UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN

ESTRATEGIAS JURÍDICAS Y TECNOLÓGICAS DE PROTECCIÓN DE DATOS PERSONALES

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

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

P R E S E N T A :

ARGUMEDO CALDERÓN JUAN CARLOS

ASESOR: PROF. Antonio Reyes Cortés

Ciudad Nezahualcóyotl, Estado de México, a 21 de agosto 2018

DEDICATORIAS Y AGRADECIMIENTOS.

A MIS PADRES,

Gracias por ser los mejores ejemplos que seguir, no cabe duda de que son unos excelentes abogados, los mejores consejeros y mis mejores amigos.

Gracias por haberme forjado como la persona que soy en la actualidad; muchos de mis logros, son de Ustedes, entre los que se incluye este. Me formaron con reglas y algunas libertades, pero al final de cuentas, me motivaron constantemente para alcanzar mis anhelos.

Los amo muchísimo.

A MIS ABUELOS HERMINIA Y JORGE,

Puedo decir plenamente que Ustedes además de mis abuelos, son mis segundos padres, y los valores y aportes que han realizado en mi vida son simplemente invaluables.

Gracias por estar conmigo, apoyandome en todo momento sin importar las circunstancias, gracias por su amor incondicional.

Ojalá algún día pueda retribuirselos.

A MIS ABUELOS CRISTINA Y VICTOR,

Cada día que he pasado a su lado, no lo cambiaría por nada, muchas gracias por siempre recibirme con un abrazo y una sonrisa.

Gracias por haber criado a mi padre, como lo hicieron, gracias por siempre apoyarme a ser mejor persona. No cabe duda, que ustedes han sido pieza fundamental de este logro, que hoy tengo la fortuna de poder compartirlo con Ustedes.

A MI TÍA VERÓNICA,

Eres mi mejor amiga, mi apoyo incondicional, este logro es tuyo.

Hemos compartido infinidad de momentos que han alimentado mi alma, tanto buenos como malos, y hoy doy gracias de tener a alguien como tú en mi vida.

No tengo palabras para decirte lo mucho que te amo y para agradecerte todo lo que has hecho por mi.

Te amo Vero.

A MI HERMANA ALEJANDRA,

La vida no me pudo dar una mejor compañera de vida que tu, eres una luz en mi vida y es un orgullo tenerte como mi hermana.

Estar bendecido con tener una hermana, no se puede describir, eres mi gemela, eres mi compañera y mi consejera.

Caminemos juntos, que jamás te dejaré sola hermanita.

Te amo.

A JUAN MANUEL LUNA CENOBIO,

Hoy en día, tengo una pasión que vivo día a día y es gracias a ti. Este trabajo, este tema, no lo hubiera conocido ni logrado sino fuese por ti.

Existen logros y personas momentáneas, sin embargo, lo que hemos construido a lo largo de estos años entre familias, no está cerca de ser algo pasajero. Hoy reafirmo mi lealtad hacia ti y tu familia, sin embargo, no tengo palabras para poder describir lo agradecido que estoy contigo, no tengo más que decirte, gracias amigo, gracias por tus consejos y por creer en mi.

A MI EMPRESA OPTIMITI NETWORK,

Mi total agradecimiento a Optimiti Network, que me brindó la oportunidad de crecer y experimentar en ésta facinante área del Derecho.

Por haberme animado a emprender la elaboración de esta tesis. A veces, en los proyectos interfieren factores que los dilatan en el tiempo y sin su apoyo incondicional, su estoica paciencia y sus consejos este trabajo no habría podido hacerse realidad.

No tengo duda de que estoy con las personas adecuadas, en el momento adecuado.

A MI UNVIERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN,

Agradezco a la Universidad por haberme aceptado ser parte de ella y abierto las puertas de su seno científico para poder estudiar mi carrera, así como también a los diferentes docentes que brindaron sus conocimientos y su apoyo para seguir adelante día a día.

A mi hermosa Universidad Nacional Autónoma de Mexico que la llevo en mi corazón siempre, que me dio todo y abrió sus puertas del conocimiento. Es un honor ser parte de su historia, cultura y tradición.

"Homo locum ornat, non hominem locus"

“Sin continuo crecimiento y perseverancia, palabras como mejora, logro y éxito no tienen significado.” Benjamin Franklin.

ESTRATEGÍA JURÍDICA-TECNOLÓGICA DE PROTECCIÓN DE DATOS PERSONALES

ÍNDICE

INTRODUCCIÓN

En los primeros años del régimen nazi, el gobierno nacionalsocialista estableció campos de concentración para detener a oponentes políticos e ideológicos tanto reales como supuestos. En los años previos al estallido de la guerra, los oficiales de la SS y la policía encarcelaban en estos campos a cada vez más judíos, romaníes y otras víctimas del odio étnico y racial, para concentrar y controlar a la población judía; lográndose así, lo hoy conocido cómo "El Holocausto"[1].

El Holocausto fue la persecución y el asesinato sistemático, burocráticamente organizado y auspiciado por el Estado, de seis millones de judíos por parte del régimen nazi y sus colaboradores. "Holocausto" es una palabra de origen griego que significa "sacrificio por fuego".

Cabe mencionar, en el año de 1933, la población judía de Europa ascendía a más de nueve millones, y la mayoría de los judíos europeos vivía en países que la Alemania nazi ocuparía o dominaría durante la Segunda Guerra Mundial. Para el año 1945, los alemanes y sus colaboradores habían asesinado aproximadamente a dos de cada tres judíos europeos como parte de la "*Solución final*"[2], la política nazi para asesinar a los judíos de Europa. Bajo la premisa de que los alemanes se consideraban "raza superior" y los judíos "inferiores"; estos últimos eran una amenaza extranjera para la llamada comunidad racial alemana.

Ahora, es menester entrar en estudio de lo considerado como "El Holocausto"; para lograr un exterminio de tal magnitud, se tuvo realizó un tratamiento de datos personales por parte de la Alemania Nazi, es decir, se

[1] Museo Memoria y Tolerancia (2019) El Holocausto. Recuperado de: https://www.myt.org.mx/memoria/holocausto
[2] *Ibídem*

obtuvieron datos personales de millones de judíos, tales como creencia religiosa, origen racial, datos de salud, identificación, entre otros.

La era de estudio es llamada "sociedad de la información"; si bien es cierto que se es más fácil tener un acceso a cualquier tipo de información a través de las diferentes tecnologías de la información, no menos cierto es que la cultura de los ciudadanos es mayor.

Aunado a lo anterior, tenemos que tener en claro que ahora se vive una transformación digital, en donde todo es automatizado por tecnologías avanzadas de procesamiento de información y datos personales, tal es el caso de "*Big Data*", dando origen a un inminente tratamiento de datos personales más rápido y con un mayor alcance que en 1933. Debido a lo anterior, es necesario tener una sólida estrategia de protección de datos personales, con un enfoque holístico, teniendo en cuenta varios aspectos, tales como jurídicos, tecnológicos y culturales.

Tecnología y Derecho, en un principio puede pensarse que son dos cosas muy distantes una de la otra, sin embargo, conforme avanza el tiempo ambos fenómenos sociales y en consecuencia productos culturales, se hallan más cercanos y vinculados, ello como consecuencia de la aceleración tecnológica y científica que trae aparejado un aumento exponencial del tráfico de información, permitiendo que las relaciones humanas en nuestra vida cotidiana se lleguen a presentar en formas que jamás imaginamos.

En ese orden de ideas, los abogados empresariales, consultores, asesores, en materia de protección de datos personales no podemos abstraernos a los cambios que la realidad nos plantea. En este contexto, en mi vida laboral, me he enfrentado a algunos retos en la realidad que nos ocupa, y que hubiera sido de gran provecho que en mi formación profesional se abordaran problemáticas informáticas desde la perspectiva

jurídica, y no sólo como comentarios de cumplimiento únicamente con el Aviso de Privacidad, porque en los retos en los que me he vuelto inmerso, la cultura empresarial cuenta con una falsa creencia de cumplimiento en ésta materia, lo cual se traduce en riesgos jurídicos, por ende económicos, operacionales y tecnológicos, dejando en un estado de inseguridad tanto al sector empresarial cómo a los Titulares de datos personales.

Considero que el mal manejo de datos personales resulta ya en un menester jurídico – tecnológico. Por lo anterior, durante el desarrollo acoté el tema y encontré el nombre adecuado, relacionado con los puntos desde el punto de vista del sustentante, los más sobresalientes que hoy en día debemos de tomar en cuenta, debido a las altas ciberamenazas existentes en el mundo. Las organizaciones, deben de partir de un estado de conciencia, en dónde no existe un ecosistema digital 100% seguro, (y mucho menos físico), es decir, todo software, hardware y aún más los humanos, contamos con vulnerabilidades que permiten comprometen el estado idóneo de sus funciones, debido a esto es imperante que cuenten con los mecanismos necesarios y suficientes para minimizar en la mayor medida de los posible la brecha de seguridad existente.

Inicialmente pensé que en mi investigación era posible abarcar todos los tópicos que encierra la protección de datos personales en el ámbito digital, pero al comenzar el estudio, poco a poco me di cuenta de que sería necesario señalar el objeto a un problema específico, la falta de estrategias jurídicas y tecnológicas para una adecuada protección de datos personales.

En un desarrollo en un entorno empresarial, el abogado requerirá del manejo de técnicas jurídicas y tecnológicas que favorecerán su desempeño. Por ello considero que la base para realizar cambios sociales únicamente se puede lograr a través de la educación y la formación de

nuevos abogados con un perfil adecuado a los cambios tecnológicos, con una visión holística y con herramientas para resolver problemas más amplios y más rápido.

Consecuencia de lo anterior y en razón de una exigencia metodológica, este trabajo de investigación es eminentemente cualitativo por las siguientes razones:

En el primer capítulo se aplicará el método histórico exegético, a partir del cual podré presentar el inicio de la regulación internacional de la protección de datos personales.

En el segundo capítulo se utilizará el método descriptivo, para mostrar cuales han sido las normas jurídicas mexicanas en la protección de los datos personales.

En el tercer capítulo también se describirán la trascendencia de la responsabilidad y el Deber de seguridad que cualquiera persona debe tener en el uso de sus datos personales.

Finalmente, en el apartado denominado Propuesta de Reforma al Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares en cuanto a las medidas de seguridad técnicas. Propuesta, se utilizará el método sintético propositivo, pues en el mismo en forma sintética y basado en toda la investigación se presenta la propuesta de solución desde el punto de vista personal, acerca de la problemática investigada de la protección de los Datos Personales, basado en los puntos más importantes a consideración del sustentante, *obtención, uso y acceso* desde una perspectiva jurídica y tecnológica.

CAPÍTULO 1.

ANTECEDENTES DE LA PROTECCIÓN DE DATOS PERSONALES EN EL MUNDO.

Antes de entrar en materia, se debe analizar a profundidad los antecedentes que existen en el Mundo respecto a la protección de datos personales. En virtud de que 107 países (de los cuales 66 son países en vías de desarrollo) han emitido legislación para asegurar la protección de los datos personales y la privacidad. Asia y África muestran un nivel similar de adopción, con menos del 40% de los países con algún tipo de ley en vigor[3].

Teniendo la siguiente comparación:

- 58% de países cuenta con legislación en el mundo.
- 21% de países no cuentan con legislación.
- 10% de países cuentan con un borrador.
- 12% sin información.

Ahora, existen organizaciones de carácter mundial que han emitido ciertas normativas; sus esfuerzos se han considerado excelentes por algunos países, a tal grado que han sido las bases para emitir algún tipo de regulación al respecto, tales son los casos como:

- Organización de las Naciones Unidas,
- Organización para la Cooperación y el Desarrollo Económico,
- Consejo de Europa, específicamente Convenio 108, y
- Foro de Cooperación Económico Asia – Pacífico (APEC, por sus siglas en inglés).

[3] Sanz Salguero, Francisco Javier. (2016). Relación entre la protección de los datos personales y el derecho de acceso a la información pública dentro del marco del derecho comparado. Ius et Praxis, 22(1), 323-376.

1.1. Organización de las Naciones Unidas.

Al dar termino la segunda guerra mundial, la comunidad internacional decidió bosquejar una carta de derechos que afirmara los valores defendidos en la lucha contra el fascismo y el nazismo. El armado de dicha carta fue confiado a un comité presidido por Eleanor Rossvelt y compuesto por miembros de 18 países, la carta fue redactada por el canadiense John Peters Humphrey y revisada luego por el francés René Cassin. El texto final es pragmático, resultado de numerosos consensos políticos, de manera tal que pudiera ganar una amplia aprobación.

La *Declaración Universal de Derechos Humanos*, fue adoptada por la tercera Asamblea General de las Naciones Unidas, el 10 de diciembre de 1948 en París, Francia. Teniendo como uno de los principales objetivos, "*ser el estándar común a ser alcanzado por todos los pueblos y naciones*"

Teniendo como una de sus máximas, la libertad, la justicia y la paz en el mundo, reconociendo la dignidad intrínseca de los derechos iguales e inalienables de todos los miembros de la familiar humana. Tal y como se menciona en el preámbulo de la misma.

> *"… DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS*
>
> *Preámbulo*
>
> *Considerando que el desconocimiento y el menosprecio de los derechos humanos han originado actos de barbarie ultrajantes para la conciencia de la humanidad, y que se ha proclamado, como la aspiración más elevada del hombre, el advenimiento de un mundo en que los seres humanos, liberados del temor y de la miseria, disfruten de la libertad de palabra y de la libertad de creencias;*

Considerando esencial que los derechos humanos sean protegidos por un régimen de Derecho, a fin de que el hombre no se vea compelido al supremo recurso de la rebelión contra la tiranía y la opresión…"[4]

La Declaración Universal de Derechos Humanos, en su artículo 12 dice:

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[5].

Haciendo un estudio de dicho artículo, se puede tomar como uno de los derechos humanos la protección a la vida privada, es decir, a sus datos personales, tales como la familia, domicilio o correspondencia, que de manera análoga es un inicio que nos da origen a tener como base para no atentar contra este principio.

Y a efecto de reforzar lo anterior, la Asamblea General de las Naciones Unidas, en su resolución 2200 A (XXI) de fecha 16 de diciembre de 1966, emite el *Pacto Internacional de Derechos Civiles y Políticos*, en el que considera que, conforme a los principios enunciados en la Carta de las Naciones Unidas, la libertad, la justicia y la paz en el mundo tienen por base el reconocimiento de la dignidad inherente a todos los miembros de la familia humana y de sus derechos iguales e inalienables.

Es decir, no puede realizarse el ideal del ser humano libre en el disfrute de las libertades civiles y políticas, y liberado el temor y de la miseria, a menos que se creen condiciones que permitan a cada persona gozar de

[4] ONU (2015) DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS. Recuperado de: https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf
[5] *Ibídem*

sus derechos civiles y políticos, tanto como de sus derechos económicos, sociales y culturales.

Profundizando en el artículo 17, bajo sus 2 máximas:

"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."[6]

Amén de lo anterior, quedan plasmado como un antecedente subjetivo el aspecto de la vida privada, libertad civil, política, económica, social y cultural como un derecho humano para todas las naciones unidas. Sin embargo, surge la necesidad de que la Asamblea General de las Naciones Unidas se pronuncie respecto a la privacidad en la era digital, teniendo como resultado la *Resolución 68/167 de la Asamblea General de las Naciones Unidas*, emitida en fecha 18 de diciembre de 2013, "***El derecho a la privacidad en la era digital***"[7].

Particularmente, reafirma el derecho a la privacidad, según el cual nadie debe ser objeto de injerencias arbitrarias o ilegales en su vida, su familia, su domicilio, o su correspondencia, y el derecho a la protección de la ley contra tales injerencias, establecidos en el artículo 12 de la Declaración Universal de los Derechos Humanos y el artículo 17 del Pacto Internacional de los Derechos Civiles y Políticos. Asimismo, afirma que los derechos de las personas también deben estar protegidos en internet, incluido el derecho a la privacidad.

---

[6] *Ibídem*

[7] Carbonell, M. (2015) El Derecho a la Privacidad en la era digital. Recuperado de: http://www.miguelcarbonell.com/docencia/El_Derecho_a_la_Privacidad_en_la_era_digital.shtml

Y termina exhortando a todos los Estados miembros a[8]:

- Respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales;
- Examinen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales.

En el anterior orden de ideas, puede deducirse que, en esta última asamblea de 2013, México al ser un miembro de la Organización de las Naciones Unidas, tiene un imperativo necesario respecto a la protección de datos personales, obligando a tomar conciencia y medidas de seguridad respecto al tratamiento de datos personales bajo 2 premisas, la primera de ellas en un ámbito digital, y la segunda a través de una protección integral, es decir, con controles tecnológicos, jurídicos y culturales.

1.2. Organización para la Cooperación y el Desarrollo Económico (OCDE): Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales.

