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

“Plataforma digital interactiva para promover y facilitar el cumplimiento de las obligaciones en materia de protección de datos personales en posesión de particulares”

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

Presenta:

Martha Judith Sánchez Álvarez

Asesora:

Dra. Paulina Elisa Lagunes Navarro

Ciudad de México, 25 de noviembre 2022

CONACYT

INFOTEC POSGRADOS

Autorización de impresión

INFOTEC
POSGRADOS

AUTORIZACIÓN DE IMPRESIÓN Y NO ADEUDO EN BIBLIOTECA

Maestría en Derecho de las Tecnologías de la Información y Comunicación, MDTIC.

Ciudad de México, 17 de noviembre de 2022.

La Gerencia de Capital Humano / Gerencia de Investigación hacen constar que el trabajo de titulación intitulado:

"Plataforma digital interactiva para promover y facilitar el cumplimiento de las obligaciones en materia de protección de datos personales en posesión de particulares"

Desarrollado por la alumna: **Martha Judith Sánchez Álvarez,** bajo la asesoría de la **Dra. Paulina Elisa Lagunes Navarro;** 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 debe material de la Biblioteca de INFOTEC.

Vo. Bo.

Mtro. Felipe Alfonso Delgado Castillo
Gerente de Capital Humano

Anexar a la presente autorización al inicio de la versión impresa del trabajo referido que ampara la misma.

C.p.p Servicios Escolares

Agradecimientos

A mi esposo y familia por su paciencia, motivación y apoyo fundamental en el recorrido del posgrado, pero sobre todo por su acompañamiento en este logro educativo.

A mis padres por ser los impulsores de mi carrera académica y a quienes les debo la culminación de este proyecto.

A la Dra. Paulina Elise Lagunes Navarro por sus revisiones, consejos y guía durante el trayecto de aprendizaje, creatividad y elaboración de este documento.

Muchas gracias.

Tabla de contenido

Índice de figuras

Índice de Tablas

Índice de Diagramas

Siglas y abreviaturas

AEPD: Agencia Española de Protección de datos

ARCO: derechos de acceso, rectificación, cancelación u oposición.

ARCOP: derechos de acceso, rectificación, cancelación, oposición y portabilidad.

EUA: Estados Unidos de América

INAI: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

LGTAIP: Ley General de Transparencia y Acceso a la Información Pública

LGPDPPSO: Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados

LFPDPPP: Ley Federal de Protección de Datos Personales en Posesión de los Particulares

LFTAIP: Ley Federal de Transparencia y Acceso a la Información Pública

LFTAIPG: Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental

OEA: Organización de los Estados Americanos

TIC: Tecnologías de la Información y Comunicación

Introducción

Las Tecnologías de la Información y Comunicación (TIC) actualmente son un catalizador para la evolución y crecimiento económico de las empresas. Han permitido que los negocios se transformen, se creen nuevas formas o mecanismos de actividades comerciales, e incluso han replanteado cómo los mercados se desenvuelven.

La utilización de las TIC dentro de los negocios se ha convertido en un elemento esencial para la mejora de sus procesos internos o de desarrollo, de su gestión, diversificación, automatización, el cómo ofrecen sus productos y a quién. Así pues, para las empresas que buscan obtener resultados económicos positivos y ventajas competitivas frente a terceros, las TIC son una herramienta fundamental.

El almacenamiento masivo de información es uno de los diversos y amplios usos que las empresas le dan a las TIC. Sin embargo, dentro de dicho acopio se encuentra la información de carácter personal, misma que es utilizada para crear perfiles económicos, campañas publicitarias personalizadas, ofrecer productos o servicios, obtener clientes, entre otras acciones.

En ese tenor, gracias a la rápida y veloz obtención de datos personales y su resguardo es que las empresas pueden hacer uso de tal información para conseguir un beneficio económico; no obstante, esto implica que la utilización de información personal ponga en riesgo o vulnere derechos humanos, como lo son el de privacidad y la protección de datos personales.

Debido al flujo, transmisión, acceso, almacenamiento y procesamiento de información personal por medio de las TIC, sin duda, la privacidad y la protección de datos personales son temas que toman relevancia por su latente necesidad de salvaguarda ante la utilización de las herramientas tecnológicas y sus innovaciones.

En México, el derecho humano a la protección de datos personales se consolidó como derecho fundamental en la Constitución Política de los Estados Unidos Mexicanos, al momento en el que se introdujo en su artículo 16 el derecho

que tienen todas las personas al acceso, rectificación, cancelación y oposición de los datos personales.[1]

En atención a ello, se emitió la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), publicada el 05 de julio del 2010 con el objetivo de regular el tratamiento legítimo de los datos personales para que se realice de forma informada y controlada, con lo cual se garantice la privacidad y la autodeterminación informativa de las personas.[2]

Para efecto de lo anterior, la norma impone a las personas físicas o morales de carácter privado que obtengan, usen, almacenen o divulguen información personal un marco amplio de obligaciones que deben cumplir desde el momento en el que toman posesión de algún dato personal.

Así, para atender los principios y obligaciones previstos en la normativa los responsables deben elaborar documentos, capacitar personal, crear procedimientos internos, aplicar medidas de seguridad, entre otras gestiones, con las cuales se preserven los derechos de protección de datos personales y privacidad.

Sin embargo, de la revisión a estudios e información estadística que se mostrará durante el presente documento, se infiere que algunas de las diversas causas de transgresión a los principios y deberes establecidos en la norma o de la falta de cumplimiento de las obligaciones, es el desconocimiento de una persona física o moral sobre el hecho de ser responsable en términos de la ley, así como de las acciones y gestiones que deben llevar a cabo para cumplir con esta.

Por lo antes señalado, es que la presente propuesta busca fijar los elementos para la creación de una herramienta digital mediante la cual los usuarios en México conozcan, en primer lugar, si son responsables del tratamiento de datos personales en términos de la LFPDPPP, como también cuenten con los conocimientos de cuáles son las obligaciones que deben de cumplir, para que se encuentren en

[1] Cámara de Diputados, Constitución Política de los Estados Unidos Mexicanos, *Diario Oficial de la Federación*, México, 5 de febrero de 1917, última reforma publicada 28 de mayo de 2021, artículo 16, párrafo segundo, *https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf*.

[2] Cámara de Diputados, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación*, México, 05 de julio de 2010, artículo 1°, *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf*.

posibilidad de garantizar a sus clientes el derecho a la protección de datos personales.

Asimismo, se busca precisar las obligaciones que los responsables en términos de la LFPDPPP deben de cumplir, así como los documentos que deben efectuar para garantizar el derecho de protección de datos personales, como también, contrastar las herramientas digitales existentes que permiten a los responsables la elaboración de documentos legales para atender dichas obligaciones.

Por ello, con la finalidad de demostrar la viabilidad del proyecto que se presenta, se desarrollan cuatro capítulos que contienen el sustento jurídico del tema, la vinculación de este con las TIC, la justificación que pone de manifiesto la necesidad de describir los elementos que debe contener con un sitio web que sea utilizado como un medio para solucionar una problemática en el área y la aptitud de su aplicación en los sectores público, privado o académico.

En ese sentido, en el capítulo 1 se hará alusión al marco conceptual de los derechos a la protección de datos personales y privacidad, partiendo desde su entendimiento como derechos humanos. Asimismo, se referirán diversos conceptos de estos derechos, su naturaleza jurídica, su limitación y alcances, las diferencias y similitudes entre ellos, así como los aspectos relevantes de las TIC, incluyendo su conceptualización.

Con el objetivo de exponer el fundamento jurídico del proyecto, en el capítulo 2, se desarrolla el marco normativo de la protección de datos personales desde un panorama internacional y nacional, incluyendo el marco jurídico de la materia aplicable en Europa, norteamericana y Latinoamérica, así como el mexicano.

Para efecto de sustentar la importancia de la determinación de los elementos para la creación de la plataforma que se propone, en el capítulo 3, se establece cuándo se considera a una persona física o moral como responsable y se indican las obligaciones que estos deben de cumplir en términos de la LFPDPPP. Por otro lado, se incorporan estadísticas e informes de los que se infiere la situación o nivel de cumplimiento de la citada ley en México y los motivos por los cuáles se estima se incumple.

Por último, en el capítulo 4, se contrastan las herramientas digitales existentes y que son similares a la propuesta que se efectúa en este proyecto, se indican los elementos que se consideran las hacen amigables y entendibles, como también, en algunos casos, su funcionamiento y los resultados que pueden brindar. Posteriormente, se describen las características, bosquejo y diseño de la página web, así como algunos diagramas que muestran el flujo a seguir al momento del llenado del formulario de la plataforma.

Capítulo 1.

Marco Conceptual

Capítulo 1. Marco conceptual

Se ha señalado que el objeto de este proyecto es establecer los elementos para crear una plataforma digital con la que se facilite de forma sencilla a los usuarios, el conocer si son responsables del tratamiento de los datos personales y, por consiguiente, saber cuáles son sus obligaciones en la materia para que así cuenten con la información básica y necesaria que les permita garantizar la protección de datos personales y privacidad.

En esa tesitura, para hacer latente la importancia de la determinación de los elementos para la creación de un entorno web con las características que se desarrollarán en el capítulo 4, se estima necesario referir al reconocimiento que los derechos mencionados tienen como derechos humanos y los textos jurídicos que los contemplan en esta categoría o de los que se derivan.

Cabe destacar que, parte de la necesidad de la defensa de los derechos de privacidad y protección de datos personales, deviene del carácter que tienen como derechos humanos y por el papel que desempeñan para que el titular pueda desarrollar su personalidad dentro de la sociedad. Es por ello que, en este capítulo, se hace una breve referencia del contexto del que derivan y por el que se les da tal categoría.

Adicionalmente, se incluye un análisis sobre las generalidades sobre la privacidad y protección de datos personales, se desarrollan sus conceptos atendiendo al desarrollo que han tenido conforme su evolución desde que se han originado. De igual forma, se hace referencia a su connotación, características y elementos esenciales de su existencia mediante la referencia de ciertas posturas sobre su naturaleza jurídica.

Asimismo, en virtud de que los derechos humanos no son absolutos y pueden ser limitados mediante justificaciones expresas y válidas, es que también son referidos los límites y alcances que son aplicables para los derechos en estudio. En seguimiento a ello, para mostrar el bien jurídico que tutela cada derecho, de igual manera se mencionan las diferencias y similitudes que existentes entre ambos.

