MDTIC

MAESTRÍA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

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

DIRECCIÓN ADJUNTA DE INNOVACIÓN Y CONOCIMIENTO
GERENCIA DE CAPITAL HUMANO
POSGRADOS

Incorporación de acciones preventivas para el fortalecimiento del deber de seguridad de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

SOLUCIÓN ESTRATÉGICA
Que para obtener el grado de MAESTRA EN DERECHO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Presenta:

Grace Carolina Conde López

Asesor:

Dr. Jesús Manuel Niebla Zatarain

Ciudad de México, mayo 2023

CONACYT

INFOTEC POSGRADOS

GOBIERNO DE MÉXICO | CONAHCYT CONSEJO NACIONAL DE HUMANIDADES CIENCIAS Y TECNOLOGÍAS | INFOTEC

AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

Maestría en Derecho de las Tecnologías de Información y Comunicación (MDTIC)

Ciudad de México, 11 de mayo de 2023

Unidad de Posgrados
PRESENTE

Por medio de la presente se hace constar que el trabajo de titulación

"Incorporación de acciones preventivas para el fortalecimiento del deber de seguridad de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares"

Desarrollado por la alumna: **Grace Carolina Conde López**, y bajo la asesoría del **Dr. Jesús Manuel Niebla Zatarain** cumple con el formato de Biblioteca. Por lo cual, se expide la presente autorización para impresión del proyecto terminal al que se ha hecho mención. Asimismo, se hace constar que no adeuda materiales de la biblioteca de INFOTEC.

No omito mencionar, que se deberá anexar la presente autorización al inicio de la versión impresa del trabajo referido, con el fin de amparar la misma.

Sin más por el momento, aprovecho la ocasión para enviar un cordial saludo.

Mtro. Carlos Josué Lavandeira Portillo
Director Adjunto de Innovación y Conocimiento

CJLP/jah

C.c.p. Felipe Alfonso Delgado Castillo.- Gerente de Capital Humano.- Para su conocimiento
Grace Carolina Conde López.- Alumna de la Maestría en Derecho de las Tecnologías de Información y Comunicación.- Para su conocimiento

Agradecimientos

A todas y todos quienes me acompañaron
durante el largo proceso de redacción de
mi trabajo de investigación.

Gracias

Tabla de contenido

Índice de cuadros

Siglas y abreviaturas

ARCO Acceso, Rectificación, Cancelación y Oposición

ANPD Autoridad Nacional de Protección de Datos Personales (Brasil)

GDPR Reglamento General de Protección de Datos (Europa)

INAI Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (México)

LFPDPPP Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México)

LGPD Ley General de Protección de Datos Personales (Brasil)

Introducción

En las últimas décadas, el uso de tecnologías de la información ha potencializado la utilización de datos personales en todos los aspectos de la vida en sociedad, sea para acceder a servicios, adquirir productos o simplemente comunicarse. Se puede decir que los datos hoy son un activo igual de importante que el dinero.

Hoy las empresas recaban, analizan y explotan más datos personales que nunca, dentro de una diversidad de sistemas de tratamiento y almacenamiento de datos, sean estos electrónicos o en la nube, los cuales debido a su naturaleza tecnológica se encuentran expuestos a vulnerabilidades y amenazas cuya materialización puede traducirse riesgos altos y desconocidos para los datos personales.

En este sentido, y desde un punto de vista jurídico, la adecuación de los marcos regulatorios en materia de privacidad y protección de datos se ha vuelto una tarea obligatoria para los órganos legislativos de los países alrededor del mundo, de forma que sean acordes a la realidad actual.

México no se quedó atrás, y hoy cuenta con un marco regulatorio de protección de datos para el sector público y privado, expedidos con la finalidad de regular el tratamiento legítimo de los datos, controlado e informado para garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.[1]

En lo que respecta al sector privado, el marco regulatorio está compuesto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, su Reglamento y distintos lineamientos en la materia. De ellos se desprenden

[1] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Diario Oficial de la Federación, 05 de julio 2010, México, art. 1.

diversas obligaciones impuestas a los responsables del tratamiento de los datos en materia de seguridad de la información, para evitar vulneraciones de seguridad que puedan afectar la integridad, confidencialidad y disponibilidad de los datos personales.

No obstante, ese conjunto de obligaciones resulta deficiente en virtud de que no propicia una protección preventiva frente a los riesgos por vulneraciones de seguridad que pueden ocurrir a los sistemas de tratamiento de los responsables.

Por lo dicho, el presente trabajo de investigación aporta una solución estratégica para una migración efectiva hacia un esquema preventivo de Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en lo que respecta al principio de responsabilidad y deber de seguridad.

La estructura del trabajo de investigación está compuesta de 3 capítulos. En el primero se abordan los aspectos generales sobre los datos personales para ofrecer un entendimiento integral respecto de su definición, clasificación y naturaleza jurídica, así como de su regulación en México.

El segundo capítulo aborda los aspectos relativos al deber de seguridad y las obligaciones que este conlleva con relación a los responsables del tratamiento. Se analiza cada una de ellas y se justifican las razones por las que se consideran insuficientes para garantizar una adecuada protección a los datos personales.

Asimismo, se contrastan los marcos regulatorios de protección de datos europeo y brasileño, que en la actualidad son los más robustos y protectores de los derechos de los titulares de los datos.

En el tercer y último capítulo, se ofrece la propuesta de solución estratégica, consistente en una reforma a diversos artículos de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, de tal manera que el deber de

seguridad transite de ser reactivo a ser preventivo, garantizando efectivamente el derecho a la protección de los datos personales.

Capítulo 1. Aspectos generales sobre los datos personales

Para definir lo que es un dato personal, primero se debe partir de la raíz etimológica de las palabras de su composición. Por un lado, dato viene del latino *datum* que significa lo que se da, y cuyo significado es "información sobre algo concreto que permite su conocimiento exacto o sirve para deducir las consecuencias derivadas de un hecho".[2]

Dato puede ser cualquier información que se desprenda de algún objeto o hecho, no es exclusivo para las personas y su información personal. Por otro lado, personal viene del latino *personalis* que significa "perteneciente o relativo a la persona".[3]

Tomando en consideración ambas definiciones, si el dato es aquello que describe o detalla algo, y personal es lo relativo a una persona, podemos concluir que el dato personal será cualquier información que permita el conocimiento exacto o sirva para deducir lo relativo a una persona determinada.

Ahora bien, conforme a la definición oficial contemplada en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares de México (en adelante LFPDPPP) el dato personal es "cualquier información concerniente a una persona física identificada o identificable"[4] , y para hacer referencia a esa persona física se establece el término "titular", este es, a quien corresponden los datos personales.

De manera similar, el Reglamento de la Unión Europea 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, conocido como Reglamento General de Protección de Datos Personales, (en

---

[2] Real Academia Española, "dato", en *Diccionario de la Lengua Española*, 23 edición, 2014, España. Recuperado de *https://dle.rae.es/dato?m=form*

[3] *Ibidem*, véase "personal".

[4] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Diario Oficial de la Federación, 05 de julio 2010, México, art. 3.

adelante RGPD) establece que los datos personales serán "…toda información sobre una persona física identificada o identificable".[5]

A diferencia de la LFPDPPP, el RGPD establece el término "interesado" para hacer referencia a la persona física identificable cuyos datos son objeto de protección, haciendo mayor énfasis en el cómo es que se puede determinar a dicha persona:

> *"Toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".*[6]

Como estas definiciones lo establecen, se considera dato personal a aquel relativo a una persona física, excluyendo a la información de las personas morales, puesto que estas no son titulares del derecho a la intimidad y a la vida privada.

De manera particular, el artículo 5 del reglamento de la LFPDPPP excluye de manera expresa la aplicabilidad de sus disposiciones para cuando se trata de información relativa a las personas morales. No obstante, dicha postura habría de modificarse, toda vez que la Suprema Corte de Justicia de la Nación determinó mediante la tesis P. II/2014 (10a.) que las personas morales sí tendrán derecho a la protección de los datos que puedan equipararse a los personales, aun cuando hayan sido entregados a una autoridad, en virtud de que:

> *El contenido de este derecho puede extenderse a cierta información de las personas jurídicas colectivas, en tanto que también cuentan con determinados espacios de protección ante cualquier intromisión*

---

[5] Reglamento 2016/679 del Parlamento Europeo y del Consejo, Diario Oficial de la Unión Europea, 27 de abril de 2016, art. 4**.**

[6] *Ídem*

arbitraria por parte de terceros respecto de cierta información económica, comercial o relativa a su identidad que, de revelarse, pudiera anular o menoscabar su libre y buen desarrollo.[7]

Esta determinación no implica que al hacer referencia a datos personales también se contemple la información de las personas morales, sino que está enfocada en garantizar la protección de la información durante su tratamiento, en cumplimiento de las disposiciones de la LFPDPPP y su reglamento.

Ahora que ya se tiene una definición clara sobre los datos personales, se abordará lo relativo a las distintas clasificaciones que se establecen en las leyes de México y la Unión Europea.

1.1 Clasificación de los datos personales

Existen distintas clasificaciones o categorías especiales para los datos personales, dependiendo el aspecto de la persona y su vida privada al que se hace referencia.

La principal clasificación es la que existe entre datos personales y datos personales sensibles.

1.2.1. Datos personales sensibles

En México la LFPDPPP establece en su artículo 4 que serán datos personales sensibles:

Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos datos que puedan revelar aspectos como origen

[7] P. II/2014 (10a.), Semanario judicial de la federación y su gaceta, Décima época, Libro 3, febrero de 2014, Tomo I, página 274.

racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual".[8]

La diferencia principal entre datos personales y datos personales sensibles radica en el nivel de privacidad y secrecía con que se protegen estos últimos, así como el nivel de dificultad para deducirlos, puesto que mientras que el titular decida no revelarlos, no existirá una fuente pública o privada desde donde se puedan obtener, a diferencia de los datos personales como el nombre, fecha de nacimiento, domicilio que se pueden encontrar en documentos oficiales, comprobantes de servicios, etcétera.