Las organizaciones mundiales de diferentes ámbitos se han preocupado en demasía por este tema, en la evolución tecnológica, cultural y de negocios se ha visto involucrada de alguna manera un tratamiento de datos personales ya sea de manera adecuada o inadecuada, por esto México, debe estar presente en estas iniciativas, recomendaciones y no solamente como observador, sino debería de estar en un rol sumamente participativo.

Ahora, las directrices sobre protección de la privacidad y flujos transfronterizos de datos personales fueron adoptadas como una

[8] ONU (1976) Pacto Internacional de Derechos Civiles y Políticos. Recuperado de: https://www.ohchr.org/SP/Professionalinterest/Pages/CCPR.aspx

recomendación del Consejo de la OCDE apoyando los tres principios que aglutinan a los países de la OCDE: *democracia pluralista, respeto de los derechos humanos y economías de mercado abiertas.*

Los principios abarcan todos los medios del procesamiento informático de datos sobre individuos (desde computadoras locales a redes con complejas ramificaciones nacionales e internacionales), todos los tipos de procesamiento de datos personales (desde la administración de personal hasta la compilación de perfiles de consumidores) y todas las categorías de datos (desde datos de tráfico hasta datos de contenidos, desde el más trivial al más delicado).

Los principios básicos de aplicación nacional son los siguientes[9]:

- **Principio de limitación recogida.**

Debería haber límites a la recopilación de datos personales y cualquiera de esos datos debería ser obtenido por medios legales y honestos y, en su caso, con el conocimiento o consentimiento del sujeto de los datos.

- **Principio de calidad de los datos.**

Los datos personales deberían corresponder a los fines para los que se van a usar y, en la medida en que sean necesarios para esos fines, deberían ser correctos y completos, y estar actualizados.

- **Principio de especificación de los fines.**

Los fines para los que los datos personales se recogen deberían especificarse en el momento en que se recogen, y su uso posterior estaría limitado al cumplimiento de esos fines o de otros que no sean incompatibles con esos fines y se especifiquen cada vez que haya un cambio de fines.

[9] OCDE (2016) Principios de Gobierno Corporativo de la OCDE. Recuperado de: https://www.oecd.org/daf/ca/corporategovernanceprinciples/37191543.pdf

- **Principio de limitación de uso.**

Los datos personales no se deberían revelar, poner a disposición del público ni usar para fines que no sean los especificados de conformidad con el apartado 9 anterior, excepto:

a) con el consentimiento del sujeto de los datos; o

b) por imperativo legal.

- **Principio de salvaguarda de la seguridad.**

Los datos personales deberían estar protegidos por las oportunas medidas de salvaguarda contra riesgos como pérdida o acceso no autorizado, destrucción, uso, modificación o revelación de datos.

- **Principio de transparencia.**

Debería haber una política general de transparencia en lo concerniente al tratamiento, el uso y las políticas relativos a los datos personales. Se deberían poner los medios para establecer la existencia y la naturaleza de los datos personales, así como los fines principales para los que se van a usar, así como la identidad y el domicilio habitual del inspector de datos.

- **Principio de participación individual**

Toda persona física debería tener derecho a:

a) conseguir, a través de un inspector de datos o de otra manera, la confirmación de si el inspector tiene o no tiene datos relativos a su persona;

b) que se le comunique cualquier dato relativo a ella:

- en un plazo de tiempo razonable;
- con una tarifa, en su caso, que no sea excesiva; m de manera razonable; y
- de forma que pueda entender fácilmente;

c) que se le den las razones de por qué se rechaza una petición hecha de conformidad con lo establecido en los apartados (a) y (b), y poder recurrir ese rechazo;

d) recusar los datos relativos a ella y, si la recusación tiene éxito, hacer que se eliminen, rectifiquen, completen o modifiquen los datos.

- **Principio de responsabilidad.**

A todo inspector de datos se le deberían pedir responsabilidades por el cumplimiento de las medidas que permiten la aplicación de los principios antes expuestos.

1.3. Consejo de Europa – Convenio 108.

El convenio número 108 del Consejo de Europa, de fecha 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, considera menester llevar a cabo una unión más íntima entre sus miembros, basada en el respeto particularmente de la preeminencia del derecho así como de los derechos humanos y de las libertades fundamentales; Considerando lo deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada, teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados[10].

Asimismo, el 12 de junio de 2018, se publicó en el Diario Oficial de la Federación el decreto por el cual se aprueban dos importantes documentos:

[10] Perdiguero Jiménez, M. Á. (2018). Nueva Normativa Europea sobre Protección de Datos. Delegado de Protección de Datos. Málaga: IC Editorial.

- El convenio para para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y,
- Su protocolo adicional del 08 de noviembre de 2001, relativo a las autoridades de control y a los flujos transfronterizos de datos.

Éste es uno de los documentos más importantes en el ámbito internacional, porque busca crear un marco global legal en materia de protección de datos personales, así como es el primer documento abierto a países no miembros de la Unión Europea y es también considerado el primer instrumento internacional jurídicamente vinculante en el área de protección de datos personales, de esa forma se obliga a las partes firmantes a tomar las medidas necesarias para adecuar la legislación a los principios que se establecen en el Capítulo II "*Principios básicos para la protección de datos*", mismos que a continuación se mencionan[11]:

> "*Compromiso de las partes.*
> *Cada Parte tomará, en su derecho interno, las medidas necesarias para que sean efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.*
> *Dichas medidas deberán adoptarse a más tardar en el momento de la entrada en vigor del presente Convenio con respecto a dicha Parte.*
> *Calidad de los datos.*
> *Los datos de carácter personal que sean objeto de un tratamiento automatizado:*
> *a) Se obtendrán y tratarán leal y legítimamente;*
> *b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades;*

[11] DOF (2018) Promulgatorio del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo, Francia.

c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado;

d) serán exactos y si fuera necesario puestos al día;

e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

Categorías particulares de datos.

Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales.

Seguridad de los datos.

Se tomarán medidas de seguridad apropiadas para la protección de datos de carácter personal registrados en ficheros automatizados contra la destrucción accidental o no autorizada, o la pérdida accidental, así como contra el acceso, la modificación o la difusión no autorizados.

Garantías complementarias para la persona concernida.

Cualquier persona deberá poder:

a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero;

b) obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernan a dicha persona, así como la comunicación de dichos datos en forma inteligible;

c) obtener, llegado el caso, la rectificación de dichos datos o el borrado de los mismos, cuando se hayan tratado con infracción de las disposiciones del derecho interno que hagan efectivos los principios básicos enunciados en los artículos 5 y 6 del presente Convenio;

d) disponer de un recurso si no se ha atendido a una petición de confirmación o, si así fuere el caso, de comunicación, de ratificación o de borrado, a que se refieren los párrafos b) y c) del presente artículo.

Excepción y restricciones.

1. No se admitirá excepción alguna en las disposiciones de los artículos 5, 6 y 8 del presente Convenio, salvo que sea dentro de los límites que se definen en el presente artículo.

2. Será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente Convenio cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática:

> *a) Para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales;*
>
> *b) para la protección de la persona concernida y de los derechos y libertades de otras personas.*

3. Podrán preverse por la ley restricciones en el ejercicio de los derechos a que se refieren los párrafos b), c) y d) del artículo 8 para los ficheros automatizados de datos de carácter personal que se utilicen con fines estadísticos o de investigación científica, cuando no existan manifiestamente riesgos de atentado a la vida privada de las personas concernidas.

Sanciones y recursos.

Cada Parte se compromete a establecer sanciones y recursos convenientes contra las infracciones de las disposiciones de derecho interno que hagan efectivos los principios básicos para la protección de datos enunciados en el presente capítulo.

Protección más amplia.
Ninguna de las disposiciones del presente capítulo se interpretará en el sentido de que limite la facultad, o afecte de alguna otra forma a la facultad de cada Parte, de conceder a las personas concernidas una protección más amplia que la prevista en el presente Convenio".

1.4. Foro de Cooperación Económica Asia – Pacífico – Marco de Privacidad y las reglas transfronterizas de privacidad.

Las Economías Miembros del Foro de Cooperación Económica Asia Pacífico (APEC por sus siglas en inglés), reconocen la importancia de proteger la privacidad de la información y mantener los flujos de información entre Economías de la región Asia Pacífico y entre sus socios comerciales. Como lo reconocieron los Ministros de APEC al aprobar el Programa para la Acción en el Comercio Electrónico en 1998, el potencial del comercio electrónico no puede llevarse a cabo sin la cooperación del gobierno y de las empresas privadas "…para desarrollar e implementar tecnologías y políticas que establezcan confianza en cuanto a comunicación, información y sistemas de entrega seguros, protegidos y fidedignos, y que traten asuntos que incluyan la privacidad..."[12]. La falta de confianza del consumidor hacia la privacidad y seguridad de transacciones en línea y redes de información es un elemento que puede impedir a las

[12] APEC (2005) MARCO DE PRIVACIDAD DEL FORO DE COOPERACIÓN ECONÓMICA ASIA PACÍFICO (APEC). Recuperado de: https://sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf

Economías Miembro, obtener todos los beneficios del comercio electrónico. Las Economías de APEC se dan cuenta que una parte de los esfuerzos clave para mejorar la confianza del consumidor y asegurar el crecimiento del comercio electrónico, debe ser la cooperación para balancear y promover la protección de la privacidad de la información y el libre flujo de información en la región Asia Pacífico.

Ahora, en concordancia con los demás instrumentos internacionales y de los que México es parte, así como se ha mencionado en líneas anteriores, la economía mundial y los flujos transfronterizos son temas que ocupan abordar la protección de datos personales o bien, la privacidad, como lo marca el Foro de Cooperación Económica Asia Pacífico.

En un mundo que cada vez más utilizamos tecnologías de información y comunicación, incluyendo tecnologías móviles que se conectan a Internet, internet de las cosas y a otras redes de información, han hecho posible recopilar, almacenar y acceder a la información desde cualquier parte del mundo; sin embargo, estás tecnologías de información y comunicación, deben asegurar la confidencialidad, integridad y disponibilidad de la información de la que se está haciendo un uso, a través de diversas técnicas informáticas como jurídicas para minimizar la brecha existente y estar así en posibilidades de realizar transacciones transfronterizas y aprovechar su gran potencial para beneficios económicos y sociales para las empresas, los individuos y los gobiernos, incluyendo aumento en las opciones del consumidor, expansión del mercado, productividad, educación e innovación de productos y servicios.

En virtud de lo anterior, nace la necesidad de crear un marco de referencia para el sector Asia–Pacífico, a raíz de esto en el Marco de Privacidad de dicho Foro, hace mención de unos principios para alentar el

desarrollo de protecciones apropiadas a la privacidad de la información y para asegurar el libre flujo de información en la región, tales como[13]:

- Previniendo Daño

  Reconocer los intereses del individuo para legitimar expectativas de privacidad, la protección de la información personal debe ser diseñada para prevenir el mal uso de la tal información. Además, reconocer el riesgo de que puede haber daños por el mal uso de la información personal, obligaciones específicas deben tomar en cuenta tal riesgo y medidas de saneamiento deben ser proporcionales a la probabilidad y severidad del daño amenazado por la recolección, uso y transferencia de información personal.

- Aviso

  Controladores de Información Personal deben proporcionar declaraciones claras y de fácil acceso acerca de sus prácticas y políticas por lo respectivo a la información personal, que deben incluir:

  a) el hecho de que información personal está siendo recopilada;

  b) los propósitos para los que se está recopilando la información personal;

  c) los tipos de personas u organizaciones a las que se les podría revelar la información personal;

  d) la identidad y ubicación del controlador/ director de información personal, incluyendo información de cómo contactarlos respecto a sus prácticas y manejo de la información personal;

  e) la elección de medios que el controlador/ director de la información personal ofrece a los individuos para limitar el uso, revelación, acceso y corrección de su información.

- Limitación de Recolección

  La recolección de la información personal deberá ser limitada a aquella información que sea relevante a los propósitos de recolección y dicha información deberá ser obtenida por medios legales y justos,

[13] *Ibídem*

y cuando sea apropiado, con consentimiento y dando aviso al individuo en cuestión.

- Usos de la Información Personal

  La información personal recopilada sólo debe ser usada para cumplir con los propósitos de recolección y otros propósitos compatibles o relacionados, excepto:

  a) con el consentimiento del individuo cuya información personal es recopilada;
  b) cuando sea necesaria para proporcionar un servicio solicitado por el individuo; o,
  c) por la autoridad de la ley y otros instrumentos legales, proclamas y pronunciamientos de efecto legal.

- Elección

  Cuando sea apropiado, se le deben proporcionar a los individuos mecanismos claros, prominentes, de fácil entendimiento, accesibles y asequibles para ejercitar la elección en relación a la recolección, uso y revelación de su información personal. Puede que no sea apropiado que los controladores de la información personal proporcionen estos mecanismos cuando recopilen información disponible para el público

- Integridad de la Información Personal

  La información personal debe ser exacta, completa y debe estar actualizada al grado necesario para los propósitos para los que será usada

- Medidas de Seguridad

  Los controladores de información personal deben proteger la información personal que guarden con medidas de seguridad apropiadas contra riesgos, tales como pérdida o acceso desautorizado a la información personal, o destrucción desautorizada, uso, modificación o revelación de información o cualquier otro uso incorrecto. Tales medidas de seguridad deben ser proporcionales a la probabilidad y severidad del daño obtenido, a la

sensibilidad de la información y al contexto en el que es guardada y que darán sujetas a una revisión periódica y a una nueva evaluación.

- Acceso y Corrección

  Los individuos deben ser capaces de:

  a) obtener confirmación del controlador de información acerca de si éste posee información personal acerca de ellos
  b) haberles comunicado, tras haber proporcionado pruebas suficientes de su identidad, información personal acerca de ellos;
  i. dentro de un tiempo razonable;
  ii. a un costo, si es que hay alguno, que no sea excesivo:
  iii. de manera razonable;
  iv. de forma entendible: y,

  c) desafiar la exactitud de la información relacionada con ellos y, si es posible y como sea adecuado, rectificar, completar, corregir o borrar la información.

  Tal acceso y oportunidad para corrección deberá ser proporcionado, excepto cuando:
  (i) la carga o el gasto de hacerlo no fuera razonable ni proporcional a los riesgos sobre la privacidad del individuo en el caso en cuestión;
  (ii) la información no deberá ser revelada por razones legales o de seguridad, ni para proteger información comercial confidencial; o
  (iii) la privacidad de la información de personas, y no del individuo, fuera violada.

  Si una solicitud bajo (a) o (b), o un desafío bajo (c) es negada, se deberán proporcionar al individuo las razones del por qué, y éste será capaz de desafiar tal negación.

- Responsabilidad

  Un controlador de información personal deberá ser responsable de cumplir con medidas que causen efecto al Principio estipulado arriba.

Cuando la información personal vaya a ser transferida a otra persona u organización, nacional o internacional, el controlador de la información personal deberá obtener consentimiento del individuo o actuar con la debida diligencia y tomar las medidas razonables para asegurar que la persona u organización receptora, protegerá la información consistentemente con estos Principios.

La intención de este Marco es proporcionar una clara orientación y dirección a empresas dentro de las Economías de APEC, sobre asuntos comunes de privacidad y del impacto de estos asuntos en la forma en cómo se conducen negocios legítimos, y lo hace destacando las expectativas razonables del consumidor moderno de que las empresas reconocerán sus intereses de privacidad de forma consistente con los Principios explicados líneas anteriores.

CAPÍTULO 2

MARCO JURÍDICO PROTECCIÓN DE DATOS PERSONALES EN MÉXICO.

Para entrar en materia de la protección jurídica de datos personales en México, es menester hablar de la importancia que tiene la Declaración Universal de los Derechos Humanos, recuérdese que en 1948 se reconoció el derecho a la vida de las personas; con esto, el derecho a la Protección de Datos Personales es reconocido a nivel internacional; este derecho es subjetivo, autónomo y de tercera generación, el cual garantiza la libertad del individuo en el seno de una sociedad democrática.

Posteriormente, se promulga la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental el 11 de junio de 2002, en la cual prácticamente se puede partir como el primer adelanto histórico en México, respecto a esta materia, porque contiene en su Capítulo IV habla respecto a la Protección de Datos Personales, sin embargo, únicamente regula el sector público federal, y es la primera aparición de definición de Sujetos Obligados (el Poder Ejecutivo Federal, la Administración Pública Federal y la Procuraduría General de la República; el Poder Legislativo Federal, integrado por la Cámara de Diputados, la Cámara de Senadores, la Comisión Permanente y cualquiera de sus órganos; el Poder Judicial de la Federación y el Consejo de la Judicatura Federal; los órganos constitucionales autónomos; los tribunales administrativos federales, y cualquier otro órgano federal). Por lo cual se entiende que su ámbito de aplicación quedó supeditado a estas autoridades, dejando de lado todos los particulares.

