, divulgación o transferencia de datos sensibles para fines secundarios, y

5) recabar datos de forma engañosa y fraudulenta.

Las infracciones serán sancionadas por el Instituto como se indica a continuación:

a) apercibimiento en el caso de no cumplir con la solicitud del titular para el acceso, rectificación, cancelación u oposición;

b) multa de 100 a 160,000 días de salario mínimo vigente en el Distrito Federal, y

c) multa de 200 a 320,000 días de salario mínimo vigente en el Distrito Federal (hoy Unida de Medida y Actualización).

Además, se impondrá de 3 meses a 3 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 custodia. 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 persona autorizada para transmitirlos. En todos los casos, las penas se duplicarán si se trata de datos sensibles.

Sin duda alguna, la ley busca fomentar el desarrollo de las TIC con la conciencia de que las bases de datos y el tratamiento de las mismas están siempre al servicio del hombre y que, por lo tanto, deben respetarse las libertades y derechos fundamentales de las personas físicas, en particular la protección de sus datos personales.[36]

Por otro lado, a pesar de que su aparición es muy tardía, permite que México esté a la altura de los países miembros de la OCDE, de APEC y de la Unión Europea, y cumplir con los estándares internacionales en materia de privacidad, aprobados en la conferencia Mundial de Comisionados de Privacidad y Protección de Datos, en noviembre del 2009; produciendo un efecto muy positivo en la economía nacional, puesto que dota de certeza jurídica a los intercambios comerciales transfronterizos, propiciando así, mayores flujos de inversión extranjera directa y generación de empleos.

[36] Al respecto, el entonces senador por el Partido del Trabajo Ricardo Monreal Ávila señaló que: "*El manejo de intercambio de carácter personal se ha convertido lamentablemente en México en una práctica habitual, mucho de abuso de poder y control de parte del sector público y privado, y ahora recientemente hasta en los tianguis puedes encontrar base de datos de la región más alejada del país, digna y actualizada del último día de movimientos registrados en las oficinas correspondientes de su población*". Véase en: Sesión ordinaria de la Cámara de Senadores celebrada el martes 27 de abril de 2010. Senado de la República. Versión estenográfica. Disponible en: http://www.senado.gob.mx/64/version_estenografica/2010_04_27/935 [Fecha de consulta: 05 de marzo de 2018]

2.2.8. Ley Federal del Derecho de Autor

Las bases de datos se encuentran doblemente protegidas, primero, por normas de privacidad y, segundo, por normas de derechos de autor. En este aspecto, el Convenio de Berna establece que las bases de datos son protegidas como compilaciones y no como bases de datos en forma expresa.[37]

A su vez, la legislación nacional las reconoce expresamente como obras protegidas,[38] siempre que, por razones de selección y disposición de su contenido o materias, constituyan una creación intelectual.[39]

Adicionalmente, el artículo 108 señala que "*las bases de datos que no sean originales*[40] *quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de cinco años*."[41]

Esta protección se da, pero no precisamente para el autor, sino para el titular del derecho patrimonial, ya que el artículo 110 otorga (al titular del derecho patrimonial) facultades exclusivas respecto a la forma de expresión de la estructura de la base de datos, para autorizar o prohibir cualquiera de las siguientes acciones:

1) Su reproducción permanente o temporal, total o parcial, por cualquier medio y, de cualquier forma;

---

[37] Artículo 2(5) del Convenio de Berna para la protección de las obras literarias y artísticas. Disponible en: https://www.wipo.int/treaties/es/text.jsp?file_id=283700#P91_12057 [Fecha de consulta: 12 de marzo de 2018]

[38] Cfr. Artículo 13 de la Ley Federal del Derecho de Autor. Publicada en el DOF el 24 de diciembre de 1996. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/122_150618.pdf [Fecha de consulta: 15 de marzo de 2018]

[39] Véase artículo 107 de la Ley Federal del Derecho de Autor.

[40] La originalidad reside en razones de selección y disposición de su contenido o materias.

[41] Véase artículo 108 de la Ley Federal del Derecho de Autor.

2) su traducción, adaptación, reordenación y cualquier otra modificación;

3) la distribución del original o copias de la base de datos;

4) la comunicación al público; y

5) la reproducción, distribución o comunicación pública de los resultados de las operaciones mencionadas en la fracción II del presente artículo.

2.2.9. Ley Federal de Protección al Consumidor

La Ley Federal de Protección al Consumidor se publicó en el DOF el 24 de diciembre de 1992[42] y mediante una reforma en el año 2000, se adicionó el capítulo VIII Bis, titulado: "*De los derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología*".

Al respecto, el artículo 76 Bis de la citada ley refiere que, en la celebración de transacciones efectuadas a través del uso de medios electrónicos, se deberá cumplir con lo siguiente:

- Protección a la información personal: el proveedor utilizará la información proporcionada por el consumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente.
- Uso tecnológico a favor de la seguridad: el proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos.
- El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los

[42] Texto disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/113_250618.pdf

que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones.

- Prácticas engañosas: el proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella.

- Información del producto: el consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor.

- Anti-Spam: el proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y

- Protección de población vulnerable: el proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, en especial tratándose de prácticas de mercadotecnia dirigidas a la población vulnerable, como los niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población.

De lo anterior se advierte que, previo a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, ya existía un exiguo marco protector a los datos personales. Adicionalmente, se advierte que en México el "*spam*"[43]

[43] El Proyecto Norteamericano sobre Protección al Consumidor en Comercio Electrónico (North American Consomer Project on Electronic Commerce, NACPEC), una organización sin fines de lucro define el spam en los términos siguientes: "*mensajes indeseados o no solicitados que son enviados en cantidades masivas y recibidos en las secciones "in-box o bulk" de las direcciones de correo electrónico, sin existir relación previa alguna entre el iniciador del mensaje y el destinatario del mismo y normalmente sin el consentimiento expreso o la aprobación de este último.*

(práctica de enviar correos electrónicos masivos para publicitar productos o servicios) está regulado a través de los artículos 17, 18, 76 Bis y 128 de la Ley Federal de Protección al Consumidor, de conformidad con lo siguiente:

> *Artículo 17: En la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor; de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la Procuraduría.*
>
> *El consumidor podrá exigir directamente a proveedores específicos y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, no ser molestado en su domicilio, lugar de trabajo, dirección electrónica o por cualquier otro medio, para ofrecerle bienes, productos o servicios, y que no le envíen publicidad. Asimismo,* ***el consumidor podrá exigir en todo momento a proveedores y a empresas que utilicen información sobre consumidores con fines mercadotécnicos o publicitarios, que la información relativa a él mismo no sea cedida o transmitida a terceros, salvo que dicha cesión o transmisión sea determinada por una autoridad judicia****l.* [Énfasis añadido]
>
> *Artículo 18: La Procuraduría podrá llevar, en su caso, un registro público de consumidores (Registro Público para Evitar Publicidad, REPEP) que no deseen que su información sea utilizada para fines mercadotécnicos o publicitarios. Los consumidores podrán comunicar por escrito o por correo*

El spam ha evolucionado en forma alarmante en los últimos años; comenzó como una simple molestia y se ha convertido en un grave problema que conlleva consecuencias fraudulentas y penales tanto para los usuarios finales como para las redes de cómputo. El spam traspasa medidas técnicas, políticas regulatorias, amenaza el uso y buen funcionamiento de las redes empresariales, públicas y académicas, sirve como un conducto para el crimen informático, pone en riesgo la confianza del consumidor y desalienta el uso del correo electrónico entre los Internautas." Disponible en: http://www.nacpec.org/es/links/spam/index.html [Fecha de consulta: 16 de marzo de 2018]

electrónico a la Procuraduría su solicitud de inscripción en dicho registro, el cual será gratuito.

De igual importancia es el artículo 18 BIS, que limita el uso de los datos personales de los consumidores por parte de las empresas:

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

Básicamente, estos artículos prohíben dos cosas a los prestadores de servicio: utilizar la información sobre consumidores con fines mercadotécnicos o publicitarios, y enviar publicidad a los consumidores, a menos que hubieren manifestado su voluntad de recibirla, es decir, si el consumidor acepta el envío de publicidad, no habrá ninguna infracción a la norma.

2.2.10. Autoridades nacionales de la materia

2.2.10.1. IFAI/INAI

2.2.10.1.1. Creación del Instituto

La derogada Ley Federal de Acceso a la Información Pública Gubernamental, en su momento estableció como autoridad competente para proteger los datos personales al extinto IFAI.

En este sentido, el IFAI se transformó en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) tras la publicación de la Ley General de Transparencia y Acceso a la Información Pública en el DOF el 5 de mayo de 2015.

Al hablar ahora del INAI, podemos decir, que se trata de un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y

patrimonio propio, con plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales, tanto en el sector público como en el sector privado, en términos del artículo 6 de la CPEUM

2.2.10.2. Facultades

Específicamente, en materia de Protección de Datos Personales, se destacan las siguientes atribuciones:

- interpretar en el ordenamiento jurídico aplicable en materia de protección de datos personales;
- conocer y resolver los recursos de revisión interpuestos por los solicitantes;
- establecer y revisar los criterios de clasificación, desclasificación y custodia de la información reservada y confidencial;
- elaborar los formatos de solicitudes de acceso y corrección de datos personales;
- establecer los lineamientos y políticas generales para el manejo, mantenimiento, seguridad y protección de los datos personales, que estén en posesión de las dependencias, entidades y los particulares;
- promover y, en su caso, ejecutar la capacitación de los servidores públicos en materia de acceso a la información y protección de datos personales;
- difundir entre los servidores públicos y los particulares, los beneficios del manejo público de la información, como también sus responsabilidades en el buen uso y conservación de aquélla;
- elaborar y publicar estudios e investigaciones para difundir y ampliar el conocimiento sobre la materia de protección de datos personales, y
- cooperar respecto a la legislación aplicable a la protección de datos personales con los demás sujetos obligados, las entidades federativas, los municipios, o sus órganos de acceso a la información, mediante la celebración de acuerdos o programas.