Por otra parte, debido a que en la presente propuesta se recurren a las TIC como un método de solución a la controversia planteada, y con la finalidad de advertir la vinculación entre las TIC y los derechos humanos en análisis, es que se alude a lo que se entiende por éstas, sus características, categorías e importancia que tiene su aplicación dentro de la sociedad.

Lo anterior, tiene como objeto el sustentar la importancia de la precisión de los elementos para la creación de la página web, pues si mediante esta herramienta digital se aumenta el nivel de usuarios que conocen si son responsables en términos de la ley, sus obligaciones y con ello cuentan con los insumos para cumplir con la protección de los derechos aludidos, en consecuencia, se justifica su origen al estar destinada a la defensa de derechos humanos.

1.1 Derechos humanos vinculados a la privacidad y protección de datos personales

De acuerdo con Ramón Gil Carreón el término de derechos humanos puede referir a dos tradiciones jurídicas diversas: la que vincula al derecho con una pretensión moral cuyo amparo es necesario preverse en normas jurídicas, esto es, afirmar la existencia de derechos en el ámbito moral con el alcance de ser positivos; y la que alude a figuras jurídicas reconocidas y tuteladas en un sistema jurídico como los derechos contenidos en una Constitución o tratados internacionales.[3]

Para Lucerito Ludmila Flores los derechos humanos *… son el conjunto de prerrogativas inherentes a la naturaleza de la persona y cuya realización efectiva resulta indispensable para el desarrollo integral del individuo que vive en una sociedad jurídicamente organizada*.[4] Sin estos derechos una persona no puede vivir

[3] Carreón Gallegos, Ramón Gil, "Derechos humanos, garantías individuales y derechos fundamentales. Problema terminológico o conceptual", Universidad Autónoma de Coahuila, Poder Judicial del Estado de Coahuila, Comisión de los Derechos Humanos del Estado de Coahuila, Editora Laguna, S.A. de C.V., 2012, pp. 133-134, *https://archivos.juridicas.unam.mx/www/bjv/libros/7/3171/7.pdf*.

[4] Flores Salgado, Lucerito Ludmila, *Temas actuales de los derechos humanos de última generación*, Puebla, México, Benemérita Universidad Autónoma de Puebla, 2015, p. 14, *https://archivos.juridicas.unam.mx/www/bjv/libros/9/4304/13.pdf*.

como ser humano, por lo tanto, pueden entenderse como las prerrogativas por las cuales se afirma la dignidad del individuo frente al Estado.[5]

En suma, los derechos humanos son aquellas potestades que una persona goza por el solo hecho de ser persona, pueden estar o no reconocidas en una Constitución o tratado internacional, pero si no son respetados por los demás individuos o asegurados por el Estado, la persona se verá obstaculizada para desarrollar su personalidad e integrarse dentro de su sociedad.

Así, la necesidad de proteger y amparar los derechos humanos deriva de su importancia para que la persona pueda desarrollarse de forma integral dentro de su entorno. Por ello, deben buscarse los mecanismos para que sean respetados, sobre todo por las autoridades.

En cuanto a las características que distinguen estos derechos sobre de aquellos que conforman el derecho positivo se encuentran las siguientes: son inherentes a la persona pues para su existencia no se requiere de un reconocimiento formal; son supremos al situarse en un nivel superior jerárquico frente a otros derechos; son transnacionales al atribuirse a la persona por su condición de ser humano y no se circunscriben a una reconocimiento por un poder público y son irrenunciables ya que su vigencia y validez no está sujeta a la voluntad del Estado o una persona.[6]

Por su parte, el Poder Judicial de la Federación resalta que los derechos humanos son universales al corresponderles a cualquier persona y al concernir a la comunidad internacional, y si bien son inviolables no son absolutos; son inalterables al tener un núcleo intangible; son interdependientes e indivisibles al estar relacionados entre sí, y son progresivos ya que constituyen el compromiso de que los Estados adopten lo necesario para que progresivamente se logre la plena efectividad de los derechos, esto es que de forma gradual y constante se llegue a su completa realización.[7]

---

[5] *Ibidem*, p. 18.
[6] *Ibidem*, pp. 23-26.
[7] Tesis I.4o.A.9 K (10a.), *Semanario Judicial de la Federación y su Gaceta*, Décima época, t. III, abril de 2013, p. 2254, *https://sjf2.scjn.gob.mx/detalle/tesis/2003350*.

Es menester mencionar que, los derechos humanos adoptaron una relevancia jurídica, social y académica con la emisión de la Declaración Universal de los Derechos Humanos aprobada por la Asamblea General de las Naciones Unidas en el año 1948,[8] la cual devino de la necesidad del reconocimiento de la dignidad intrínseca y los derechos iguales e inalienables de las personas al ser la base de la libertad, la justicia y la paz del mundo.[9]

La dignidad humana si bien no está definida textualmente en alguna norma jurídica, puede considerarse como aquella que debe protegerse y reconocerse para todos los individuos por igual sin distinción alguna, por el solo hecho de ser humano.[10] Esta es la base de la que se originan el cúmulo de derechos y libertades que le permiten al individuo desenvolverse y desarrollarse tal y como lo desea dentro de la sociedad, por lo cual, las autoridades deben respetarla y garantizarla en todo momento.

En concatenación con ello, es que se estima que los derechos de privacidad y protección de datos personales entran dentro de esta categoría al estar directamente vinculados con la dignidad humana y al ser sumamente necesarios para el desarrollo de la personalidad del individuo.

Ello es así, pues la privacidad otorga la potestad a su titular de decidir qué información de su vida privada hace pública o comparte con la sociedad y cuál restringe, aunado a que dentro de esta se contemplan los aspectos más personales del individuo. Mientras que la protección de datos personales otorga a la persona la facultad de decidir sobre el control y flujo de su información personal.

Ahora bien, previo a apuntar a los textos internacionales y nacionales que reconocen a los derechos ya mencionados y que les dan la calidad de derechos humanos, se mencionarán algunos casos de espionaje e intervención de comunicaciones que se suscitaron durante la segunda guerra mundial que motivaron la necesidad de protección del derecho a la privacidad.

---

[8] Flores Salgado, Lucerito Ludmila, *Temas actuales de los derechos humanos*,… *op. cit*, p. 21.
[9] Organización de las Naciones Unidas, *Declaración Universal de Derechos Humanos*, 10 de diciembre 1948, *https://www.humanium.org/es/ddhh-texto-completo*.
[10] Lefranc Weegan, Federico, *Holocausto y Dignidad Significado y fin de la invocación a la dignidad humana en el Preámbulo de la Declaración Universal de Derechos Humanos*, México, UBIJUS Editorial p. 101, *http://movaprinting.com/HOLOCAUSTO_Y_DIGNIDAD.pdf*.

Uno de los hechos más conocidos de espionaje e intervención de comunicaciones fue la intercepción de mensajes a las fuerzas alemanas, para ser descifrados con un tiempo sumamente reducido a través de la máquina conocida como la "Bomba" creada por Alan Turing junto con Gordon Welchman. Esta máquina decodificaba los mensajes encriptados por la máquina llamada "Enigma", la cual fue creada y utilizada por los alemanes para cifrar y descifrar mensajes.[11]

Con la utilización de la máquina creada por Alan Turing se lograron descifrar importantes mensajes que fueron clave para que los países aliados como Inglaterra, Estados Unidos e Italia ganaran batallas, e incluso, se afirma que jugaron un alto papel para la finalización de la Segunda Guerra Mundial; sin embargo, este tipo de acciones fueron en detrimento de la privacidad de las personas a quienes se les intervinieron sus comunicaciones, quienes fueron perseguidos u observados dentro de su esfera de vida privada.

Otro caso relevante sobre espionaje fue el de Virginia Hall, considerada por los nazis como una de las espías más peligrosa. Esta mujer estadounidense fue figura clave durante la Segunda Guerra Mundial, pues los servicios de inteligencia que prestó iban desde la recopilación de información, informante, implantación de bombas, intercepción de comunicaciones, entre otras;[12] no obstante, de la misma manera que en el caso de Alan Turing una de sus funciones era a transgredir las comunicaciones de las personas como también la privacidad de éstas.

Estos casos demuestran que durante la Segunda Guerra Mundial hubo un alto grado de violaciones a derechos humanos entre ellos el de la privacidad, lo cual detonó que en las normas que se crearon posterior a estos sucesos incorporaran la protección de este derecho o de sus elementos constituyentes.

En principio, la Declaración Universal de Derechos Humanos en su artículo 12, dispone que ninguna persona puede ser objeto de injerencias arbitrarias en su domicilio, familia, correspondencia, vida privada, y tampoco puede ser objeto de

[11] González, Guadalupe, "Legado tecnológico de la Segunda Guerra Mundial", *Prisma Tecnológico*, Universidad Tecnológica de Panamá, Editorial Tecnología, vol. 9, núm. 1, diciembre 2018, p. 40, *https://revistas.utp.ac.pa/index.php/prisma/article/view/2067/pdf*.

[12] Sadurní, J.M., "Virginia Hall, la espía más peligrosa de los aliados", 21 agosto de 2020, *https://historia.nationalgeographic.com.es/a/virginia-hall-espia-mas-peligrosa-aliados_15606*.

vulneraciones a su honra o reputación; por lo tanto, la persona tiene derecho a la protección de la ley contra tales ataques.[13]

En un nivel regional, y en el mismo sentido que la Declaración, la Convención Americana sobre los Derechos Humanos en su precepto 11 dispone que los individuos poseen derecho a que se reconozca su dignidad y se respete su honra; que ninguna persona puede ser atacada en su honra o reputación, ni debe tener injerencias arbitrarias en su vida privada, domicilio, correspondencia o familia; por lo cual, ostentan el derecho a la protección de las leyes contra esos abusos.[14]

En sentido similar, la Constitución Política de los Estados Unidos Mexicanos en su artículo 16, párrafo primero, prevé que ninguna persona puede ser molestada en su familia, domicilio, papeles, posesiones o en su persona, salvo por determinación de una autoridad competente en la que se funde y motive legalmente la causa del procedimiento.[15]

En tal tenor, se concluye que el derecho a la privacidad se encuentra reconocido indirectamente en textos internacionales protectores de derechos humanos, como también se ampara en la Constitución Política de los Estados Unidos Mexicanos mediante la defensa de otros derechos que son elementos constitutivos de la privacidad.