Aunado a lo anterior, dicha Ley Federal establece como obligación para los sujetos obligados, adoptar procedimientos adecuados para recibir

y responder las solicitudes de acceso y corrección de datos; adoptar las medidas necesarias que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado. Mismos que en evidencia clara, el día de hoy quedan superados por cualquier ámbito, tecnológico, jurídico, económico y social.

Asimismo, cabe mencionar la creación del órgano garante en esta materia en México, que fue el Instituto Federal de Acceso a la Información Pública (IFAI), en 2002. Asimismo, en 2007 se reformó el artículo 6° de la Constitución Política de los Estados Unidos Mexicanos, con el que se estableció el derecho a la información pública como un derecho fundamental para los mexicanos[14].

2.1. Reforma a la Constitución Política de los Estados Unidos Mexicanos

En junio de 2009, se adicionó al artículo 16 Constitucional con la consagración de la protección de datos personales, donde establece que "… Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros…"

El relacionamiento económico, adelanto jurídico y tecnológico en el mundo, y la colaboración internacional que tuvo México en esa época fue sustancial para que se diera la reforma Constitucional en esta materia, porque se tuvo una evolución positiva tomando como consideración las organizaciones internacionales que se mencionaron en el Capítulo 2.

[14] Garriga Dominguez , A. (2009). Tratamiento de Datos Personales y Derechos Fundamentales. Madrid : Dykinson.

El entorno jurídico internacional cambió el paradigma completo de lo plasmado en la Ley Federal de Acceso a la Información Pública de 2002, derivado de esto, en el primer semestre de 2010, el Congreso de la Unión aprobó la Ley Federal de Protección de Datos Personales en Posesión de Particulares, lo cual amplió sustancialmente las facultades, atribuciones y responsabilidades del Instituto Federal de Acceso a la Información Pública, al ser considerado como autoridad nacional en la materia. Asimismo, modificó su nombre al de "Instituto Federal de Acceso a la Información y Protección de Datos". A partir de julio del mismo año, el IFAI inició un proceso de reestructuración y capacitación tanto de su personal como de todos aquellos sujetos, físicos o morales, poseedores de una base de datos, el cual concluyó en enero de 2012, fecha en la que el derecho de las personas a ser protegidas en sus datos tuvo plena vigencia.

2.2. Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento.

El 05 de julio de 2010 se publicó la Ley Federal de Protección de Datos Personales en Posesión de Particulares, misma que tiene como objetivo regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas, a raíz de esto todas las personas físicas y morales que realicen un tratamiento de datos personales son considerados sujetos regulados por dicha Ley, teniendo como excepción:

- Las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y
- Las personas que lleven a cabo la recolección y almacenamiento de datos personales, que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.

Asimismo, el 21 de diciembre del 2011 se publicó en el Diario Oficial de la Federación el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares que, en obviedad de gramática, su objeto es reglamentar las disposiciones contenidas en la Ley Federal de Protección de Datos Personales, es decir, es la parte adjetiva en materia de protección de datos personales.

De lo anterior, se debe entrar en un preámbulo general de los diversos factores importantes que juegan en la protección de datos personales. En razón de lo anterior, en la parte sustantiva de la materia, se introducen diversas figuras en el tratamiento de datos personales, tales como Titular (persona física a quién pertenecen los datos), Responsable (persona física o moral de carácter privado que decide sobre el tratamiento de datos personales), Tercero (persona física o moral, nacional o extranjera, distinta del titular o del responsable de los datos) y Encargado (Quien solo o conjuntamente con otros trata datos por cuenta del responsable).

Asimismo, en dicha Ley se establecieron varios principios y deberes que los responsables, encargados y/o terceros deben tomar en consideración al momento de realizar un tratamiento de datos personales, porque en dichos principios se plasmaron una serie de requisitos y medidas de seguridad que se deben de abordar de manera integral, tanto de carácter legal como tecnológico.

- Principio de Licitud

  Este principio, se encuentra plasmado en el artículo 7 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares[15]:

[15] Ley Federal de Protección de Datos Personales en Posesión de Particulares. Texto vigente 21/12/2011.

"Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta Ley y demás normatividad aplicable.

La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.

En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley"

Asimismo, en el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares estableció en su numeral 10:

"El principio de licitud obliga al responsable a que el tratamiento sea con apego y cumplimiento a lo dispuesto por la legislación mexicana y el derecho internacional"

De esto se deduce que en cualquier tratamiento de datos personales que se realice, los responsables, encargado y/o terceros deberán de estar en cabal cumplimiento con los artículos mencionados, aunado a que deberá de haber una concordancia con cada uno de los principios que le siguen a este, y en caso de que exista alguna falta a alguno de estos, el responsable o encargado serán acreedores a una multa, como se establece en el Capítulo X de la citada ley sustantiva de la materia.

- Consentimiento

Analizando de manera internacional la protección de datos personales, y tomando en cuenta los antecedentes que existen antes

de las regulaciones, este principio cobra suma importancia en todo tratamiento realizado, porque sin el consentimiento de los Titulares no se podría llevar a cabo, partiendo de los supuestos en los que es imperativo el consentimiento. Y antes de señalar los requisitos establecidos en la parte sustantiva, la parte adjetiva nos señala varios supuestos que debemos considerar.

1. El consentimiento que otorgue el Titular deberá ir relacionado a una finalidad o finalidades determinadas.
2. Para el caso de que los datos personales se obtengan directamente del titular, el consentimiento deberá ser previo a cualquier tipo de tratamiento.

Aunado a lo anterior, en el artículo 8 de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, establece que "…*Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley. El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos. Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición. Los datos financieros o patrimoniales requerirán el consentimiento expreso de su titular, salvo las excepciones a que se refieren los artículos 10 y 37 de la presente Ley*"[16]

Asimismo, en dicha Ley se establece un requisito especial para el tratamiento de datos personales sensibles, que de acuerdo con el

[16] *Ibídem*

artículo 3 fracción VI los datos personales sensibles son: *Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual;* por lo que en su artículo 9 establece que el consentimiento deberá ser expreso y por escrito del Titular.

Derivado de lo anterior se desprende que existen 2 variaciones para obtener el consentimiento de los Titulares, siendo la primera de ellas de manera tácita y la segunda de manera expresa; sin embargo, para ambos supuestos el artículo 12 del reglamento de dicha Ley, establece las características que son preponderantes ante una obtención del consentimiento, apegada al principio de licitud, mismos que deberán ser libre, específico e informado.

Libre, sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular;

Específica, referida a una o varias finalidades determinadas que justifiquen el tratamiento, e

Informada, es decir, que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento.

Sumado a lo anterior, y no menos importante, los responsables del tratamiento de datos personales deben establecer mecanismos para que los titulares de datos personales puedan revocar el consentimiento otorgado tácita o expresamente, siempre y cuando no exista un impedimento legal; extendiéndose este derecho de los

titulares a los encargados de los que los responsables hayan remitidos sus datos.

Por último, en el artículo 12 de la Ley establece que "… *si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular…*"[17]

- Información

  El principio de información que se encuentra plasmado en el artículo 15 de la Ley y 23 de su reglamento, establece que el responsable tiene la obligación de informar a los titulares sobre la existencia y características principales del tratamiento al que serán sometidos sus datos personales, con objeto de que pueda ejercer sus derechos a la autodeterminación informativa, privacidad y protección de datos personales materializando este principio a través del Aviso de Privacidad en sus tres modalidades establecidas en los Lineamientos del Aviso de Privacidad.

  Asimismo, y en concordancia con el artículo 23 del reglamento, el responsable deberá dar a conocer al titular la información relativa a la existencia y características principales del tratamiento a que serán sometidos sus datos personales a través del Aviso de Privacidad; en el artículo 16 de la Ley se establece lo mínimo necesario que un Aviso de Privacidad debe contener.

  1. La identidad y domicilio del responsable que los recaba;
  2. Las finalidades del tratamiento de datos;

[17] *Ibídem*

3. Las opciones y medios que el responsable ofrezca a los titulares para limitar el uso o divulgación de los datos;
4. Los medios para ejercer los derechos de acceso, rectificación, cancelación u oposición, de conformidad con lo dispuesto en esta Ley;
5. En su caso, las transferencias de datos que se efectúen, y
6. El procedimiento y medio por el cual el responsable comunicará a los titulares de cambios al aviso de privacidad, de conformidad con lo previsto en esta Ley.

   En el caso de datos personales sensibles, el aviso de privacidad deberá señalar expresamente que se trata de este tipo de datos.

Y dicho aviso de privacidad deberá ponerse a disposición del titular a través de formatos impresos, digitales, visuales, sonoros o cualquier otra tecnología de la siguiente manera:

1. Cuando los datos personales hayan sido obtenidos personalmente del titular, el aviso de privacidad deberá ser facilitado en el momento en que se recaba el dato de forma clara y fehaciente, a través de los formatos por los que se recaban, salvo que se hubiera facilitado el aviso con anterioridad, y

2. Cuando los datos personales sean obtenidos directamente del titular por cualquier medio electrónico, óptico, sonoro, visual, o a través de cualquier otra tecnología, el responsable deberá proporcionar al titular de manera inmediata, al menos la información a que se refiere las fracciones I y II del artículo

anterior, así como proveer los mecanismos para que el titular conozca el texto completo del aviso de privacidad.

Por último, tomando en consideración el presente principio de información, y que el derecho a la protección de datos personales permite garantizar a la persona el poder de disposición y control que tiene sobre sus datos personales, y sobre el uso y destino que se le da a los mismos, el 13 de enero del 2013 se publicó en el Diario Oficial de la Federación los **Lineamientos del Aviso de Privacidad**, que tiene como objeto establecer el contenido y alcance de los avisos de privacidad, tras lo cual resulta de observancia obligatoria en todo el territorio nacional, para los particulares que realicen un tratamiento de datos personales.

Derivado de lo anterior, se debe partir que el **Aviso de Privacidad**, es un "…*documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del titular, previo al tratamiento de sus datos personales*…"[18] y a que a través de este documento se materializa el principio de información; por lo que los avisos de privacidad tienen como objetivo "…*delimitar los alcances y condiciones generales del*
tratamiento, así como informarlos a los titulares, a fin de que estén en posibilidad de tomar decisiones informadas sobre el uso de sus datos personales, y de mantener el control y disposición sobre ellos. Asimismo, el aviso de privacidad permite al responsable transparentar dicho tratamiento, y con ello fortalecer el nivel de confianza de los titulares…" tal como se establece en el artículo octavo de los Lineamientos[19].

[18] Lineamientos del Aviso de Privacidad. Texto vigente: DOF: 17/01/2013.
[19] Véase Marco, I. S. (2013). Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento. México : THEMIS.

Aunado a lo anterior, los Lineamientos en su artículo décimo, emiten las características que deben tener los avisos de privacidad.

1. No usar frases inexactas, ambiguas o vagas;
2. Tomar en cuenta para su redacción los perfiles de los titulares;
3. No incluir textos o formatos que induzcan al titular a elegir una opción en específico;
4. En caso de que se incluyan casillas para que el titular otorgue su consentimiento, no se deberán marcar previamente, y
5. No remitir a textos o documentos que no estén disponibles para el titular.

Asimismo, es de suma importancia tener claro en qué momento se deben usar las modalidades que los Lineamientos mencionan en su artículo decimoctavo (ver Tabla 1):

1. Aviso de Privacidad **Integral.**
2. Aviso de Privacidad **simplificado**
3. Aviso de Privacidad **corto**

Tabla 1 Contenidos de los Avisos de Privacidad

Integral	**Simplificado**	**Corto**
Identidad y domicilio del responsable	Identidad y domicilio del responsable	Identidad y domicilio del responsable
Datos personales que serán sometidos a tratamiento	Finalidades del tratamiento	Finalidades del Tratamiento
Señalamiento expreso de los datos personales sensibles que se tratarán	Mecanismos que el responsable ofrece para que el titular conozca el aviso de privacidad integral	Mecanismos para que el titular conozca el aviso de privacidad integral

Finalidades del Tratamiento		
Mecanismos para que los titulares manifiesten su negativa para el tratamiento de sus datos personales para aquellas finalidades que no son necesarias, ni hayan dado origen a la relación jurídica con el responsable		
Transferencia de Datos personales, el tercero receptor de los datos personales y las finalidades de las mismas		
Cláusula que indique si el titular acepta o no la transferencia, cuando así se requiera		
Los medios y el procedimiento para ejercer los derechos ARCO		
Los mecanismos o el procedimiento para que el titular pueda revocar el consentimiento al tratamiento de sus datos personales		
Opciones y medios que el responsable ofrece al titular para limitar el uso o divulgación de sus datos personales		
Información sobre el uso de mecanismos en medios remotos o locales de comunicación electrónica, óptica y otra tecnología, que permitan recabar datos personales de manera automática y simultánea al tiempo que		

el titular hace contacto con los mismos		
Procedimientos y medios a través de los cuáles el responsable comunicará a los titulares los cambios al aviso de privacidad		

Asimismo, los Avisos de Privacidad, en sus diferentes modalidades están plasmadas en el artículo decimonoveno de los Lineamientos, como se puede ver en la Tabla 2.

Tabla 2 Aplicación de Modalidades

Integral	Simplificado	Corto
Cuando los datos personales se obtengan directamente del Titular	Cuando los datos personales se obtengan directa o indirectamente del Titular, se podrá optar por el Integral o Simplificado.	Cuando el espacio utilizado para la obtención de los datos personales sea mínimo y limitado, de forma tal que los datos personales recabados o el espacio para la difusión o reproducción del aviso de privacidad también lo sean

- Calidad

Los responsables del tratamiento de datos personales deben tener en cuenta que el presente principio, tiene 2 puntos de suma importancia de acuerdo al artículo 36 del Reglamento, el primero de ellos es que establece que "…*se cumple con el principio de calidad cuando los datos personales tratados sean exactos, completos, pertinentes, correctos y actualizados según se requiera para el cumplimiento de la finalidad para la cual son tratados.* ***Se presume que se cumple con la***

calidad en los datos personales cuando éstos son proporcionados directamente por el titular, y hasta que éste no manifieste y acredite lo contrario, o bien, el responsable cuente con evidencia objetiva que los contradiga…"[20]

Por otro lado, de acuerdo con los numerales 37 y 38 de dicho Reglamento, exigen a los responsables un periodo de bloqueo que de conformidad con el artículo 3 fracción III establece como bloqueo lo siguiente: "*Bloqueo: La identificación y conservación de datos personales una vez cumplida la finalidad para la cual fueron recabados, con el único propósito de determinar posibles responsabilidades en relación con su tratamiento, hasta el plazo de prescripción legal o contractual de éstas. Durante dicho periodo, los datos personales no podrán ser objeto de tratamiento y transcurrido éste, se procederá a su cancelación en la base de datos que corresponde.*", por lo que una vez terminado el periodo de bloqueo se deberán de suprimir dichos datos personales, y tomando la definición que establece el artículo 2 fracción XII del Reglamento, respecto a la supresión es "*Supresión: Actividad consistente en eliminar, borrar o destruir el o los datos personales, una vez concluido el periodo de bloqueo, bajo las medidas de seguridad previamente establecidas por el responsable.*"[21]

Derivado de lo anterior, y en concordancia con el numeral 19 de la Ley que establece: "…*Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan*

[20] Ibídem
[21] Ibídem

proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado…", asimismo, el artículo 2 fracción VI inciso d) que determina: "… Medidas de seguridad físicas: Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para*: garantizar la eliminación de datos de forma segura…"*[22]

Por último, se debe dejar claro que este principio se encuentra consagrado en la Carta Magna, en su artículo 16, párrafo segundo, que dice lo siguiente: "… *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…",* así como en el artículo 25 de la Ley.

- Finalidad

"El tratamiento de datos personales deberá limitarse al cumplimiento de las finalidades revistas en el aviso de privacidad. Si el responsable pretende tratar los datos para un fin distinto que no resulte compatible o análogo a los fines establecidos en aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular", por lo que *la finalidad o las finalidades establecidas en el aviso de privacidad deberán ser determinadas, lo cual se logra cuando con claridad, sin lugar a confusión y de manera objetiva se especifica para qué objeto serán tratados los datos personales.*

Los responsables y por consecuencia los encargados, deben tener absolutamente claro cuáles son las finalidades del tratamiento

[22] Ibídem

de datos personales, diferenciando las que dieron origen y son necesarias para la relación jurídica entre el responsable y el titular, de aquellas que no lo son; sin embargo, el reglamento establece que se podrá llevar a cabo un tratamiento para finalidades que se resulten compatibles o en su caso análogas con aquellas de las que dieron origen o sean necesarias, y en caso contrario, el responsable deberá de estarse a lo establecido en el principio de consentimiento, es decir, deberá de recabar el consentimiento del Titular para este supuesto.