En los últimos años, el papel del Instituto se ha destacado por contribuir al desarrollo y enriquecimiento del derecho a la protección de datos personales, en particular a través de dos vertientes:

- La emisión de resoluciones por parte del Pleno del INAI donde se han establecido una serie de criterios relevantes respecto al acceso y corrección de datos personales, principalmente en los casos denominados de "*tensión de derechos*".
- La expedición de disposiciones como instrumento de desarrollo de la Ley General de Transparencia, a efecto de contar con normas específicas en materia de manejo, mantenimiento, seguridad y protección de los datos personales en posesión de los entes públicos federales, tales como los Lineamientos Generales de Protección de Datos Personales para el Sector Público.[44]

2.2.10.1.3. Reformas del 22 de agosto de 2013

El 22 de agosto de 2013, la Cámara de Diputados aprobó un dictamen de reformas constitucionales en materia de transparencia y rendición de cuentas que modificaron trascendentalmente al entonces IFAI ahora INAI.[45]

Esencialmente, las reformas se expresaron en los siguientes términos:

1) Se le dotó de autonomía constitucional al INAI.

---

[44] Disponibles en: http://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018 [Fecha de consulta: 20 de marzo de 2018]

[45] Véase: nota de prensa titulada "Aprueban diputados, en lo general, reformas del IFAI para dotarlo de más autonomía y discuten en lo particular una veintena de reservas presentadas". Nota de prensa número 3973. Comunicación social de la Cámara de Diputados, 22 de agosto de 2013. Disponible en: http://www3.diputados.gob.mx/camara/005_comunicacion/b_agencia_de_noticias/009_2013/08_agosto/22_22/3973_aprueban_diputados_en_lo_general_reformas_del_ifai_para_dotarlo_de_mas_autonomia_y_discuten_en_lo_particular_una_veintena_de_reservas_presentadas [Fecha de consulta: 01 de abril de 2018]

2) Se amplió el universo de sujetos obligados que tendrán que transparentar el uso de recursos públicos, incluyendo a los fideicomisos, personas físicas y morales. También se prevé que sindicatos y partidos deberán rendir cuentas de manera directa, de los recursos públicos que reciban. Es decir, ya no responderán en materia de transparencia al Instituto Nacional de Transparencia, sino a la Suprema Corte de Justicia de la Nación.

   Otro tema muy criticable es que se excluyeron como sujetos obligados directos a los partidos políticos, entidades que reciben grandes cantidades de recursos públicos (y que ya son sujetos obligados directos en 17 legislaciones estatales sobre acceso a la información). En este punto, es de mencionar que los Diputados no aprobaron incluirse como sujetos obligados vía grupos parlamentarios.

3) El INAI puede presentar acciones de inconstitucionalidad cuando haya una posible contradicción en una norma, y tendrá facultad de atracción cuando las resoluciones de otros órganos garantes no satisfagan al ciudadano solicitante de la información, o cuando así lo estime conveniente.

4) No serán atacables sus resoluciones excepto cuando se trate de resoluciones en materia de seguridad nacional; es de notar que cualquier funcionario podrá acudir a la Suprema Corte de Justicia de la Nación, de ser necesario, cuando considere que la información que solicita el ciudadano contraviene la Seguridad Nacional.

   Al respecto, conviene aclarar que las resoluciones del INAI solo podrán ser impugnadas por la Procuraduría General de la República, el Banco de México, la Consejería Jurídica del Ejecutivo Federal y la Comisión Nacional de los Derechos Humanos. Lo anterior, en otras palabras, implicaría “la judicialización de un derecho fundamental que, hasta ahora, se ha ejercido

en México en forma gratuita, pronta y expedita, y que ha colocado a nuestro país como referencia mundial en la materia."[46]

5) En lo que toca a la estructura orgánica del ahora INAI, en el *adendum* del Dictamen, se estipuló que los comisionados tendrán un Consejo Consultivo integrado por 10 consejeros que serán elegidos por el voto de las dos terceras partes de los miembros presentes de la Cámara de Senadores. El mecanismo para elegir a los comisionados será a través del Senado, pero el presidente podrá objetar el nombramiento hasta en dos ocasiones (la elección de dos comisionados nuevos deberá ser realizada a más tardar 90 días después de haberse publicado el decreto constitucional).

6) Cada entidad federativa deberá dotar de autonomía a sus órganos de Transparencia; tenían un plazo de un año para armonizar su normatividad. Para ello, el Congreso de la Unión tenía un plazo de un año para expedir una Ley General del artículo 6 de la Constitución, así como las reformas que correspondan a la entonces Ley Federal de Transparencia.

2.2.10.1.4. Reformas del 5 de mayo de 2015

Además del nombre, el INAI renovó su misión, visión y objetivos; creó comisiones de trabajo y aprobó 84 proyectos estratégicos con los que el INAI ejercería sus nuevas funciones y atribuciones legales. Dentro de los elementos destacables, tenemos los siguientes:

Tanto a nivel federal como local, los funcionarios públicos deberán dar detalles del dinero público que reciben por concepto de bonos, ingresos, prestaciones, primas y gratificaciones.

La Ley General de Transparencia detalla cuando un sujeto obligado podrá reservar información y cuando deberá hacerla pública a través de la prueba de daño

[46] Véase al respecto: Comunicado IFAI/077/13. "Posicionamiento del IFAI frente al proyecto de dictamen de los diputados del 19 de agosto de 2013". IFAI, 20 de agosto de 2013. Disponible en: http://inicio.ifai.org.mx/comunicados/comunicado%20ifai-077-13.pdf [Fecha de consulta: 02 de abril de 2018]

y prueba de interés público. Se generó la obligación del INAI de elaborar un nuevo padrón de sujetos obligados, pues se deberá garantizar el acceso a la información en manos de las dependencias y organismos de los poderes Legislativo y Judicial, además de los partidos políticos y los sindicatos.

Uno de los retos más grandes fue el compromiso de establecer un sistema nacional de transparencia, acceso a la información pública y protección de datos personales, así como el diseño de la plataforma nacional de transparencia.

2.2.10.2. PROFECO

La PROFECO fue creada en 1976, y a partir de entonces México se convirtió en el primer país latinoamericano en tener una institución encargada de defender los derechos de los consumidores, prevenir abusos y garantizar relaciones de consumo justas.

Para 1982 la institución ya contaba con 32 oficinas en las principales ciudades del país. Actualmente, la PROFECO cuenta con un total de 32 delegaciones y 19 subdelegaciones, lo cual suma un total de 51 oficinas en toda la República.

La Procuraduría encuentra su fundamento constitucional en el artículo 28, y se desenvuelve dentro del marco jurídico de la Ley Federal de Protección al Consumidor, así como su Reglamento, Acuerdos, Circulares, Avisos, Normas Oficiales Mexicanas, entre otras disposiciones como el Código Civil Federal, el Código de Comercio, Ley Federal de Competencia Económica, Ley Federal sobre Metrología y Normalización, que convergen con la materia.

El objetivo de este órgano es proteger y promover los derechos de los consumidores, garantizando relaciones comerciales equitativas que fortalezcan la cultura de consumo responsable y el acceso, en mejores condiciones de mercado, a productos y servicios, asegurando certeza, legalidad y seguridad jurídica dentro del marco normativo de los derechos humanos reconocidos para los consumidores, a través de los siguientes ejes:

- Proteger y defender los derechos del consumidor

- Generar una cultura de consumo responsable
- Asegurar información adecuada para la toma de decisiones en el consumo, e
- Implementar métodos de atención pronta y accesible a los ciudadanos mediante el uso de tecnologías de la información

En cuanto a datos personales, como se ha mencionado anteriormente, en el capítulo VIII Bis de la Ley Federal de Protección al Consumidor, titulado, *"De los derechos de los consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología"*, se establecen reglas para el tratamiento de datos personales, cuando se realice con fines mercadológicos, específicamente en los artículos 17, 18, 76 Bis y 128 de dicho ordenamiento.

Dentro de sus atribuciones, la PROFECO tiene la facultad de imponer sanciones y las infracciones respecto a los artículos antes mencionados, estableciendo multas de $617.41 a $2'414,759.14 pesos mexicanos.

Por último, PROFECO –además de pertenecer al Comité de Políticas del Consumidor de la OCDE- pertenece a "*Comerce.gov*", un proyecto internacional donde se apoya al consumidor en lo referente a reclamaciones por transacciones electrónicas realizadas en el extranjero.

2.2.10.3. CONDUSEF

La CONDUSEF es una institución pública dependiente de la Secretaría de Hacienda y Crédito Público. Tiene labores preventivas, tales como: orientar, informar, promover la Educación Financiera, y correctivas, entre las que se destacan, atender y resolver las quejas y reclamaciones de los usuarios de servicios y productos financieros.

Entre sus principales objetivos, se encuentran:

- Fomentar la Educación Financiera entre la población.
- Desarrollar productos y herramientas que apoyen, asesoren y orienten a los usuarios de servicios financieros, y

- Buscar una relación justa y equitativa entre los usuarios y las instituciones financieras.