No obstante que la LFPDPPP prevé la categoría de datos personales sensibles, no contempla un catálogo de los datos que deberán ser considerados dentro de la misma, únicamente menciona algunos de manera enunciativa. Esto es así en virtud de la propia naturaleza de los datos sensibles, depende del contexto y consecuencias del tratamiento si un dato personal se considera dato personal sensible, con relación a si permitirá inferir información particularmente sensible de una persona.

La ausencia de un catálogo o listado de los datos personales que deben ser considerados como sensibles se traduce en una dificultad para los responsables del tratamiento al momento de dar cumplimiento a las disposiciones aplicables para este tipo de datos.

Por ejemplo, el artículo 9 de la LFPDPPP establece que, tratándose de datos personales sensibles, el responsable deberá de obtener el consentimiento expreso y por escrito del titular previo a su tratamiento.[9] Por otro lado, también se prohíbe la

[8] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *op. cit.,* art 3.

[9] *Ibidem*, art. 9.

creación de bases de datos sensibles sin que medie una justificación para finalidades legítimas.

Al no existir un catálogo de los datos sensibles, el responsable del tratamiento, que dentro de su desconocimiento recaba este tipo de datos de buena fe, pudiera incumplir con las disposiciones de la LFPDPPP sin siquiera estar consciente de ello.

Esto cobra relevancia al tomar en cuenta que, tratándose de datos sensibles, las penas previstas para el tratamiento indebido de datos personales se duplicarán, de conformidad con el artículo 69 de la LFPDPPP.

1.2.2. Datos genéticos

1.2.2.1 En la Unión Europea

Dentro del cuerpo normativo del RGPD se define a los datos genéticos como:

> *"Aquellos datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona".*[10]

Los datos genéticos serán aquellos que se obtienen a partir de una muestra biológica de la persona y sirven para determinar aspectos del origen o salud de esta, no siendo posible identificarlos o deducirlos a simple vista. Su carácter de especiales atiende a que estos pueden revelar predisposiciones genéticas de las personas, mismas que pudieran tener consecuencias no sólo para el titular de los datos sino para su descendencia.

Por otro lado, los datos genéticos pueden revelar información sobre la cultura de las personas, y en determinadas situaciones esto pudiera conllevar un riesgo

[10] Reglamento 2016/679 del Parlamento Europeo y del Consejo, *op. cit*., art. 4.

grave para su integridad o incluso pudieran ser los causantes de tratos discriminatorios.

Aunado a lo anterior, y tomando en consideración la importancia actual de los datos genéticos para el avance y desarrollo científico es que cobra relevancia la protección especial de la cual están dotados.

La utilización de los datos genéticos humanos se encuentra reglamentada por principios internacionales de derecho, como los que se adoptaron en la Declaración Internacional sobre los Datos Genéticos Humanos por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura en 2003.

Estos principios tienen el objetivo de velar por el respeto de la dignidad humana y la protección de los derechos humanos y las libertades fundamentales en la recolección, el tratamiento, la utilización y la conservación de las muestras biológicas, atendiendo a los imperativos de igualdad, justicia y solidaridad, y a la vez, prestando la debida consideración a la libertad de pensamiento y de expresión, comprendida la libertad de investigación.[11]

En el artículo quinto de esta Declaración se enuncian las finalidades bajo las cuales podrán ser recolectados, tratados, utilizados y conservados los datos genéticos:

> *i) diagnóstico y asistencia sanitaria, lo cual incluye la realización de pruebas de cribado y predictivas;*
>
> *ii) investigación médica y otras formas de investigación científica, comprendidos los estudios epidemiológicos, en especial los de genética de poblaciones, así como los estudios de carácter antropológico o arqueológico, que en lo sucesivo se designarán*

[11] UNESCO, Declaración Internacional sobre los Datos Genéticos Humanos, 16 de octubre 2013, Art. 1, *http://portal.unesco.org/es/ev.php-URL_ID=17720&URL_DO=DO_TOPIC&URL_SECTION=201.html*

colectivamente como "investigaciones médicas y científicas";

iii) medicina forense y procedimientos civiles o penales u otras actuaciones legales,

iv) cualesquiera otros fines compatibles con la Declaración Universal sobre el Genoma Humano y los Derechos Humanos y el derecho internacional relativo a los derechos humanos.[12]

Como se aprecia, las finalidades son limitativas y están encaminadas al desarrollo médico y científico, o bien, aquellas compatibles con otros instrumentos jurídicos que garanticen en igual medida el derecho a la protección de los datos genéticos de las personas.

Por otro lado, se tiene la Declaración Universal sobre el Genoma Humano y los Derechos Humanos adoptada en 1997, que fungió como antecedente para la Declaración Internacional sobre los Datos Genéticos Humanos. En ambas declaraciones se busca la prevalencia del respeto a los derechos humanos, libertades fundamentales y dignidad humana de los individuos, ante cualquier investigación científica, de igual manera se refuerza la necesidad de solicitar el consentimiento informado de las personas que ceden sus muestras biológicas, dejando en claro que se debe respetar el carácter único de cada persona.

1.2.2.2 En México

Los datos genéticos en el contexto mexicano encuadrarían como datos personales sensibles, puesto que conforme a la definición prevista en el artículo 4 de la LFPDPPP, los datos personales sensibles abarcan a los datos que pueden revelar el estado de salud presente o futuro.

[12] UNESCO, *op. cit.,* Art. 5.

1.2.3 Datos biométricos

1.2.3.1 En la Unión Europea

La definición proporcionada por el RGPD para los datos biométricos contempla:

> *Aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.* [13]

A partir de la definición proporcionada, se pueden distinguir dos categorías de datos biométricos, una será aquella que se refiere a las características físicas de la persona, como puede ser el rostro (reconocimiento facial), huellas dactilares, la retina, el iris, geometría de la mano, entre otros. Por otro lado, la segunda será aquella que se refiere al comportamiento o rasgos de la personalidad de la persona, como la voz, la escritura, la firma autógrafa, entre otros.

La particularidad de los datos biométricos es que permiten la identificación inequívoca de su titular. En ese orden de ideas, el RGPD establece que los datos biométricos sólo podrán usarse de manera adecuada, pertinente y no excesiva, lo cual supone una estricta valoración de la necesidad y proporcionalidad de los datos tratados.[14]

Se considera que la protección especial que tienen los datos biométricos es totalmente justificada, en virtud de la sensibilidad de dicha información y de los riegos que pudieran implicar a los titulares en caso de una revelación o tratamiento

[13] Reglamento 2016/679 del Parlamento Europeo y del Consejo, *op. cit*., art.4.

[14] Grupo de Trabajo del art 29, WP 80 Documentos de trabajo sobre biometría, agosto 2003, p.8.

no autorizados. El hecho de que sean unívocos requiere de un mayor nivel de seguridad para garantizar su protección.

1.2.3.2 En México

Si bien los datos biométricos no se encuentran señalados de manera expresa en la LFPDPPP, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (en adelante INAI) ha publicado una guía para el tratamiento de datos biométricos en donde se aborda el tratamiento al que se encuentran sujetos.

La guía retoma la definición de datos biométricos que estableció el Grupo de Trabajo del artículo 29, organismo de la Unión Europea que tiene carácter consultivo en materia de protección de datos, y cuya definición es:

> *Propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad.*[15]

Dichas características únicamente podrán ser consideradas como datos personales cuando cumplan con las condiciones emanadas de la definición de dato personal, a saber:

i) que se refieran a una persona física, y

ii) que permitan la identificación de dicha persona.

Poniendo como ejemplo la característica física del rostro, esta sí permite la identificación a simple vista de una persona, por lo que sí es considerada como dato personal, no así la huella dactilar que a simple vista no permite inferir en la identidad de su titular.

[15] Grupo de Trabajo del art 29, Dictamen 4/2007 sobre el concepto de datos personales, junio 2020.

La huella dactilar únicamente podrá considerarse como dato personal cuando se le apliquen técnicas o procedimientos automatizados que permitan su identificación o su verificación dentro de un sistema.

Por un lado, la identificación consiste en comparar la muestra biométrica recolectada de una persona frente a una base completa de datos biométricos registrados previamente. En lo que respecta a la verificación, es un método cuyo primer paso es la individualización del usuario mediante algún método, y la obtención de su muestra biométrica la cual es convertida en una plantilla para posteriormente comparar la plantilla que se registra con la que se encuentra previamente registrada.[16]

Como puede observarse, para la identificación o verificación se requiere de un registro previo del dato biométrico que será almacenado en una base de datos propiedad del responsable del tratamiento. Aquí es cuando cobra relevancia la protección especial que gozan este tipo de datos, que en México encuadran como datos sensibles.

Los responsables del tratamiento están obligados a implementar suficientes medidas de seguridad para garantizar su protección, aunado a que el principio de proporcionalidad se vuelve más estricto para este tipo de datos, en virtud de que los responsables deben de justificar la necesidad de recabarlos, almacenarlos y compilarlos.

1.2.4 Datos patrimoniales y financieros.

Ahora bien, existe una última clasificación que no se encuentra definida propiamente, no obstante, en México la LFPDPPP hace una distinción de estos para efectos del tipo de consentimiento que requiere recabar el responsable, me refiero a los datos financieros o patrimoniales.

[16] Instituto Nacional de Acceso a la Información, Transparencia y Protección de Datos Personales, Guía para el tratamiento de datos biométricos, México, marzo 2018, p.13.

Para efectos de proporcionar al lector una referencia a estos, se tomará la definición que el INAI proporciona en su manual de metodología de análisis de riesgo BAA (Beneficio, Accesibilidad y Anonimidad del Atacante):

> *Datos patrimoniales o financieros: aquellos que permiten inferir el patrimonio de una persona, que incluye entre otros, los saldos bancarios, estados y/o número de cuenta, cuentas de inversión, bienes muebles e inmuebles, información fiscal, historial crediticio, ingresos, egresos, buró de crédito, seguros, afores, fianzas, sueldos y salarios, servicios contratados. Incluye el número de tarjeta bancaria de crédito y/o débito.*[17]

Para que un responsable pueda recabar este tipo de datos, requiere del consentimiento expreso del titular, de conformidad con el artículo 8 de la LFPDPPP. A diferencia de los datos personales generales, los datos financieros y patrimoniales presuponen un mayor riesgo, que a su vez implica un mayor cuidado por parte de los responsables del tratamiento.