Los titulares, así como tienen el derecho de reservarse u otorgar su consentimiento, también tienen derecho a revocar el consentimiento otorgado para las finalidades que sean distintas a las que dieron origen o sean necesarias para la relación jurídica entre el responsable y el titular, sin que tenga como consecuencia el cese de dicha relación.

- Proporcionalidad

Este principio, es fundamental para la toma de decisiones respecto a los demás principios, y se podría tomar como base para la implementación del principio de responsabilidad y el deber de seguridad que hace mención la ley y su reglamento, en virtud de que se debe priorizar los datos personales que resulten necesarios, adecuados y relevantes con relación directa con las finalidades para las cuales serán objeto de un tratamiento. Además, se obliga al responsable que los datos personales sean los mínimos necesarios de acuerdo con la finalidad del tratamiento que tenga lugar.

Partiendo del criterio de minimización que estable el artículo 46 del Reglamento, y haciendo un análisis de la relación con los demás principios y con el deber de seguridad, los responsables se tendrían

que preguntar, ¿si al realizar un tratamiento de datos personales con los mínimos necesarios, se reduciría la brecha de seguridad y por ende las medidas de seguridad tendrían que ser menores?

2.3. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

En el capítulo anterior, se realizó un preámbulo de Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento, tras lo cual ambas regulaciones están enfocadas a la protección de datos personales en el sector privado, es decir, personas físicas o morales tal y como se establece en su artículo 2 de dicha Ley, sin embargo, el sector público también realiza un tratamiento de datos personales, razón por la cual se tuvo que regular este tratamiento y en 26 de enero del 2017 se publicó en el Diario Oficial de La Federación la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados que tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados.

Se definen a los sujetos obligados de la siguiente manera: en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos. Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales, de conformidad con la normatividad aplicable para la protección de datos personales en posesión de los particulares[23].

[23] LEY GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS. Texto vigente: DOF 26-01-2017.

Y teniendo como objetivo los siguientes puntos:

1. Distribuir competencias entre los Organismos garantes de la Federación y las Entidades Federativas, en materia de protección de datos personales en posesión de sujetos obligados;
2. Establecer las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos de acceso, rectificación, cancelación y oposición, mediante procedimientos sencillos y expeditos;
3. Regular la organización y operación del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales a que se refieren esta Ley y la Ley General de Transparencia y Acceso a la Información Pública, en lo relativo a sus funciones para la protección de datos personales en posesión de sujetos obligados;
4. Garantizar la observancia de los principios de protección de datos personales previstos en la presente Ley y demás disposiciones que resulten aplicables en la materia;
5. Proteger los datos personales en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de la Federación, las Entidades Federativas y los municipios, con la finalidad de regular su debido tratamiento;
6. Garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales;
7. Promover, fomentar y difundir una cultura de protección de datos personales;

8. Establecer los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio que correspondan para aquellas conductas que contravengan las
9. disposiciones previstas en esta Ley, y
10. Regular los medios de impugnación y procedimientos para la interposición de acciones de inconstitucionalidad y controversias constitucionales por parte de los Organismos garantes locales y de la Federación; de conformidad con sus facultades respectivas.

2.4. Reglamento General de Datos Personales de la Unión Europea.

El 24 de octubre de 1995 el Parlamento y Consejo Europeo emitieron la "Directiva /46/CE" relativa a la protección de personas físicas en lo respectivo al tratamiento de datos personales y a la libre circulación de estos datos; con lo cual es el antecesor jurídico al actual Reglamento General de Datos Personales de la Unión Europea, mismo que se publicó el 27 de abril del 2016 y entró en vigor el 25 de mayo del 2018, y surge ante la necesidad de que las personas de la Unión Europea tengan mayor control sobre sus datos personales y que las organizaciones traten dichos datos personales de manera correcta.

¿En México se considera como regulación aplicable?

La respuesta es, sí en términos del artículo 3 establece:

"Ámbito territorial

1. El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la

Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con:

a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o

b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público."[24]

Derivado de lo anterior, es que se puede considerar aplicable a los responsables y/o encargados que realicen actividades comerciales a través de la oferta de bienes o servicios con países miembros de la Unión Europea, y cuándo por cualquier situación tengan un tratamiento de datos personales aún cuándo no estén dentro del territorio de la Unión Europea. Es por ello, que la principal razón de la existencia del presente reglamento es otorgar más control a los titulares de datos personales respecto a su tratamiento.

[24] Consejo de la Unión Europea. (2016) Reglamento General de Datos Personales de la Unión Europea. Recuperado de: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32016R0679

Con el preámbulo anterior, podemos entrar al análisis jurídico y tecnológico de los puntos a consideración del sustentante, más relevantes del Reglamento en comento. Siendo el primero de ellos la responsabilidad "proactiva" que prácticamente se basa en los responsables tienen la obligación de cumplir y hacer cumplir las obligaciones contenidas en el Reglamento General de Protección de Datos Personales, así como ser capaz de demostrar dicho cumplimiento, por lo cual la documentación y trazabilidad son requisitos indispensables. El segundo punto, es el enfoque basado en riesgos; aquí debemos partir que no existe lograr un estado completamente sin riesgos o bien, totalmente seguro, motivo por el cual el enfoque basado en riesgos debe ser para que los responsables y/o encargado tomen acciones necesarias y pertinentes para minimizar los riesgos detectados en el tratamiento de datos personales. El tercer punto, es la creación de la figura Oficial de Protección de Datos, que si bien, en la Legislación mexicana en su artículo 30 hace mención de una persona o departamento de datos personales, en este reglamento internacional establece que se deberá de nombrar un Oficial de Protección de Datos teniendo como actividades principales el asesoramiento al responsable y/o encargado y sus empleados, supervisar el cabal cumplimiento de las obligaciones, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes y como punto de contacto con Autoridades. Y el cuarto punto son las evaluaciones de impacto en protección de datos personales, si bien ya hablamos del enfoque basado en riesgos, estás evaluaciones de impacto se deben tomar en cuenta cuándo en el tratamiento de datos personales estén involucradas nuevas tecnologías y/o que por su naturaleza, alcance, contexto o fines que signifiquen un alto riesgo para los titulares.

Aunado a lo comentado en líneas anteriores, existe una relación entre la Legislación en Materia de Protección de Datos Personales en México y el Reglamento General de Datos Personales de la Unión Europea, y es que ambas regulaciones, toman en consideración la seguridad de los datos personales, para la Comunidad Europea, en su Sección 2, artículo 32 establece que: "*el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo*"[25], materializándose las medidas técnicas y organizativas en:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Sin embargo, para la Ley Federal de Protección de Datos Personales en Posesión de Particulares, y su Reglamento, la seguridad de los datos recae en un deber de seguridad establecido en el artículo 19 de la Ley, materializándose en el artículo 2 fracciones V, VI y VII del Reglamento, que profundizaremos en el siguiente Capítulo.

[25] *Ibídem*

CAPÍTULO 3

PRINCIPIO DE RESPONSABILIDAD

El principio de responsabilidad y el deber de seguridad, en el tratamiento de datos personales, no solamente se encuentra plasmado en la legislación mexicana, sino en los diferentes órganos internacionales, hacen mención en estos aspectos, ya que si bien, permiten que se realice un tratamiento de datos personales, y que este sea legítimo, controlado e informado, las organizaciones y sector público deben tener implementadas medidas de seguridad que minimicen las brechas de seguridad inherentes a un tratamiento de datos personales, y así, aumentar el grado de seguridad en cuanto a la confidencialidad, integridad y disponibilidad de los mismos.

El informe del Comité Jurídico Interamericano de la OEA[26] incluye entre sus principios también el de responsabilidad, sobre el que indica, con carácter general, que "los controladores de datos adoptarán e implementarán las medidas correspondientes para el cumplimiento de estos principios", de forma que la "responsabilidad" de quien trata los datos personales es fundamental para "la protección efectiva de los derechos individuales de protección de la privacidad y de los datos". A continuación, incide en el hecho de que este principio:

> "requiere el establecimiento de metas apropiadas en lo que se refiere a la protección de la privacidad, a las cuales los controladores de datos (organizaciones y otras entidades) deben adherirse, permitiéndoles determinar las medidas más apropiadas para alcanzar esas metas y vigilar su cumplimiento."

[26] http://www.oas.org/es/sla/ddi/docs/CJI-doc_474-15_rev2.pdf

A nivel internacional, en cuanto a la definición de este concepto, debe hacerse referencia al Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE[27], que ha tratado este principio en su Dictamen 3/2010 sobre el principio de responsabilidad (WP 173)[28] indicando sobre este término que "proviene del mundo anglosajón donde es de uso general y donde se da una comprensión ampliamente compartida de su significado, aunque la definición exacta de «responsabilidad» resulta compleja en la práctica. Pero de forma general, el término apunta sobre todo al modo en que se ejercen las competencias y al modo en que esto puede comprobarse. Competencia y responsabilidad son dos caras de la misma moneda y sendos elementos esenciales de la gobernanza. Solo cuando la responsabilidad funciona en la práctica puede desarrollarse la confianza suficiente."[29]

La responsabilidad se refiere, por tanto, a "las medidas que pudieran adoptarse o preverse para garantizar la observancia en materia de protección de datos."[30]

Por establecer un punto de partida en cuanto a la inclusión y reconocimiento de este principio en instrumentos internacionales sobre protección de datos personales, el Dictamen del Grupo de Trabajo del artículo 29 de la Directiva 95/46/CE menciona que "el principio de responsabilidad no es exactamente nuevo. Su reconocimiento expreso

---

[27] Creado en virtud del citado artículo de la 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, como un grupo consultivo e independiente que, conforme al apartado 2 de dicho artículo, "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." Y el artículo 30 de la Directiva le confiere las siguientes atribuciones:

> "a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la presente Directiva con vistas a contribuir a su aplicación homogénea;

[28] Adoptado el 13 de julio de 2010 y disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2010/wp173_es.pdf

[29] Apartado 21 del citado Dictamen. Pág. 8.

[30] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2010/wp173_es.pdf, pág. 8.

figura en las directrices sobre privacidad adoptadas en 1980 por la Organización de Cooperación y Desarrollo Económicos (OCDE). El principio de responsabilidad de estas reza así: «Todo responsable de datos debería ser responsable de cumplir con las medidas que hagan efectivos los principios materiales expuestos».”[31]

De nuevo, hay que mencionar el informe del Comité Jurídico Interamericano de la OEA sobre las implicaciones del principio de responsabilidad, indica que los principios de la protección de datos personales dependen de la capacidad de quienes recopilan, procesan y retienen datos personales para tomar decisiones responsables, éticas y disciplinadas acerca de los datos y su uso durante todo el ciclo de vida de los datos. Estos gerentes de datos deben actuar en calidad de buen custodio de los datos que les proporcionen o confíen.

Al principio de responsabilidad hacen también referencia los Estándares Internacionales sobre Protección de Datos Personales y Privacidad (Resolución de Madrid)[32] en su artículo 11, que indica:

> “La persona responsable deberá:
>
> a. adoptar las medidas necesarias para cumplir con los principios y obligaciones establecidos en el presente Documento y en la legislación nacional aplicable, y
>
> b. dotarse de aquellos mecanismos necesarios para evidenciar dicho cumplimiento, tanto ante los interesados como ante las autoridades de supervisión en el ejercicio de sus competencias, conforme a lo establecido en el apartado 23.”

[31] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionesrecomendation/files/2010/wp173_es.pdf pág. 7.

[32]https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Cooperation/Conference_int/09-11-05_Madrid_Int_standards_ES.pdf

Sobre el principio de responsabilidad, el Dictamen con proyecto de Decreto por el que se expide la Ley Federal Protección de Datos Personales en Posesión de Particulares indica que "debe entenderse en el sentido de que corresponderá a la entidad o persona responsable el deber de velar por el cumplimiento de los principios y rendir cuentas al titular en caso de incumplimiento."[33]

Y, a continuación, el citado Dictamen destaca también que este principio de responsabilidad "es la verdadera garantía para el titular de los datos quien deposita su confianza en el responsable, mismo que deberá tomar todas las previsiones para que los datos sean tratados de acuerdo con la voluntad del dueño de la información y bajo las medidas de seguridad que se prevean por la vía contractual."

Es así que, en la práctica, como termina indicando el Dictamen, el principio de responsabilidad implica que "dado que existe un tráfico de datos intenso y en muchas ocasiones este se da fuera de las fronteras de nuestro país, el ciudadano tendrá la tranquilidad de que, si su información ha trascendido a manos de terceros en otras latitudes, éste estará enterado de las cautelas con que debe tratar su información."

En relación con este principio, citando, de nuevo, la Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, ésta indica que este principio "cierra el círculo con relación a los principios que regulan la protección de los datos personales. A este principio se le conoce también como el principio de "rendición de cuentas", ya que establece la obligación de los responsables de velar por el cumplimiento del resto de los principios, adoptar las medidas necesarias para su aplicación, y demostrar ante titulares y la

[33]http://www3.diputados.gob.mx/camara/content/download/231031/621446/file/Version_final_ley_proteccion_datos_personales.pdf

autoridad, que cumple con sus obligaciones en torno a la protección de los datos personales."[34]

En ese sentido, en este Capítulo se analizará el principio de responsabilidad y el deber de seguridad contenido en la Ley Federal de Protección de Datos Personales en Posesión de Particulares y el Reglamento a la Ley Federal de Protección de Datos Personales en Posesión de Particulares, en virtud de que el presente trabajo de investigación, es en cuanto a las estrategias jurídicas y tecnológicas para la protección de datos personales; debido a lo anterior dichas estrategias serán únicamente en dónde el tratamiento de datos personales, se realice en un ambiente digital.

El principio de responsabilidad, está estrechamente ligado con las medidas de seguridad que los responsables y/o los encargados deben tener implementadas en sus sistemas de tratamiento de datos personales, si bien dicho principio se encuentra literalmente plasmado en los artículos 14 de la Ley, 47 y 48 del Reglamento, también es que se debe tomar en cuenta el deber de seguridad que se encuentran en el artículo 19 de la Ley; artículos 2 fracción V, VI y VII, 52, 60, 61, 62 y 63 y 66 del Reglamento.

Lo anterior, en virtud de que "…*el responsable tiene la obligación de velar y responder por el tratamiento de los datos personales que se encuentren bajo su custodia o posesión, o por aquéllos que haya comunicado a un encargado, ya sea que este último se encuentre o no en territorio mexicano*…"[35], partiendo de la que se podría llamar definición del principio de responsabilidad, disponible en el artículo 47 primer párrafo de la Ley, los responsables deben tener en cuenta no solamente el siguiente listado que hace mención el artículo 48 del Reglamento:

[34] http://inicio.inai.org.mx/DocumentosdeInteres/Guia_obligaciones_lfpdppp_julio2014.pdf
[35] REGLAMENTO DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES. Texto vigente: DOF: 21/12/2011.

"…Entre las medidas que podrá adoptar el responsable se encuentran por lo menos las siguientes:

1. *Elaborar políticas y programas de privacidad obligatorios y exigibles al interior de la organización del responsable;*
2. *Poner en práctica un programa de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales;*
3. *Establecer un sistema de supervisión y vigilancia interna, verificaciones o auditorías externas para comprobar el cumplimiento de las políticas de privacidad;*
4. *Destinar recursos para la instrumentación de los programas y políticas de privacidad;*
5. *Instrumentar un procedimiento para que se atienda el riesgo para la protección de datos personales por la implementación de nuevos productos, servicios, tecnologías y modelos de negocios, así como para mitigarlos;*
6. *Revisar periódicamente las políticas y programas de seguridad para determinar las modificaciones que se requieran;*
7. *Establecer procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales;*
8. *Disponer de mecanismos para el cumplimiento de las políticas y programas de privacidad, así como de sanciones por su incumplimiento;*
9. *Establecer medidas para el aseguramiento de los datos personales, es decir, un conjunto de acciones técnicas y administrativas que permitan garantizar al responsable el*

cumplimiento de los principios y obligaciones que establece la Ley y el presente Reglamento, o

10. *Establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento.*

El principio de responsabilidad y el deber de seguridad se deben de analizar de manera conjunta, en virtud de que ambos tocan puntos medulares para la implementación de medidas de seguridad administrativas, físicas y técnicas a que hacen mención los artículos 19 de la Ley.

> "… *Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado…"*[36]

Así como el artículo 2 fracción V, VI y VII del Reglamento que desglosa puntualmente las *medidas de seguridad administrativas, técnicas y físicas.*

> "… ***Medidas de seguridad administrativas**: Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales;*

[36] *Ibídem*

***Medidas de seguridad físicas**: Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para: a) Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información; b) Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones; c) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y d) Garantizar la eliminación de datos de forma segura;*

***Medidas de seguridad técnicas**: Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que: a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados; b) El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones; c) Se incluyan acciones para la adquisición¸ operación, desarrollo y mantenimiento de sistemas seguros, y d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales;…";*[37].