Esta institución se desarrolla dentro de un marco jurídico que se encuentra en constante adecuación, y que busca atender los problemas y realidades de la sociedad mexicana en el sector financiero. De este marco destacan:

- La Ley de Protección y Defensa al Usuario de Servicios Financieros
- El Estatuto Orgánico de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros
- La Ley para la Transparencia y Ordenamiento de los servicios Financieros, y
- El Reglamento de supervisión de la CONDUSEF

Viene al caso mencionar a la CONDUSEF interviene en la protección de los datos personales, ya que está facultada para analizar y verificar que la información publicitaria, y toda aquella utilizada por las instituciones financieras para comunicar los beneficios o compromisos que el usuario asume al adquirir un producto o contratar un servicio, sea veraz, efectiva y que no induzca a confusiones o interpretaciones equívocas.

Al respecto, hasta el mes de julio de 2013, la CONDUSEF había atendido a 777,831 usuarios respecto a “acciones de defensa al usuario”,[47] las cuales se traducen en un 82% de asesorías técnico-jurídicas y el 17% a controversias, entre las que se destacan reclamaciones presentadas por usuarios a una institución financiera. Conviene referir que, dentro de dichas controversias, el 60% correspondieron a los bancos, el 14% a aseguradoras, el 14% a SICs, el 5% a

[47] Véase en: Acciones de defensa que realiza la CONDUSEF en beneficio de los usuarios de servicios financieros para el periodo 1999-2017. CONDUSEF. Disponible en: https://www.condusef.gob.mx/gbmx/documentos/estadistica/estad2017/historia-1999-2017.pdf

AFORES y el otro 5% a SOFOMs.

No obstante, en cuanto a infracciones en materia de protección de datos personales, es necesario hacer especial énfasis en que sólo el INAI tiene facultades para imponer sanciones a particulares cuando se violen los derechos de los titulares de los datos, aun cuando se traten de instituciones financieras reguladas por una ley especializada.

Capítulo 3

Valor e importancia de la protección de la información en las empresas.

Capítulo 3: Valor e importancia de la protección de la información en las empresas

3.1. Tratamiento de información y datos personales en las empresas

Uno de los elementos clave que dan lugar a un cambio social y cultural es sin duda el efecto que generan en el hombre los descubrimientos científicos y los avances tecnológicos. El desarrollo constante de nuevas tecnologías ofrece novedosas y útiles herramientas que facilitan el día a día de la sociedad entera.

Debido al imparable desarrollo de las tecnologías es posible almacenar un número ilimitado de datos personales de millones de individuos y utilizarlos para fines indistintos, los cuales pueden circular en cuestión de segundos entre personas, países, empresas privadas, entidades de gobierno y redes abiertas.

La red de Internet y las múltiples aplicaciones y funcionalidades tecnológicas son ahora aliados y, mejor dicho, elementos indispensables para que la oferta de productos y prestación de servicios sea más atractiva para las empresas y para los usuarios consumidores. Es por ello que las empresas en la prestación de sus servicios, cualquiera que sea la industria, sector o segmento al que pertenezcan, necesariamente generen, usen y administren bases de datos con información de personas que les resulta en una ventaja competitiva para asegurar su permanencia en el mercado, su posicionamiento, y su crecimiento constante (sustentabilidad).

Tenemos entonces que, resulta necesario para las empresas evaluar el factor "*riesgo-beneficio*" de manejar información y datos personales como principal "*asset*" (valor o insumo). Esto se explica, que al incrementar el volumen de información en una empresa, se incrementa automáticamente el riesgo de que dicha información sea vulnerada, por lo que, dicha empresa se ve obliga a tomar medidas emergentes para controlar la contingencia y disminuir riesgos, o bien, en el mundo ideal, que dicha empresa de manera preventiva, previsora y responsable, cuente desde un inicio con esquemas de protección, tales como programas de gestión de información, políticas de seguridad de la información y datos personales, esquemas de autorregulación, etcétera.

Por el otro lado, se encuentran las personas físicas, titulares de los derechos de protección de personales e información que necesariamente ponen a disposición de las empresas responsables para la adquisición de un bien, un servicio, para formalizar una relación laboral o simplemente, ante cualquier acercamiento con una empresa. El derecho de protección de estos datos personales, también llamado derecho a la autodeterminación informativa, se traduce como el poder de disposición y control que faculta a su titular a decidir cuáles datos proporciona a un tercero. Es decir, es el derecho que tiene toda persona a conocer y decidir, quién, cómo y de qué manera recaba y utiliza sus datos personales. Este nuevo derecho implica la libertad que tiene toda persona para elegir qué desea comunicar, cuándo y a quién, manteniendo el control personal sobre la propia información.[48]

3.2. Importancia económica de los datos personales en las empresas

Al formar parte de una sociedad cada vez más controlada y vigilada por las empresas multinacionales que acceden a todo tipo de información, por gobiernos que bajo el argumento de "*seguridad nacional*" usan los más sofisticados sistemas de comunicación y captación para revisar el flujo de información dentro y fuera de sus jurisdicciones sin tomar en cuenta los límites impuestos por aquellas legislaciones que protegen la privacidad de las personas.

En 1948, George Orwell, en su novela política de ficción *1984* profetizó una sociedad futura que acabaría vigilándose a sí misma. La trama plantea la existencia de un Estado totalitario donde siempre se halla la figura omnipresente del "*Gran Hermano*", el que todo lo ve, todo lo escucha y todo controla. Es una representación adelantada de la sociedad actual.

[48] Para mayor información sobre el carácter fundamental y autónomo, véase: Sentencia 292/2000, de 30 de noviembre emitida por el Tribunal Constitucional de España. Disponible en: http://hj.tribunalconstitucional.es/HJ/cs-CZ/Resolucion/Show/SENTENCIA/2000/292

En efecto, a través de la vigilancia exhaustiva de llamadas telefónicas, mensajes de texto, localización a través de sistemas GPS, redes sociales, entre muchas otras actividades cotidianas de cualquier individuo, los gobiernos, partidos políticos, empresas y consorcios globales, saben hasta el más ínfimo detalle de la vida y quehaceres cotidianos de las personas en aras de crear hábitos de consumos predefinidos y "*personalizados*".

De manera inevitable, al formar parte de una sociedad digital y con el imparable desarrollo de las tecnologías de la información, los datos personales, especialmente los compartidos a través de internet, se han consolidado como un bien muy preciado en el mercado. Así lo demuestran las cifras que arroja un estudio de la compañía consultora "*Roland Berger*", publicadas recientemente en el periódico francés "*Le Figaro*": los datos personales que venden y compran las grandes compañías, están valorados en el mercado en más de 100,000 millones de dólares.[49]

Este mercado compete, principalmente, a los cinco grandes actores de Internet: "*Facebook*, *Google*, *Amazon*, *Apple* y *Microsoft*". Estos gigantes pueden anticipar mejor las necesidades de los usuarios y ofrecer publicidad muy específica, y lo logran gracias a que disponen de enormes bases de datos sobre los usuarios y las venden a las compañías para una colocación más acertada de anuncios publicitarios de sus productos o servicios.

De acuerdo con el artículo, existe un complejo sistema de precios, según el cual el precio para el acceso a los datos de personas dependerá de ciertas categorías, por ejemplo: la información sobre 1000 compradores potenciales de productos de la industria ligera, puede venderse por unos dos dólares, mientras que los datos de 1000 compradores de automóviles cuestan unos 85 dólares. Un dato revelador es que una

[49]Véase: "*Données personnelles: un marché de 100 milliards de dollars en France*" Le Figaro, 21 de julio de 2013. Disponible en: http://www.lefigaro.fr/mon-figaro/2013/07/21/10001-20130721ARTFIG00115-donnees-personnellesun-marche-de-100milliards-de-dollars-en-france.php

de las categorías más caras en este mercado son las personas que padecen cáncer, ya que los datos de 1000 enfermos valen aproximadamente 260 dólares.

Stephen Baker, escritor y periodista norteamericano, explica este complejo fenómeno de modo ameno y amigable en su libro "*The Numerat"*, [50] el cual por la información y estadísticas que ofrece pareciera ser de ciencia ficción, pero en realidad refleja las estrategias actuales del *marketing*, que, si bien son totalmente innovadoras y eficaces, también violan el derecho a la privacidad, transgrediendo todo lo relativo a la protección de los datos personales.

La información generada día a día con el acceso a Internet, con llamadas telefónicas, mensaje de celular, correo electrónico, uso de tarjetas de crédito, etcétera esa información que queda a disposición de empresas como "*Amazon, Google, Facebook,* y *Yahoo*"*,* es posteriormente analizada y procesada por especialistas que generan perfiles comerciales o que establecen ánimos de consumo.

Los analistas comerciales han sido llamados por Baker como los "*Numerati"* (parafraseando a aquella sociedad secreta y grupo político-económico de poder del siglo XVIII, los *"Illuminati"*).[51] Esta obra explica cómo es que los expertos utilizan dicha información para predecir con cierta exactitud las decisiones de consumo de las personas, no obstante, los "*Numerati"* en realidad buscan influenciar en el ánimo de consumo del usuario sin que pueda percatarse.

> *(Los numerati) ya están empleando nuestros datos en modelos predictivos, y apenas es el comienzo. En la próxima década cada uno de nosotros generará, a menudo sin saberlo, modelos propios en cada uno de los aspectos de la vida. Nos moldearán como empleados, pacientes, soldados, amantes, consumidores y lectores. (...) Seas lo que seas -y cada uno de nosotros somos muchas cosa-, compañías y gobiernos quieren localizarte.*[52]

---

[50] Baker, Stephen. Los Numerati. Planeta, México, 2009, p. 57.