En México, los datos financieros, en específico los datos transaccionales derivados de las operaciones que un usuario de servicios financieros realiza ante las instituciones de crédito como los depósitos, operaciones o servicios, etcétera, tienen una especial protección y gozan de confidencialidad irrevocable conocida como el secreto bancario, dicha protección se encuentra consagrada dentro del artículo 142 de la Ley de Instituciones de Crédito, que a la letra dice:

> *Artículo 142.- La información y documentación relativa a las operaciones y servicios a que se refiere el artículo 46 de la presente Ley, tendrá carácter confidencial, por lo que las instituciones de crédito, en protección del derecho a la privacidad de sus clientes y usuarios*

[17] Instituto Nacional de Acceso a la Información, Transparencia y Protección de Datos Personales, Metodología de análisis de riesgo BAA, México, junio 2015, pp. 4.

que en este artículo se establece, en ningún caso podrán dar noticias o información de los depósitos, operaciones o servicios, incluyendo los previstos en la fracción XV del citado artículo 46, sino al depositante, deudor, titular, beneficiario, fideicomitente, fideicomisario, comitente o mandante, a sus representantes legales o a quienes tengan otorgado poder para disponer de la cuenta o para intervenir en la operación o servicio. [18]

Derivado del secreto bancario, las instituciones de crédito tienen prohibido divulgar o transferir la información de sus usuarios, de lo contrario pueden estar sujetas a multas desde 30,000 hasta 10,000 días de salario, de conformidad con el artículo 108 de la Ley de instituciones de Crédito.

En este caso en particular, la autoridad facultada para vigilar y regular respecto de la confidencialidad de los datos transaccionales en términos de la Ley de Instituciones de Crédito es la Comisión Nacional Bancaria y de Valores, organismo independiente de la Secretaría de Hacienda y Crédito Público.

1.3 Naturaleza jurídica de los datos personales

Los datos personales no son un derecho en sí, sino que forman parte del objeto de protección que es la persona en sí misma. Los datos, concebidos como parte fundamental de la vida privada de las personas, están dotados de protección, para evitar invasiones a la vida privada o bien restricciones a otros derechos humanos.

Los titulares de los datos personales gozan de distintos derechos que están relacionados entre sí y que buscan su protección:

[18] Ley de Instituciones de Crédito, Periódico Oficial de la Federación, 19 de julio de 1990, México, art. 142.

Derecho a la vida privada: que es un derecho de la personalidad que protege a las personas de no ser interferidas en lo que respecta a su vida personal, es decir, en el ámbito que se decide no hacer público y que está relacionado con la intimidad.

Derecho a la autodeterminación informativa: que es un derecho fundamental que faculta a los titulares a decidir cómo y cuándo se utilizan sus datos personales, así como decidir sobre la difusión de estos.

Derecho a la protección de los datos personales: que se trata de un derecho humano que busca garantizar que el tratamiento de los datos personales de las personas sea lícito, facultando a los titulares para decidir sobre sus datos personales.[19]

El derecho a la protección de datos personales es reconocido a nivel internacional. Su principal antecedente lo encontramos en el artículo 12 de la Declaración Universal de los Derechos Humanos de 1948, en donde se reconoció por primera vez a la vida privada de una persona como un derecho humano.

> *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.*[20]

Posterior a esta declaración, en diversos instrumentos internacionales se hizo un reconocimiento a la vida privada, y si bien no se hace una mención específica como tal al derecho a la protección de los datos personales, entendemos que dicho reconocimiento fue la base para lo que hoy conocemos como derecho.

---

[19] Instituto Nacional de Acceso a la Información, Transparencia y Protección de Datos Personales, Diccionario de protección de datos personales, Conceptos fundamentales, México, 2019.

[20] Declaración Universal de los Derechos Humanos, 10 de diciembre de 1948, París, art. 12.

Tal es el caso de la Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica) que en su artículo 11 habla sobre lo relativo a la protección de la honra y de la dignidad:

> *1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.*
>
> *2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.*
>
> *3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.*[21]

Por otro lado, el Pacto Internacional de Derechos Civiles y Políticos en su artículo 17 establece que:

> *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.*[22]

Ahora bien, en lo que respecta a México, fue a partir de la reforma a la Constitución Política de los Estados Unidos Mexicanos del 01 de junio de 2009 cuando se adicionó un reconocimiento expreso al derecho a la protección de los datos personales en el artículo 16, mediante el cual se reconoció que:

> *Toda persona tiene derecho a la protección de sus datos personales,*

---

[21] Convención Americana de Derechos Humanos, 22 de noviembre de 1969, San José, Costa Rica, art 11.

[22] Pacto Internacional de Derechos Civiles y Políticos, Nueva York, 16 de diciembre de 1966, Art 17.

al acceso, rectificación y cancelación de estos, 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.[23]

Cobra relevancia el siguiente cuestionamiento, el derecho a la protección de datos personales ¿se trata de un derecho humano o un derecho fundamental?

Previo a emitir una respuesta, resulta necesario definir qué es cada uno. Un derecho humano es una prerrogativa sustentada en la dignidad humana, cuya realización efectiva resulta indispensable para el desarrollo integral de la persona, es inherente a todos los seres humanos, sin distinción alguna de nacionalidad, lugar de residencia, sexo, origen nacional o étnico, color, religión, lengua, o cualquier otra condición.[24]

Por otro lado, un derecho fundamental es:

Aquel derecho subjetivo que corresponde universalmente a todos en cuanto dotados del estatus de personas, de ciudadanos o de personas con capacidad de obrar, entendiendo -derecho subjetivo- como cualquier expectativa positiva o negativa adscrita a un sujeto por una norma jurídica.[25].

Así pues, la diferencia entre un derecho humano y un derecho fundamental radica en que aquel es gozado por las personas por el simple hecho de haber

---

[23]Constitución Política de los Estados Unidos Mexicanos, Diario Oficial de la Federación, México, 5 de febrero de 1917, Art. 16.

[24] CNDH, "¿Qué son los derechos humanos?", Portal de la CNDH, *https://www.cndh.org.mx/derechos-humanos/que-son-los-derechos-humanos*

[25] Carbonell, Miguel, Los derechos fundamentales en México, México, UNAM, 2004, p.12, *http://ru.juridicas.unam.mx/xmlui/handle/123456789/10341*

nacido, mientras que uno fundamental deberá de estar reconocido en una carta magna u ordenamiento legal, y su aplicación podrá variar en cuanto a territorio u otra condición que se establezca.

Una vez entendida la diferencia, se puede concluir que el derecho a la protección de los datos personales es un derecho humano, y que en México se encuentra reconocido en la Constitución Política de los Estados Unidos Mexicanos.

1.4 Regulación de los datos personales en México

Como se mencionó en el capítulo anterior, a partir de la reforma a la Constitución Política Mexicana de 2009 en materia de derechos humanos, se reconoció y elevó a rango constitucional el derecho a la protección de datos personales como derecho fundamental, consagrándose dentro del artículo 16 Constitucional.

A su vez, se reconoció el derecho de acceso, mediante el cual el titular de los datos puede conocer los datos personales que se tienen registrados de su persona y el aviso de privacidad que rige su tratamiento; el derecho de rectificación, que faculta al titular de los datos para solicitar actualizaciones o modificaciones cuando estos sean inexactos; el derecho de cancelación, que permite al titular de los datos solicitar la cancelación de estos de cualquier registro en donde se encuentren, cuando se considere que el tratamiento no es el adecuado, y por último el derecho de oposición, a través del cual el titular de los datos puede oponerse al tratamiento de finalidades específicas de sus datos.

No fue hasta el 05 de julio de 2010, un año después de que se reconociera a nivel constitucional el derecho a la protección de datos personales, cuando se publicó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante, LFPDPPP), con la finalidad de regular el tratamiento

legítimo, controlado e informado de los datos personales, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.[26]

De esta manera, se tuvo por primera vez en México un instrumento legal que obligaba a los particulares a garantizar el derecho a la protección de los datos de las personas, sin intervención o participación alguna de las instituciones ý autoridades de la administración pública.

Un año después, se publica el reglamento, con el objeto de reglamentar las disposiciones de la LFPDPPP. Hoy, la LFPDPPP y su reglamento no han sufrido reformas, continúan vigentes y son los principales instrumentos legales en México para garantizar el derecho a la protección de los datos personales frente a los particulares.

En lo que respecta al sector público, el marco regulatorio se basa en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), que fue publicada el 26 de enero de 2017 y tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales. Los sujetos obligados serán todas las entidades de cualquier autoridad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.[27]

Para efectos del presente trabajo de investigación se analizaron únicamente las disposiciones del marco regulatorio del sector privado en México.

---

[26] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *op. cit.,* art 1.

[27] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Diario oficial de la federación, 26 de enero 2017, México, art. 1.

En ese sentido, y para dar una introducción a la composición del cuerpo normativo de la LFPDPPP, se menciona lo siguiente:

La LFPDPPP se encuentra dividida en apartados ordenados que proporcionan al titular y responsable una guía, iniciando por la definición de los conceptos y sujetos involucrados, mismos que a continuación se definen para dar claridad y enfoque al presente trabajo de investigación.

Se entiende por titular a la persona a la que corresponden los datos personales; por responsable a la persona física o moral que decide sobre el tratamiento de los datos personales, quien los recaba y da el tratamiento correspondiente, con excepción de las sociedades de información crediticia, en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y aquellas personas que llevan a cabo la recolección de datos personales que sea para uso exclusivamente personal, y sin fines de divulgación o utilización comercial.[28]

Por otro lado, se entenderá por encargado al tercero ajeno al responsable que trata los datos personales de los titulares por cuenta e instrucciones del responsable, mediante la remisión de los datos cuya formalización debe existir en cláusulas contractuales y/o instrumentos legales que permiten determinar el alcance de dicha remisión.[29]

Siguiendo el orden de la LFPDPPP, posterior a definir los conceptos señala los principios y deberes que deben observar los responsables durante el tratamiento de los datos. Dentro de los principios que se definen se encuentra el de información, que obliga a los responsables a informar a los titulares la información que se recaba

---

[28] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *op. cit.,* art 2.