Adicionalmente, se colige que el derecho de la privacidad al ser un componente de la dignidad humana y una prerrogativa inherente a la persona que le permite desarrollarse integralmente e integrarse dentro de la sociedad es un derecho humano.

Por otra parte, el objetivo del derecho de protección de datos personales consiste en garantizar el tratamiento legal de la información personal de las personas físicas identificadas o identificables, por lo que, esta potestad les otorga

---

[13] Organización de las Naciones Unidas, *Declaración Universal de Derechos Humanos*,… *op. cit.*, artículo 12.

[14] Organización de los Estados Americanos, *Convención Americana sobre Derechos Humanos*, San José, Costa Rica, artículo 11, p. 6-7, *https://www.cndh.org.mx/sites/default/files/doc/Programas/TrataPersonas/MarcoNormativoTrata/Ins Internacionales/Regionales/Convencion_ADH.pdf*.

[15] Cámara de Diputados, *Constitución Política de los Estados Unidos Mexicanos*,… *op. cit.,* artículo 16, párrafo primero.

la facultad de controlar y decidir de forma libre e informada sobre las condiciones y características del tratamiento de sus datos personales.[16]

Se resalta que la protección de datos personales sí se encuentra reconocida expresamente en la Constitución Política de los Estados Unidos Mexicanos, y aunado a que es un derecho intrínseco de la persona al dotarle de facultades para desarrollarse dentro de la sociedad, se desprende que es un derecho humano autónomo y de carácter instrumental.

Es un derecho humano autónomo pues permite al titular controlar el flujo de su información personal, con lo que pasa a ser patrimonio jurídico inherente de las personas, otorgándole además la facultad de oponer este derecho frente a otros particulares tomando así dimensiones reales.[17] Tiene el carácter de instrumental en tanto que a través de su ejercicio se pueden ejecutar o proteger otros derechos fundamentales como el honor, la intimidad, la privacidad, la imagen, o la salud.

Sostiene lo anterior, lo establecido por el Tribunal Constitucional Español en su sentencia 292/2000 de fecha 30 de noviembre, en la que determina que el hecho que los datos sean de carácter personal no significa que solo protejan los relativos a la vida íntima o privada del titular, sino también aquellos que permitan su identificación o que en determinadas circunstancias constituyan una amenaza para la persona.[18]

En concatenación con lo antes mencionado, sobre la jerarquía de la implementación de derechos humanos en México, el artículo 1 de la Constitución Política de los Estados Unidos Mexicanos dispone que *… todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado mexicano sea parte, así como de las*

---

[16] Davara, Isabel, Cervantes Padilla, *et. al.*, "Protección de datos personales", en Davara, Isabel (coord.), *Diccionario de Protección de Datos Personales Conceptos fundamentales*, México, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, primera edición, noviembre de 2019, p. 687, *https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf*.

[17] Tenorio Adame, Manuel, "La protección de datos personales desde el derecho al acceso al a información y como derecho fundamental autónomo, el caso mexicano", Colombia, *Revista Internacional de Protección de Datos* Personales, núm. 1, julio-diciembre de 2012, p. 10, *https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/5_-Manuel-Tenorio_FINAL.pdf*.

[18] Tribunal Constitucional de España, *Sentencia 292/200*, Madrid, 30 de noviembre 2000, *http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276*.

garantías para su protección…,[19] de igual manera indica que las normas relativas a estos derechos se interpretarán favoreciendo la protección más amplia y en todo momento a la persona,[20] es decir, se establece el principio pro persona.

En tal tenor, mediante jurisprudencia se ha determinado que el artículo 1 de la Constitución Política de los Estados Unidos Mexicanos reconoce una serie de derechos humanos que surgen de la propia constitución y de los tratados internacionales de los cuales el Estado mexicano sea parte, que su ejercicio únicamente puede ser restringido mediante una limitación expresa, y que se mantendrá en orden superior sobre el resto de las disposiciones jurídicas, debido a que la Constitución es una norma fundamental del orden jurídico mexicano. Por lo tanto, los derechos humanos son un parámetro de control de regularidad constitucional.[21]

Por lo que hace, al régimen interamericano sobre los derechos humanos y que es aplicable a México, de igual forma, la Suprema Corte de Justicia de la Nación falló que la jurisprudencia generada por la Corte Interamericana de Derechos Humanos, independientemente de que México haya sido parte o no, es vinculante para el Estado Mexicano, puesto que tal carácter se desprende del artículo 1 constitucional indicando con la aplicación del principio pro persona.[22]

En ese sentido, se trae a colación que la Corte Interamericana de Derechos Humanos sobre el derecho a la vida privada ha resuelto varios criterios relacionados con temas como la protección de familia, domicilio y correspondencia; la restricción de la vida privada conforme a los principios de legalidad y proporcionalidad; diferencias entre el derecho al honor y la reputación; la inviolabilidad del domicilio familiar y de comunicaciones; la intimidad; intercepción de conversaciones

---

[19] Cámara de Diputados, *Constitución Política de los Estados Unidos Mexicanos*,… *op. cit.,* artículo 1, párrafo primero.
[20] Cámara de Diputados, *Constitución Política de los Estados Unidos Mexicanos*,… *op. cit.,* artículo 1, párrafo segundo.
[21] Tesis P./J. 20/2014 (10a.), *Seminario Judicial de la Federación*, 25 de abril de 2014, *https://sjf.scjn.gob.mx/SJFSem/Paginas/Reportes/ReporteDE.aspx?idius=2006224&Tipo=1*.
[22] Tesis P./J. 21/2014 (10a.), *Seminario Judicial de la Federación,* 25 de abril de 2014, *https://sjf.scjn.gob.mx/SJFSem/Paginas/Reportes/ReporteDE.aspx?idius=2006225&Tipo=1*.

telefónicas durante un proceso penal; médicos e información confidencial; la libertad de expresión frente al derecho al honor, entre otros.[23]

En suma, los derechos a la privacidad y protección de datos personales están relacionados con el amparo de la dignidad humana, y ambos otorgan facultades con las que se permite el desarrollo de la personalidad del individuo dentro de la sociedad. Adicionalmente, pueden ser considerados como derechos fundamentales, puesto que en la Constitución Política de los Estados Unidos Mexicanos se establece la defensa de elementos constitutivos de la privacidad y la protección de datos personales se prevé de forma textual.

Por lo anterior, la propuesta de determinar los elementos para crear una herramienta digital con la que se facilite a los responsables el conocimiento de si son responsables en términos de la LFPDPPP y por esto deben observar las obligaciones que emanan de ella, tiene como objetivo el que de manera indirecta se resguarden los derechos de privacidad y protección de datos personales de las personas de quienes se tratan sus datos personales.

1.2 Generalidades sobre la privacidad

1.2.1 Concepto de privacidad

La privacidad ha sido un valor que se ha reconocido durante épocas y al que se le ha dado una apreciación de acuerdo con el contexto social, la ubicación geográfica y la temporada de la línea del tiempo en la que se ubique la persona.

Se puede decir que se originó a finales del siglo XVIII cuando se efectuó la separación del Estado y del ciudadano, es decir, entre lo público y lo privado; como también al momento en el que en los marcos jurídicos reconocieron los derechos individuales de las personas. Sin embargo, la noción de privacidad ha evolucionado durante el paso de los años teniendo diferentes concepciones en el entorno social, en la academia y en el propio derecho.

Alberto Sánchez, en su análisis sobre la privacidad desde el enfoque de las capacidades, consideró que en el continente europeo el pensamiento liberal de

[23] Silva García, Fernando, *Jurisprudencia Interamericana sobre derechos Humanos Criterios esenciales,* México, 2011, pp. 177-179, *https://www.corteidh.or.cr/tablas/r28946.pdf*.

Locke influyó en el entendimiento del derecho a la privacidad, en virtud de que afirmaba que éste responde a la necesidad intrínseca de cada persona de controlar sus asuntos; pero fue Immanuel Kant quien tuvo una mayor resonancia al estimar que la persona disfruta del derecho al respeto de sus semejantes y está obligado recíprocamente a brindar ese respeto, ello debido a que el hombre debe tenerse siempre como un fin y no como un medio, pues en esto reside su dignidad.[24]

Louis Brandeis, coautor del artículo *The Right to Privacy* a inicios del siglo XX, señalaba que el derecho más comprensivo y valorado por los hombres civilizados era la privacidad. Incluso a finales del siglo XIX Thomas Cooley indicaba que la privacidad refería al derecho que tiene la persona de dejarlo a estar solo.[25]

No obstante, con la intromisión de las TIC en la vida cotidiana de las personas, el uso de redes sociales y el flujo de millones de datos personales a través del Internet, han contribuido a que el concepto de privacidad haya evolucionado, lo cual ocasiona que se amplíen y modifiquen sus alcances y límites; es decir, si bien su significado no ha sido replanteado, los términos de su aplicación en el entorno de la persona son distintos y dependen de las circunstancias que se presenten como del contexto.

En la Constitución Política de los Estados Unidos Mexicanos no existe una mención directa a la salvaguarda del derecho a la privacidad con la que se defina concretamente, pero como se abordará posteriormente, este derecho al tener diversas facetas se ha visto protegido por medio de otros derechos que se encaminan a defender la esfera jurídica y privada de los individuos como, por ejemplo, el que nadie puede ser molestado en su familia, persona, o domicilio, o el que refiere a la inviolabilidad de las comunicaciones.

En el ámbito académico, Jacqueline Peschard sostiene que la privacidad hace referencia a una esfera de la vida que está protegida del escrutinio de los otros

[24] Sánchez Rojo, Alberto, "El derecho humano a la privacidad desde el enfoque de las capacidades: una reflexión educativa", *EDETANIA*, Madrid, España, julio 2017, p. 160, *https://riucv.ucv.es/bitstream/handle/20.500.12466/574/113-Texto%20del%20art%c3%adculo-306-1-10-20171109.pdf?sequence=1&isAllowed=y*.