[51] *Ibidem,* p. 57.

[52] *Ibidem*, p. 132.

Es así que los consumidores y usuarios de Internet se han habituado a tener una actividad, de alguna forma, predeterminada por una estrategia comercial.

3.3. Principio de "*responsabilidad demostrada*" ("*accountability*")

El término "*accountability*" no tiene una traducción textual al idioma español, no obstante, se trata de un principio que intenta regular la responsabilidad de una entidad en el manejo de sus operaciones. Existen países cuyas legislaciones, esquemas o modelos de protección de información definen al concepto "accountability" explicando los siguientes elementos:

i) Rendición de cuentas,

ii) Responsabilidad, y

iii) Responsabilidad demostrada o demostrable.

Este concepto se ha definido en el ámbito de los negocios como "la obligación de un individuo o una empresa de rendir cuentas de sus actividades, aceptar la responsabilidad de las mismas, y dar a conocer los resultados de una manera transparente".[53]

En el campo de la protección de datos personales, "*accountability*" significa la obligación de reportar y explicar los procesos de tratamiento de datos personales, a fin de identificar y documentar las medidas implementadas para dar cumplimiento con los requisitos de ley.

La figura del "*accountability*" tiene por objeto identificar fallas o brechas de seguridad para la toma de acciones correctivas y preventivas. Con la implementación de un sistema de "*accountability*", las empresas deben ser capaces de explicar o rendir cuentas de su cumplimiento en materia de protección de datos personales, tanto a los individuos respecto de los cuales tratan sus datos personales, como de las autoridades garantes de ese cumplimiento.

---

[53] Definición de accountability. Business Dictionary. Disponible en: http://www.businessdictionary.com/definition/accountability.html#ixzz3q4OP2Sta [Fecha de consulta: 19 de abril de 2018]

En México el concepto "*accountability*" no está previsto como tal en la legislación, pero esto no significa, que la entidad responsable en el manejo de información y datos personales no deba responder por los daños causados por el mal manejo de los mismos, ni que garantice la disminución en los efectos e impacto de la contingencia.

En este sentido, se considera que el término "*accountability*" debe ser incorporado a aquellas modelos de autorregulación, políticas de seguridad de la información, esquemas de protección, como una herramienta más que garantiza al usuario el manejo y trato seguro de sus datos personales e información. Por su parte, la empresa responsable, ante la existencia de este elemento, debe ser cuidadosa de cumplir con las políticas de seguridad de la información o esquemas de protección a que se haya sometido, o bien, generar mejoras que permitan ofrecer un ambiente de seguridad en su beneficio y desde luego, en favor de los individuos.

3.4. Empresas que califican para un modelo de protección de datos especifico

"*La mercadotecnia no es un concepto unívoco, sino que el género comprende varias especies correspondientes a los distintos giros o actividades del mundo de la comunicación comercial*."[54]

Lo anterior significa que todas las entidades (personas físicas o morales) que manejan información o datos personales con un fin de comercialización de productos o servicios, usan de manera indirecta datos personales para realizar actividades de mercadotécnica, publicidad, promoción o venta, por lo tanto, son entidades que califican para la implementación de un modelo de auditoria de protección de información y datos personales.

El giro de las empresas que se mencionan a continuación tiene por objeto promover o promocionar la venta de productos o servicios, las cuales

[54] Vera Vallejo, Luis. La Protección de datos en el ámbito de la mercadotecnia, en: Ornelas Núñez, Lina y Pinar Mañas, José Luis, *op. cit.* p. 472.

indudablemente son ejes que fomentan el desarrollo del comercio tanto a nivel nacional como internacional.

Agencias de publicidad

A las agencias de publicidad se les encarga la creación, desarrollo y diseño de campañas de comunicación, promoción y difusión de una imagen comercial, en donde la creatividad del concepto, diseño y desarrollo es el elemento clave para el éxito en la comercialización de bienes y servicios. Las campañas de referencia pueden clasificarse en: publicitarias, políticas, de comunicación e imagen gubernamental.

Empresas de investigación de mercado

Estas empresas se dedican a realizar actividades de análisis de mercado y a investigar e identificar el potencial mercado, la conducta del consumidor, la operación de los competidores en un segmento determinado, factores entorno a una industria o sector determinado, prospectiva comercial de un producto o servicio, encuestas para general una postura derivada de la opinión pública, la determinación de condiciones sociales que muestran flujos comerciales, eficiencia publicitaria de un producto o servicio en una zona determinada, comportamientos y patrones de consumo en relación a diversos factores, etcétera; siendo lo más importante, el uso de información y datos personales como el factor determinante del estudio económico.

Empresas de mercadotecnia directa

Estas empresas tienen por objeto realizar campañas de comunicación "*uno a uno*", cuyo trabajo fino es identificar directamente al consumidor a partir de su investigación y análisis, así como el establecimiento de mecanismos de interacción que dan como resultado los elementos informativos, para poder diseñar ofertas realmente sintonizadas con los intereses y preferencias del consumidor, estableciendo relaciones duraderas y exitosas.

Empresas recolectoras y comercializadoras de bases de datos

Estas empresas, como se percibe, se dedican prácticamente a la recolección de datos de personas para ser clasificados de acuerdo a diversos criterios mercadotécnicos, como pueden ser edad, género, posición geográfica, hábitos de consumo, capacidades económicas, etcétera sin que previamente hayan sido requeridas por un proveedor de productos o servicios. Estas empresas que evidentemente dan un tratamiento a la información de datos personales debidamente clasificados y ordenados, según los criterios mencionados, bien sea vendiéndolos o rentándolos o cualquier otra modalidad comercial.

Centros de contacto (call centers)

Se trata de empresas con una plataforma eficiente para generar un contacto entre un cliente potencial y un proveedor de bienes o servicios. Últimamente estas empresas han crecido en forma importante dentro de la actividad mercadotécnica. Su éxito radica en que existe una gran necesidad de acercarse y tener un contacto personal y directo, que generalmente es a distancia, vía telefónica o por medio de Internet para llevar al conocimiento del potencial consumidor, la información correspondiente a la oferta de productos y servicios, así como brindar una atención tercerizada como atención al cliente, resolución de dudas, orientación técnica, etc. En algunos casos ofrecen sus servicios vía tercerización (outsourcing), respecto de empresas que les proveen la información y los datos para acceder a los consumidores.

Bancos y empresas de tarjetas de crédito

En este rubro agrupamos a todas las instituciones de servicios financieros. También manejan tarjetas de crédito, bajo distintas marcas (visa, MasterCard, etc.), y aprovechan sus bases de datos para efectos de comercialización e inclusive para promover la venta de productos no financieros.

Las empresas de tarjetas de crédito, de igual forma crean y mantienen grandes bases de datos de sus tarjeta-habientes y utilizan sus bases de datos para la comercialización de sus servicios y en algunos casos, para comercializar con terceros la utilización de dichas bases de datos.

Tiendas departamentales y ventas por Internet

Estas empresas generalmente manejan bases de datos de sus clientes y desarrollan mecanismos de fidelidad, lealtad y trato diferenciado con premios y promociones. Cuando desean publicitar sus productos y servicios, regularmente utilizan dichas bases de datos en sus campañas a través de correo directo, e-mail o telemarketing.

Empresas en general

Hoy día y con el apoyo de los equipos y sistemas de las tecnologías de la información, las principales empresas normalmente crean, tienen y utilizan y en ocasiones comercializan para sí u otros, sus propias bases de datos las cuales se recolectan por diversos mecanismos entre los que pueden señalarse medios impresos, o bien, mayormente a través de medios electrónicos, como páginas web y eventos marketing como promociones y puntos de contacto en tiendas o plazas comerciales.

3.5. La importancia de una auditoria en un modelo de protección de información

3.5.1. Definición

La palabra auditoria proviene del latín "*auditorius*" que quiere decir oír y revisar cuentas. Para el caso de auditoría de sistemas se debe entender como la recolección y evaluación de evidencias sobre la eficiencia y eficacia en el uso de los sistemas en la organización.

De acuerdo a la Real Academia Española, auditoría se define como: "revisión de cuentas colegiado". En un principio esta definición carece de la explicación del objetivo fundamental que persigue todo auditor: evaluar la eficiencia y eficacia.

En este sentido, una auditoría podría definirse como la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que la han sido prescritas.[55]

[55] Piattini Velthuis, Mario Gerardo, y Del Peso Navarro, Emilio. Auditoría informática:

3.5.2. Antecedentes

Existe evidencia de que en tiempos remotos ya se practicaban auditorías. Al animo tributario y recaudatorio justificó la necesidad de revisiones independientes.

La auditoría como profesión fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas de 1862. Hasta el año de 1905, la profesión de la auditoría creció y floreció en Inglaterra, y se introdujo en los EUA hacia 1900. Los objetivos principales eran:

- La detección y prevención de fraude, y
- La detección y prevención de errores.

3.5.3. Tipos de auditoría

Existen diferentes tipos de auditoría, que según el objeto de estudio y la finalidad con que se realiza definen el tipo, siendo éstas las siguientes:

- Auditoría externa.
- Auditoría financiera.
- Auditoría fiscal.
- Auditoría integral.
- Auditoría interna o de campo.
- Auditoría interna y auditoría contable financiera.
- Auditoría informática, y
- Auditoría de protección de datos y seguridad de la información.