[29] *Ídem*

de ellos y las finalidades del tratamiento, a través del respectivo aviso de privacidad que aquél debe poner a disposición previo a recabar los datos.

El principio de calidad obliga al responsable a mantener los datos personales actualizados, correctos y pertinentes para los fines para los cuales fueron recabados.

Los principios de licitud y lealtad exigen que los datos sean recabados de manera lícita, sin utilizar medios engaños o fraudulentos y siempre en cumplimiento de la legislación aplicable.

Por su parte, el principio de proporcionalidad exige que solamente sean recabados los datos personales necesarios para dar cumplimiento a la finalidad, buscando así una minimización en la entrega de información personal por parte del titular de los datos, privilegiando su privacidad.

De manera similar, el principio de finalidad exige que los datos personales sean utilizados únicamente para los fines para los que fueron recabados, mismos que deben informarse en el aviso de privacidad.

Si bien todos los principios son importantes, el principio de consentimiento es uno de los principales y a partir del cual se derivan los demás, puesto que exige a los responsables la obtención del consentimiento de los titulares de los datos previo a recabarlos, siempre y cuando éste sea exigible de conformidad con el artículo 8 de la LFPDPPP y cuando no se actualice alguno de los supuestos de excepción al consentimiento del artículo 10.

En lo que respecta a los deberes, se prevén dos, el deber de confidencialidad y el deber de seguridad. El deber de confidencialidad obliga a los responsables a mantener la secrecía de los datos personales que los titulares le entregan, y garantizar la privacidad de estos. Esta obligación se extiende a todo el personal bajo

el cargo del responsable o bien los encargados y/o terceros que participen en el tratamiento de los datos.

El deber de seguridad obliga a los responsables a implementar y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales en contra del tratamiento no autorizado, daño, robo o extravío.[30] Este deber tiene una estrecha relación con el principio de responsabilidad, en virtud de que el responsable debe garantizar el debido tratamiento, la privacidad y los intereses del titular de los datos.

Siguiendo el orden del cuerpo normativo de la LFPDPPP, se contempla un apartado relativo a los derechos de acceso, rectificación, cancelación y oposición, mejor conocidos como derechos ARCO, que si bien los titulares tienen facultad de ejercerlos en cualquier momento que deseen, se prevén algunos supuestos de excepción. Tal es el caso los previstos en el artículo 26, que de actualizarse alguno de ellos, el responsable no estará obligado a cancelar los datos personales, sea porque existan de por medio obligaciones legales derivadas de un contrato privado o de disposiciones legales, o bien por ser necesarios para dar cumplimiento a interés del propio titular o de la sociedad en general (interés público).

En lo que respecta al ejercicio de estos derechos, la LFPDPPP establece los plazos en que se deberán de atender las solicitudes que realicen los titulares, que son lo suficientemente amplios para que los responsables puedan dar una respuesta certera y en todo caso hacerla efectiva, estando obligados a designar a una persona o departamento para la atención de dichas solicitudes y que a su vez fomente la cultura de la protección de datos dentro de la organización del responsable.

[30] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *op. cit.,* art 19

Estos cuatro derechos forman la base para la autodeterminación informativa de los titulares de datos personales, y se encuentran reconocidos en nuestra carta magna. Su importancia es tal que, en caso de que una solicitud de ejercicio de derechos ARCO no sea atendida dentro de los plazos establecidos, o bien el titular considere que la respuesta dada no es conforme a la ley, este puede iniciar un procedimiento de protección de derechos a través del cual se solicita la intervención del INAI, quien mediante una resolución podrá confirmar, revocar o modificar la decisión del responsable del tratamiento.

Ahora bien, y siguiendo el orden de la LFPDPPP, se establece un apartado relativo a las transferencias de datos. Se parte de la premisa de que toda transferencia de datos requiere ser informada y autorizada por el titular de los datos, lo cual se considera adecuado en virtud de que el titular debe mantener el control de su información personal aún y cuando esta haya sido proporcionada a un responsable.

La LFPDPPP distingue entre transferencias nacionales e internacionales, mismas que requieren de distintas formalidades y que se encuentran señaladas en el reglamento, no obstante, no serán materia de estudio en el presente trabajo de investigación. Únicamente se resalta que, si bien debe mediar el consentimiento del titular para llevar a cabo una transferencia, también se prevén supuestos de excepción.

Tal es el caso de supuestos en que la transferencia esté prevista en una ley, como por ejemplo lo serán las transferencias que realizan las Administradoras de Fondos para el Retiro al resto de participantes del Sistema de Ahorro para el Retiro; o bien cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, como lo serían las transferencias de los resultados de pruebas de COVID-19 a las autoridades sanitarias, para efectos de métricas nacionales; incluso se prevé un supuesto para que los responsables transfieran datos a sociedades controladoras, subsidiarias o afiliadas bajo el mismo control que estos, y que se rijan

con las mismas políticas internas, un ejemplo pudiera ser la transferencia que realice una institución bancaria a otra entidad de su mismo grupo financiero.

El resto de la LFPDPPP se aboca a señalar a la autoridad reguladora, los procedimientos administrativos que pueden iniciar los titulares o el propio INAI de oficio, y por supuesto las sanciones previstas para cada infracción de la LFPDPPP.

Ahora que ya se ha revisado el origen del derecho a la protección de los datos, su importancia y las previsiones normativas que existen en México en torno al derecho, se procederá a estudiar el deber de seguridad estipulado en la LFPDPPP.

Capítulo 2. El deber de seguridad

2.1 Deber de seguridad conforme a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

De la LFPDPPP se desprende el deber de seguridad al que se encuentran sujetos los responsables del tratamiento, y que se traduce en la obligación de establecer y mantener medidas de seguridad tanto técnicas, físicas y administrativas, que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.[31]

Esta obligación será aplicable para cualquier sistema de tratamiento, sea físico o electrónico, asimismo será aplicable a todos los responsables en igual medida, sea que recaben datos de una docena o millones de titulares.

En lo que respecta a las medidas o controles de seguridad, son definidos como medidas de seguridad técnicas o administrativas para evitar, contrarrestar o minimizar la pérdida o falta de disponibilidad debido a las amenazas que actúan por una vulnerabilidad asociada a la amenaza. [32]

Con base en las definiciones previstas en el artículo 2 del reglamento de la LFPDPPP, debemos entender por medidas administrativas al 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

[31] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2016, México.

[32] Organización Internacional de Normalización, ISO 27000, 2018, *https://normaiso27001.es/referencias-normativas-iso-27000/#terminos*

protección de datos personales.[33]

Por medidas de seguridad físicas al conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para prevenir accesos no autorizados, proteger los equipos y proveerlos de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad.

Y por medidas de seguridad técnicas al conjunto de actividades, controles o mecanismos que se valen de la tecnología para asegurar que los accesos a los datos sean autorizados y proporcionales, así como acciones para la adquisición, operación, desarrollo y mantenimiento de sistemas seguros.

Por su parte, una amenaza será, en el contexto de la seguridad de la información, cualquier cosa que pueda causar un daño grave a un sistema de información. Una amenaza es algo que puede o no puede ocurrir, pero tiene el potencial de causar daños graves. Por otro lado, una vulnerabilidad será cualquier tipo de debilidad en el propio sistema de información, o a un conjunto de procedimientos o a cualquier cosa que deje a la información expuesta a una amenaza.[34]

Comprender esos términos es la base para una correcta aplicación de las disposiciones de la LFPDPPP. Ya sea que los responsables realicen el tratamiento manual, esto es, en documentos físicos o tratamiento automatizado, a través de sistemas informáticos que les permitan gestionar los datos, estarán obligados a implementar medidas de seguridad para evitar vulneraciones o incidentes de seguridad, protegiendo así a los datos personales.

---

[33] Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Diario Oficial de la Federación, 2 de diciembre de 2011, México, art. 2.

[34] *Ídem*

Del artículo 19 de la LFPDPPP se desprende la obligación para los responsables de implementar 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, no debiendo de adoptar medidas menores a aquellas que mantengan para el manejo de su propia información.[35]

Asimismo, en el artículo 60 del reglamento se contemplan los factores para que el particular pueda determinar las medidas de seguridad adecuadas para el tratamiento, entre los cuales se encuentra el riesgo inherente por tipo de dato personal; la sensibilidad de los datos personales tratados; el desarrollo tecnológico, y las posibles consecuencias de una vulneración para los titulares. [36]

De manera adicional, y para efectos de determinar las medidas de seguridad adecuadas, la LFPDPPP establece que los particulares deberán de considerar el número de titulares, las vulnerabilidades que hayan ocurrido con anterioridad en el sistema o sistemas de tratamiento y los riesgos que pudieren tener los datos personales.

Esto sugiere que previo al tratamiento, el responsable debería de correr un análisis de riesgos que le permita identificar las amenazas y vulnerabilidades a las que pudieran estar expuestos, no obstante, el hecho de que la disposición normativa lo establezca como “procurar” implica la no obligatoriedad de su ejecución.

Por último, en el artículo 61 se enlistan las acciones de seguridad mínimas que deberán considerar los responsables para mantener la seguridad de los datos

[35] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *op. cit*, art. 19.

[36] Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *op. cit,* art. 60.

personales, entre las que se encuentran la elaboración de un inventario de datos, contar con un análisis de riesgos, realizar análisis de brecha, elaborar un plan de trabajo para remediar brechas, capacitación del personal, entre otras.

Dichas acciones de seguridad conforman las etapas de un sistema de gestión de seguridad basado en la norma “ISO 27001 seguridad de la información”, no obstante, el hecho de que la LFPDPPP no establezca la obligatoriedad para el particular de demostrar el cumplimiento de dichas acciones previo al tratamiento de los datos, propicia a que no se lleven a cabo.

Los artículos anteriores conforman el marco regulatorio del deber de seguridad para los datos personales que debe observar el particular, quedando facultado para que implemente aquellas medidas de seguridad que considere adecuadas según sus propios sistemas de tratamiento de la información.