Y partiendo de la premisa de que se realice un tratamiento en el denominado cómputo en la nube, también se debe analizar el artículo 52 del Reglamento.

"…Para el tratamiento de datos personales en servicios, aplicaciones e infraestructura en el denominado cómputo en

[37] *Ibídem*

la nube, en los que el responsable se adhiera a los mismos mediante condiciones o cláusulas generales de contratación, sólo podrá utilizar aquellos servicios en los que el proveedor:

I. Cumpla, al menos, con lo siguiente: a) Tener y aplicar políticas de protección de datos personales afines a los principios y deberes aplicables que establece la Ley y el presente Reglamento; b) Transparentar las subcontrataciones que involucren la información sobre la que se presta el servicio; c) Abstenerse de incluir condiciones en la prestación del servicio que le autoricen o permitan asumir la titularidad o propiedad de la información sobre la que presta el servicio, y d) Guardar confidencialidad respecto de los datos personales sobre los que se preste el servicio, y

II. Cuente con mecanismos, al menos, para: a) Dar a conocer cambios en sus políticas de privacidad o condiciones del servicio que presta; b) Permitir al responsable limitar el tipo de tratamiento de los datos personales sobre los que se presta el servicio; c) Establecer y mantener medidas de seguridad adecuadas para la protección de los datos personales sobre los que se preste el servicio; d) Garantizar la supresión de los datos personales una vez que haya concluido el servicio prestado al responsable, y que este último haya podido recuperarlos, y e) Impedir el acceso a los datos personales a personas que no cuenten con privilegios de acceso, o bien en caso de que sea a solicitud fundada y motivada de autoridad competente, informar de ese hecho al responsable…"[38]

[38] *Ibídem*

Del análisis anterior, es que el principio de responsabilidad, no solamente se centra en los artículos literales, sino se tiene que hacer un análisis integral del principio de responsabilidad y deber de seguridad, para estar en posibilidades de poder cumplir cabalmente con las medidas de seguridad administrativas, físicas y técnicas.

Para finalizar este capítulo, podemos decir que el principio de responsabilidad, desde el punto de vista del sustentante, es el principio más complejo de poder cumplir por parte de los responsables del tratamiento, en virtud de que se tiene garantizar, en la mayor medida de lo posible y de acuerdo con el nivel de sensibilidad, el nivel de riesgo de los datos personales que se están tratando, y la infraestructura donde reside los datos personales de las organizaciones.

Como parte de un Sistema de Gestión de Seguridad de Datos Personales y para implementar prácticas responsables en materia de protección de datos personales, la necesidad del apoyo y compromiso de la alta dirección debe:

1. Designar a la persona o al área que asumirá la función de protección de datos dentro de la organización,

2. Aprobar y monitorear el Sistema de Gestión de Seguridad de Datos Personales, e

3. Contar con un mapeo de datos personales, partiendo de su ciclo de vida para poder implementar las medidas de seguridad necesarias para resguardar los datos y cumplir con el presente principio.

CAPÍTULO 4

ESTRATEGIA JURÍDICA – TECNOLÓGICA DE PROTECCIÓN DE DATOS PERSONALES

Consecuencia de todo lo anterior, y en concordancia con el título del presente trabajo de investigación, es que el sustentante considera que todos los responsables y por ende los encargados, deben implementar un Sistema de Gestión de Seguridad de Datos Personales, dónde el enfoque sea integral, tanto jurídico como tecnológico. Derivado de lo anterior se debe partir en el supuesto en el que una organización ya realiza un tratamiento de datos personales, por ende, debe de asegurarlos en la mayor medida de lo posible al implementar las medidas de seguridad a que se refiere el principio de responsabilidad y el deber de seguridad, sin embargo, al enfrentarnos en un entorno digital, las medidas de seguridad deben ser más robustas y completas (tomando como base, las ciberamenazas que cada vez son más sofisticadas, por lo cual las estrategias a seguir deben ser equitativas), dejando a las organizaciones la obligación de considerar la protección de datos personales a través de la gestión de cada una de las fases del ciclo de vida de los datos personales, comprendiendo y analizando cada una de estas fases en relación con una organización proporciona una mayor claridad de cómo proteger los datos personales[39].

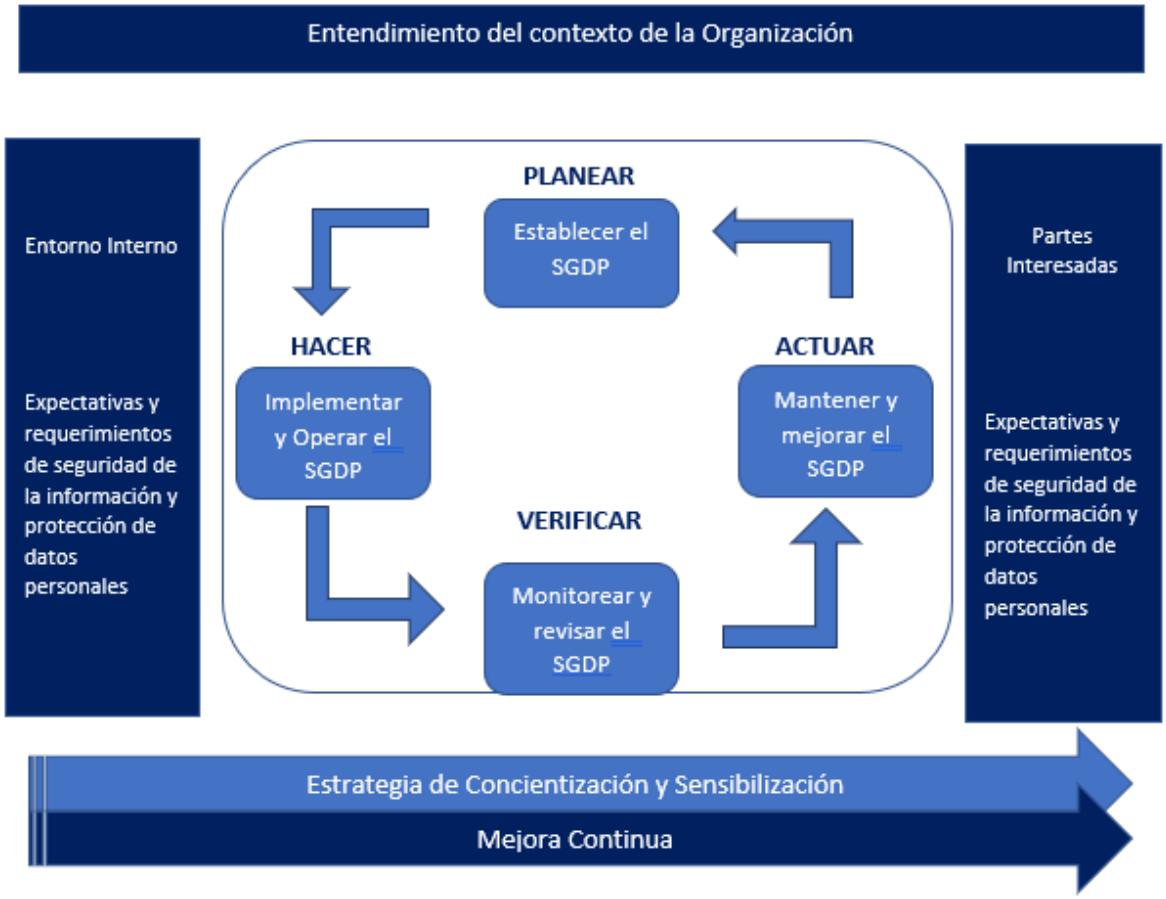
El Sistema de Gestión de Seguridad de Datos Personales (SGSDP) está basado en la gestión del ciclo de vida de los datos desde un enfoque en políticas para gestionar el flujo de información a través de un ciclo de vida desde la creación hasta la disposición final. SGSDP proporciona un enfoque

[39] Dempsey , T., & Rosenquist , M. (2015). Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers . Chicago: Caxton Business & Legal, Inc.

holístico de los procesos, roles, controles y medidas necesarios para organizar y mantener los datos.

Una estrategia de SGSDP bien escrita y bien planificada proporciona revisiones de políticas de manejo de datos, actividades de procesamiento, almacenamiento, intercambio, control de accesos, y destrucción de datos, así como el establecimiento de roles y responsabilidades de los empleados para cada etapa del proceso. Tal como se muestra en la Figura 1.

Figura 1 Estrategia de Sistema de Gestión de Seguridad de Datos Personales (SGSDP)



Sin embargo, la presente investigación no se sustentará en lo plasmado dentro los Parámetros de Autorregulación en Materia de Protección de Datos Personales, ni tampoco en las recomendaciones que ha tenido a bien emitir el Instituto Nacional de Transparencia, Acceso a la Información y

Protección de Datos Personales (INAI) en cuanto al Sistema de Gestión de Seguridad de Datos Personales. Sino por el contrario, se trata de incluir 2 mundos, el jurídico y el tecnológico.

Y como dice el título de esta investigación, es una estrategia jurídica-tecnológica; así, el hecho de que el aumento mundial en la adopción de servicios y dispositivos digitales haya creado muchos nuevos riesgos de privacidad no significa que todas las tecnologías de la información tengan un efecto perjudicial sobre la privacidad. De hecho, la tecnología ha sido un tema de investigación activo en ciencias de la computación en las últimas décadas y se ha propuesto una variedad de técnicas para contribuir a una mejor aplicación de los derechos de privacidad[40]. Es cierto que la adopción de la mayoría de estas técnicas es aún bastante limitada, incluso si está creciendo, especialmente después de recientes escándalos de violación de la privacidad. Sin embargo, en un momento en que los riesgos de privacidad nunca han sido más altos y el cumplimiento de los derechos de protección de datos personales nunca ha sido tan desafiante, probablemente no sería una buena estrategia descuidar el potencial de las tecnologías disponibles para mejorar la privacidad.

Muchos factores tienen un impacto en la adopción de tecnologías que ayudan a transformar la forma en que las empresas protegen y administran la protección de los datos personales, incluidos los requisitos legales, la protección que brindan y su utilidad. Además, la privacidad es un área de investigación relativamente joven y de rápido desarrollo en informática, por lo cual su progreso y nuevas herramientas son el resultado de una imparable evolución en los entornos digitales y por consecuencia (no creo que sea

[40] Goldberg, Ian, David Wagner, Eric A. Brewer, "Privacy-Enhancing Technologies for the Internet", IEEE COMPCON ´97, Febrero 1997.

algo "natural", sin embargo, es la realidad), la evidente falta de evolución legislativa.

Nuestro objetivo en este capítulo no es discutir la viabilidad de los Parámetros de Autorregulación en Materia de Protección de Datos Personales, sino reforzar las estrategias que las organizaciones como responsables del tratamiento de datos personales, deben implementar, si bien es cierto que no podemos dejar pasar de lado un Sistema de Gestión de Seguridad de Datos Personales (materializado hasta cierto punto en los Parámetros, la Ley y su Reglamento), también es cierto que la constante evolución digital ha dejado un hueco en las medidas de seguridad que la Ley y su Reglamento hasta el día de hoy tienen considerados, por lo cual la estrategia a seguir es lograr una vinculación de la parte jurídica con la tecnológica, en ese sentido nos centramos en un aspecto clave, el uso de tecnologías para la administración y protección de los datos personales en entornos digitales; discutimos en particular las garantías de la oferta, las partes interesadas involucradas en su agotamiento y, entre estas partes interesadas, las partes en las que se debe confiar. De hecho, se puede argumentar que, al final del día, el principal beneficio del uso de tecnologías es contar con una política de cero confianza. Asimismo, sucedería al realizar operaciones con partes interesadas (incluidos los encargados, terceros, sin mencionar a los desarrolladores de la tecnología en sí) y la tecnología puede, en el mejor de los casos, ayudar a reducir el riesgo de la pérdida de los principios de la seguridad de la información.

Este capítulo no pretende ser una presentación técnica exhaustiva, sino más bien un análisis de la situación actual real que afrontan las compañías, y la estrategia que deben seguir para mejorar la protección de datos personales desde una perspectiva de cero confianza. Aquí, nos centramos en tecnologías específicamente diseñadas para mejorar la protección y administración de los datos personales en entornos digitales.

Clasificamos las tecnologías que se pueden usar para imponer la privacidad en dos categorías principales:

1. Tecnologías para evitar o reducir en la medida de lo posible la divulgación de datos personales.

2. Tecnologías para controlar los datos personales cuando se procesan.

Estas dos categorías corresponden a dos tipos de derechos de privacidad y la estrategia jurídica – tecnológica se subdivide en dos tácticas complementarias para individuos: primero, reduciendo al máximo la divulgación de sus datos personales (principio de minimización); luego, controlar e identificar el procesamiento de los datos personales.

El considerando del Reglamento general europeo de protección de datos (acordado por el Parlamento Europeo, el Consejo y la Comisión en diciembre de 2015) define la minimización de datos como el requisito de que los datos sean "adecuados, relevantes y limitados a lo necesario en relación con los fines para los cuales son procesados". Derivado de esto, además, exigen que "los datos personales solo se procesen si el propósito del proceso no puede cumplirse por otros medios". Y en la legislación mexicana, lo plasma en el principio de proporcionalidad, consagrado en el artículo 45 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares "sólo podrán ser objeto de tratamiento los datos personales que resulten necesarios, adecuados y relevantes en relación con las finalidades para las que se hayan obtenido." Por otro lado, nos encontramos con un reto que las organizaciones deben de empezar a afrontar, que es la trazabilidad del dato personal, es decir, el artículo 48 del Reglamento (Principio de Responsabilidad), hace mención que "se debe establecer medidas para la trazabilidad de los datos personales, es decir, acciones, medidas y procedimientos técnicos que permiten rastrear a los datos personales durante su tratamiento."

Hacer cumplir la minimización de datos sería una tarea fácil si el sujeto de los datos no tuviera necesidad de interactuar con el mundo exterior. Es un desafío precisamente porque está en tensión con otros requisitos y, por lo tanto, la divulgación de cierta información. En esta sección, partimos de la necesidad o requisito original (es decir, la necesidad de proteger los datos personales en un entorno digital, respecto a su procesamiento) y estructuramos la presentación de las tecnologías disponibles en tres recursos principales de funcionalidades:

Recurso de comunicación: un usuario de un sistema o aplicativo (correo electrónico, SMS, mensaje instantáneo, comunicación remota, servidores, data centers, etc.) necesita comunicar información a otro usuario, por lo cual necesita acceder a un activo de información;

Recurso de acceso: los usuarios que necesitan comunicarse deben de mostrar algún tipo de credencial para obtener acceso a un sistema o aplicativo, por ejemplo, al hacer log in a su cuenta de correo electrónico institucional;

Recurso de mapeo: las organizaciones deben de contar con una trazabilidad del dato personal, debido a que cuentan con un acceso a sus activos de información, y estos, están siendo comunicados.

Una realidad en la que vivimos hoy en día es que las tecnologías de la información y comunicación permiten que los empleados puedan trabajar desde casa, o simplemente por el rol que desempeña un consultor, directivo, etc., necesitan acceder a los recursos de la organización.

En el supuesto de que una organización, permite a sus empleados acceder a los recursos y/o activos desde sus smartphones o dispositivos móviles para acceder a los recursos de la empresa de forma remota, los empleados ponen en riesgo tanto su dispositivo móvil y/o smartphone (y la

información que contienen), como la integridad y confidencialidad de los activos de información de su empresa, claro, al no contar con controles tecnológicos suficientes y eficientes. Actualmente, las organizaciones cuentan con una VPN[41], sin embargo, debido a las amenazas tan sofisticas que hoy en día vivimos, las VPN´s ya resultan obsoletas.

Los datos enviados a través de la red de la compañía pueden ser vistos y capturados por los ciber atacantes, los datos almacenados en el dispositivo o computadora del empleado también pueden ser atacados, y los usuarios y organizaciones jamás enterarse de estos sucesos.

Técnicamente hablando, la inobservabilidad es más fuerte que el anonimato; en ese sentido a continuación, analizaremos, a modo de antecedente a las VPN´s, porque de cierto modo era innovador al momento de su creación, pero como pasa con infinidad de situaciones y cosas, la evolución trae consigo más y nuevos retos, dejando vulnerable a las organizaciones, en virtud de que las VPN´s, se han vuelto un vector de ataque principal utilizado por los hackers; existen estudios de carácter internacional que solo un tercio de las compañías mundiales saben cuántos proveedores acceden a sus sistemas, se afirma que "la red de la compañía promedio es visitada por 89 proveedores diferentes cada semana". El Informe (FireEye Company, 2016), recomienda: "No le dé acceso a su proveedor de servicios subcontratados por VPN, de sitio a sitio. Deles acceso solo a la aplicación o dispositivo que necesiten. Haga que utilicen la autenticación de múltiples factores". Ahora considere que se han robado más de 3,7 mil millones de registros desde 2013, según lo informado por el Índice de nivel de incumplimiento, de esa forma se podría decir que las VPN, especialmente los que están protegidos con solo un nombre de usuario y contraseña, no son seguros.