3.5.4. Fases de la auditoría

La auditoría consta de las siguientes fases:

- Fase de planeamiento

---

un enfoque práctico. Alfa Omega. Segunda edición, México, 2001, p. 4.

- Fase de ejecución
- Fase del informe de auditoría. [56]

3.5.5. Finalidad de auditoría

El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procedimiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados en los servicios que proporcionan los sistemas computacionales a la empresa.[57]

3.5.6. Antecedentes de la auditoria informática

A finales del siglo XX, los sistemas informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial.[58]

La informática está relacionada estrechamente con la gestión integral de la empresa. Cabe aclarar que la informática no gestiona propiamente la empresa, sino que sólo ayuda a la toma de decisiones. Por ende, debido a su importancia en el funcionamiento de una empresa, existe la auditoria informática.

El auditor informático ha de velar por la utilización de los amplios recursos que la empresa pone en juego para disponer de un eficiente y eficaz sistema de

---

[56] Oviedo Sotelo, Patricia Beatriz. Fases de la auditoría. Disponible en: https://www.monografias.com/trabajos60/auditoria-financiera/auditoria-financiera2.shtml [Fecha de consulta: 01 de mayo de 2018]

[57] Muñoz Razo, Carlos. Auditoría en sistemas computacionales. Pearson Educación, México, 2002, p. 19.

[58] Auditoría Informática. Disponible en: http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml [Fecha de consulta: 02 de mayo de 2018]

información.

Se debe entender a la empresa en su más amplio sentido, ya que una universidad, un ministerio o un hospital son empresas, pero en su forma de operar se distinguen entre sí. Hoy día todas las empresas utilizan la informática para gestionar sus "*negocios*" de forma rápida y eficiente con el fin de obtener beneficios económicos y reducción de costos.

3.5.7. Concepto de auditoría informática

La auditoría informática es un mecanismo diseñado para la salvaguardia de los sistemas tecnológicos y para mantener la integridad de la información de la empresa, u organización.

3.5.8. Objetivos de la auditoría informática

La auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoria.

3.5.8.1. Objetivo general

Su objetivo general consiste en la evaluación de un sistema informático para poder:

- Emitir una opinión sobre la fiabilidad y exactitud de los datos procesados.
- Detectar y corregir errores encontrados y asegurar la continuidad del soporte automatizado de la gestión, y
- Elaborar un informe de recomendaciones y plan de acción.

3.5.8.2. Objetivos específicos

Su objetivo específico consiste en la aplicación que servirá de guía u orientación sistemática y ordenada para que el auditor pueda allegarse de elementos informativos:

- El control de la función informática (sistema de información y las TIC).
- El análisis de la eficiencia de los sistemas de información y las TIC.
- La verificación del cumplimiento de la normativa general de la organización.

- La verificación de los planes, programas y presupuestos de los sistemas informáticos.
- La revisión de la eficaz gestión de los recursos materiales y humanos e informáticos.
- La revisión y verificación de controles técnicos generales y específicos de operatividad.
- La revisión y verificación de las seguridades.
- Cumplimiento de normas y estándares.
- Sistema operativo.
- Seguridad de software.
- Seguridad de comunicaciones.
- Seguridad de base de datos.
- Seguridad de proceso.
- Seguridad de aplicaciones.
- Seguridad física.
- Suministros y reposiciones.
- Contingencias
- El análisis del control de resultados. y
- El análisis de verificación y de exposición de debilidades y disfunciones.

3.5.9. Seguridad de la información

La información es un activo más en una empresa, no obstante, tiene un valor tal que la permanencia de la empresa depende de la integridad en el manejo y conservación de la información, por lo que resulta primordial asegurar su protección. La seguridad de la información ofrece una franja de protección ante una gama de amenazas permitiendo la continuidad del negocio, minimizando daños, asegurando el retorno de inversión, así como el desarrollo de oportunidades.

La seguridad de la información se caracteriza como el aseguramiento de:

a. Confidencialidad: asegurando que el acceso a la información sea solamente a aquellos que están autorizados.
b. Integridad: salvaguardar la exactitud e integridad de la información y los métodos de procesamiento, y
c. Disponibilidad: asegurando que los usuarios autorizados tengan acceso a la información en el momento que es requerido.

La seguridad de la información se logra mediante la implementación de una serie de controles que pueden ser políticas, prácticas, procedimientos, estructuras organizacionales y funciones de software.

3.5.10. Metodologías para la implementación de seguridad de la información (norma ISO 27001)

La norma ISO/IEC 27001 cuyas siglas significan "*Technology Security Techniques*" viene a ser la evolución del estándar de buenas prácticas ISO creado en 1995, para lo cual su creación conlleva un progreso certificable llamado estándar 27001.

Para esta norma "*la información es un activo, y como cualquier otro activo importante de un negocio, tiene un valor para una empresa, y por consiguiente debe ser adecuadamente protegido*".

Esta norma tiene como principal objetivo proporcionar una metodología que permita la implementación de la seguridad de la información en cualquier tipo de organización.

La norma determina cómo gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información. Este sistema está conformado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información.

3.6. Análisis del procedimiento "*Safe Harbor*" como auditoria

La Directiva 95/46/CE de la Comisión Europea entró en vigor en octubre de 1998, y se redactó luego de que la Unión Europea considerara diversos puntos respecto a la protección de los datos personales, tales como:[59]

a) El desarrollo de la sociedad de la información y del comercio electrónico se traduce, a escala mundial, en un crecimiento exponencial de la circulación de los datos y de los riesgos vinculados a los abusos en la utilización de dichos datos;

b) Los abusos relacionados con la circulación de datos personales al afectar la confianza del consumidor además de frenar el desarrollo del comercio electrónico, representan un atentado contra los derechos y las libertades de las personas y, en particular, el derecho a la intimidad;

c) La protección de los datos significa proteger a la persona a la que se refieren las informaciones tratadas y dicha protección es uno de los derechos fundamentales reconocidos por la Unión (artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, mencionado en el artículo 6 del Tratado de la Unión, y artículo 286 del Tratado CE);

d) La Directiva, de conformidad con el Convenio no. 108 (1981) del Consejo de Europa, con las orientaciones de la OCDE (1980) y de las Naciones Unidas (1990), basa dicha protección en determinar los derechos específicos de que goza la persona interesada, así como las correspondientes obligaciones tanto de las personas que tratan los datos como de las que controlan dicho tratamiento;

[59] Directiva 95/46/CE disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML

e) La protección de datos resulta inútil si se limita al territorio de la Unión y no se garantiza, como prevé la Directiva, una protección adecuada también en los países terceros a los que se transfieren los datos;

f) Se requiere un nivel adecuado de protección de los datos personales en todos los países en los que se admite la transferencia de datos, para evitar que distintos niveles de protección produzcan distorsiones en la utilización de los datos y desplazamientos en su tratamiento, en violación de los acuerdos "*GATS*", y

g) La Comisión es responsable de asegurarse, en nombre de los ciudadanos de la Unión y de los Estados miembros, de que en los países terceros existe una protección adecuada.

La intención era prohibir la transferencia de datos personales a países no pertenecientes a la Comunidad Europea que no cumplieran con la normatividad idónea para la protección a la privacidad, de acuerdo a los estándares de la Unión.

En el caso de EUA, aún y cuando este país ya tenía normas regulatorias para la protección de la privacidad de sus ciudadanos, su enfoque es muy diferente al de la Unión Europea, éste es sectorial y se basa en una combinación de legislación, regulación y autorregulación; por su parte, la Unión Europea tiene una legislación integral que requiere, entre otras cosas, la creación de agencias autónomas para la protección de datos, exige el registro de bases de datos en dichos organismos y, normalmente, requiere de su aprobación previa, antes de que se pueda comenzar con el procesamiento de los datos personales de los ciudadanos.

Estas diferencias dificultaron considerablemente la capacidad de las organizaciones norteamericanas para participar en una serie de transacciones transatlánticas. De manera que, para superar estos obstáculos y proporcionar un medio simplificado y rentable para las organizaciones estadounidenses que pudiera satisfacer los requerimientos de la adopción de la Directiva, el Departamento de Comercio de EUA, en consulta con la Comisión Europea, elaboró el marco de "*Safe Harbor"* (Puerto Seguro), el cual fue aprobado por la Unión Europea en el año 2000.

Actualmente, es un importante marco de referencia para las empresas estadounidenses, que les evita enfrentarse con interrupciones e inconvenientes durante sus relaciones comerciales con la Unión Europea, o para aquellas que se encuentren en conflicto frente a las autoridades de los Estados miembros de la Unión Europea.

El marco "*Safe harbor*" representa un sistema de "auto-certificación" entre EUA y la Unión Europea, que ofrece mayor certeza a las organizaciones de la Unión Europea y que se sustenta en la expectativa razonable de que las empresas estadounidenses proporcionarán una protección adecuada a la privacidad de sus ciudadanos.

3.6.1. Principios generales de privacidad en el marco "*Safe Harbor*"

Los principios que evoca el marco "*Safe Harbor*" son los que se enlistan a continuación:[60]

- **Aviso (notificación)**: las organizaciones deben notificar a las personas acerca de los fines para los que recogen y utilizan información sobre ellos. Se debe proporcionar información sobre cómo las personas pueden ponerse en contacto con la organización para realizar cualquier pregunta o queja, la clase de terceros a los que se les proporcionará la información, y las opciones y medios que la organización ofrece para limitar su uso y divulgación.
- **Elección**: las organizaciones deben dar a los individuos la oportunidad de elegir si su información personal será compartida con un tercero, o será utilizada para un fin incompatible con el propósito para el cual fue

[60] Decisión de la Comisión de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de EUA. Comisión de las Comunidades Europeas. Bruselas. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32000D0520 [Fecha de consulta: 13 de abril de 2018]

originalmente recopilada, o subsecuentemente autorizada por el individuo. Para obtener información sensible, se debe manifestar la aceptación de manera expresa, también debe dar a elegir si la información ha de ser divulgada a terceros o utilizados para un fin distinto al previsto.