Ahora bien, no obstante que existe un marco regulatorio sobre el deber de seguridad, este presenta deficiencias que impiden su cumplimiento efectivo, en virtud de que dicho marco no propicia a una protección preventiva frente a los riesgos por vulneraciones de seguridad que pueden ocurrir a los sistemas de tratamiento de los responsables.

2.2 Áreas de oportunidad con relación al deber de seguridad

Hoy, los titulares se encuentran frente a un precipicio al momento de proporcionar sus datos personales a un particular, puesto que no tienen manera de verificar si el sistema de tratamiento de datos del responsable es seguro, o si mantienen implementadas medidas de seguridad suficientes que garantizarán la protección de sus datos.

Los titulares únicamente tienen posibilidad de consultar el Aviso de Privacidad, y en dicho documento no es obligatorio el informar las medidas de

seguridad, certificaciones y/o verificaciones que tiene el responsable del tratamiento, incluso, los titulares no tienen manera de confirmar que lo informado en el Aviso sea acorde a la realidad.

Si bien, la LFPDPPP establece los parámetros y criterios mínimos para garantizar la protección de datos personales y su adecuado tratamiento por parte de los particulares, este no es suficiente para asegurar que los responsables efectivamente implementarán las medidas de seguridad adecuadas, en virtud de que no existe un procedimiento de certificación previo al tratamiento de los datos, en donde el INAI como autoridad reguladora pueda cerciorarse de que el sistema de tratamiento que empleará el responsable es seguro.

Lo que sí existe es un procedimiento de verificación mediante el cual el INAI puede auditar a los responsables, y determinar si dan efectivo cumplimiento a las disposiciones de la LFPDPPP, pero los datos actuales e históricos nos señalan que este procedimiento no se inicia sino hasta que un titular denuncia por presunta violación a sus datos o a la LFPDPPP, esto es, posterior a que ha ocurrido una vulneración con afectaciones directas al titular de los datos.

Para evidenciar lo anterior, se revisaron los informes de labores del INAI que se encuentran disponibles en su sitio web oficial, y se extrajeron los datos de los procedimientos de verificación que se han iniciado en los últimos 6 años.

Para efectos de demostrar la hipótesis, se seleccionó al sector de servicios financieros y de seguros como muestra, en virtud de que para operar, los responsables necesariamente recaban datos personales financieros de sus clientes.

En la siguiente tabla se pueden apreciar los procedimientos de verificación iniciados como consecuencia de una denuncia realizada por el titular de datos personales.

Ejercicio	Total de procedimientos de verificación iniciados	Corresponden al sector financiero
2015	32	9
2016	75	30
2017	55	14
2018	120	10
2019	774	8
2020	63	15
Total	**1,119**	**86**

Cuadro 1.
Fuente: Informes de labores del INAI.
Elaboración propia.

Es importante destacar que en los informes de labores no se encontró el dato de las verificaciones iniciadas de oficio por parte del INAI, por lo que se realizó una solicitud de información vía Plataforma Nacional de Transparencia, en la cual se solicitó el número de los procedimientos de verificación iniciados de oficio, por año, específicamente para el sector de servicios financieros y de seguros.

En tiempo y forma se obtuvo respuesta a la consulta realizada, mediante el oficio INAI/SPDP/DGIVSP/2198/22, en el cual la Dirección General de Investigación y Verificación del Sector Privado del INAI informó lo siguiente:

Ejercicio 2015	
Total de Procedimientos de Verificación iniciados de oficio (Sector, Servicios Financieros y de Seguros)	0
Ejercicio 2016	
Total de Procedimientos de Verificación iniciados de oficio (Sector, Servicios Financieros y de Seguros)	1
Ejercicio 2017	
Total de Procedimientos de Verificación iniciados de oficio (Sector, Servicios Financieros y de Seguros)	1
Ejercicio 2018	
Total de Procedimientos de Verificación iniciados de oficio (Sector, Servicios Financieros y de Seguros)	1
Ejercicio 2019	
Total de Procedimientos de Verificación iniciados de oficio (Sector, Servicios Financieros y de Seguros)	0
Ejercicio 2020	
Total de Procedimientos de Verificación iniciados de oficio (Sector, Servicios Financieros y de Seguros)	0

Cuadro 2.
Fuente: Oficio INAI/SPDP/DGIVSP/2198/22
Elaboración propia.

Como se puede apreciar, desde el año 2015, año en que se creó el INAI, únicamente se han iniciado 3 procedimientos de verificación de oficio. En ese tenor, queda claro que el papel del INAI como órgano encargado de garantizar la protección de los datos personales no está operando de manera proactiva para la prevención de las vulneraciones e incidentes de seguridad.

Para contrastar los datos obtenidos con el total de los establecimientos existentes en México, se revisó el Censo económico 2019 del Instituto Nacional de Geografía, Estadística e Informática. De conformidad con el Censo, en 2019 existían

6,373,169 establecimientos activos en México, de los cuales el 2.4% corresponde al sector de servicios financieros y de seguros, esto es, 152,956 establecimientos.

Tomando en consideración que en los últimos 6 años el INAI únicamente ha verificado a 86 responsables del sector de servicios financieros y de seguros, se concluye que solamente el 0.05% de los responsables que recaban datos personales financieros en México pasó por un procedimiento en donde el INAI pudo determinar el cumplimiento efectivo del deber de seguridad y la implementación de medidas de seguridad adecuadas para proteger los datos personales frente a vulneraciones.

Este es un porcentaje muy reducido por no decir nulo. El resto de los establecimientos del sector financiero que recaban datos personales pudieran o no encontrarse vulnerables, poniendo en riesgo la privacidad de los titulares, y estos hoy se encuentra imposibilitados para prevenirlo.

En este sentido, surge el cuestionamiento, ¿Por qué debemos esperar a que se materialice una vulneración a los datos personales para que se verifique el nivel de cumplimiento de un responsable?

Ahora bien, cuando ha ocurrido una vulneración a la seguridad de los datos, la LFPDPPP en su artículo 20 establece la obligatoriedad para que el particular notifique al titular de los datos de manera inmediata de tal suerte que pueda tomar las medidas correspondientes para la defensa de sus derechos[37], más no así notificar al INAI.

Esta medida es insuficiente, en virtud de que el INAI, órgano especializado que en todo caso pudiera recomendar al responsable las medidas de seguridad

[37] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *op. cit,* art. 20.

adecuadas para evitar otra vulneración, no se entera de la misma, a menos de que el titular afectado presente una denuncia ante dicho Instituto.

De tal suerte que, el responsable cumple notificando al titular afectado, no obstante, nadie asegura que implementó la corrección adecuada para prevenir otra vulneración, ni mucho menos se asegura la remediación del daño ocasionado al titular debido a la divulgación no autorizada, robo o extravío de sus datos personales.

Por las razones antes expuestas es que el deber de seguridad presenta deficiencias, derivado de un marco regulatorio reactivo, en donde se privilegia al desarrollo económico de las empresas antes que el derecho a la protección de datos y privacidad de los titulares.

Estas deficiencias cobran relevancia en la actualidad, en donde las tecnologías como el big data recaban, analizan y explotan cantidades inmensas de datos y metadatos de una persona, en virtud de que el impacto en los derechos de la persona es mucho mayor, y las consecuencias de una vulneración a sus datos se multiplica considerablemente.

Ahora bien, se procederá a comparar el marco regulatorio de protección de datos y deber de seguridad existente en otras partes del mundo, para demostrar que existen serias deficiencias en México que pueden solucionarse con medidas de prevención proactivas.

Se han seleccionado dos marcos regulatorios, el primero corresponde al de la Unión Europea en virtud de ser el más robusto que existe en la actualidad. Por otro lado, y para tener una comparación con otro país de América latina, se seleccionó el marco regulatorio de Brasil.

2.3 Deber de seguridad conforme al Reglamento General de Protección de Datos Personales de la Unión Europea.

El parlamento Europeo y el Consejo publicaron el 25 de abril de 2016 el Reglamento relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos, en adelante RGPD), derogando con ello a la Directiva 95/46/CE.

Dicho 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.[38]

Asimismo, 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 la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o el control de su comportamiento.[39]

Ahora bien, en lo que respecta al deber de seguridad, el RGPD, de manera similar que la LFPDPPP, en su artículo 32 establece la obligatoriedad para el responsable de implementar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

Esto debe de realizarse teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del

[38] Reglamento 2016/679 del Parlamento Europeo y del Consejo, *op. cit*., art. 3

[39] *Idem*

tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.[40]

Para efectos de demostrar el cumplimiento del deber de seguridad, el RGPD prevé la posibilidad para el responsable de adherirse a códigos de conducta o mecanismos de certificación aprobados por la Comisión.

En lo que respecta a la información a la que puede acceder un titular ya sea ejerciendo sus derechos o consultando la política de privacidad del responsable, el RGPD, en igual circunstancia que la LFPDPPP, no prevé que el responsable se encuentre obligado a informar al titular las medidas de seguridad que mantiene implementadas dentro del sistema de tratamiento de los datos personales o bien, algún certificado expedido por la autoridad reguladora que les permita cerciorarse de que sus datos estarán seguros.

En lo que respecta a la notificación de una violación de seguridad, a diferencia de la LFPDPPP, el RGPD obliga a los responsables a notificar tanto al titular afectado como a la autoridad de control competente, a más tardar 72 horas después de que haya tenido conocimiento de ella.

De manera adicional, se obliga al responsable a documentar la violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas.[41] Dicha documentación permite a la autoridad de control verificar el cumplimiento de las medidas correctivas de tal suerte que las afectaciones a los titulares de los datos se vean disminuidas, en su caso evitar que vuelvan a ocurrir.

El hecho de que la autoridad de control reciba las notificaciones de las violaciones ocurridas, da pie a que el responsable del tratamiento sea sancionado,

[40] *Ibidem*, art. 32

[41] *Ibidem*, art. 33.

lo cual conlleva a que dicho responsable realmente implemente las medidas de seguridad que prevengan una violación futura, porque es bien sabido que a partir de una multa es cuando los responsables se preocupan por dar cumplimiento efectivo a ley.