[41] Virtual Private Networks

Claramente, el mundo del acceso remoto ha crecido significativamente en los últimos años, más personas trabajan desde casa o en camino a algún lugar. La cantidad de subcontratación de mano de obra o servicios de TI está aumentando. A los usuarios de BYOD[42] también se les está concediendo acceso a la red en masa y a medida que cambian los medios de conectividad, seguimos viendo empresas que conectan a los usuarios con sus redes a través de dispositivos tradicionales de firewall/VPN. En 2013, Forrester[43] creó su Modelo de "Zero Trust" diciendo que "los profesionales de la ciberseguridad deben dejar de confiar en los paquetes como si fueran personas. En "Zero Trust", todo el tráfico de la red no es de confianza". Sin embargo, continuamos viendo que los dispositivos de firewall / VPN se utilizan como la seguridad principal, control que otorga al usuario acceso a toda la red de una organización; en palabras "coloquiales", entregando las llaves del reino a cualquier persona.

Los *Hackers* (piratas informáticos) muestran una y otra vez al mundo que las defensas perimetrales tradicionales no son suficientes, luego entonces, ¿por qué seguimos usando los mismos controles de seguridad? ¿por qué si existen estudios y pruebas fehacientes de que las VPN´s o la seguridad tradicional ya resulta insuficiente, no evolucionamos?

La solución es bastante simple, fácil y ya se mencionó anteriormente. No otorgue acceso a toda la red, sino solo a los recursos especificados (servidor, dispositivo o aplicación) necesarios. Las defensas perimetrales tradicionales no son suficientes, así que vea la identidad como el nuevo perímetro, esto se hace con MFA (múltiple factor de autenticación). Con MFA, el área de Tecnologías de la Información sabe que el usuario autorizado real se está

[42] Bring Your Own Device.
[43] Forrester (2019) Recuperado de: www.forrester.com

autenticando y no un pirata informático que tomó uno de los varios mil millones de nombres de usuario / contraseñas legítimas robados.

Así es como propondría poner fin a las VPN´s como se conoce y utiliza hoy en día, hoy tenemos que evolucionar legislativa y jurídicamente (viéndose como legislativa única y exclusivamente a las leyes *per se* y como jurídica tanto al proceso legislativo, como a los jurisconsultos), hoy tenemos una brecha jurídica – tecnológica en nuestra legislación en la materia; en ese tenor tenemos que actuar y tratar de evolucionar al ritmo de las ciberamenazas, en razón de que se debe de contar con una cultura de "Zero Trust", por lo cual debemos de considerar seriamente la administración de identidad como una de las acciones tácticas de nuestra estrategia.

La administración de identidad incluye los procesos involucrados en la verificación de la identidad de una persona, grupo, proceso o dispositivo. La identificación a través de la mayoría de los sistemas informáticos consiste en que una persona escriba sus credenciales (con múltiples factores de autenticación) en una pantalla de login[44]. Muchas computadoras requieren que el usuario proporcione credenciales para iniciar sesión, las cuales a veces también autentica al usuario para acceder a la red de la organización. Después de que se produce una autenticación, la autorización aún debe realizarse para garantizar que un usuario pueda acceder a un recurso o ejecutar un comando. Incluso si un usuario tiene acceso a una carpeta, no significa que la persona pueda acceder a todos los archivos de una carpeta. Y tener acceso a un archivo no significa que el usuario pueda modificar el archivo o incluso imprimirlo. La lista de control de acceso se usa normalmente para determinar qué permisos tiene un usuario para un recurso en particular.

[44] En español, se considera como "entrar" a un sistema informático.

La gestión de acceso es una herramienta esencial para hacer cumplir los requisitos de privacidad con respecto a quién accede a los datos, en ese sentido se pueden restringir las personas, dispositivos o servicios que acceden a acceder a un recurso o conjunto de recursos. Las sofisticadas técnicas de administración de acceso pueden restringir el acceso a los datos según el tipo de datos a los que se accede, el rol de la persona que accede a los datos, la ubicación del usuario, la hora del día y/o el tipo de dispositivo que se utiliza para acceder a los datos. Si bien una administración de acceso sólida puede garantizar que las personas correctas accedan a los datos correctos de la manera correcta, no puede garantizar que las personas con acceso legítimo a los datos hagan lo correcto con los datos una vez que estén en su poder.

Un usuario siempre puede usar los datos para un propósito incorrecto, compartirlos con la entidad incorrecta, colocarlos en un almacenamiento sin protección o simplemente venderlos, sin embargo, se desprenden aquí varios aspectos a considerar; si el usuario legítimo realiza una acción que vulnere los datos personales, se tendrá plenamente identificado porque, como se mencionará más adelante, no contará con los permisos suficientes para tratar de ocultar sus rastros. Por otro lado, también sale a relucir las capacitaciones y concientizaciones que las organizaciones deben de implementar a todos sus usuarios que traten datos personales, a efecto de que los empleados comprendan sus obligaciones y responsabilidades antes de acceder a los datos. Es por ello, la necesidad y obligación de que las organizaciones cuenten con un SGSDP.

Por último, partamos de un estado de conciencia, las organizaciones no pueden proteger lo que no pueden encontrar. La protección de datos personales primero requiere conocimiento respecto a qué datos cuentan y en segundo lugar donde residen esos datos. Una realidad que hoy en día vivimos es que "históricamente" la protección de datos personales (en

cuánto a su mapeo y descubrimiento) ha sido más sobre políticas, procesos y entrevistas para recopilar información sobre qué datos recopilan y procesan las empresas. Sin embargo, en entornos digitales (y físicos), no podemos dejar en manos de los que se considera por muchos expertos, la capa con la mayor vulnerabilidad (personas), la trazabilidad de los datos personales.

Hoy, en entornos digitales, es prácticamente imposible lograr descubrir en su totalidad, y mapear los flujos que sigue cada dato personal, en cada sistema, en cada aplicativo, de manera tradicional, es decir, con entrevistas, inspecciones, que al final del día, se deja en manos de las personas. A raíz de lo anterior debemos de optar por controles tecnológicos que nos permitan exploración y descubrimiento de datos avanzados en cualquier lugar dentro de una empresa moderna, ya sea en la nube o en el centro de datos.

Las organizaciones deben de empezar a usar machine learning[45] para poder estar en posibilidades de realizar un mapeo de sus datos y así, poder contar con un inventario respecto a "cualquier información concerniente a una persona física identificada o identificable"; esto debido, como se dijo anteriormente, al día de hoy una organización moderna, cuenta con una infinidad de bases de datos, aplicativos, data centers, servidores, etc., y en todos y cada uno de ellos, residen y procesan datos personales, por lo cual al hablar de un mapeo de datos personales, se trata de lograr obtener toda una trazabilidad de los mismos dentro y fuera de su organización (teniendo ubicado a dónde se fueron, sin extralimitarse a las bases de datos, aplicativos de terceros), así como también los flujos por los que los datos personales están siendo procesados, es decir, el usuario Carlos Calderón accedió a la base de datos "A" y después la envió por correo electrónico

[45] Para más información se puede revisar: Alpaydin, E. (2016) Machine Learning: The New AI. MIT Press.

al usuario Juan Argumedo, y este usuario la almacenó en su repositorio de Office 365. Sin embargo, también se tiene que considerar cualquier estructura de datos en cualquier idioma para comprender qué datos se almacenan, en dónde y a quién pertenecen. Esto incluye bases de datos estructuradas, archivos compartidos no estructurados, correo electrónico, registros, Big Data, almacenes de datos, mainframe, SAP, Salesforce, MS Azure, AWS, middleware y más.

Una gestión efectiva de la protección de datos personales está basada en una Estrategia Jurídica-Tecnológica que tiene como bases la implementación de un Sistema de Seguridad de Datos Personales, sin embargo y no menos importante que los Avisos de Privacidad, Política de Protección de Datos Personales, y en general medidas de seguridad administrativas, técnicas y físicas, es la precisión, el inventario y mapeo de datos personales. Hasta ahora la mayoría de las organizaciones solo podían valerse de entrevistas, y luego diagramar en Excel, Visio, o herramientas similares, y otra realidad es que actualmente las organizaciones manejan cada vez más información y datos personales, a diferencia de décadas anteriores, hoy se habla del manejo de Petabytes, en ese tenor, ya se ha superado la capacidad humana para realizar el mapeo, inventario y flujo de datos.

4.1. Problemática ante la falta de mapeo del Dato Personal en entornos digitales.

El capítulo que antecede, nos indica las medidas de seguridad que los responsables y/o encargados deben implementar al realizar un tratamiento de datos personales, sin embargo, ¿son suficientes las medidas de seguridad establecidas en la legislación actual?

La presente propuesta de regulación está basada en la necesidad con la que cuenta el Reglamento de la Ley Federal de Protección de Datos

Personales en Posesión de Particulares, basándose en los puntos que a consideración del sustentante dicha legislación cuenta con más carencias, como son la obtención, uso y acceso, pero que forman parte de todo el ciclo de vida del dato personal, es decir, obtención, uso, acceso, monitoreo, procesamiento, almacenamiento, bloqueo y supresión, por lo cual la estrategia de seguridad y jurídica se basa al tener mapeado todo el ciclo de vida del dato personal en el responsable y/o encargado.

La finalidad que tiene el mapeo del ciclo de vida del dato personal es que en cada ciclo se logre identificar, controlar y personalizar para las necesidades que tiene cada responsable, partiendo de algunos principios de la seguridad de la información, tales como la confidencialidad, integridad y disponibilidad de los activos de información, si bien se tiene como base el deber de seguridad y confidencialidad que marca dicha legislación, así como el artículo 19 segundo párrafo; la ley y su reglamento dejan una brecha de seguridad en cuanto a las medidas de seguridad que los responsables deben implementar en cada ciclo de los datos personales, lo cual nos lleva a preguntarnos ¿la legislación tomó en cuenta los avances tecnológicos para establecer las medidas de seguridad?

Por otro lado, un pilar básico y fundamental de un efectivo sistema de protección de datos personales es la garantía de la seguridad de la información en los datos personales, que se encuentran resididos en Internet, o en software informáticos. Este campo de estudio le ha correspondido al derecho informático, que también incluye las telecomunicaciones en su espectro más amplio. A partir de las reformas al Código de Comercio, a la Ley Federal de Protección al Consumidor, Código Civil y Código de Procedimientos Civiles, en nuestro país se regula el comercio electrónico. La novedosa forma de intercambio comercial por medios electrónicos, compras en Internet o intercambio de datos e información entre los usuarios,

dan cuenta de la importancia de proteger los derechos de la privacidad e intimidad de las personas[46].

Ahondando sobre el tema que nos ocupa, la problemática de la inseguridad de datos personales, partiendo de un entorno digital. Se ha observado que en la actualidad la tecnología, especialmente la informática, ha avanzado vertiginosamente y a pasos agigantados, de manera tal, que las regulaciones tienen que valerse de técnicas especializadas en materia de seguridad de la información, así como estar en un estado de constante cambio, porque si bien las tecnologías de la información y comunicación han permitido el intercambio online de información, eliminando las barreras que los medios físicos provocaban, al hacerla tardada y engorrosa, también es cierto que dichas tecnologías de la información y comunicación se pueden valer para usos de índole ilegal, tal es el caso de robos de identidad en entornos digitales, la técnica conocida como "*man in the middle*" (hombre en medio), compromiso de usuarios privilegiados o bien el acceso no autorizado a sistemas y equipos de cómputo, por mencionar algunos.

Por ejemplo:

En abril del 2018, Banco de México junto con cinco instituciones financieras fueron involucrabas en un ciberataque teniendo como objetivo generar transferencias electrónicas de fondos hacia cuentas bancarias específicas, con el fin de sustraer ilegítimamente recursos monetarios. No se trató de un ataque al sistema central del SPEI operado por el Banco de México, ni a alguna infraestructura de este, sino de un ataque en el que se comprometieron elementos de los sistemas para la generación y envío de órdenes de transferencias.

[46] Valdés, J. T. (2009). Derecho Informático. Distrito Federal: McGRAW-HILL/INTERAMERICANA EDITORES, S.A. DE C.V.

Para estos ataques, se utilizaron técnicas conocidas como robo de credenciales, escalamiento de privilegios, movimientos laterales entre servidores, inserción de archivos o ejecución de instrucciones y borrado de bitácoras.

Con lo anterior, y al hacer un análisis legal e informático, se da lugar a la problemática con la que se enfrenta el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares; si bien es cierto que el objetivo final de los cibercriminales no fue el robo de datos personales que residen en la infraestructura del Banco de México, también es cierto que se les dio un tratamiento inadecuado a los mismos. Hay que dejar claro la situación, la problemática cuenta con dos vertientes, la primera de ellas evidentemente es el ataque por parte de los cibercriminales, sin embargo, la segunda debemos de preguntarnos ¿Qué medidas de seguridad cuentan los usuarios conocidos como Super Administradores, Administradores y/o *Root*? y ¿los usuarios "normales" tienen los privilegios correctos?

¿Pueden considerarse iguales a todos los usuarios de negocio? La respuesta es no, en especial cuando se tienen en cuenta cuestiones de seguridad, debido en medida a que las cuentas privilegiadas pueden hacer mucho más daño que los usuarios promedio y eso supone un riesgo potencial que no les incluye sólo a ellos. Al alcance de sus propias acciones, hay que sumar el potencial dañino de un ataque externo perpetrado a través de la captación de las credenciales de este tipo de usuarios.

Dado el poder que se atribuye a las cuentas privilegiadas, a diferencia de lo que sucedería con el nivel de autorización de acceso que se atribuye a otros usuarios de negocio, quienes tienen una asignada puede visualizar cualquier tipo de dato, interactuar con él e, incluso, practicar

modificaciones en esa información, sin importar el lugar donde se aloje o el dispositivo que se esté empleando para hacerlo.

Asimismo, el organismo de investigación internacional Forrester estimó que el 80% de las infracciones de seguridad implican credenciales privilegiadas. Por otro lado, Gartner el otro organismo de investigación internacional, publicó que la gestión de cuentas privilegiadas debería de ser el primer proyecto que las organizaciones deben considerar para el 2019.

Por último, en un tratamiento de datos personales en entorno digital, otra de las problemáticas a las que se enfrentan los responsables y/o encargados es que carecen de medidas de seguridad implementadas que partan de los principios de "need to know", "least priviledge", no repudio, así como autorizar, autentificar y auditar a los usuarios "normales" y privilegiados[47].

¿cuándo se materializa una vulneración de datos personales, realmente los responsables están en posibilidades de contar con las evidencias suficientes y necesarias para delimitar responsabilidades?

Los controles tradicionales partían de una sensación falsa de seguridad, en virtud de que únicamente se preocupaban por aspectos perimetrales, es decir, se valían de proteger la red fuera de su perímetro y jamás se preocuparon por proteger la seguridad dentro del perímetro. En analogía, cuando construimos un casa, por lo que más nos preocupamos es que la barda este lo suficientemente alta, fuerte y reforzada para que los ladrones no se puedan meter a robar, así como la chapa del portón y en ocasiones se llegan a colocar hasta 2 chapas, y colocamos sistemas de videovigilancia alrededor de la casa, sin embargo, jamás nos preocupamos por contar con cerraduras en cada puerta de la casa y menos aún sistemas

[47] Garriga Dominguez, A. (2009). Tratamiento de Datos Personales y Derechos Fundamentales. Madrid : Dykinson.

de videovigilancia que monitoreen dentro de la casa, en cada habitación, en ese sentido, en sistemas tradicionales de seguridad, es lo mismo, únicamente nos preocupamos por estar protegiéndonos de las amenazas del exterior, cuando realmente tendríamos que estar protegiéndonos de amenazas externas como internas, como es el caso de usuarios con excesivos privilegios y de los usuarios privilegiados.

En resumen, el tratamiento de datos personales en un entorno digital debe considerar una estrategia que tome aspectos de la seguridad de la información, a efecto de robustecer las medidas de seguridad técnicas establecidas el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, porque la seguridad de los datos personales tradicionales ya no es suficiente para los negocios modernos de hoy. En un entorno empresarial ágil el cual está cada vez más expuesto a amenazas sofisticadas y de alto impacto, la protección de datos personales se debe basar no solamente en aspectos reactivos, sino en aspectos preventivos, de detección, analíticos y predictivos.

La propuesta del sustentante es que se establezca una estrategia de seguridad basada en todo el ciclo de vida del dato personal, reforzando en cada fase aspectos de la seguridad de la información como:

1. Confidencialidad
2. Integridad
3. Disponibilidad
4. "Need to know"
5. "Least priviledge"
6. Autorización, autenticación y auditoría
7. No repudio.