- **Transferencia progresiva (transferencias a terceros)**: para revelar información a un tercero, las entidades deberán aplicar los principios de notificación y de elección. Cuando una organización desea transferir información a un tercero que actúa como un agente, puede hacerlo si se asegura de que el tercero cumple con los principios de puerto seguro o está sujeto a la Directiva o a alguna otra reglamentación que se adecue. Como alternativa, la organización puede entrar en un acuerdo por escrito con dicha tercera parte que requiere que proporcione al menos el mismo nivel de protección de privacidad que es requerido por los principios pertinentes.
- **Acceso**: las personas deben tener acceso a la información personal que posee una organización y tener la libertad de corregir, modificar o eliminar dicha información si ésta fuera incorrecta, salvo que la carga o gasto sean desproporcionados en relación a los riesgos a la privacidad del individuo, en el caso de que se trate.
- **Seguridad**: las organizaciones deben tomar las precauciones razonables para proteger la información personal de la pérdida, mal uso y acceso no autorizado, revelación, alteración y destrucción.
- **Integridad de los datos**: la información personal debe ser pertinente según los fines para los que se va a utilizar. Una organización debe tomar medidas razonables para asegurar que los datos son confiables, precisos, completos y actuales para el uso previsto.
- **Aplicación:** con el fin de garantizar el cumplimiento de los principios del marco "*Safe harbor*", las organizaciones deberán establecer:

  a) Mecanismos de recursos independientes, fácilmente disponibles y asequibles para que las quejas y disputas de cada individuo puedan ser

investigadas, resueltas e indemnizadas de acuerdo con la ley aplicable, o con las iniciativas del sector privado que se dispongan;

b) Procedimientos para verificar que las empresas cumplen los compromisos a los que se adhieren, y

c) La obligación de solucionar los problemas derivados de un incumplimiento de los principios. Las sanciones deben ser lo suficientemente rigurosa para garantizar el cumplimiento por la organización. Las organizaciones que no presenten cartas anuales de auto certificación ya no aparecerán en la lista de participantes y los beneficios que ofrece el marco "*Safe Harbor*" ya no estarán garantizados.

Tales principios se aplicarán únicamente a los datos personales procedentes de la Unión Europea, con valor de norma voluntaria, sugerida a las empresas que tengan la intención de recibir datos de la Unión Europea, pero serán vinculantes para las empresas que opten por adherirse a dichos principios y podrán aplicarlos los organismos privados de solución de litigios y los organismos públicos competentes para obtener indemnizaciones por prácticas desleales o engañosas.

Cabe aclarar que una protección "*adecuada*" no entraña por sí misma que el país tercero disponga de normas análogas a las de la Unión, sino que, independientemente del tipo de protección jurídica vigente en dicho país, el titular de los datos ha de recibir protección efectiva.

En el país tercero, la protección se ha de considerar efectiva cuando se pueda medir su eficacia con referencia a datos objetivos, como por ejemplo la posibilidad de identificar al titular de las obligaciones, el tipo de datos tratados, el uso que pueda hacerse de los mismos y los mecanismos establecidos para garantizar la protección.

3.6.2. Beneficios del sistema "*Safe Harbor*"

El programa "Safe Harbor" ofrece una serie de beneficios importantes tanto para las empresas de EUA, como para las de la Unión Europea:[61]

1. Se presumirá que las organizaciones (empresas) participantes proporcionan una protección adecuada de la privacidad, es decir, son confiables en el tratamiento de los datos personales;
2. El requisito de los Estados miembro respecto a la aprobación previa para que las organizaciones (empresas) estadounidenses procedan a la transferencia de datos podrá ser prescindida o bien, la aprobación de los Estados miembro se concederá de forma automática;
3. Las reclamaciones presentadas por ciudadanos de la Unión Europea contra las organizaciones de EUA serán ventiladas, con limitadas excepciones, en los EUA;
4. Los requisitos de cumplimiento se simplifican y se vuelven más rentables, benefician especialmente a las pequeñas y medianas empresas.
5. Una organización de la Unión Europea puede garantizar que está enviando información a una organización de EUA, y que participan en el programa "*Safe Harbor*", mediante la visualización de la lista pública de organizaciones de puerto seguro publicada en sitio web de "*Safe Harbor*" del Departamento de Comercio de EUA.[62]

Esta lista contiene los nombres de todas las organizaciones estadounidenses que tienen auto certificación según el acuerdo entre EUA y la Unión Europea:

---

[61] Cfr. U.S.-EU & U.S.-Swiss Safe Harbor Frameworks. Disponible en: https://build.export.gov/main/safeharbor/index.asp [Fecha de consulta: 18 de abril de 2018]

[62] Lista de organizaciones de puerto seguro, disponible en: *http://export.gov/safeharbor/eu/*

"*Marco de Safe Harbor*". Asimismo, se actualiza periódicamente, de modo que es evidente que las organizaciones tienen la garantía de los beneficios de puerto seguro.

3.6.3. Certificación del marco "*Safe Harbor*"

La decisión de las empresas estadounidenses para adherirse al programa "*Safe Harbor*" es totalmente voluntaria. Aquellas que resuelvan participar en el programa, deben cumplir con los requisitos establecidos y declarar públicamente que lo hacen. Para que exista mayor certeza de la vigencia de dicha auto certificación, las empresas deberán hacerlo anualmente ante el Departamento de Comercio de EUA, manifestando por escrito que están de acuerdo en cumplir con los requisitos del marco "*Safe Harbor*" entre EUA y la Unión Europea, lo cual incluye elementos tales como avisos, alternativas, acceso y ejecución ("*enforcement*"). Asimismo, se hará constar en su declaración de política de privacidad publicada, que se adhiere a los principios de "*Safe Harbor*".

Para calificar en el programa "*Safe Harbor*" entre EUA y la Unión Europea, una organización puede: unirse a un programa de privacidad de autorregulación que se adhiera a los requisitos del marco "*Safe Harbor*"; o desarrollar su propia política de privacidad de autorregulación que se ajuste al marco de "*Safe Harbor*".

3.6.4. Retos o áreas de oportunidad

Ahora bien, para aquellas empresas que generan publicidad o promoción (particulares) se establece la obligación de obtener el consentimiento del titular de la información (dato personal).

Es evidente que con el crecimiento y desarrollo de Internet por medio del uso de dispositivos móviles y de las redes sociales cada día las empresas están recabando más información de datos personales, lo cual implica que empresas de todo tipo y tamaño se adhieran a esquemas de autorregulación que cumplen con el marco de "*Safe Harbor*".

Las pequeñas empresas que muchas veces no cuentan con una infraestructura tecnológica robusta deben considerar la implementación de políticas

de privacidad de autorregulación o bien adherirse a programas de privacidad que cumplen con el marco "*Safe Harbor*", si realmente quieren un crecimiento de sus empresas ya que la internacionalización de una empresa dependerá en gran medida de que tan preparados están para proteger los datos de sus clientes a nivel Internacional y no solamente local.

El establecimiento de medidas que fomenten la confianza de los consumidores deriva en gran medida en la implementación de medidas de seguridad preventivas, las cuales en muchas ocasiones no pueden ser entendidas por los tomadores de decisiones de las empresas.

Capítulo 4

Propuesta de modelo de protección de información y datos personales en una empresa.

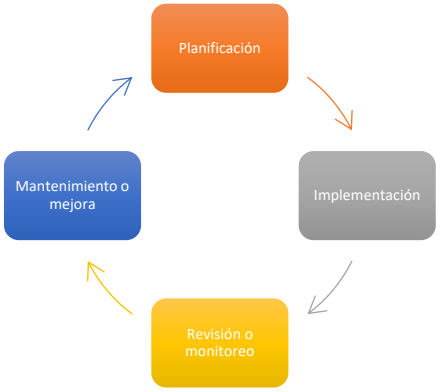
Capítulo 4: Propuesta de modelo de protección de información y datos personales en una empresa

En primer lugar, se precisa que el Modelo de Protección de Información y Datos Personales (Modelo de Protección) que se propone no es un simple ejercicio de auditoría que dictamina el estatus de cumplimiento de una organización (empresa) frente a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, su Reglamento y lineamientos aplicables, ni una evaluación que dicte las medidas urgentes o acciones a tomar a mediano o largo plazo para minimizar riesgos y controlar impactos, si no se trata de un sistema permanente de protección, el cual se hace en ciclos o etapas para garantizar su constante actualización, mejora y eficiencia.

El Modelo de Protección supone una revisión exhaustiva (auditoría) que permita identificar los elementos de protección para la construcción de una plataforma de gestión y sobre todo de control de la información y los datos personales. Esta plataforma es diseñada para ser susceptible de revisiones constantes, de actualizaciones y de modificaciones que garanticen el acompañamiento de la información a proteger junto con el avance tecnológico y las necesidades de la propia empresa conforme a su modelo de negocio.

El Modelo de Protección que se propone consta de cuatro ciclos base. La planificación, implementación, revisión y mejora.

Figura 2. Ciclos del modelo de protección de información y datos personales.



Fuente: Elaboración propia.