[25] Peschard, Jacqueline, "Cien años del derecho a la privacidad en la Constitución", *Cien ensayos para el centenario*, Instituto de Investigaciones Jurídicas, tomo 2, núm. 786, México, 2017, p. 362, *https://archivos.juridicas.unam.mx/www/bjv/libros/9/4319/23.pdf*.

ya que solo atañe a la persona en lo individual, aunado a que está fuera de la intromisión del Estado.[26]

Ileana Hidalgo apunta que el derecho a la privacidad protege al humano de cualquier intromisión no consentida, en su vida, familia o propiedad, como en lo que respecta a su imagen ante la sociedad. Esto implica que el Estado mediante su normativa interna otorgue garantías legales con las que se obstaculice la injerencia arbitraria.[27]

Por su parte Olivia Andrea Mendoza Enríquez dispone que es el derecho que posee el individuo de separar aspectos de su vida privada del escrutinio público, esto es, a desarrollarse en un espacio reservado a ciertos ámbitos de la vida personal.[28]

Desde una aproximación objetiva a la privacidad, ésta puede entenderse como la injerencia mínima del poder público en las relaciones de los sujetos; mientras que desde un punto subjetivo se contempla a los individuos como titulares de derechos y a quienes mediante normas se les otorgan facultades y atribuciones para resguardar elementos de su entorno y vida basados en los límites autoimpuestos.[29]

En conclusión, existen varios elementos que se pueden resaltar derivado del análisis de las definiciones señaladas con antelación respecto al derecho a la privacidad: el bien jurídico tutelado es la esfera privada de la persona; busca evitar intromisiones por parte de los poderes públicos; son los titulares de la información quienes controlan y deciden con quién y en qué momento compartirla.

Ahora bien, para tener un contexto amplio sobre la esfera jurídica que se pretende proteger dentro de la privacidad, se considera necesario hacer alusión a

---

[26] *Idem.*

[27] Hidalgo Rioja, Ileana, *Derecho a la protección de datos personales*, México, Instituto Nacional de Estudios Históricos de las Revoluciones de México, Instituto de Investigaciones Jurídicas, p. 7, *https://inehrm.gob.mx/recursos/Libros/DerProtectDatos.pdf*.

[28] Mendoza Enríquez, Olivia, "Privacidad", en Davara, Isabel (coord.), *Diccionario de Protección de Datos Personales Conceptos fundamentales*, México, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, primera edición, noviembre de 2019, p. 672, *https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf*.

[29] Kubli-García, Fausto, "Componentes del derecho a la privacidad", *Revista del Posgrado en Derecho de la UNAM*, nueva época, año 4, núm. 7, julio-diciembre 2017, p. 28, *http://revistaderecho.posgrado.unam.mx/index.php/rpd/article/view/109/118*.

otros dos términos que convergen con este derecho siendo la intimidad y la vida privada.

La intimidad refiere al espacio exclusivo que todas las personas disfrutan independientemente de si son personajes públicos o particulares, pues gozan de la no interferencia de los demás. Por esto, se constituye en el ámbito que cada una persona tiene preservado al mundo exterior, en donde encuentra las posibilidades de desarrollo y fomento de su personalidad.[30]

Mientras que la vida privada, alude a las acciones que no se desempeñan en la actividad pública, y los terceros no tienen acceso a estos datos; por lo que acapara a todas las acciones y manifestaciones que están apartadas de la proyección pública de la persona que representa en la sociedad por las que se le imponen ciertas relaciones o contactos con terceros. [31]

Así pues, se puede aseverar que el entendimiento del derecho a la privacidad ha cambiado durante el paso de los años y se ha adaptado de acuerdo con el contexto social, económico y contemporáneo en el que se ubica; y su interpretación depende de la demarcación territorial en la que se encuentre la persona, o si está en el ámbito digital o fuera de él.

Si bien es un derecho que no se encuentra textualmente expresado en textos jurídicos internacionales o en la Constitución, su reconocimiento se ha dado por medio de otros derechos y a través de las determinaciones de tribunales en la jurisprudencia o en la doctrina.

De la conjunción de las interpretaciones que se han emitido se afirma que la privacidad brinda a los individuos el derecho de elegir qué información de su vida privada hacen pública o la comparten con la sociedad y cuál restringen a su núcleo familiar, de amigos o incluso para sí mismos.

Una vez establecido un marco de referencia de lo que se entiende por el derecho a la privacidad, se estima conveniente hacer alusión a las características con las que se determine el régimen aplicable a este derecho, en virtud de esto, en seguida se analizará la naturaleza jurídica de la privacidad.

---

[30] Hidalgo Rioja, Ileana, *Derecho a la protección de datos personales,… op. cit.,* p.5.
[31] *Ibidem*, p. 6.

1.2.2 Naturaleza jurídica de la privacidad

El artículo *The Right to Privacy* publicado por Warren y Brandeis en 1890 es conocido como la fuente doctrinal jurídica más influyente en Estados Unidos de Norteamérica sobre la protección de la privacidad, pues en este se habla del necesario reconocimiento a no ser molestado, a ser dejado solo. Con esta propuesta, los autores contemplan que este derecho contiene una dimensión individual y colectiva, pues además instaura los límites de control del Estado sobre sus ciudadanos.[32]

La propuesta realizada por Warren y Brandeis se dirige a englobar dentro de la privacidad al derecho de aislarse y el de controlar la información personal, incluso cuando ya fue divulgada.[33] Esto es, que se rechaza cualquier injerencia sin consentimiento dentro de la vida de la persona, incluyendo la obstaculización de la intromisión del Estado en la vida privada.

Fausto Kubli-García señala que si bien la privacidad asume aspectos de vaguedad en su delimitación como otros derechos humanos y hace referencia a lo que se opone a lo público; lo cierto es que, debe considerarse como un principio jurídico, de naturaleza abstracta, que pretende ser el punto de partida para la creación de una instrumentación posterior, y además resulta ser el fundamento y causa de las normas sobre privacidad.[34]

En México, la Primea Sala de la Suprema Corte de Justicia de la Nación ha resuelto que la noción de privacidad refiere a: lo que no constituye vida pública; al ámbito que se reserva ante la acción y conocimiento de los demás; aquello que se decide compartir con quienes la persona elige; a las actividades del individuo en su esfera particular vinculadas con la familia y hogar y a las acciones que las personas no desempeñan en su carácter de servidores públicos.[35]

---

[32] Saldaña Nieves, María, "*The Right to Privacy*. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis", *UNED. Revista de Derecho Político*, núm. 85, septiembre-diciembre 2012, pp. 197-199, *http://revistas.uned.es/index.php/derechopolitico/article/view/10723/10242*.

[33] Mendoza Enríquez, Olivia, "Privacidad", en Davara, Isabel (coord.), *Diccionario de Protección, … op. cit.*, p. 673.

[34] Kubli-García, Fausto, "Componentes del derecho a la privacidad", *Revista del Posgrado en Derecho de la UNAM*,… *op. cit.*, p. 26.

[35] Tesis 1ª. CCXIV/2009, *Semanario Judicial de la Federación y su Gaceta,* Novena Época, diciembre 2009, p. 277, *https://sjf2.scjn.gob.mx/detalle/tesis/165823*.

Jacqueline Peschard menciona que este concepto muestra varias dimensiones: la física, la psicológica, la social y la informativa; y que su naturaleza no solo refiere a un derecho intrínseco de la persona, sino que abarca un catálogo de derechos que sitúan como centro la protección de diversas áreas de la actividad individual. Asimismo, indica que este derecho atiende a limitaciones, siempre que sean justificadas, como lo pueden ser aquellas en las que se pone en riesgo el interés público.[36]

Por su parte Olivia Mendoza coincide que este derecho se compone esencialmente de la prerrogativa a aislarse y del control de la información de carácter personal por parte del titular. Así, el derecho a la privacidad contempla algunos elementos inherentes encaminados a evitar intromisiones al sujeto como lo son la inviolabilidad del domicilio, de las conversaciones telefónicas y de comunicaciones, la salvaguarda del derecho a la reputación, a la honra y a la vida privada.[37]

En conclusión, se sostiene que los elementos de la privacidad consisten en que las acciones que suceden en el ámbito de la vida privada son susceptibles de defenderse; brinda el derecho a aislarse y controlar la información personal; no constituye a la vida pública; se comparte la información personal con quien se elige; y se reduce a la esfera particular relacionada con el hogar y la familia.

Finalmente, es de destacar que como el resto de los derechos humanos el de la privacidad no es un derecho absoluto, y ante él cabe la imposición de límites. Incluso, tanto en la doctrina como en las determinaciones judiciales se ha abundado sobre los alcances y términos de este derecho, lo cual se abunda en el siguiente apartado.

1.2.3 Límites y alcances de la privacidad

La Suprema Corte de Justicia de la Nación ha determinado que los derechos fundamentales no son absolutos y que pueden ser limitados mediante justificaciones válidas y previstas en la norma. De la misma manera, ha indicado

[36] Peschard, Jacqueline, "Cien años del derecho a la privacidad en la Constitución",… *op. cit.*, p. 363.
[37] Mendoza Enríquez, Olivia, "Privacidad", en Davara, Isabel (coord.), *Diccionario de Protección,… op. cit.*, p. 672.

que es posible la existencia de conflictos entre derechos ante lo cual cabe decidir qué derecho prevalece sobre el otro.[38]

En esa tesitura, cuando se habla de conflictos entre derechos, a manera de ejemplo, se hace referencia a la problemática que se crea cuando se confrontan el ejercicio del derecho a la libertad de expresión con el de la privacidad, al presentarse una vulneración a la vida privada e intimidad de una persona por la exposición de su información al público. En este caso, se advierte la existencia de un conflicto entre derechos fundamentales, por ello es necesario aplicar una ponderación de derechos.[39]

En virtud de que, la solución del conflicto delimitará los alcances que tendrán uno u otro derecho, se requiere efectuar un estudio del caso en concreto utilizando el criterio de proporcionalidad en el que se analicen los elementos de idoneidad, necesidad y proporcionalidad, para con ellos legitimar la preferencia de un derecho sobre el otro.[40]

Se reitera que, como todos los derechos humanos la limitación del derecho a la privacidad es excepcional y solo una autoridad competente puede determinarla, justificando y motivando las razones por las cuales es procedente tal reducción. Por esto, el estándar de la limitación de la libertad de carácter personal solo puede deberse a la tutela de otro derecho como el de acceso a la información pública o la libertad de expresión, pero en todo momento la afectación a la privacidad debe estar justificada válidamente.[41]

1.3 Aspectos relevantes sobre la protección de datos personales

1.3.1 Concepto de protección de datos personales

A diferencia del concepto estudiado anteriormente, la protección de datos personales es un derecho que fue reconocido en marcos jurídicos el siglo pasado.