Lo anterior, en aras de que el tratamiento de datos personales se encuentre lo más seguro posible y que en caso de que se materialice una vulneración

de datos personales, se cuenta con la evidencia jurídica-tecnológica necesaria para determinar responsabilidades y acciones legales a seguir.

4.2. Propuesta de reforma al marco jurídico.

Es un hecho, como ya se ha señalado, de manera global se ha incrementado los avances de las tecnologías de la información y comunicación; obviamente tal acontecimiento ha impactado de manera determinante a varias actividades como el comercio, las educativas, financieras y otras más en las que se da todo el ciclo de vida del dato personal, y se ha puesto de manifiesto las vulnerabilidades con las que se cuentan los entornos digitales y por ende el efecto nocivo que muchas veces ha ocasionado el desarrollo de la tecnología.

Tales circunstancias han hecho imperiosa la necesidad de tomar medidas, para lograr una debida protección y seguridad de los datos personales de los que se realiza un tratamiento; debiendo señalar que también se ha hecho urgente tal necesidad, debido a que, paralelo al avance de la tecnología, igualmente ha crecido la inseguridad, misma que es ocasionada por individuos o grupos delictuosos quienes por cualquier medio obtienen información personal, y a través de la intimidación, la materialización de delitos como robo de identidad, fraude electrónico, entre otros, afectan directamente a los titulares[48].

Todo lo analizado en el cuerpo de este trabajo nos lleva a concluir que la ley citada, no cuenta con las medidas de seguridad suficientes para garantizar el adecuado tratamiento de datos personales en cuanto a la obtención, uso y acceso de estos en entornos digitales, pues como se ha mencionado en repetidas ocasiones, los negocios que vivimos en 2019 están

[48] Muñoz Torres, I. (2009). Delitos Informáticos Diez Años desupúes. México : UBIJUS Editorial .

basados en entornos digitales, desapareciendo poco a poco el tratamiento de datos personales de manera física (papel).

Por ello, uno de los motivos que se persiguen con el presente trabajo de investigación, es el de aumentar los niveles mínimos necesarios para contar con sistemas de tratamiento que resulten suficientes para garantizar todo el ciclo de vida del dato personal.

Por tanto, los responsables y/o encargados deben partir de un análisis del giro de la empresa, de la infraestructura que se cuenta, y las personas que realizan o realizarán un manejo de los datos personales, a efecto de que, del resultado de dicho análisis, estén en posibilidades de empezar a mapear el ciclo de vida del dato personal y poder determinar que controles se aplicarán en cada fase, en esta investigación se ahondarán únicamente los puntos de obtención, uso y acceso, porque a consideración del sustentante son los puntos más vulnerables que la legislación cuenta al día de hoy.

Se propone reformar el artículo 2 fracciones VI y VII, a efecto de que se robustezcan las medidas de seguridad físicas y técnicas, partiendo de que la gran mayoría del tratamiento de datos personales en la actualidad, están basados en entornos digitales, en consecuencia, la legislación en esta materia debe estar en una constante evolución logrando minimizar las brechas de seguridad y evitando dejar pase libre para los cibercriminales.

Analizaremos las fases de obtención, uso y acceso como partes del ciclo de vida del dato personal con el objetivo de establecer los criterios mínimos que se deben considerar para lograr una efectiva seguridad jurídica basada en principios informáticos.

4.2.1. OBTENCIÓN DE DATOS PERSONALES.

La obtención de datos personales es el primer punto de partida, sin la obtención de estos y por ende sin el consentimiento de los titulares, no se podría dar un tratamiento. Por principio de cuentas la Ley establece la obtención de los datos personales bajo el principio del consentimiento, plasmado en sus artículos 7, 8 y 9 que a la letra dicen[49]:

> "***Artículo 7.-*** *Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta Ley y demás normatividad aplicable.*
>
> *La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos.*
>
> *En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley.*
>
> ***Artículo 8.-*** *Todo tratamiento de datos personales estará sujeto al consentimiento de su titular, salvo las excepciones previstas por la presente Ley.*
>
> *El consentimiento será expreso cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos.*

[49] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Op. Cit.

Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición.

Los datos financieros o patrimoniales requerirán el consentimiento expreso de su titular, salvo las excepciones a que se refieren los artículos 10 y 37 de la presente Ley.

El consentimiento podrá ser revocado en cualquier momento sin que se le atribuyan efectos retroactivos. Para revocar el consentimiento, el responsable deberá, en el aviso de privacidad, establecer los mecanismos y procedimientos para ello.

***Artículo 9.-** Tratándose de datos personales sensibles, el responsable deberá obtener el consentimiento expreso y por escrito del titular para su tratamiento, a través de su firma autógrafa, firma electrónica, o cualquier mecanismo de autenticación que al efecto se establezca.*

No podrán crearse bases de datos que contengan datos personales sensibles, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos que persigue el sujeto regulado."

Aunado a lo anterior, el Reglamento de la Ley en sus artículos 11, 12, 13, 14, 15 y 16 habla del consentimiento y sus características, sin embargo, existen 2 puntos principales que debemos considerar:

- Consentimiento tácito
  Cuando habiéndose puesto a disposición el aviso de privacidad, no manifieste su oposición.

- Consentimiento expreso

  "Cuando la voluntad se manifieste verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos"

  Y el consentimiento expreso es obligatorio cuándo se realizará datos personales sensibles, así como los financieros o patrimoniales.

¿Cómo se puede manifestar nuestro consentimiento en entornos digitales?

Hoy en día, existen 2 tipos de consentimientos que se utilizan en entornos digitales, especialmente en Internet, el primero de ellos sería ***browse wrap*** utilizado especialmente para el consentimiento tácito, qué se materializa cuándo el titular de datos personales navega por internet; y ***click wrap,*** es utilizado para el consentimiento expreso, y se materializa en dos opciones para consentir, la primera de ellas es cuándo hacemos clic para no aceptar *Opt-out;* y la segunda de ellas, es cuando hacemos clic para aceptar *Opt-in.*

Y a manera de ejemplo, en la figura 2 podemos visualizar los diferentes tipos de consentimientos en internet.

Figura 2 Ejemplo de formas de concentimiento en una página web

Sin embargo, ¿debemos considerar como aceptable la práctica de Opt-In y/u Opt-Out como signos inequívocos para la manifestación de la voluntad de los titulares?

Al analizar la conducta inmediata anterior, debemos de partir del supuesto en el que Carlos Calderón, titular de datos personales desea realizar una compra en Amazon, de esa forma, se le requerirán datos personales sensibles, tales como nombre, domicilio, número de tarjeta bancaria, fecha de vencimiento de la tarjeta y el código de seguridad, por lo cual desde el momento en el que el titular de los datos ingresó a Amazon para realizar una búsqueda del artículo que desea comprar, se podría tomar como la manifestación de su voluntad y a su vez el consentimiento expreso que exige la multicitada ley, sin embargo, el sustentante considera que no es suficiente dicha exteriorización de la voluntad del titular, en virtud de que no existen mecanismos suficientes para garantizar que el titular este

exteriorizando su voluntad y menos aún que realmente sea el titular. Si dicho Titular, fue víctima de un robo de identidad, Amazon, ¿cómo se aseguraría de que el que hizo la compra, no fue el criminal que usurpó la identidad del titular?

Conductas como las anteriores, es decir, al realizar una obtención de datos personales sensibles en entornos digitales, de manera exprofesa los responsables y/o encargados deberían de efectuar más pasos de autentificación, a través del concepto conocido como múltiple factor de autenticación, dónde al titular se le realiza una serie de pasos para autentificar que realmente sea quien dice ser.

Una vez que una persona ha sido identificada a través de la identificación de usuario o un valor similar, debe ser autentificada, lo cual significa que debe demostrar que es quien dice ser. Se pueden usar tres factores generales para la autenticación: *algo que sabes, algo que tienes, y algo que eres.*

Algo que sabes puede ser, por ejemplo, una contraseña, un PIN, el nombre de la madre o la combinación de un candado. El inconveniente de este método es que otra persona puede adquirir estos conocimientos y obtener acceso no autorizado a un recurso.

Algo que tienes puede ser, una llave, tarjeta magnética, tarjeta de acceso, una credencial o un token. Este método es común para acceder a las instalaciones, pero también podría usarse para acceder a áreas sensibles o para autenticar sistemas; en ese tenor una de las desventajas de este método es que el artículo puede ser perdido o robado, lo cual podría resultar en un acceso no autorizado.

Algo que eres, se vuelve un poco más interesante, porque esto no se basa si la persona es judía, marciana o chichimeca, sino se basa en un

atributo físico, la autenticación de la identidad de una persona basada en un atributo físico único se conoce como biometría.

La autenticación segura contiene dos de estos tres métodos, el uso de un sistema biométrico por sí solo no proporciona una autenticación sólida porque proporciona solo uno de los tres métodos; la biometría proporciona lo que una persona es, no aquello que una persona sabe o tiene, para que in proceso de autenticación de cadenas esté en su lugar, un sistema biométrico debe estar al menos acoplado con un mecanismo que verifique uno de los otros dos métodos, por ejemplo, muchas veces la persona tiene que escribir un número de PIN en un teclado número antes de que se realice el escaneo biométrico, esto satisface la categoría "algo que sabe", a la inversa, se podría requerir que la persona pase una tarjeta magnética a través de un lector antes de la exploración biométrica, esto satisfaría la posesión de la persona, sea cual sea el sistema de identificación que se use, para que la autenticación fuerte esté en el proceso debe incluir al menos dos de las tres categorías.

En ese orden de ideas, los responsables y/o encargados deben tomar en consideración, es la implementación de múltiples factores de autenticación, al momento de que el titular de los datos personales exteriorice su consentimiento. A raíz de lo anterior se reduciría en gran cantidad el robo de identidad y el fraude electrónico.

Finalmente, retomando el supuesto en el que Carlos Calderón desea realizar la compra de un artículo en Amazon, y partiendo de que Amazon contará con un múltiple factor de autenticación, Amazon se aseguraría de que efectivamente soy Carlos Calderón y está exteriorizando su voluntad de consentir el acto de comercio; y a su vez, Carlos Calderón tiene la certeza de que si llegará a sufrir la pérdida de una credencial o un robo de su equipo móvil, no podrán hacer uso de su identidad en Amazon.

4.2.2. USO DE DATOS PERSONALES

El uso de datos personales en una organización, para el sustentante es uno de los puntos más importantes en todo el ciclo de vida de estos; que los usuarios que usan los datos personales se vuelven críticos para los responsables y/o encargados, en virtud de que dichos usuarios pueden hacer un mal uso, extendiéndose el mal uso a la pérdida de la confidencialidad, integridad y disponibilidad de ellos.

Antes de entrar de fondo a este punto, debemos de analizar el principio de finalidad establecido en la Ley y su Reglamento, porque el uso está estrechamente ligado con las finalidades que se encuentran plasmadas en el Aviso de Privacidad, y para las cuales se recabaron dichos datos personales.

> **Artículo 40.-** Los datos personales sólo podrán ser tratados para el cumplimiento de la finalidad o finalidades establecidas en el aviso de privacidad, en términos del artículo 12 de la Ley.
>
> Para efectos del párrafo anterior, la finalidad o las finalidades establecidas en el aviso de privacidad deberán ser determinadas, lo cual se logra cuando con claridad, sin lugar a confusión y de manera objetiva se especifica para qué objeto serán tratados los datos personales.

El artículo en cita comienza que los datos personales únicamente podrán ser tratados conforme a las finalidades descritas en el Aviso de Privacidad; bajo el supuesto de que una de las finalidades descritas en el Aviso de Privacidad, es el pago de nómina de los trabajadores de Amazon; por lo cual el área de recursos humanos, se podría considerar critica, sí solo sí, no se cuenta con los controles de seguridad suficientes y necesarios para

que dichos individuos, operen conforme a sus funciones. Si bien es cierto que el artículo 2 fracción VII inciso a) y b) del Reglamento establece que el acceso a base de datos lógicas sea por usuarios identificados y autorizados y que el acceso sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones, también es cierto que dichos usuarios requieren un acceso con múltiple factor de autenticación, así como que sean auditados y cumplan con el principio de la seguridad de la información, no repudio.

Partiendo de los últimos 2 supuestos del párrafo anterior, es que, en temas de seguridad de la información, existen un control llamado "AAA", Autenticación, Autorización y Auditoría, tanto de usuarios privilegiados y normales. Asimismo, el principio de no repudio que, en términos generales, es garantizar las identidades de los actores en una transacción o mensaje, emisor y receptor no podrán negar haber enviado o recibido dicha transacción y/o mensaje. Sin embargo, entraremos a más detalle, fundamentando el por qué es necesario estos controles en la regulación y en el ciclo de vida de los datos personales.

Derivado de lo anterior, es que los responsables y/o encargados deben implementar herramientas de auditoría, porque son controles técnicos que rastrean la actividad de red o en una computadora específica (quien maneja la base de datos de nómina, por ejemplo); aunque la auditoría no es una actividad que le negará a una entidad el acceso a una red o computadora, hará un seguimiento de las actividades para que el administrador de la red pueda comprender el tipo de acceso que tuvo lugar, identificar una brecha de seguridad o advertir al administrador de actividades sospechosas. Esta información se puede usar para señalar las debilidades de otros controles técnicos y ayudar al administrador a comprender dónde se deben hacer los cambios para preservar el nivel de seguridad necesario dentro del entrono digital.

Las capacidades de auditoría es asegurar que los usuarios sean responsables de sus acciones, verifiquen que las políticas de seguridad se apliquen y puedan usarse como herramientas de investigación, en consecuencia existen varias razones por las cuales los responsables y/o encargados deben asegurarse de que los mecanismos de responsabilidad estén en su lugar y configurarlos correctamente: para poder rastrear las malas acciones de los individuos, detectar intrusiones, reconstruir eventos y condiciones del sistema, proporcionar evidencias para la toma de decisiones en cuestiones legales.

El seguimiento de la responsabilidad se realiza mediante el registro de las actividades del usuario, del sistema y de los aplicativos, esta grabación se realiza a través de funciones y mecanismos de auditoría dentro de un sistema operativo o aplicativo, las pistas de auditoría contienen información sobre las actividades del sistema operativo, los eventos del aplicativo y las acciones del usuario. El cable del camino de auditoría se usa para verificar el estado de un sistema al verificar la información de rendimiento o ciertos tipos de errores y condiciones. Después de que un sistema falla, un administrador de red a menudo revisará los "logs" de auditoría para tratar de reconstruir el estado del sistema e intentar comprender qué eventos podrían atribuirse a la interrupción, en ese sentido, las pistas de auditoría también se pueden utilizar para proporcionar alertas sobre cualquier actividad sospechosa que se pueda investigar en un momento posterior, además, pueden ser valiosos para determinar exactamente hasta dónde ha ido un ataque y la magnitud del daño que pudo haber causado, es importante asegurarse de que mantenga una cadena de custodia adecuada para garantizar que los datos recopilados puedan ser representados de manera adecuada y precisa en caso de que deban utilizarse para eventos posteriores, tales como investigaciones para delimitar responsabilidades de carácter civil, administrativo y/o penal.

A manera de ejemplo, si un intruso irrumpe en su casa, hará todo lo posible para cubrir sus huellas al no dejar huellas dactilares o ninguna otra pista que pueda usarse para vincularlo a la actividad criminal, lo mismo ocurre en el entorno digital donde residen los datos personales, el intruso hará todo lo posible para cubrir sus huellas, porque a menudo eliminan los "logs" de auditoría que contienen esta información incriminatoria.

De lo anterior da lugar a que sólo ciertos individuos (el administrador y personal de seguridad) deban ser capaces de ver, modificar y borrar información de logs de auditoría y no todos los individuos, debido a que se tiene que garantizar la integridad de los logs con el uso de firmas digitales, herramientas de *hashing* y controles de acceso (múltiple factor de autenticación).

Los logs de auditoría se vuelven parte fundamental para la delimitación de responsabilidades al momento de que se materialice una vulneración a los datos personales, ya que son datos de prueba para la culpabilidad o no de un individuo, y la demostración de cómo un ataque se llevó a cabo. Al hacer un análisis en conjunto de los puntos de Auditoría, Autenticación y No repudio, se podría determinar que son medidas de seguridad que resultan necesarias para el tratamiento de datos personales, en virtud de que al momento de materializarse una vulneración de datos personales, las organizaciones estén en posibilidades de poder determinar cómo se llevó a cabo el ataque y quién es responsable del ataque o bien, simplemente quién uso de manera inadecuada los datos personales, alterando su confidencialidad, integridad y disponibilidad.

4.2.3. ACCESO A LOS DATOS PERSONALES

Un punto de suma importancia en el ciclo de vida del dato personal es el acceso a las bases de datos en entornos digitales, en virtud de que, si un

usuario no tiene acceso, no puede comprometer la confidencialidad, disponibilidad e integridad de estos, o bien, si un atacante accede a dicha base de datos, podría realizar prácticamente cualquier acción que desee.