Los ciclos del Modelo de Protección presuponen un programa de gestión integral de información y datos personales, no obstante, para efectos del presente trabajo, se propone el análisis de los ciclos planificación e implementación, de los cuales deriva buena parte del éxito y eficiencia del programa de gestión completo.

4.1. Planificación

En esta etapa se establecen los objetivos de la seguridad de la información, se describen los elementos de protección, se elaboran los criterios y políticas de gestión, se determinan las acciones a realizar y se genera un plan de trabajo.

Los objetivos de seguridad deben estar alineados con los presupuestos exigidos por la ley, los lineamientos internos, mejores y buenas prácticas o políticas de seguridad globales.

Los elementos de protección son el conjunto de cosas, derechos y efectos relacionados con una persona o con la empresa, que van a ser resguardados bajo el esquema de protección implementado finalmente por la empresa.

Los criterios y políticas de gestión serán aquellos lineamientos, acuerdos o líneas de acción o pensamiento que los directivos de la empresa van a discutir, aprobar y posteriormente a respetar, para el correcto funcionamiento del modelo de protección.

Las acciones a seguir deben estar diseñadas de acuerdo a la estructura y naturaleza de la empresa, de manera que sea un trabajo realizable y alcanzable.

El plan de trabajo debe ser elaborado tomando en cuenta los recursos de la empresa, la capacidad instalada, presupuestos y los tiempos deseados.

En el ciclo de planificación, se lleva a cabo por primera y única vez, el ejercicio de auditoria o revisión exhaustiva que hace el auditor respecto de los procesos, procedimientos, documentos, contratos e instrumentos por los que la entidad auditada (empresa) recaba información y datos personales, a fin de elaborar políticas de privacidad, de seguridad de la información, así como los avisos de privacidad correspondientes, de acuerdo a los requerimientos de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, su

Reglamento, lineamientos expedidos por el órgano regulador, así como las buenas prácticas internacionales en la materia, o bien, de acuerdo a las políticas globales a las que la empresa pueda estar sujeta.

Posterior a la revisión de la información proporcionada, y a la elaboración de los avisos de privacidad, se lleva a cabo una asesoría para la designación de la persona responsable de la protección de los datos personales en la empresa, así como los lineamientos para la implementación de los avisos de privacidad. Cabe señalar, que la asignación de la persona a cargo, puede ser una persona física, un área o un comité, dependiendo de las necesidades y recursos de la propia empresa.

Consecuentemente, se crea un procedimiento interno para la atención de solicitudes de derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) de titulares de datos personales y se diseña un formato estándar para facilitar el ejercicio de estos derechos.

Finalmente, se elabora una política de privacidad y protección de datos para la empresa, el cual será el documento que va a regir internamente el tratamiento de los datos personales.

4.2. Implementación

En el ciclo de implementación, la empresa en ejercicio de sus recursos y con ayuda del agente de auditoría, implementa aquellas recomendaciones, medidas, ajustes, correcciones, cambios, nuevos procesos, políticas, prácticas, protocolos incluyendo documentos, formatos, instructivos, etcétera, los cuales ayudarán a construir la plataforma de gestión de información.

Cabe mencionar que la implementación incorpora las medidas técnicas de gestión, tales como programas, sistemas, servidores, equipos y demás dispositivos tecnológicos por los cuales se recaban, almacenan, usan y conservan datos personales e información de la empresa.

El proceso de implementación no tiene un tiempo definido, ya que tarda el tiempo que le lleve a la empresa la adopción técnica de nuevos programas, sistemas y dispositivos, así como el tiempo que lleve la comunicación interna de las

medidas o políticas.

Comunicación interna significa el conocimiento, explicación, adopción e incorporación de las nuevas medidas entre el personal involucrado de las distintas áreas de la empresa.

4.3. Revisión

La etapa o fase de revisión consiste en el proceso periódico de monitoreo del funcionamiento del Sistema de Gestión de la Seguridad de la Información, y en la cual se verifica si los resultados cumplen los objetivos establecidos. Está etapa se agenda de manera periódica y de acuerdo a los lineamientos planteados en el ciclo de planificación.

4.4. Mantenimiento y actualización

En esta etapa se aplican aquellos cambios o ajustes que se determinen como necesarios en la etapa de revisión, con el objetivo de disminuir todos los incumplimientos detectados en la fase anterior, y, sobre todo, de mantener actualizado el sistema de gestión que forma parte del modelo de protección de información y datos personales en la empresa.

A continuación, se presentan gráficamente los ciclos de planificación e implementación del modelo de protección de datos e información propuesto para una empresa:

4.5. Proyecto y plan de trabajo

Cuadro 1. Modelo de protección de información y datos personales.

MODELO DE PROTECCION	OBJETIVOS	ACTIVIDADES	RESULTADOS
CICLO 1 **PLANIFICACIÓN**	Análisis y evaluación de cumplimiento de la Ley Federal de Protección de Datos Personales en Posesión de	Revisión de datos personales que se recaban (clientes, proveedores, empleados).	Dictamen de cumplimiento de la empresa a la LFPDPPP. Instrucciones para la implementación de los

	los Particulares (LFPDPPP). Análisis y evaluación de la plataforma técnica para la gestión del Modelo de Protección.	Análisis del diagrama de flujo de vida de los datos personales. Descripción del tratamiento de datos personales (explicar el uso, finalidades y en su caso transferencias para cada supuesto). Análisis de políticas internas o globales para privacidad y protección de datos.	avisos de privacidad y políticas de privacidad. Diagrama de flujo de vida de los datos personales. Sugerencias para adecuar instrumentos. Plan de trabajo.
CICLO 2 **IMPLEMENTACIÓN**	Nombramiento del encargado de datos personales Procedimiento para la atención de Derechos ARCO. Avisos de Privacidad. Implementación de las Políticas de Privacidad Implementación de nuevos instrumentos.	Designación de la persona o área responsable de datos personales. Implementación de avisos de privacidad. Incorporación de políticas de privacidad de la información. Implementación del proceso de ejercicio de derechos ARCO. Se implementan las tareas asignadas a las distintas áreas. Se implementan los nuevos formatos de instrumentos.	Designación del responsable de protección de datos personales Diagrama de atención de solicitudes de derechos ARCO y formato de solicitud. Implementación de avisos de privacidad Implementación de políticas de privacidad y seguridad de la información. Adopción de nuevos instrumentos.
CICLO 3 **REVISIÓN**	Revisión de cumplimiento y eficiencia en el modelo de	Ejecución del programa de revisión y actualización del modelo de protección.	Protocolo de revisión periódica de elementos que integran el modelo de protección.

	protección de datos personales.		Dictamen de cumplimiento. Plan de trabajo de actividades a efectuar. Sugerencias.
CICLO 4 **MANTENIMIENTO O MEJORA**	Mantenimiento y mejora del modelo de protección de datos personales.	En base a los resultados de la Fase 3. Descripción de las actividades conforme al plan de trabajo. Identificación de nuevos elementos de protección.	Protocolo de mantenimiento y mejora al modelo de protección. Ejecución del plan de trabajo. Dictamen de cumplimiento.

Fuente: Elaboración propia.

Sin que se entienda que las primeras etapas del proyecto no son importantes, esta última etapa resulta de crucial importancia para la eficiencia del esquema de protección de datos e información en una empresa, toda vez que, al considerar que el proyecto se concluyó y que las actividades de actualización y mejora son de rutina, es muy común que el personal, áreas o comités encargados del mantenimiento del esquema de protección pierdan fácilmente la esencia del esquema de protección, esto es, la información y datos.

Si el trabajo de actualización y mejora se enfoca en la administración y operación de las bases de datos, en el mantenimiento técnico de la plataforma o en la actualización de los programas de cómputo e incluso hardware; el trabajo de "*mantenimiento*" no se estaría realizando correctamente.

Precisamente, el criterio de preservación de la protección de datos e información no solo se refiere a la guarda y custodia de datos estadísticos e históricos, sino en la identificación permanente de los "*bienes intangibles*" que se

generan dentro de una empresa, y que dichos bienes intangibles no es el valor de una marca ni el posicionamiento de la empresa en el mercado, si no la inmaterialidad contenida en nueva información comercial, que se encuentra dispersa en: estrategias de marketing, planes de negocios, precios y costos de producción, análisis de mercado, referencias de competidores, nuevas listas de clientes y proveedores; reportes de empleados, niveles de crecimiento, evaluaciones de desempeño, planes de trabajo, formación y capacitación, por mencionar algunos.

Conclusiones

Conclusiones

La propuesta del esquema de protección de datos e información en una empresa tiene un componente "*estático*" y uno "*dinámico*".

El estático se refiere a la protección de datos personales y sensibles de los candidatos a puestos de trabajo, empleados, clientes y proveedores, el cual se limita al manejo correcto de los avisos de privacidad, a los consentimientos y ciertas políticas de resguardo de información, y obviamente a un buen manejo del protocolo del ejercicio de derechos ARCO.

El elemento "*dinámico*" se refiere al ánimo permanente de prever, identificar y preservar en completa confidencialidad, aquellos bienes intangibles que representan una ventaja competitiva para la empresa. No se trata de secretos industriales, si no de datos e información que más allá de ser el número de registro de una marca, o las reivindicaciones de una patente, tiene que ver con los instructivos no escritos para llevar a una empresa a un nivel óptimo de rentabilidad y sustentabilidad.

Solo aquellos empresarios que han logrado a base de esfuerzos tener un mejor costo de adquisición, un menor costo de producción, un mejor plan de negocios, una estrategia venida de múltiples experiencias, una depurada lista de clientes, podría entender casi automáticamente, la diferencia entre el resguardo de un derecho de propiedad industrial, un derecho de autor, un dato sensible de un empleado, un secreto industrial y los datos e información inherentes a la operación exitosa de su empresa.