[38] Tesis 1a. CCXV/2013 (10a.), *Seminario Judicial de la Federación y su Gaceta*, Décima época, julio de 2013, t. I, p. 557, *https://sjf2.scjn.gob.mx/detalle/tesis/2003975*.
[39] Tesis 1a. XLIII/2010, *Semanario Judicial de la Federación y su Gaceta*, Novena época, t. XXXI, marzo de 2010, p. 928, *https://sjf2.scjn.gob.mx/detalle/tesis/164992*.
[40] Tesis I.4o.A.70 K, *Semanario Judicial de la Federación y su Gaceta*, Novena época, t. XXIV, agosto 2006, p. 2346, *https://sjf2.scjn.gob.mx/detalle/tesis/174338*.
[41] Hidalgo Rioja, Ileana, *Derecho a la protección de datos personales,… op. cit.,* p.11.

Pero hasta hace algunas décadas se inició la conversación sobre la necesidad de proteger algunos derechos vinculados directamente con la persona como lo eran la responsabilidad del Gobierno sobre el debido tratamiento de la información que poseían de sus ciudadanos.

Fue en 1970 que el estado de Hesse en Alemania promulgó la Ley de Protección de Datos, convirtiéndose así en la primera norma en regular lo referente a los datos personales. En 1973, Suecia emitió su propia ley, y en 1974, el Congreso norteamericano emitió el *Privacy Act* en el que se incluyeron los principios esenciales de este derecho.[42]

A través de las leyes emitidas en la década de los años setenta, es que se asentaron las bases y principios para la adopción de la defensa de derechos como el acceso y corrección de datos personales, estos bajo el sustento de los principios de seguridad, calidad y finalidad.[43]

Para el año de 1990, la Asamblea General de la Organización de las Naciones Unidas emitió las Directrices para la Regulación de los Archivos de Datos Personales Informatizados, mediante las cuales se previeron las garantías mínimas para su amparo, adoptando los principios de legalidad, lealtad, exactitud, finalidad, acceso, no discriminación, y seguridad.[44]

En el año 1999, el Foro de Cooperación Económica Asia Pacífico (APEC) aprobó el Marco de Privacidad APEC con el que se buscó advertir la importancia de desarrollar la protección apropiada de los datos personales para con ello facilitar el libre flujo de la información.[45]

En México, antes del año 2002 no existía una legislación que regulara lo referente a la protección de datos personales, y si bien el Gobierno mexicano era parte de organizaciones internacionales que reconocían principios y derechos que defendían el bien jurídico tutelado como la ONU, la OCDE y APEC, fue hasta que se promulgó la Ley Federal de Transparencia y Acceso a la Información Pública

[42] Peschard, Jacqueline, "Cien años del derecho a la privacidad en la Constitución",… *op. cit.*, p. 372
[43] *Idem.*
[44] *Idem.*
[45] *Ibidem*, p. 373.

Gubernamental (LFTAIPG) que se introdujo en la normativa mexicana la facultad expresa de los ciudadanos sobre el manejo de su información personal.

Cinco años después de la entrada en vigor de la Ley, a nivel constitucional en el artículo 6 se estableció que la información de la vida privada y los datos personales debían ser salvaguardados en los términos y excepciones que fijaran las leyes, pero fue hasta el año 2009 con la reforma al artículo 16 constitucional que se reconoció a la protección de datos personales como un derecho fundamental.[46]

Cabe hacer mención que, con la introducción en la Constitución Política de los Estados Unidos Mexicanos del derecho fundamental a la protección de datos y la emisión de la LFTAIPG, se impusieron obligaciones y prohibiciones directas a las instituciones y autoridades públicas para garantizar el uso adecuado de los datos personales. No obstante, el alcance que se tuvo con estas disposiciones fue a nivel de sector público, dejando de lado cualquier deber por parte de las empresas y particulares sobre la información personal de sus clientes.

Con el objetivo de llenar el vacío legal existente sobre la regulación de la protección de datos personales dentro del sector privado, y por la necesidad de atender los requerimientos internacionales del comercio, es que se emitió la LFPDPPP, la cual impone los principios, deberes, obligaciones y delimitaciones de los derechos de la protección de datos personales a nivel federal en el sector privado.

Como se observa, el reconocimiento del derecho a la protección de datos personales a nivel internacional es relativamente nuevo y en México escasamente completa dos décadas. Por ello, lo que puede entenderse por este derecho, así como su alcance no ha evolucionado en la misma medida que el concepto de privacidad.

Ante lo anterior, a continuación, se hace una referencia a algunos conceptos a través de los cuales se puede identificar el bien jurídico tutelado por este derecho y que servirán para vislumbrar el por qué a través de la propuesta que en el presente trabajo se hace se podrá impulsar la protección de este derecho.

[46] *Ibidem*, p. 376.

Partiendo del ámbito internacional, la Unión Europea resuelve que los datos personales son *… cualquier información relacionada con una persona identificada o identificable, también denominada el interesado.*[47] Por su parte, la Agencia Española concreta que el derecho fundamental a la protección de datos *… reconoce al ciudadano la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre los mismos*,[48] precisando además que dichos datos permiten identificar a una persona, ya sea de manera directa o indirecta.

Mientras que en Inglaterra la Ley de Protección de Datos tiene el objetivo de controlar cómo las empresas, organizaciones y el gobierno utiliza la información personal. En suma, se advierte que en Europa se considera a la protección de datos personales como el derecho que tienen las personas para decidir sobre el tratamiento de sus datos personales.

En México, en el diccionario de protección de datos personales emitido por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), se le define como un derecho humano dirigido a proteger a una persona física identificada o identificable ante el tratamiento indebido o ilegal de su información personal, para lo cual se le brinda la facultad de controlar y decidir sobre las condiciones y características dicho tratamiento de una forma libre y formada, aunado a que pueden ejercer diversos derechos y medios de tutela jurídicos para salvaguardar la eficacia de ellos.[49]

Por lo que hace, al contenido esencial de la protección de datos personales, es conveniente citar a Víctor Hugo Magallanes Martínez quien señala que su núcleo duro se localiza en la atribución del titular del derecho para que su información sea tratada de forma adecuada, y que en caso de que el legislador intervenga sobre su

---

[47] Unión Europea, *Reglamento general de protección de datos*, 26 de marzo de 2021, *https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm*.

[48] Agencia Española de Protección de Datos, *Guía del derecho fundamental a la protección de datos de carácter personal*, 2004, p. 5, *https://datos.redomic.com/Archivos/GuiasUtiles/G33.pdf*.

[49] Davara, Isabel, Cervantes Padilla, *et. al.*, ”Protección de datos personales”, en Davara, Isabel (coord.), *Diccionario de Protección*,*… op. cit.*, p. 687.

regulación puede sustentarse en las teorías externas de interpretación de los derechos fundamentales.[50]

Ahora bien, la protección de datos personales brinda al titular la potestad de ejercer ciertos derechos como el de acceso (permite al titular allegarse de cualquier información personal que obre en posesión de un responsable); rectificación (se requiere la modificación, corrección o actualización de un dato personal); cancelación (la eliminación o supresión de datos personales en archivos, registros, expedientes o sistemas, con la finalidad de que dejen de ser tratados por quien los posee); y oposición (los datos personales dejan de ser tratados de alguna forma en específica o permite el cese de su tratamiento); a estos se les conocen como derechos ARCO.

No existe como tal una clasificación de datos personales que prevalezca tanto en Inglaterra, España, México o Latinoamérica, pero sí se reconocen categorías especiales de datos personales a las que se les debe dar un tratamiento especial por su sensibilidad. Es decir, en atención a que de darse a conocer cierta información personal que ocasione una vulneración o perjuicio al titular es que se les otorga una protección mayor.

Por ejemplo, la Unión Europea reconoce como categoría especial de datos personales el origen racial o étnico, las convicciones religiosas o filosóficas, la afiliación sindical, datos biométricos, orientación sexual y opiniones políticas. Cabe destacar que, dentro de esta clasificación también se incorporan a los datos genéticos y a las condenas e infracciones penales, mismos que no están aún considerados de tal forma en la normativa mexicana.

No obstante, de forma académica se han creado diversas categorías para la clasificación de los datos personales en las que se les distingue por el diferente nivel de tutela que merecen los datos, pues se afirma que no todos deben contar con la misma rigidez de protección.

Así, esta clasificación se divide en: los datos que son de libre circulación (nombre, documento de identidad, identificación tributaria, ocupación, fecha de

[50] Magallanes Martínez, Víctor Hugo Hiram, “Derecho a la protección de datos personales. Su diseño constitucional”, *Estudios en Derecho a la Información*, núm. 2, julio-diciembre de 2016, p. 38, *https://revistas.juridicas.unam.mx/index.php/derecho-informacion/article/view/10486/12651*.

nacimiento y domicilio); los de circulación restringida o a un sector (susceptibles de tratamiento con causa justificada y legítima); y los de obtención prohibida (su difusión afectaría la intimidad personal o familiar se conocen como datos sensibles).[51]

Por su parte, Marcelo Richter sostiene que se pueden distinguir diversas categorías de datos personales como los de identificación (nombre, teléfono, firma, nacionalidad, domicilio); patrimoniales (historial crediticio, ingresos, egresos, cuentas bancarias); laborales (centro de trabajo, puesto, escalafón); características físicas (tatuajes, señas particulares, altura); salud (padecimientos, enfermedades, historial clínico); características personales (huella digital, iris, tipo de sangre); y las que se componen de hábitos y preferencias (origen, preferencia sexual o política).[52]

En tal tenor, se concluye que el objetivo principal de la protección de datos personales es la defensa del individuo frente al tratamiento ilícito de su información personal mediante de cualquier medio incluido el de las TIC, esto independientemente de su categoría o su clasificación; empero, existe alguna información personal que amerita un mayor grado de protección por motivo de la vulneración que puede ocasionar al titular de los datos.

Finalmente, dentro de sus elementos se encuentran el que protege a una persona física identificada o identificable frente al tratamiento ilícito de sus datos personales; brinda al titular la facultad de decidir y controlar las condiciones y características del tratamiento de los datos personales; es instrumental al permitir el ejercicio de determinados derechos, y al manifestarse a través de ciertos principios y deberes; y es un derecho humano universal, inalienable, irrenunciable, intransferible, imprescriptible e indivisible.

---

[51] Mendoza Enríquez, Olivia Andrea, "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento", *Revista IUS,* 2018, vol. 12, núm. 41, Puebla, enero-junio, pp. 267-291, *http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267*.

[52] Richter, Marcelo, "La protección de datos de carácter personal como derecho humano", *Revista Auctoritas Prudentium*, Guatemala, año VII, núm. 12, primer semestre del 2015, pp. 18-29, *https://dialnet.unirioja.es/servlet/articulo?codigo=5002034*.