En el mismo tenor, retomando los conceptos que se han mencionado en los 2 puntos que anteceden, el acceso debe ser implementado también con controles eficientes que garanticen que quien acceda, es quien diga ser, que no pueda negar haber realizado acciones y se esté en posibilidades de contar con los logs de auditoría para verificar sus acciones.

Partiendo una vez más, en dos supuestos, el primero de ellos es respecto a lo concerniente a los usuarios; a que estos deberían de contar con el acceso a lo mínimo necesario para poder operar sus funciones y tener los mínimos privilegios respecto a los activos que operara, aunado a que al momento de acceder cuente con factores de múltiple autenticación y no repudio. Y el segundo supuesto es para los super usuarios, en virtud de que ellos, por la naturaleza de sus funciones, pueden realizar acciones de lectura, modificación, creación y eliminación, por lo cual ellos además de los 2 controles mencionados para los usuarios, deben contar con el control implementado de auditoría, a efecto de que los responsables y/o encargados cuenten con registros de los logs de dichos usuarios, para determinar responsabilidades en caso de alguna eventualidad.

Asimismo, y retomando el punto que se platicó en líneas anteriores, es que tanto los titulares de datos personales deban de contar con un múltiple factor de autenticación al querer hacer una compra en línea, como se expuso a manera de ejemplo; también es que los empleados de una organización que manejen los datos personales de sus clientes deban de contar con un múltiple factor de autenticación. Una vez que una persona ha sido identificada a través de la identificación de usuario o un valor similar, debe ser autentificada, lo cual significa que debe demostrar que es quien

dice ser. Se pueden usar tres factores generales para la autenticación: *algo que sabes, algo que tienes, y algo que eres.* Y también se denominan comúnmente autenticación por conocimiento, autenticación por propiedad y autenticación por característica.

Y como se cexplicó en la página 89 de la presente investigación, el múltiple factor de autenticación, se puede utilizar para identificar a la persona, sin embargo, pars este punto también deberíamos de considerar que no solo se debe de identificar, sino también autenticar a efecto de que quiera acceder a una base de datos, es por eso que debemos de contemplar el múltiple factor de autenticación para estos 2 rubros mencionados.

CONCLUSIONES.

La protección de datos personales en un ámbito digital se ha vuelto una problemática para el sector empresarial, en virtud de que las organizaciones visualizan un gasto innecesario, lejos de verlo como una inversión. Sin embargo, la historia nos sirve para aprender y analizar las cuestiones que se han suscitado en materia de protección de datos personales, y por ende prevenir posibles escenarios en el presente y/o futuro, tras lo cual hoy no podemos no estar preparados ante un incidente de seguridad de datos personales, como se ha mencionado, contamos con avances tecnológicos que nos pueden permitir poder empezar a minimizar la brecha de seguridad existente.

PRIMERA.- La historia, en general, nos sirve a manera de aprendizaje en todos los aspectos desde todas las perspectivas; esto nos conlleva a analizar lo sucedido en el Holocausto, lamentablemente fue un genocidio por una ideología racista de un tirano con poder; sin embargo, una realidad es que el Holocausto tuvo éxito gracias a una base de datos que hoy se consideran personales. Es por ello, a partir de este suceso trágico, se crearon organizaciones de índole internacional, en pro de las personas sin importar género, raza, descendencia o creencias religiosas y que al día de hoy contamos con regulaciones locales e internacionales que promueven y obligan la protección de datos personales en todo el mundo.

SEGUNDA.- En el mundo, si bien es cierto que ya contamos con regulaciones que promueven y obligan la protección de datos personales, también es cierto que la tecnología ha avanzado de manera vertiginosa, y en especial en el campo de la informática; lo cual ha venido a influir de manera determinante son las tecnologías de la información y comunicación, afectando la privacidad de las personas y la seguridad de sus datos personales en entornos digitales, en virtud de que vivimos en un mundo en

dónde el intercambio comercial, cultural, educativo, por mencionar algunos, se ha vuelto tan ágil, que en cuestiones de segundos podemos estar realizando estos intercambios con cualquier parte del mundo y que hasta cierto punto se ha ponderado más el intercambio instantáneo, que la privacidad de las personas y el aseguramiento de sus datos personales en los intercambios. Ante este reto, las Autoridades mexicanas, deben de preocuparse por contar con una política que esté basada en menos burocracia y mayor adaptación de las regulaciones a las necesidades y cambios que presenta la tecnología.

TERCERA.- Actualmente la protección de datos personales es un ecosistema corresponsable, en virtud de que las distintas directrices, reglamentos y leyes internacionales, así como la legislación en México, parte en dos grandes rubros: el primero de ellos, es evidentemente que los responsables y/o encargados del tratamiento de datos personales cuenten con medidas de seguridad que minimicen las brechas de seguridad para otorgar a los titulares un nivel de certeza de seguridad jurídica de que sus datos están siendo tratados adecuadamente; y el segundo y no menos importante, es que lo titulares tengan un control de sus datos, es decir, ¿cómo? ¿dónde? ¿cuándo? Y ¿por qué? deben de otorgar sus datos personales a las organizaciones, pero este punto es dónde la cultura ha ido creciendo paulatinamente y no se ha logrado el fin por el cual se creó la Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento. Y aunado a esta problemática, está el crecimiento vertiginoso de las tecnologías de la información y comunicación es por eso, que las leyes deben velar por los intereses de los titulares, tengan o no una cultura de esta materia, obligando a los responsables y/encargados al implementar mayores controles de seguridad, porque no se puede controlar, aquello que no se puede ver.

CUARTA.- Los responsables y/o encargados si bien es cierto que sus líneas de negocio no lo son el tener pleno conocimiento de la materia que nos ocupa, también es cierto que deben de contar con áreas que soporten estás líneas de negocio, porque al no contar con un soporte integral de áreas como tecnologías de la información, recursos humanos, sistemas y evidentemente legal, las organizaciones están en un riesgo bastante alto de que sufran un impacto económico y/o reputacional. Las organizaciones deben de hacer de la protección de datos personales una práctica común dentro de su compañía, adoptando en la medida de sus posibilidades controles para contar con una certeza jurídica en caso de que se materialice una vulneración de datos personales y lograr minimizar el impacto económico y reputacional.

QUINTA.- Para que la aplicación del derecho a la protección de datos personales en México sea lo más exitoso posible deben intervenir diferentes factores: una modernización en nuestras normas jurídicas que estén a la vanguardia de los desarrollos tecnológicos, y por ende que exista una congruencia legislativa entre la informática y el derecho; un órgano garante sancionador; ética profesional de quienes trabajan directamente con los datos; y finalmente una corresponsabilidad de todos los actores involucrados. De esta manera podrá lograrse la armonía necesaria para que los diversos sectores realicen sus actividades dentro del marco de la protección del derecho a la protección de datos personales.

SEXTA.- Las medidas de seguridad plasmadas en el principio de responsabilidad y el deber de seguridad, resultan insuficientes, en razón de que como se ha mencionado en repetidas ocasiones, el sector empresarial se afronta a crímenes mucho más sofisticados, y de los que tienen la responsabilidad de estar preparados para cualquier eventualidad, por lo cual hasta en tanto no se cuente con una modificación al Reglamento, los responsables y/o encargados deben valerse de estándares, mejores

prácticas y esquemas de autorregulación. Así como, dejar de ver la protección de datos personales como una materia de esfuerzos aislados, debemos de unir conocimientos técnicos (informáticos) y sociales (derecho). En medida de que minimicemos la brecha de seguridad existente del bien jurídico tutelado en entornos digitales, menor será el riesgo latente día a día.

Los retos que afrontan todos los días el sector empresarial al tratar los datos personales en entornos digitales, es cada vez mayor. Consecuencia de lo anterior, es que debemos de crear conciencia y dejar de ver como un gasto la protección y empezar a visualizarlo como una inversión.

SÉPTIMA.- El conocimiento de los datos es esencial para verificar la recopilación y el procesamiento de datos personales. Si bien es cierto que se ha comentado que las tecnologías de la información y comunicación han puesto de cierta manera comprometida la privacidad y seguridad de las personas, también es cierto que debemos de valernos de estás tecnologías para poder contar con un mayor control respecto de los datos personales. Hoy en día las organizaciones tienen que realizar una trazabilidad de los datos personales que tratan, sin embargo, el o los encargados de realizar esta trazabilidad se valen de encuestas que les hacen a las personas que manejan los datos personales día a día, sin embargo, hoy en día no podemos confiar en dichas personas y no porque sean malintencionadas, simplemente porque el factor humano nos deja con muchos márgenes de error, como, por ejemplo, la memoria.

Aunado a lo anterior, cabe mencionar que las encuestas carecen de precisión, porque se basan en la interpretación y el recuerdo de las personas. En ese sentido, las personas son falibles e imprecisas en el mejor de los casos, pero cuando se trata de memorizar el inventario, la ubicación y el uso de los datos, son lo contrario de los conservadores de registros controlados por datos. Las personas simplemente no pueden "verificar" nada que ver con el

lugar donde se recopilan, almacenan o procesan los datos sin una auditoría de datos. Y, una auditoría de datos requiere una exploración, no una encuesta. Además, es prácticamente imposible que las personas puedan capturar los cambios de los datos personales en tiempo real.

Dicen que los datos son el nuevo petróleo. Y si bien esa metáfora es positivamente cierta cuando se trata de valor y cómo los datos impulsan la economía moderna de Internet, también lo es cuando se trata de cómo se filtra y fluye. En un entorno digital, los datos no son estáticos, se mueven se agregan, se transforman, se comparten y se analizan. A raíz de esto podemos concluir parcialmente que el cambio es la única constante en el tratamiento de datos personales. Desafortunadamente, ninguna persona puede proporcionar un informe completo de cómo cambian los datos sin realizar una auditoría primero, pero las organizaciones se encontrarían un paso atrás en la protección de sus datos personales.

La privacidad de los datos puede ser (debería ser) una preocupación corporativa, pero la información sobre los datos puede no ser una preocupación de todos los empleados. Hoy en día las organizaciones que realizan un mapeo de datos a través de encuestas (incluso suponiendo que el mejor de los casos el resultado sea representativo), puede extenderse fácilmente de semanas a meses y la inversión en tiempo, dinero y esfuerzo de las organizaciones pueden finalizar en resultados que afecten directa y proporcionalmente a sus objetivos[50].

Finalmente, podemos concluir que debemos de evolucionar respecto a la efectividad que tanto las organizaciones realizar la trazabilidad, inventario y mapeo de datos personales, como la legislación *per se* en virtud de que se tiene que volver exigible la forma de generar inventarios y mapas, a efecto

[50] Wright , D., & De Hert , P. (2016). Enforcing Privacy Regulatory, Legal and Technological Approaches . USA: Springer International Publishing Switzerland.

de que sea lo más precisos utilizando escaneos de datos personales en toda su infraestructura y que sean auditables. Ya que uno de los objetivos principales de la Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento es la adecuada protección de datos personales.

Un principio bien entendido en el mundo de la seguridad de la información es que no puedes proteger lo que no puedes encontrar. Debido a que las consideraciones de privacidad son cada vez más importantes para la forma en que las organizaciones recopilan y procesan los datos, es evidente que un principio similar se aplica a la protección de los datos personales; no pueden proteger los datos personales si no puede encontrarlos primero. Y con las grandes brechas existentes de los datos personales que se han sabido los últimos años, ese aforismo nunca ha sido más cierto. Para proteger los datos personales, primero debe determinar dónde residen los datos de cada persona. Encontrar datos en una organización nunca ha sido una tarea fácil, tan es así que fue difícil cuando los datos se limitaban en gran medida a bases de datos relacionales, archivos compartidos, correo electrónico y mainframes. Ahora es más difícil con la proliferación de todo tipo de nuevos y grandes almacenes de datos, SaaS, IaaS y todo tipo de sistemas de contenido distribuidos tanto en el centro de datos como en la nube. Peor aún, la dificultad del descubrimiento se ha hecho más difícil por la necesidad de no solo encontrar los datos personales identificados, sino también de la información más amplia los datos personales identificables, donde lo definitorio de la información personal no es absoluto sino relativo. La incapacidad de entender el contexto de identidad como un componente integral del descubrimiento de datos ha limitado la aplicabilidad de las herramientas de descubrimiento de datos de ayer a los desafíos de privacidad de hoy. Hoy en día contamos con tecnologías que han adoptado un enfoque fundamentalmente diferente para el descubrimiento de datos,

arraigado en machine learning y la inteligencia de identidad para desarrollar un enfoque centrado en las personas para encontrar y comprender los datos porque la privacidad se basa fundamentalmente en la protección de los datos de una persona.

Finalmente, la estrategia jurídica – tecnológica que se propone está en qué las organizaciones sepan que datos personales manejan y cuál es su flujo dentro de la organización; que cuenten con un múltiple factor de autenticación en todos lados y a todos sus usuarios; y contar con controles tecnológicos que les permitan autorizar, auditar y que no repudien sus acciones. Que todo esto, ayudará al Sistema de Gestión de Seguridad de Datos Personales que hoy en día promueve el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, a través de sus Esquemas de Autorregulación.

FUENTES CONSULTADAS

LIBROS

Alpaydin, E. (2016*) Machine Learning: The New AI*. MIT Press.

Dempsey , T., & Rosenquist , M. (2015). *Navigating the Digital Age: The Definitive Cybersecurity Guide for Directors and Officers*. Chicago: Caxton Business & Legal, Inc.

Densmore, R. (2013). *Privacy Program Management Tools for Managing Privacy Within your organization*. New Hampshire: International Association of Privacy Proffesionals.

Garriga Dominguez , A. (2009). *Tratamiento de Datos Personales y Derechos Fundamentales*. Madrid: Dykinson.

Goldberg, Ian, David Wagner, Eric A. Brewer, "Privacy-Enhancing Technologies for the Internet", IEEE COMPCON ´97, Febrero 1997.

Marco, I. S. (2013). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento*. México: THEMIS.

Muñoz Torres, I. (2009). *Delitos Informáticos Diez Años desupúes*. México: UBIJUS Editorial.

Perdiguero Jiménez, M. Á. (2018). *Nueva Normativa Europea sobre Protección de Datos. Delegado de Protección de Datos*. Málaga: IC Editorial.

Sanz Salguero, Francisco Javier. (2016). *Relación entre la protección de los datos personales y el derecho de acceso a la información pública dentro del marco del derecho comparado*. Ius et Praxis, 22(1), 323-376.

Stevens, E. (2014). *Privacy in Technology Standars and Practices for engineers and security and IT Professionals* . New Hampshire : International Association of Privacy Professionals.

Valdés, J. T. (2009). *Derecho Informático*. México: McGRAW-HILL/INTERAMERICANA EDITORES, S.A. DE C.V.

Wright , D., & De Hert , P. (2016). *Enforcing Privacy Regulatory, Legal and Technological Approaches*. USA: Springer International Publishing Switzerland.

FUENTES ELECTRÓNICAS

APEC (2005) MARCO DE PRIVACIDAD DEL FORO DE COOPERACIÓN ECONÓMICA ASIA PACÍFICO (APEC). Recuperado de: https://sellosdeconfianza.org.mx/docs/marco_de_privacidad_APEC.pdf

Carbonell, M. (2015) El Derecho a la Privacidad en la era digital. Recuperado de: http://www.miguelcarbonell.com/docencia/El_Derecho_a_la_Privacidad_en_la_era_digital.shtml

Consejo de la Unión Europea. (2016) Reglamento General de Datos Personales de la Unión Europea. Recuperado de: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32016R0679

Forrester (2019) Recuperado de: www.forrester.com

OCDE (2016) Principios de Gobierno Corporativo de la OCDE. Recuperado de: https://www.oecd.org/daf/ca/corporategovernanceprinciples/37191543.pdf

ONU (1976) Pacto Internacional de Derechos Civiles y Políticos. Recuperado de: https://www.ohchr.org/SP/Professionalinterest/Pages/CCPR.aspx

ONU (2015) DECLARACIÓN UNIVERSAL DE DERECHOS HUMANOS. Recuperado de: https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf

Prefaneta – Rodríguez, Javier, ***Protección de datos de carácter personal e Internet,*** *[*En línea]: Artículos doctrinales: Derecho Informático, agosto 2002. Recuperado de: http://noticias.juridicas.com/areas/20-Derecho%Inform%E1tico/10-Art%Edculos/200208-5556153161023211 1.hmtl#foot11

Harris, Shon. (2013). *CISSP Examen Guide Sixth Edition.* U.S.A: MacGraw-Hill.

Museo Memoria y Tolerancia (2019) El Holocausto. Recuperado de: https://www.myt.org.mx/memoria/holocausto

LEGISLACIÓN

Constitución Política de los Estados Unidos Mexicanos.

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

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

Lineamientos del Aviso de Privacidad

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

Reglamento General de Datos Personales.

Parámetros de Autorregulación en Materia de Protección de Datos Personales.