Bibliografía

Acciones de defensa que realiza la CONDUSEF en beneficio de los usuarios de servicios financieros para el periodo 1999-2017. CONDUSEF. Disponible en: https://www.condusef.gob.mx/gbmx/documentos/estadistica/estad2017/historia-1999-2017.pdf

ARAUJO CARRANZA, Ernesto. *El derecho a la información y la protección de datos personales en el contexto general y su construcción teórica y jurídica*. IUS Revista del Instituto de Ciencias Jurídicas de Puebla, A.C., núm. 23, 2009, pp. 174-213 Instituto de Ciencias Jurídicas de Puebla, A. C. Puebla, México. Disponible en: https://www.redalyc.org/pdf/2932/293222963009.pdf

Auditoría Informática. Disponible en:

http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

BAKER, Stephen. Los Numerati. Planeta, México, 2009.

CHERKI, Marc. "Données personnelles: un marché de 100 milliards de dollars en France". Le Figaro, 21 de julio de 2013. Disponible en: http://www.lefigaro.fr/mon-figaro/2013/07/21/10001-20130721ARTFIG00115-donnees-personnellesun-marche-de-100milliards-de-dollars-en-france.php

Comunicado IFAI/077/13. "Posicionamiento del IFAI frente al proyecto de dictamen de los diputados del 19 de agosto de 2013". IFAI, 20 de agosto de 2013. Disponible en: http://inicio.ifai.org.mx/comunicados/comunicado%20ifai-077-13.pdf

Convención Americana sobre Derechos Humanos, OEA, Costa Rica, 22 de noviembre de 1969. Disponible en: https://www.oas.org/dil/esp/tratados_b-32_convencion_americana_sobre_derechos_humanos.htm

Convenio de Berna para la protección de las obras literarias y artísticas. Disponible en: https://www.wipo.int/treaties/es/text.jsp?file_id=283700#P91_12057

Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (Convención o Convenio Europeo de Derechos Humanos). Consejo de Europa, 4 de noviembre de 1950, Roma. Disponible en: https://www.echr.coe.int/Documents/Convention_SPA.pdf

CORONEL CARCELÉN, Felipe Francisco. *La protección del derecho a la vida privada en internet y otros medios de comunicación electrónicos*. Borrador de tesis. Pontificia Universidad Católica de Chile. Disponible en: http://www.alfa-redi.org/sites/default/files/articles/files/coronel.pdf

Decisión de la Comisión de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de EUA. Comisión de las Comunidades Europeas. Bruselas. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32000D0520

Declaración Universal de los Derechos Humanos, ONU, Francia, 10 de diciembre de 1948. Disponible en: http://www.un.org/es/universal-declaration-human-rights/

Decreto por el que se abroga la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental y se expide la Ley Federal de Transparencia y Acceso a la Información Pública. Publicado en el DOF el 9 de mayo de 2016. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFTAIP_270117.pdf

Decreto por el que se adiciona un segundo párrafo con siete fracciones al Artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos. Publicado en el DOF el 20 de julio de 2007. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=4994148&fecha=20/07/2007

Definición de accountability. Business Dictionary. Disponible en: http://www.businessdictionary.com/definition/accountability.html#ixzz3q4OP2Sta

Definición de spam. Proyecto Norteamericano sobre Protección al Consumidor en Comercio Electrónico. Disponible en: http://www.nacpec.org/es/links/spam/index.html

DHONT, Jan; PÉREZ ASINARI, María Verónica, y POULLET, Yves. *Safe Harbour Decision Implementation Study*. Universidad de Namur, Bélgica. 19 de abril de 2004. Disponible en:

http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/07_etude_safe-harbour-2004_/07_etude_safe-harbour-2004_en.pdf

Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Parlamento Europeo y Consejo de la Unión Europea. Luxemburgo. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML

Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones. Parlamento Europeo y Consejo de la Unión Europea. Bruselas. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:ES:HTML

ESCOBAR FORNOS, Iván. *Introducción al derecho procesal constitucional*. Porrúa, México, 2005.

Estándares internacionales sobre protección de datos personales y privacidad. 31 Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, 5 de noviembre de 2009, Madrid. Disponible en:

https://edps.europa.eu/sites/edp/files/publication/09-11-05_madrid_int_standards_es.pdf

GREGORIO, Carlos G. y ORNELAS, Lina (Comp.). *Protección de datos personales en las redes sociales digitales: en particular de niños y adolescentes*. Memorandum de Montevideo, IFAI/ IIJusticia, México, 2011.

Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OCDE, 23 de septiembre de 1980. Disponible en: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

HERRÁN ORTIZ, Ana Isabel. *El derecho a la intimidad en la nueva Ley Orgánica de Protección de Datos Personales*. Dykinson, España, 2002. Disponible en: https://books.google.com.mx/books?id=CCVT48egc5MC&pg=PA65&lpg=PA65&dq=facultad+del+individuo,+derivada+de+la+idea+de+autodeterminaci%C3%B3n+de+decidir+b%C3%A1sicamente+por+s%C3%AD+mismo+cu%C3%A1ndo+y&source=bl&ots=qUSLJdbUFo&sig=zT5ZLp0ZTqELO_R_jjY6W2L4vHA&hl=es&sa=X&ved=2ahUKEwjv3o3T7OvfAhUm0YMKHWyTDukQ6AEwAXoECAgQAQ#v=onepage&q&f=false

HERRÁN ORTIZ, Ana Isabel. *El derecho a la protección de datos personales en la sociedad de la información*. Universidad de Deusto, Cuadernos Deusto de Derechos Humanos, núm. 26, España. Disponible en: http://www.deusto-publicaciones.es/deusto/pdfs/cuadernosdcho/cuadernosdcho26.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. México. Publicada en el DOF el 05 de julio de 2010. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. Publicada en el DOF el 11 de junio de 2002. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/abro/lftaipg/LFTAIPG_abro.pdf

Ley Federal del Derecho de Autor. Publicada en el DOF el 24 de diciembre de 1996. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/122_150618.pdf

Ley Federal de Protección al Consumidor. Publicada en el DOF el 24 de diciembre de 1992. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/pdf/113_250618.pdf

Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. Publicada el 31 de octubre en el Boletín Oficial del Estado Español. Disponible en: https://www.boe.es/boe/dias/1992/10/31/pdfs/A37037-37045.pdf

Lineamientos Generales de Protección de Datos Personales para el Sector Público. Publicados en el DOF el 26 de enero de 2018. Disponibles en: http://www.dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018

Marco de Privacidad de APEC. APEC, diciembre de 2005. Disponible en: https://sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf

Memorándum sobre la protección de datos personales y la vida privada en las redes sociales en Internet, en particular de niños, niñas y adolescentes. Seminario Derechos, Adolescentes y Redes Sociales en Internet, Montevideo, 27 y 28 de julio de 2009. Disponible en: http://www.iijusticia.org/Memo.htm

MUÑOZ RAZO, Carlos. *Auditoría en sistemas computacionales*. Pearson Educación, México, 2002.

Nota de prensa número 3973. “Aprueban diputados, en lo general, reformas del IFAI para dotarlo de más autonomía y discuten en lo particular una veintena de reservas presentadas”. Comunicación social de la Cámara de Diputados, 22 de agosto de 2013. Disponible en: http://www3.diputados.gob.mx/camara/005_comunicacion/b_agencia_de_noticias/009_2013/08_agosto/22_22/3973_aprueban_diputados_en_lo_genera

l_reformas_del_ifai_para_dotarlo_de_mas_autonomia_y_discuten_en_lo_particular_una_veintena_de_reservas_presentadas

NOVO MONREAL, Eduardo. *Derecho a la vida privada y libertad de información*. Siglo XXI Editores, México, cuarta edición, 1989.

ORNELAS NÚÑEZ, Lina y PINAR MAÑAS, José Luis. *La protección de datos personales en México*. Tirant Lo Blanch, México, 2013.

OVIEDO SOTELO, Patricia Beatriz. Fases de la auditoría. Disponible en: https://www.monografias.com/trabajos60/auditoria-financiera/auditoria-financiera2.shtml

Personal Information Protection and Electronic Documents Act. Disponible en: http://laws-lois.justice.gc.ca/eng/acts/P-8.6/

PESCHARD MARISCAL, Jaqueline. *El derecho fundamental de protección de datos personales en México*. Tirant Lo Blanch, México, 2013.

PIATTINI VELTHUIS, Mario Gerardo, y DEL PESO NAVARRO, Emilio. *Auditoría informática: un enfoque práctico*. Alfa Omega. Segunda edición, México, 2001.

Sentencia 292/2000, de 30 de noviembre emitida por el Tribunal Constitucional de España. Disponible en: http://hj.tribunalconstitucional.es/HJ/cs-CZ/Resolucion/Show/SENTENCIA/2000/292

Sesión ordinaria de la Cámara de Senadores celebrada el martes 27 de abril de 2010. Senado de la República. Versión estenográfica. Disponible en: http://www.senado.gob.mx/64/version_estenografica/2010_04_27/935

SMEDINGHOF, Thomas J. *Online law: The legal guide to doing business on the internet*. Addison-Wesley, EUA, 1996.

U.S.-EU & U.S.-Swiss Safe Harbor Frameworks. Disponible en: https://build.export.gov/main/safeharbor/index.asp

WARREN, Samuel y BRANDEIS, Louis. El Derecho a la Intimidad. Civitas, Madrid, 1995.