Además de la obligación de implementar medidas de seguridad antes señalada, el RGPD prevé dos obligaciones adicionales que propician a que el responsable sea consciente de las amenazas a las que pueden estar sujetos los datos personales que se encuentran dentro de sus sistemas de tratamiento. La primera consiste en la elaboración de un registro de actividades de tratamiento.

Este registro, de conformidad con el artículo 30, debe contener los fines del tratamiento de los datos, una descripción de las categorías de los interesados y de los datos personales, los plazos de conservación, y lo más importante, una descripción general de las medidas técnicas y organizativas de seguridad que se tienen implementadas.

El registro es una manera sencilla de llevar el control de las actividades que se realizan, y con un adecuado seguimiento, el responsable puede gestionar los riesgos de manera oportuna, sea mediante un software de gestión de la privacidad o de manera manual. A diferencia de la LFPDPPP en donde el responsable no está obligado a llevar un registro, por lo que la detección de amenazas puede retardarse y la gestión de estas requeriría de un mayor tiempo.

La segunda obligación adicional que prevé el RGPD, es la evaluación de impacto relativa a la protección de los datos. De conformidad con el artículo 35 del reglamento, cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del

tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. [42]

Retomando el ejemplo que se utilizó en el apartado del escenario en México, la utilización de sistemas de big data aumenta el nivel del riesgo y afectaciones para los titulares de los datos personales. En ese sentido, se considera totalmente acertado que el responsable deba de realizar una evaluación de impacto previo a implementar un tratamiento de esa categoría.

Las evaluaciones de impacto deben contener como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento.

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.[43]

Si del resultado de dicha evaluación se identifica que existe un riesgo alto en cuanto al tratamiento de los datos, el responsable está obligado a consultar a la autoridad de control de manera previa al inicio del tratamiento. La autoridad de control deberá de asesorar al responsable para que implemente las medidas técnicas y organizativas necesarias, o bien, realice las modificaciones pertinentes para asegurar la protección de los datos personales.

[42] *Ibidem*, art. 35.
[43] *Ídem*

Como se puede observar, el enfoque de las obligaciones del RGPD es tiene un carácter proactivo y preventivo. Se otorga un valor mayor a la garantía de privacidad y protección de los titulares de los datos personales.

2.4 Deber de seguridad conforme a la Ley 13,709 General de Protección de Datos de Brasil

El 14 de agosto de 2018 se publicó en Brasil la Ley 13,709 General de Protección de Datos Personales (LGPD) cuyo objeto es proteger los derechos fundamentales de libertad y privacidad y el libre desarrollo de la personalidad de la persona física, en lo que respecta al tratamiento de sus datos personales, incluso en medios digitales. [44]

A dos años de la publicación del RGPD, la LGPD recoge sus principios, deberes y obligaciones para los responsables del tratamiento de los datos personales, a su vez, reconoce una variedad más amplia de derechos para los titulares de los datos.

Ahora bien, en lo que respecta al deber de seguridad, la LGPD prevé distintas obligaciones que, en suma, propician a que el responsable del tratamiento tenga control sobre las posibles amenazas que pueden vulnerar a los datos personales.

En principio, y en concordancia con RGPD y LFPDPPP, se obliga a los responsables a implementar y mantener medidas técnicas y administrativas capaces de proteger los datos personales de accesos no autorizados y situaciones accidentales o ilícitas de destrucción, pérdida, alteración, comunicación o difusión.

[44] Ley 13,709 General de Protección de Datos Personales, Presidencia de la república subtitular secretaría general de asuntos jurídicos, 14 de agosto de 2018, Brasil, art. 1.

Asimismo, se prevé la posibilidad para la autoridad nacional, conocida como Autoridad Supervisora Nacional de Protección de Datos (ANPD), de disponer de normas técnicas mínimas para hacer cumplir la obligación de los responsables, mismas que deben de observarse desde la concepción de un producto o servicio, hasta su ejecución. [45]

A diferencia de la LFPDPPP, la LGPD sí obliga a los responsables a notificar a la autoridad de control y al titular de los datos cuando ocurre una vulneración a la seguridad de estos, dentro de un plazo razonable.

Dentro del contenido de dicha notificación se debe incluir:

I. una descripción de la naturaleza de los datos personales afectados;
II. información sobre los titulares involucrados;
III. la indicación de las medidas técnicas y de seguridad utilizadas para la protección de datos, en el caso de secretos comerciales e industriales;
IV. los riesgos relacionados con el incidente;
V. las razones de la demora, cuando la comunicación no fue inmediata; y
VI. Medidas que se han adoptado o se adoptarán para revertir o mitigar los efectos del daño.[46]

Lo anterior demuestra que, en esencia, la LGPD prioriza la garantía de la protección de datos personales frente a un interés económico en protección del responsable de la vulneración. Esto es así puesto que la autoridad, al tener conocimiento de las vulneraciones, tiene la oportunidad de imponer las sanciones

[45] *Ibidem*, art. 46
[46] *Ibidem*, art. 48.

correspondientes que impulsen a mejorar la seguridad de los sistemas de tratamiento de los responsables, lo cual no sucede en México en virtud de que los responsables no están obligados a notificar a la autoridad reguladora.

Por otro lado, la LGPD también obliga a los responsables a llevar un registro de las actividades de tratamiento que llevan a cabo, quedando facultada la autoridad nacional para solicitar un informe de impacto sobre la protección de datos que incluya cuando menos: la descripción de los tipos de datos recopilados, la metodología utilizada para la recopilación y garantía de la seguridad de la información y el análisis del responsable del tratamiento con respecto a las medidas, salvaguardias y mecanismos de mitigación de riesgos adoptados.[47]

Dicho registro propicia a que la responsable en primer lugar realice el análisis de riesgo e impacto, necesario para poder conocer los riesgos a los que se encuentran sujetos sus sistemas de tratamiento, lo que lleva a una segunda acción, la implementación de las medidas de seguridad adecuadas para prevenir la materialización de dichos riesgos.

La LGPD no prevé dentro de los requisitos que el responsable debe informar al titular previo a recabar sus datos, el detalle de las medidas o garantías de seguridad para proteger sus datos personales, ni tampoco lo prevé para cuando dichos titulares ejerzan el derecho de acceso.

Y en lo que respecta a buenas prácticas, la LGPD prevé la posibilidad para que un responsable implemente un programa de gobierno de privacidad que demuestre el compromiso de adoptar procesos y políticas internas que garanticen el cumplimiento integral de las normas y mejores prácticas con respecto a la protección de datos personales.[48]

---

[47] *Ibidem*, art. 38.

[48] *Ibidem*, art. 50

Dentro de dicho programa se deben establecer las normas de seguridad, normas técnicas, mecanismos de supervisión y mitigación de riesgos que serían muy útiles para ser informados al titular de los datos, de tal manera que pueda generar confianza con el responsable. No obstante, dicho programa no es obligatorio.

En conclusión, el deber de seguridad consagrado en la LGPD sí presenta diferencias en cuanto al previsto en la LFPDPPP, tal es el caso del registro de actividades de tratamiento, no obstante, no llega a tener el mismo alcance preventivo del RGPD, que de manera adicional requiere de la elaboración de evaluaciones de impacto en la privacidad para cada actividad o sistema de tratamiento.

Asimismo, el titular de datos personales en Brasil también se encuentra desprotegido al momento de proporcionar sus datos a un responsable, en virtud de que no existe una obligación legal para que este informe en su política de privacidad las medidas o garantías de seguridad que mantiene implementadas.

2.5 Comparativa del deber de seguridad en las leyes de protección de datos

Obligación	LFPDPPP	RGPD	LGPD
Implementar medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos	SI	SI	SI
Informar al titular de los datos las medidas de seguridad o estándares implementados para proteger sus datos	NO	NO	NO
Prevé certificado de seguridad emitido por la autoridad reguladora para cerciorar del cumplimiento del deber de seguridad	NO	NO	NO
Notificar a la autoridad reguladora cuando ocurre una vulneración de seguridad	NO	SI	SI
Registro de actividades de tratamiento que incluya descripción de las medidas técnicas y organizativas de seguridad que se tienen implementadas.	NO	SI	SI
Una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales	NO	SI	NO

Cuadro 3.
Elaboración propia.

A continuación se abordan los beneficios que pudieran verse aplicados en México, si las obligaciones proactivas que prevé el RGPD y LGPD se integraran a nuestro marco regulatorio:

a) Notificar a la autoridad reguladora cuando ocurre una vulneración de seguridad

Actualmente en México, los responsables no tienen la obligación de notificar al INAI cuando ha ocurrido una brecha de datos personales, que puede traducirse en la destrucción parcial o total, alguna pérdida o alteración, o bien la divulgación o el acceso no autorizado de los datos personales.

No obstante, si los responsables estuvieran obligados a hacerlo, en primer lugar se estaría promoviendo una protección efectiva de los derechos de protección de datos y privacidad de los titulares, en virtud de que existiría un punto de partida para una correcta verificación del responsable y su/s sistema/s de tratamiento.

Asimismo, estaríamos frente a la posibilidad de crear un repositorio nacional de conocimiento de vulnerabilidades comunes en los tratamientos, con las soluciones ejecutadas y recomendaciones del INAI, que a su vez serviría para la mejora continua de las actividades de tratamiento realizadas por los responsables.

Cabe señalar que la notificación a la autoridad no necesariamente debe implicar el inicio de un procedimiento sancionatorio, en virtud de que la notificación en tiempo, acompañada de la evidencia de las acciones ejecutadas para subsanar o mitigar el riesgo serían una evidencia del cumplimiento del propio deber de seguridad.

Como ejemplo de esta práctica, la Agencia Española de Protección de Datos cuenta con un sitio web para notificar las brechas de datos personales, ya sea por parte del responsable o del titular de los datos. A través de una serie de preguntas y formularios digitales, se recaba la información necesaria para que la propia Agencia pueda determinar si se cumplió con el principio de responsabilidad proactiva posterior a la brecha, o bien, para determinar el inicio de un procedimiento sancionatorio.