En seguida, se abordarán las características que constituyen el derecho a la protección de datos personales, en donde se desarrollará la concepción de la naturaleza jurídica del derecho humano analizado en este apartado.

1.3.2 Naturaleza jurídica de la protección de datos personales

Carlos E. Delpiazzo alude que la protección de datos personales ha transitado de un sentido negativo a uno positivo, pues durante la sociedad industrial solo brindaba protección a la esfera íntima de las personas evitando injerencias de terceros, es decir, mantenía un sentido negativo. Fue hasta mediados del siglo XX que obtuvo un sentido positivo al establecerse mecanismos y obstáculos para mantener la integridad de la intimidad de los sujetos.

En esa tesitura, Víctor Hugo Magallanes señala que este derecho además de haber evolucionado normativamente también lo hizo por conducto de criterios jurisprudenciales pronunciados por órganos jurisdiccionales; no obstante, su postura se centra en indicar que el núcleo duro del derecho no debe centrarse en la dignidad humana por ser un margen de identificación y aplicación muy amplio.[53]

Por ende, este derecho cuenta con la característica de ser transversal, ya que a través de él se hacen válidos otros como: el de salud, cuando se solicita el acceso a un expediente clínico; laboral, cuando se requiere la corrección de información de semanas cotizadas; penal, al momento de oponerse a la publicidad de su situación criminal apuntando a proteger su principio de presunción de inocencia.

En México, la protección de datos personales adicional a ser considerado un derecho humano también adquiere el carácter de derecho fundamental al estar reconocido en la Constitución Política de los Estados Unidos Mexicanos, con lo cual se sitúa al mismo nivel jurídico constitucional que otros derechos con los cuales frecuentemente colisiona como lo son el de acceso a la información pública y la libertad de expresión.

Aunado a lo anterior, el derecho en estudio cuenta con un carácter instrumental, al permitir la salvaguarda de bienes económicos debido al valor social y económico que poseen los datos personales en la actualidad. En ese sentido, se

[53] Magallanes Martínez, Víctor Hugo Hiram, “Derecho a la protección de datos personales. Su diseño constitucional”,… *op. cit.*, p. 36.

retoma lo afirmado por Olivia Mendoza al fijar que los datos personales tienen un valor económico equiparable a ciertos activos intangibles, como lo son el valor comercial de los nombres de dominio o el software, por lo que se les puede considerar como el petróleo de la sociedad de la información y conocimiento. [54]

De la misma manera, Nelson Remolina reconoce el carácter económico de los datos personales al señalar que la protección de estos a partir del uso de las TIC ha adquirido una nueva dimensión dentro de los modelos de negocios y en el ámbito digital que. En México, según Olivia Mendoza, esta dimensión es híbrida puesto que el modelo es el resultado de la incorporación reglamentaria europea y del derecho anglosajón.[55]

En consecuencia, el derecho a la protección de datos personales es un derecho humano y fundamental, que cuenta con el carácter de ser transversal e instrumental; otorga facultades directas a las personas para que ejerzan el control de su información personal; y brinda la posibilidad de velar por otros derechos mediante su ejercicio.

1.3.3 Límites y alcances de la protección de datos personales

En México, la Suprema Corte de Justicia de la Nación ha determinado que el Estado tiene la obligación de amparar el derecho de protección de datos personales, y debe realizar las gestiones correspondientes para potencializarlo, debido a las nuevas herramientas electrónicas pues ostentan riesgos por sus características.[56]

En ese orden de ideas, la protección de datos personales no solo es aplicable para el tratamiento de información en medios físicos, sino que aplica a todos aquellos soportes del medio digital. Es por lo que, atendiendo a la introducción de las TIC en este tratamiento que la protección de la información personal también es necesaria se traslade al ámbito digital, para que se cuenten con mecanismos que garanticen el debido tratamiento de datos personales y se resguarde la esfera jurídica de los individuos dentro ese entorno.

---

[54] Mendoza Enríquez, Olivia Andrea, "Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento",… *op. cit,* pp. 267-291.
[55] *Ibidem*, pp. 267-291.
[56] Tesis I.10o.A.6 CS (10a.)*, Gaceta del Semanario Judicial de la Federación*, Décima época, t. III, septiembre de 2019, p. 2200, *https://sjf2.scjn.gob.mx/detalle/tesis/2020564*.

No obstante, si bien este derecho ha ampliado los alcances de protección al sector tecnológico, de la misma manera presenta limitaciones. Al respecto, como se mencionó anteriormente, los derechos humanos y fundamentales no son absolutos, y ante ello puede imponerse restricciones con las que se garanticen otros derechos de la misma jerarquía.

En tal tenor, al existir la posibilidad de que el derecho a la protección de datos personales se conflictúe con otros derechos, de la misma manera que en el caso de la privacidad, se requiere de una ponderación de derechos para fijar cuál es el que debe privilegiarse de acuerdo con el contexto social y las particularidades específicas del caso en el que se presente dicha colisión.

Así, este derecho fundamental puede ejercerse por la persona en cualquier momento y deberá hacerse efectivo en los términos que la legislación lo permita; empero, hay supuestos que se exceptúan esta obligación.

El artículo 16, párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos dispone las excepciones al ejercicio de los derechos ARCO siendo: por razones de seguridad nacional, seguridad y salud públicas, cuando una disposición de orden público lo establezca, o cuando se procure la protección de derechos de terceros.

De igual forma, en la LFPDPPP y su Reglamento, se establecen supuestos de excepción para el ejercicio de este derecho y de los derechos ARCO. Algunos de estos refieren al otorgamiento del consentimiento para el tratamiento de datos; a los casos en los que el responsable no está obligado a cancelar datos personales; o la situación en la que se pueden hacer transferencias de datos sin el consentimiento del titular.

En conclusión, el derecho a la protección de datos personales es un derecho humano, pero no es absoluto. Ante él se pueden imponer ciertas limitaciones las cuales deben preverse en la legislación de manera expresa y deben estar justificadas; asimismo, sus alcances dependerán de la afectación que pueda tener al derecho de una tercera persona.

1.4 Diferencias y similitudes entre los derechos de protección de datos personales y privacidad

Como se ha mencionado, con la utilización de la herramienta digital, de la cual se proponen los elementos que le darían contenido este proyecto, se pretende que de manera indirecta se garanticen dos derechos humanos, el de la privacidad y la protección de datos personales.

Ante ello, se considera relevante observar que hay puntos en los que ambos derechos convergen, pero también hay algunos otros en los que no confluyen. Esto permite que haya una complementación para la protección integral de las personas. Por lo tanto, en este apartado se buscan resaltar las similitudes y diferencias de estos derechos.

Como punto de inicio, dentro de las similitudes que tienen estos derechos es que ambos son elementos consustanciales de la dignidad humana; son derechos que todo ser humano posee por el simple hecho de serlo; son inherentes a la personalidad del individuo; separan la vida privada de la pública; dotan al individuo del poder de decidir sobre el control y manejo de su información; y el Estado está obligado a garantizarlos por medio de normas y procedimientos, y para que puedan ser reducidos por éste dicha limitación debe estar debidamente justificada y fundamentada.

Sin embargo, dentro de las diferencias que presentan se encuentra la determinada por el Tribunal Constitucional Español en la que reconoció que la protección de datos personales tiene un objeto más amplio que el derecho a la vida privada, pues el primero amplía la garantía constitucional a los datos que no son relevantes, sean o no derechos constitucionales o relativos al honor, ideología, vida privada y familiar.[57]

Así, otro punto de diferencia es que el derecho a la privacidad no se encuentra previsto expresamente la Constitución Política de los Estados Unidos Mexicanos, en cambio la protección de datos personales sí se reconoce convirtiéndose en un derecho fundamental, además de ser un derecho humano instrumental y autónomo.

[57] Magallanes Martínez, Víctor Hugo Hiram, “Derecho a la protección de datos personales. Su diseño constitucional”,… *op. cit.*, p. 30.

Por otro lado, a partir de la protección de datos personales se derivan los derechos de acceso, rectificación, cancelación y oposición, aportando con ello mecanismos legales para garantizar la autodeterminación informativa y, por último, éste reconoce que el bien jurídico protegido no se restringe a la voluntad del titular, es decir, ampara los datos desde el momento de su recopilación.

Así pues, la protección de datos personales no implica que con su ejercicio de manera directa se ampare al derecho a la privacidad, pero sí resulta ser un elemento con el que se puede hacer efectiva su tutela, pues otorga procedimientos, mecanismos y garantías con las que se puede exigir la debida protección de la privacidad.

1.5 Aspectos relevantes de las Tecnologías de la Información y Comunicación

Las TIC son desarrolladas por los avances científicos que se originan en las áreas de la informática y las telecomunicaciones. Son el conjunto de tecnologías que permite acceder, tratar, producir y comunicar información que se presenta en diversos códigos como imágenes, videos o texto. Su elemento más representativo es el ordenador y en específico el Internet.[58]

El concepto planteado por Pedro Calandra y Manuel Araya se deriva de la conjunción de las definiciones individuales de tecnología, información y comunicación, por lo tanto, proponen que las TIC son *… cualquier soporte físico o virtual que almacene datos y códigos en una forma transportable, y que estos permitan establecer una comunicación entre seres humanos …*[59]

Juan Cristóbal Cobo indica que la definición con mayor puntaje identificada durante el *benchmarking* que realizó fue la de Fernández Muñoz, la cual señala que

[58] Ayala Ñiquen, Evelyn y González Sánchez, Santiago, *Tecnologías de la Información y la Comunicación*, Perú, Universidad Inca Garcilasco de la Vega, Fondo Editorial, 2015, p. 27, *http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/1189/Libro%20TIC%20%282%29-1-76%20%281%29.pdf?sequence=1&isAllowed=y*.