Este tipo de medio sistemático para notificar las brechas permitiría en México la trazabilidad, por lo que los responsables pudieran demostrar su diligencia y cumplimiento efectivo del deber de seguridad, en caso de requerirse.

b) Elaborar un registro de actividades de tratamiento

Un registro de actividades de tratamiento es una herramienta eficaz para mantener un control del uso de los datos personales. Tomando como referencia lo requisitado por el RGPD, el registro debería contener:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;
b) los fines del tratamiento;
c) una descripción de las categorías de interesados y de las categorías de datos personales;
d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional,
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.[49]

Dicho registro es obligatorio y debe ponerse a disposición de la autoridad cuando así sea requerido.

[49] Reglamento 2016/679 del Parlamento Europeo y del Consejo, *op. cit*., art. 30.

La obligatoriedad de mantener el registro y que incluya la descripción de las medidas de seguridad marca una pauta para que, desde el inicio del tratamiento, los responsables las implementen. Si los responsables actúan siguiendo los estándares de seguridad existentes en la actualidad, implica que se realiza un análisis previo para conocer las amenazas y vulnerabilidades asociadas a los datos personales, con el objetivo de determinar las medidas adecuadas para cada tratamiento.

Ese ejercicio previo es la clave para evitar la mayoría de las brechas y vulneraciones de seguridad, en virtud de que justamente se apuesta por la prevención.

En la actualidad existe una infinidad de softwares de privacidad que automatizan el registro e inventario de datos. Incluso, es posible asociar los registros a evaluaciones de impacto en la protección de los datos, brindando la oportunidad a los responsables de identificar los riesgos de una manera sencilla.

c) Realizar una evaluación de impacto en la protección de datos

Siguiendo la definición del RGPD, una evaluación de impacto en la protección de datos debe realizarse cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas.[50]

El corazón de la evaluación es justo la evaluación de los riesgos a los que se encuentran sujetos los datos personales y sus titulares. Este ejercicio de anticipación a escenarios amenazantes es lo que permite determinar las medidas

[50] *Ibidem*, art. 35

de seguridad adecuadas que mitigaran dichos escenarios antes de que se materialicen.

Es bien sabido que en cualquier empresa, un aspecto primordial del programa de cumplimiento es el análisis de riesgos, que permite a la alta dirección la gestión preventiva de los mismos, evitando sanciones legales, económicas, etc.

La propia norma internacional ISO 27001 que abarca la seguridad de la información recomienda la elaboración de un análisis de riesgos, que forma parte integral del sistema de gestión de seguridad de la información.

De manera adicional, el RGPD prevé que, en caso de que la evaluación arroje un alto riesgo para los titulares si el responsable no implementa medidas para mitigarlo, este debe de realizar una consulta previa a la autoridad de control, esto es, previo a implementar la actividad de tratamiento.

A través de dicha consulta, la autoridad puede asesorar al responsable para que la actividad de tratamiento no implique un riesgo a los titulares y sus datos, privilegiando así el derecho de protección de datos personales.

Como buena práctica, la Agencia Española de Protección de Datos ha emitido diversas guías como la “Gestión del riesgo y evaluación de impacto en tratamiento de datos personales” y “Guía práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD” que van guiando paso a paso al responsable, para que pueda evaluar de forma sencilla los riesgos a los que se encuentran sujetos los datos en su posesión.

De aplicarse en México, esta evaluación sería un ganar-ganar tanto para el responsable como para el INAI. Por un lado, los responsables ya están obligados a designar a una persona especializada en protección de datos que se encargue de fomentar la protección al interior de la organización, que viene siendo un homólogo

del delegado de protección de datos que se prevé en las legislaciones estudiadas en la presente investigación.

Este perfil especializado es quien pudiera realizar las evaluaciones sin representar un mayor gasto para el responsable, en virtud de que no son de una dificultad elevada, se requiere más que nada conocimiento de la operativa interna de la propia organización.

Por otro lado, el INAI ya cuenta con las con las atribuciones necesarias y con el personal con el conocimiento adecuado para emitir recomendaciones y asesorar a los responsables que en todo caso se acercaran a consultar sus actividades de tratamiento de alto riesgo.

En cuanto a las atribuciones, el artículo 39 de la LFPDPPP prevé las siguientes:

- Proporcionar apoyo técnico a los responsables que lo soliciten, para el cumplimiento de las obligaciones establecidas en Ley.
- Elaborar estudios de impacto sobre la privacidad previos a la puesta en práctica de una nueva modalidad de tratamiento de datos personales o a la realización de modificaciones sustanciales en tratamientos ya existentes; [51]

En cuanto al personal y estructura, actualmente la secretaría de protección de datos personales del INAI cuenta con una dirección de prevención y autorregulación, cuyo personal está debidamente capacitado para orientar a los responsables.

[51] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *op. cit*, art. 39

En virtud de ello, y porque no es necesario modificar nada relativo a sus atribuciones y/o estructura organizativa es que las evaluaciones de impacto serían de gran beneficio para mejorar el marco normativo del deber de seguridad.

d) Informar medidas de seguridad en el Aviso de Privacidad

En realidad esta no es una obligación que se encuentre prevista en las legislaciones estudiadas, o en alguna otra que se conozca. En parte, como profesionales de la privacidad, somos conscientes de que la gran mayoría de la población no tiene un conocimiento técnico para lograr comprender qué medidas de seguridad son adecuadas y cuáles no. También debe señalarse que no es del conocimiento del titular de los datos el tipo de sistema de tratamiento que utilizará el responsable que recaba sus datos.

No obstante, y siguiendo la línea de la responsabilidad proactiva, los responsables pudieran generar confianza e incluso fortalecer su estrategia comercial, si informaran respecto de sus esfuerzos en seguridad, para garantizar la protección de los datos.

No se espera que se detalle un listado de todas y cada una de las medidas de seguridad, pero sí pudieran categorizarse, dependiendo el tipo de sistema de tratamiento del que se trate, incluso señalar aquellos certificados que el responsable haya obtenido, como certificaciones en normas internacionales de seguridad.

Estudiando diversos avisos y políticas de privacidad de empresas reconocidas a nivel internacional, se encontró algunas de ellas sí informan un apartado de seguridad, en el cual incluyen información acerca de las medidas que mantienen implementadas, como:

- Certificados de seguridad para sus sitios web
- Control de acceso para el personal y terceros
- Acuerdos de confidencialidad para el personal y terceros

- Evaluaciones de impacto y análisis de riesgo previo a implementar una actividad de tratamiento.

De considerar a este apartado como un requisito obligatorio dentro del aviso de privacidad, no debería representar un esfuerzo desproporcionado para el responsable, en virtud de que de conformidad con el deber de seguridad, ya se encuentran obligados a implementar medidas de seguridad, sería relativamente sencillo hacer un pequeño resumen de lo que se encuentre implementado. Debido a ello es que se propone como una medida factible para mejorar en pro del titular de los datos.

Una vez comparadas las distintas legislaciones en materia de protección de datos, y vistos los beneficios de las obligaciones adicionales que estos prevén se está en posibilidad de elaborar una propuesta de reforma a la LFPDPPP, de tal manera que el deber de seguridad transite de ser reactivo a ser preventivo, garantizando así el derecho a la protección de los datos personales

Capítulo 3. Incorporación de acciones preventivas para el fortalecimiento del deber de seguridad proactiva de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares

Como se puede concluir con lo expuesto en el capítulo anterior, la LFPDPPP no contiene las medidas suficientes para que garantizar que los responsables del tratamiento de los datos realizarán los esfuerzos necesarios para prevenir las vulneraciones de seguridad y materialización de los riesgos hacia los datos personales que tienen en su posesión.

Por lo anterior, se presenta la siguiente propuesta que reforma y adiciona diversas disposiciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y a su Reglamento.

Decreto.

Primero. Se **reforman** los artículos 16 y 23 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Artículo 16. El aviso de privacidad deberá contener, al menos, la siguiente información:

I a VI. …

VII. Las medidas de seguridad administrativas, técnicas y físicas que mantiene implementadas para proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

…

Artículo 23. Los titulares tienen derecho a acceder a sus datos personales que obren en poder del responsable, así como conocer la siguiente información:

I. Las finalidades del tratamiento;
II. Las categorías de datos personales de que se trate;
III. Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales;
IV. De ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;
V. Cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;
VI. Las medidas de seguridad administrativas, técnicas y físicas que mantiene implementadas para proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

Segundo. Se **reforma** el artículo 64, 65 y se **adicionan** los artículos 48 bis, 61 bis y 61 ter del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Artículo 48 bis. Los responsables llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

I. El nombre y los datos de contacto del responsable
II. Las finalidades del tratamiento;
III. Una descripción de las categorías de interesados y de las categorías de datos personales;
IV. Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;
V. Una descripción general de las medidas de seguridad administrativas, técnicas y físicas que mantiene implementadas para proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

El responsable pondrá el registro a disposición del Instituto cuando este así lo determine.

Artículo 61 bis. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de los titulares, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

La evaluación deberá incluir como mínimo:

I. Una descripción sistemática de las operaciones y finalidades del tratamiento previstas.
II. Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
III. Una evaluación de los riesgos para los derechos y libertades de los titulares de los datos, y
IV. Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

Artículo 61 ter. El responsable consultará al Instituto antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 61 bis muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para para mitigarlo.

Cuando el Instituto considere que el tratamiento previsto puede infringir la Ley y el presente Reglamento, el Instituto deberá asesorar por escrito al responsable.

Para la consulta, el responsable del tratamiento le facilitará al Instituto la información siguiente:

I. En su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento.
II. Las finalidades y medios del tratamiento previsto;
III. Las medidas y garantías establecidas para proteger los derechos y libertades de los titulares de los datos;
IV. La evaluación de impacto relativa a la protección de datos establecida en el artículo 61 bis,
V. Cualquier otra información que solicite el Instituto.[52]

Artículo 64.