[59] Araya, Manuel y Calandra, Pedro, *Conociendo las TIC*, Santiago, Universidad de Chile, 2009, p. 16, *https://repositorio.uchile.cl/bitstream/handle/2250/120281/Calandra_Pedro_Conociendo_los_TIC.pdf?sequence=1*.

las TIC son innovaciones en microelectrónica, computación, optoelectrónica y telecomunicaciones que permiten la acumulación de grandes cantidades de información, así como su procesamiento, además de una fluida distribución de información mediante las redes de comunicación.[60]

Por su parte, Edgar Tello Leal menciona que las TIC son las tecnologías que permiten acceder y emitir abundante cantidad de información en tiempo real, con lo que se puede gestionar o transformar datos a través de herramientas que van desde ordenadores a dispositivos. Asimismo, apunta que son el resultado de la conjunción tecnológica entre diversas áreas como las de telecomunicaciones, microelectrónica, manejo de información y ciencias de la computación.[61]

De las definiciones antes mencionadas, se advierte que convergen en varios puntos en relación con lo que debe entenderse por TIC: son cualquier dispositivo o herramienta tecnológica que permite almacenar o procesar grandes cantidades de información en reducidos plazos; mediante ellas se pueden transferir grandes volúmenes de datos; permiten la comunicación entre personas las cuales pueden compartir diferentes tipos de información como videos, fotos o texto; y son aplicables a casi cualquier área o ámbito (social, económico, académico, de negocios, entre otros).

Debido a la característica de multidisciplinariedad que tienen las TIC, es que se han propuesto diversas clasificaciones sobre las mismas:

- Las blandas, pues al no ser necesariamente tangibles aluden a los conocimientos tecnológicos de tipo de comercialización, organizacional o administrativo; y las duras, que corresponden a las herramientas tangibles y se encaminan a los aspectos técnicos.
- Mass Media contempla a los elementos de difusión de un mensaje dirigido a una parte o toda la sociedad, y su objetivo es la de formar, informar y

[60] Cobo Romaní, Juan Cristóbal, "El concepto de tecnologías de información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento", *ZER: Revista de Estudios de Comunicación = Komunikazio Ikasketen Aldizkaria*, vol. 14, núm. 27, p. 305, *https://ojs.ehu.eus/index.php/Zer/article/view/2636*.
[61] Tello Leal, Edgar, "Las tecnologías de la información y comunicaciones (TIC) y la brecha digital", *Revista de Universidad y Sociedad del Conocimiento*, vol. 4, núm. 2, 2007, p. 3, *https://rusc.uoc.edu/rusc/es/index.php/rusc/article/download/v4n2-tello/305-1221-2-PB.pdf*.

entender al público que tiene acceso a dichos mensajes, lo cual sirve para la creación de opiniones e influencia en el público; y Multimedia, refieren a los dispositivos utilizados para presentar, administrar o transmitir información, esto es, el uso de software y hardware.[62]

Las categorías antes señaladas muestran la diversidad de usos y aplicaciones que tienen las TIC. Los alcances que representan van desde los aspectos técnicos y de operación hasta los mensajes e información que es compartida por y para la sociedad; finalmente, se destaca que su incursión se da en el ámbito político, económico, jurídico y social.

Las TIC se han convertido en una herramienta esencial para casi todas las áreas de la sociedad. Debido al uso del Internet o de dispositivos móviles se ha cambiado la forma en la que operan las empresas, la academia, la industria, o la sociedad, es decir, han transformado la forma en que se conducen las personas en estos sectores.

Si bien es cierto que su aplicación ha generado nuevos retos o problemáticas en diversos ámbitos, también lo es que las TIC son un elemento fundamental para la solución de problemas ya que, por ejemplo, tienen un impacto y alcance global; permiten la reducción y simplificación de pasos y procesos lo que ayuda a que cualquier persona pueda utilizarlas; tiene una alta capacidad de almacenamiento y de flujo de información, lo que permea en la toma de decisiones, generación de conocimiento y creación de opiniones.

En sentido similar, en el área de protección de datos personales y privacidad se presenta la situación que las TIC pueden generar problemáticas o nuevos paradigmas para atenderse, pero a su vez son herramientas elementales para resolver dichos problemas o retos; es decir, las TIC en vinculación con estos tópicos pueden ser parte del problema o de la solución a una circunstancia.

Un ejemplo sobre lo anterior es la creación de bases con datos personales que son utilizadas por las empresas ya sea para mejorar su forma de negocio,

[62] Echavarría, Stephania y Rocha Jenny, “Importancia de las T.I.C.s en el ambiente empresarial”, Bogotá, Universidad de La Salle, 2017, pp. 5-6, *https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=2482&context=administracion_de_empresas*.

incrementar ventas, brindar eficiente atención al cliente o facilitar información sobre servicios o productos, estas bases se resguardan por medio de programas de computación o de softwares, sin embargo, con la utilización de la tecnología se puede acceder sin autorización a dichas bases utilizando la información de forma indebida o ilegal, esto es, se crean brechas de seguridad.

Otro caso, es cuando una persona concede su información personal a través de una aplicación, página web o red social a una empresa para que le sea prestado un servicio o se le otorgue un bien lo cual es un beneficio para el titular, pero a la vez con el uso de las TIC sus datos personales son procesados y utilizados para finalidades distintas para las que fueron conferidos. Con esto, se acredita un tratamiento indebido de datos personales con el cual se transgrede el derecho humano de protección de datos personales del titular.

Las TIC representan una dualidad en cuanto a los beneficios y perjuicios que trae aparejada su aplicación en el entorno de la privacidad y protección de datos personales. En el caso en concreto del presente documento, como se abundará en el capítulo 3, se observa en México una problemática que muestra la dualidad que se menciona.

Dicha dualidad consiste en que, por motivo del uso masivo de tecnologías para el tratamiento de datos personales, en México se cuenta con un nivel de cumplimiento de obligaciones en materia de protección de datos personales en el sector privado insuficiente e ineficaz, pero a la vez se recurre a las herramientas tecnologías para colaborar en aumentar los niveles de cumplimiento aludidos.

Es por lo anterior que, en este proyecto se ha optado por recurrir a las TIC como un recurso para la solución del problema que se presenta, esto es, se propone que al establecer los elementos que darían forma y contenido a la plataforma digital con la que se ayude a parte de la sociedad mexicana a que de forma sencilla conozca, en primer lugar, si es responsable en términos de la LFPDPPP y, en segundo, si tiene la obligación de observar lo estipulado en ella, para con ello cuenten con la información que les permita cumplir con lo dispuesto en la ley.

Conforme a lo señalado, se busca fijar los elementos para crear una herramienta digital orientadora que esté al alcance de todos los mexicanos, que sea

beneficiosa para los responsables y, en consecuencia, para todos los titulares que sus datos personales sean objeto de tratamiento al existir una mayor probabilidad de que quienes deben velar por su información lo efectúen de forma debida y legal.

Capítulo 2.
Marco normativo de la protección de datos personales

Capítulo 2. Marco normativo de la protección de datos personales.

En el apartado que antecede se deja de manifiesto que los conceptos de privacidad y protección de datos personales han evolucionado conforme el paso del tiempo. De la misma manera, la normativa aplicable a estos derechos ha ido cambiando debido a las necesidades que la sociedad va presentando, pero en las décadas más recientes su modificación se debe a la introducción de las TIC en la vida cotidiana de las personas y el impacto que en ellas tiene.

El uso masivo de datos personales por parte de las empresas, la invasión a la privacidad a través de equipos o herramientas tecnológicas, el flujo de información personal por medio de redes sociales o derivado de las transferencias entre empresas trasnacionales, en general el uso incrementado de las TIC durante los últimos años son el motivo para que la regulación en la materia se haya generado y se encuentre en constante modificación.

Los cambios de algunas disposiciones normativas han delimitado los alcances y límites de los derechos de privacidad y protección de datos personales, pero también han establecido claramente quiénes son responsables sobre el tratamiento de datos personales, en qué momento, en qué lugar y cuáles son sus obligaciones y responsabilidades.

En tal tenor, la evolución del cuerpo jurídico ha tenido como objetivo el prever posibles situaciones que agraven la transgresión de los derechos señalados o establecer acciones u omisiones para resolver controversias suscitadas en relación con estos.

Así, en el presente capítulo se hará alusión a la normativa que se ha generado en distintas partes del mundo, su evolución, los alcances que han tenido y las situaciones que han regulado, ello desde una perspectiva internacional en la que se contempla la europea, la norteamericana y la latinoamericana, y desde la nacional, en la que se aludirá al marco normativo de protección de datos personales que se ha expedido en México, para finalmente hacer una comparativa de este con el de los otros países que son referenciados.

2.1 Panorama internacional

2.1.1 Europa

El continente europeo durante décadas ha sido el área geográfica en donde se ha estudiado y desarrollado en mayor medida la reglamentación en materia de protección de datos personales.

Es en la República Federal de Alemania donde se aprobó en 1970, la primera ley que reguló el tratamiento de datos personales, conocida como *Datenschutz*, misma que tuvo como objetivo otorgar garantías a las personas frente al tratamiento informatizado de sus datos nominativos por parte de las autoridades y administraciones del Estado.[63]

Tres años después, en Suecia, se publicó la norma *Datalag (1973:289)* que estableció un marco para el tratamiento de datos personales, en el que se incluyó una definición sobre lo que debía entenderse por datos personales; el otorgamiento de licencias y permisos para la creación y mantención de registros, las excepciones para las mismas; procesos de supervisión para las autoridades y las sanciones que se impondrían de ocasionarse un daño a una persona.[64]

Se resalta que en esta ley se previeron obligaciones específicas para los responsables del tratamiento de datos personales, y si bien no se señalaba que existan principios que deben observarse, sí contemplaba supuestos de los cuales ahora se puede afirmar son los que dan contenido a los principios que en la mayoría de las leyes actuales se ostentan proteger.

En el año 1977, de nueva cuenta en Alemania se regula sobre la materia con la proclamación de la Ley Federal de Protección de Datos de la República Federal Alemana, en la que se contempla un cúmulo de normas en general sobre el tratamiento de información personal, para el sector privado y el público, pero se incorporan conceptos novedosos como el bloqueo de datos o el de comisario de protección de datos.

---

[63] Cerda Silva, Alberto, "Mecanismos de control en la protección de datos en Europa", *Ius et Praxis*, Chile, Universidad de Talca, vol. 12, núm. 2, 2006, p. 222, *https://www.redalyc.org/pdf/197/19712209.pdf*.

[64] Skeriges Riksdag, *Datalag (1973:289)*, Justitiedepartementet L6, 1973, *https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/datalag-1973289_sfs-1973-289*.

En Francia, se aprobó la *Loi n.º 78-17 du janvier, relative à l'informatique, aux fichiers et aux libertés* o ley relativa a la informática, archivos y libertades el 07 de enero de 1978. Esta disposición introdujo la creación de la Comisión Nacional de la Informática y de las Libertades, siendo así la primera en su carácter encargada de supervisar el acatamiento de las normas sobre el tratamiento automatizado de información personal, como también de tramitar quejas.