…

Asimismo, el responsable estará obligado a notificar al Instituto sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de la vulneración, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de los titulares. Si la notificación al Instituto no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.[53]

Artículo 65. El responsable deberá informar al titular y al Instituto al menos lo siguiente:

I a V. **…**

[52] Reglamento 2016/679 del Parlamento Europeo y del Consejo, *op. cit*., art. 36
[53] Ibidem, art. 33

Conclusiones

Conclusiones

El tratamiento de datos personales por parte de empresas que prestan servicios o venden productos continuará en aumento conforme al aumento en la utilización de tecnologías de la información para llevar a cabo el mismo. Hoy, los marcos regulatorios de protección de datos requieren ser actualizados para no quedar desfasados y sin aplicación ante la nueva ola de sistemas de tratamiento automatizados.

En México, con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares se busca otorgar una protección a los datos personales que son tratados por los particulares, a través de diversos principios y deberes que deben observar los responsables del tratamiento durante todo el ciclo de vida de los datos personales, independientemente del sistema de tratamiento que se utilice.

Uno de los deberes que se prevén es el deber de seguridad, que impone la obligación a los responsables del tratamiento de implementar medidas de seguridad administrativas, técnicas y organizativas que ayuden a proteger los datos en contra de algún robo, pérdida, destrucción, acceso o tratamiento no autorizado.

No obstante, el deber de seguridad no cuenta con la suficiente coercitividad que se vea reflejada en una verdadera determinación de las medidas de seguridad que permitan proteger los datos, ni tampoco está dotado de un mecanismo de verificación para que los titulares de los datos puedan cerciorarse de su cumplimiento.

Como se expuso, la LFPDPPP no prevé la obligación para el responsable del tratamiento de informar al titular de los datos las medidas de seguridad o estándares implementados para proteger sus datos, dejándolos en un estado de incertidumbre y sin garantía alguna.

Tampoco la LFPDPPP prevé la emisión de un certificado de seguridad por parte del INAI o de alguna entidad certificadora, que pueda servir como una validación del cumplimiento del deber de seguridad, generando confianza a los titulares de los datos.

En lo que respecta a las notificaciones en caso de ocurrir una vulneración de seguridad a los datos personales, los responsables del tratamiento no se encuentran obligados a notificar al INAI, a diferencia de lo que ocurre en los países de la Unión Europea o Brasil, en donde sí se debe realizar una notificación detallada sobre la vulneración y las acciones tomadas para mitigar los riesgos ocasionados a los titulares de los datos.

Por lo que, si un titular sufre una afectación a sus datos personales, tendrá que iniciar un procedimiento de verificación ante el INAI por sus propios medios, y como lo demuestran las cifras oficiales del INAI, son muy escasos los procedimientos iniciados a petición de parte, y en lo que respecta a los procedimientos de verificación iniciados de oficio por el INAI, son nulos.

Dicha falta de verificación propicia a un nivel de cumplimiento dudoso e incierto por parte de los responsables del tratamiento.

Por otro lado, la LFPDPPP tampoco prevé la obligación para el responsable de mantener un registro de las actividades de tratamiento que realiza, y que incluya una descripción de las medidas técnicas y organizativas de seguridad que se tienen implementadas para proteger los datos.

Esta medida se considera una excelente práctica preventiva, para que los responsables del tratamiento tengan un mapa claro de dónde y cómo tratan los datos personales, y puedan en su caso implementar medidas de seguridad adecuadas.

Como último hallazgo del análisis realizado a la LFPDPPP, esta no establece la obligatoriedad de realizar evaluaciones del impacto en la protección de datos, que son muy útiles para detectar riesgos, amenazas y vulnerabilidades, y prevenirlos mediante la aplicación de controles de seguridad específicos para cada actividad de tratamiento.

Por lo que, si un responsable pretende implementar un nuevo tratamiento a través de algún sistema o tecnología novedosa, hoy no se encuentra obligado a identificar los posibles riesgos, por lo que mucho menos se ve obligado a contar con un plan de mitigación en caso de ocurrir una vulneración.

Por todo lo anterior es que se considera que el marco regulatorio que soporta al deber de seguridad dentro de la LFPDPPP no es preventivo, y se requiere de una reforma que propicie a proteger de manera preventiva los datos personales.

Las reformas propuestas a la LFPDPPP y su reglamento se consideran pertinentes en virtud de que están alienadas al objetivo de la propia LFPDPPP, esto es, regular el tratamiento de los datos, garantizando así la privacidad de las personas.

Aunado a lo anterior, las reformas propuestas están alineadas a los marcos regulatorios más avanzados en la actualidad, y que han dado resultados favorecedores en cuanto a aumentar el nivel de cumplimiento por parte de los responsables del tratamiento.

Se espera que el presente trabajo de investigación, sus hallazgos y propuesta sirva como guía de partida y anime a las personas que se encuentran en las posiciones adecuadas del Poder Legislativo a redactar una iniciativa de reforma efectiva para su registro ante la H. Cámara de diputados del Congreso de la Unión.

Bibliografía y fuentes consultadas

ARELLANO TOLEDO, Wilma, OCHOA VILLICAÑA, Ana, "Derechos de privacidad e información en la sociedad de la información y en el entorno TIC", *Revista IUS,* México*,* enero-junio 2013, *V*ol. 7, núm. 31, *http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472013000100010*

CARBONELL, Miguel, Los derechos fundamentales en México, México, UNAM, 2004, *http://ru.juridicas.unam.mx/xmlui/handle/123456789/10341*

Comisión Nacional de Derechos Humanos, "¿Qué son los derechos humanos?", Portal de la CNDH, *https://www.cndh.org.mx/derechos-humanos/que-son-los-derechos-humanos*

Constitución Política de los Estados Unidos Mexicanos, Diario Oficial de la Federación, México, 5 de febrero de 1917, *http://www.diputados.gob.mx/LeyesBiblio/pdf_mov/Constitucion_Politica.pdf*

Convención Americana de Derechos Humanos, San José, Costa Rica, 22 de noviembre de 1969, *https://www.cndh.org.mx/sites/default/files/doc/Programas/TrataPersonas/MarcoNormativoTrata/InsInternacionales/Regionales/Convencion_ADH.pdf*

Declaración Universal de los Derechos Humanos, París, 10 de diciembre de 1948, *https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf*

DELÓN VÁZQUEZ, Manelic, "La protección de datos personales mediante una garantía constitucional"*, Consejo de la Judicatura Federal*, serie monografías, México, 2019, vol. 4.

GARCÍA GONZÁLEZ, Aristeo, "La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado", *Boletín Mexicano de Derecho Comparado*, México, septiembre-diciembre 2007, núm. 120.

Grupo de Trabajo del art 29, Dictamen 4/2007 sobre el concepto de datos personales, junio 2020, *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf*

Grupo de Trabajo del art 29, WP 80 Documentos de trabajo sobre biometría, agosto 2003, fecha de consulta: octubre 2021, *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf*

Instituto Nacional de Acceso a la Información, Transparencia y Protección de Datos Personales, Diccionario de protección de datos personales, Conceptos fundamentales, México, 2019

Instituto Nacional de Acceso a la Información, Transparencia y Protección de Datos Personales, Guía para el tratamiento de datos biométricos, México, marzo 2018, *https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/GuiaDatosBiometricos_Web_Links.pdf*

Instituto Nacional de Acceso a la Información, Transparencia y Protección de Datos Personales, Metodología de análisis de riesgo BAA, México, junio 2015, *https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Metodolog%C3%ADa_de_An%C3%A1lisis_de_Riesgo_BAA(Junio2015).pdf*

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2016, México.

Ley 13,709 General de Protección de Datos Personales, Presidencia de la república subtitular secretaría general de asuntos jurídicos, 14 de agosto de 2018, Brasil, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Ley de Instituciones de Crédito, Periódico Oficial de la Federación, 19 de julio de 1990, México, *http://www.diputados.gob.mx/LeyesBiblio/pdf/43_200521.pdf*

Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Diario Oficial de la Federación, 05 de julio 2010, México. *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf*

Márquez Romero, Raúl. “Lineamientos para el proceso editorial”, IIJ-UNAM, México, IIJ-UNAM, 2013, *https://archivos.juridicas.unam.mx/www/bjv/libros/7/3349/3.pdf*

Organización Internacional de Normalización, ISO 27000, 2018, *https://normaiso27001.es/referencias-normativas-iso-27000/#terminos*

P. II/2014 (10a.), Semanario judicial de la federación y su gaceta, Décima época, Libro 3, febrero de 2014, Tomo I, página 274, *https://sjf.scjn.gob.mx/SJFSem/Paginas/Reportes/ReporteDE.aspx?idius=2*

005522&Tipo=1

Pacto Internacional de Derechos Civiles y Políticos, Nueva York, 16 de diciembre de 1966, *https://www.ohchr.org/sp/professionalinterest/pages/ccpr.aspx*

PESCHARD, Jacqueline, "Cien años del derecho a la privacidad en la constitución", en ESQUIVEL, Gerardo et al (coord.) *Cien ensayos para el centenario*, México, UNAM, 2017 tomo 2, pp. 361-378, *https://archivos.juridicas.unam.mx/www/bjv/libros/9/4319/1.pdf*

Real Academia Española, Diccionario de la Lengua Española, 23 edición, 2014, España. Recuperado de *https://dle.rae.es/dato?m=form*

Reglamento 2016/679 del Parlamento Europeo y del Consejo, Diario Oficial de la Unión Europea, 27 de abril de 2016, *https://www.boe.es/doue/2016/119/L00001-00088.pdf*

TENORIO CUETO, Guillermo (coord.), La protección de datos personales, revisión crítica de su garantía en el ordenamiento jurídico mexicano, México, TFJA, 2018, *http://cesmdfa.tfja.gob.mx/proteccion_datos/pdf/01.pdf*

UNESCO, Declaración Internacional sobre los Datos Genéticos Humanos, 16 de octubre 2013, Art. 1, *http://portal.unesco.org/es/ev.php-URL_ID=17720&URL_DO=DO_TOPIC&URL_SECTION=201.html*

UNESCO, Declaración Universal sobre el Genoma Humano y los Derechos Humanos, 11 de noviembre 1997, *https://www.cndh.org.mx/DocTR/2016/JUR/A70/01/JUR-20170331-ODN34.pdf*