Como se observa, diversos países en la década de los setenta comenzaron a desarrollar e instaurar un cúmulo normativo que permitieron originar las bases para un marco de protección de datos personales más integral y amplio.

No obstante, desde 1973 el Parlamento Europeo comenzaba a explorar la necesidad de contar con una política sobre la protección de los derechos fundamentales de las personas, y si bien el año siguiente se propuso la elaboración de una Directiva sobre el tema, fue hasta 1981 que se consumó la creación normativa.[65]

Así, el primer esfuerzo internacional por establecer un parámetro de regulación homogéneo entre países fue el realizado por parte del Consejo Europeo, a través de la emisión del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal o Convenio 108, pactado en Estrasburgo, el 28 de enero de 1981.

El objetivo del Convenio 108 es garantizar a las personas físicas, cualquiera que sea su nacionalidad o residencia y en el territorio de cada Parte, el respeto a sus derechos y libertades fundamentales, en específico el de la vida privada en relación con el tratamiento automatizado de sus datos personales.[66]

Su ámbito de aplicación abarca los ficheros y a los tratamientos automatizados de datos personales que surjan dentro del sector público y privado; así como al territorio del Estado miembro del Consejo de Europa que ratifique,

[65] Cerda Silva, Alberto, "Mecanismos de control en la protección de datos en Europa",… *op. cit.*, p 223.
[66] Consejo Europeo, *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, Estrasburgo, 20 de enero de 1981, artículo 1, *http://www.oas.org/es/sla/ddi/docs/u12%20convenio%20n%20108.pdf*.

acepte o apruebe el Convenio, como también el de cualquier país no miembro del Consejo pero que decida adherirse al documento.

Por lo anterior, se tiene que este es el primer instrumento internacional que prevé la emisión de supuestos y disposiciones que procuran regular el tratamiento automatizado de información personal, con la finalidad de que sean retomadas por las legislaciones nacionales y así encaminar que éstas se encuentren homologadas en el territorio europeo o entre aquellos países con los cuales se tengan relaciones económicas o políticas.[67]

Ahora bien, es conveniente resaltar que el principal ámbito de protección del Convenio es el procesamiento de datos personales de personas físicas, lo cual implica el almacenamiento, registro, difusión, extracción o borrado de la información, ya sea ejercida por el sector público o privado.

Así, en el Convenio se establece que las partes deben adoptar las medidas necesarias y suficientes para salvaguardar la protección de datos personales. A efecto de ello, se prevén los principios básicos que se requieren velar para hacer efectiva dicha protección.

En ese sentido, si bien no se contemplan categóricamente, como en otras leyes, los principios y deberes que se deben respetar, en el instrumento sí se retoman los supuestos que dan contenido a los principios de licitud, lealtad, información, calidad, proporcionalidad, como a los deberes de seguridad y confidencialidad.

Por otro lado, se sientan los parámetros para determinar la categoría de datos personales particulares o actualmente conocida como de datos personales sensibles, para esta clase el Convenio limita su tratamiento al imponer una serie de restricciones y salvaguardas para su adecuada observación, sin embargo, también permite excepciones que brindan flexibilidad sobre su uso.

Otro de los apartados que sobresalen del documento es el relativo al flujo transfronterizo de datos personales, en este, se incluyen los alcances que tendrá el

[67] Cerda Silva, Alberto, “Mecanismos de control en la protección de datos en Europa”,… *op. cit.*, p 224.

compartir información personal que sea tratada de forma automatizada o que haya sido obtenida para tal fin, entre diversos territorios.

Dentro de dichos parámetros, además, se dispone que un país no podrá someter a un tratamiento especial el flujo de la información personal con el argumento de la protección de la vida privada, pero sí tendrá facultades para imponer excepciones de forma legal.

Conforme lo anterior, se busca que el derecho interno de cada Parte cumpla con los supuestos mínimos equivalentes que el Convenio dispone para así consolidar una protección generalizada entre quienes transfieren o comparten la información de forma transfronteriza.

Aunado a ello, se considera que una parte fundamental que se incorpora es la cooperación entre países, pues con la asistencia mutua que se prevé sea brindada entre sí, se tiene un componente adicional para que se cumpla el objetivo del instrumento.

Posterior a la entrada en vigor del Convenio 108 se promulgaron otras normas que reiteraron algunas premisas del documento, como la aprobada por el Reino Unido en 1984 con el *Data Protection Act*; la Ley de Datos de la República Federal Alemana de 1990, y la Ley Orgánica 5/1992, de 29 de octubre, que regula el tratamiento automatizado de los datos de carácter personal en España.[68]

Se destaca que, la última ley aludida fue el precedente retomado por la mayoría de las legislaciones que se han decretado en Latinoamérica y México.

Por otro lado, debido al incremento del intercambio de datos personales entre países o empresas transnacionales y a la importancia que el flujo de información transfronteriza alcanzó durante las décadas siguientes a la emisión del Convenio 108 por el incipiente uso de las TIC, es que se tuvo la necesidad de establecer nuevos parámetros para regular la situación y con ello proteger los derechos humanos de las personas, en específico el de la vida privada.

Por tal motivo, es que se emitió el Protocolo adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de

[68] *Idem.*

carácter personal, a las autoridades de control y a los flujos transfronterizos de datos, en Estrasburgo, el 08 de noviembre de 2001.

El Protocolo estipula que las Partes dispondrán que la autoridad controladora que se cree será la encargada de hacer efectivas las medidas internas de los países que garantizan los principios señalados en el Convenio y en el propio protocolo. Para ello, se les dotará de independencia y de atribuciones de investigación e intervención y deberán atender las quejas presentadas en atención a la protección de datos personales.[69]

Como punto trascendente de este instrumento se resalta, la limitación del tratamiento de datos personales de forma automatizada cuando estos sean transferidos a un destinatario que no sea sujeto de aplicación del Convenio. Se establece que solo podrá realizarse la transmisión si el Estado destinatario u organización que no sea parte asegura un nivel de protección apropiado para la transferencia.[70]

Asimismo, considera algunos supuestos de excepción a lo referido en el párrafo anterior, pues se admite el compartir datos personales cuando el derecho interno del país Parte así lo prevea por motivos de intereses específicos del titular o intereses públicos importantes. De igual forma, se concede la transferencia si la autoridad competente conforme su legislación nacional contempla que el responsable otorga los medios suficientes para el debido tratamiento.

No obstante, además de las leyes específicas mencionadas y del Convenio 108 y su Protocolo, en Europa se han adoptado diversas disposiciones normativas, directrices y guías dirigidas a regular diversos aspectos vinculados con la protección de datos personales, algunos son emitidos por la Asamblea General de las Naciones Unidas, el Consejo de Europa y la Organización para la Cooperación y el Desarrollo Económicos.

---

[69] Consejo Europeo, *Protocolo adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos*, Estrasburgo, 08 de noviembre de 2001, artículo 1, *http://www.oas.org/es/sla/ddi/docs/u12%20convenio%20n%20108.pdf*.

[70] Consejo Europeo, *Protocolo adicional al Convenio para la protección… op. cit.*, artículo 3.

Las normas que se destacan por su relevancia sobre la materia son las siguientes:

Asamblea General de las Naciones Unidas

- Resolución 45/95 de la Asamblea General de la ONU, de 14 de diciembre de 1990. Su objetivo es establecer los principios rectores para la reglamentación de los ficheros computarizados de datos personales y es aplicable al sector público y privado.[71]

Consejo de Europa

- Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Su objetivo es hacer efectivo el derecho a la intimidad en relación con el tratamiento de datos personales, y prohibir la restricción de la libre circulación de los mismos por motivos vinculados con la protección.[72]
- Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE. Su objetivo es la armonización de la normativa de los Estados miembros respecto las obligaciones de los proveedores de servicios de comunicaciones electrónicas de redes públicas de comunicación en cuanto a la conservación de información obtenida o tratada por los mismos.[73]

---

[71] Asamblea General de la ONU, *Principios Rectores para la Reglamentación de los Ficheros Computarizados de Datos Personales*, 14 de diciembre de 1990, *http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf*.

[72] Consejo de Europa, *Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, Luxemburgo, 24 de octubre de 1995, artículo 1, *https://www.boe.es/doue/1995/281/L00031-00050.pdf*.

[73] Consejo de Europa, *Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE*, Estrasburgo, 15 de marzo de 2006, artículo 1, *https://www.boe.es/doue/2006/105/L00054-00063.pdf*.

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Su objetivo es reglamentar el tratamiento de datos personales y la libre circulación de los mismos; resguardar el derecho a la protección de datos personales y prohibir las restricciones a la libre circulación de información personal por motivos vinculados con la salvaguarda de las personas con respecto al tratamiento de sus datos.[74]

Cabe mencionar que, el Reglamento (UE) 2016/679 es aplicable cuando se da el tratamiento de datos personales por un establecimiento del responsable o del encargado en la Unión, ya sea de la Unión o no.[75] Por otro lado, en él se introducen una serie de derechos novedosos y recoge algunas soluciones a situaciones que se han presentado en los años más recientes con motivo del uso de las TIC.

Así pues, este reglamento pretende aplicarse a cualquier tratamiento de datos personales automatizado, no automatizado o que se resguarde los datos en un fichero.

Asimismo, como puntos novedosos instaura condiciones específicas para el tratamiento de datos del niño (artículo 8); prevé la transparencia de información, comunicación y modalidades sobre el ejercicio de los derechos (artículo 12); reconoce los derechos al olvido (artículo 17), el de la portabilidad de los datos (artículo 20) y el de las decisiones individuales automatizadas (artículo 22); prevé la protección de datos desde el diseño y por defecto (artículo 25) y la notificación por vulneraciones a la seguridad de la información personal.[76]

Por último, el Reglamento sustenta la creación del Comité Europeo de Protección de Datos como organismo de la Unión, el cual es dotado de personalidad jurídica, independencia y de atribuciones para garantizar la aplicación del

[74] Consejo de Europa, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 y por el que se deroga la Directiva 95/46/CE*, Bruselas, 27 de abril de 2016, artículo 1*, https://www.boe.es/doue/2016/119/L00001-00088.pdf*.
[75] *Ibidem*, artículo 3.
[76] *Ibidem*, artículos 8, 12, 17, 20, 22 y 25.

instrumento, mediante facultades de supervisión, asesoría, reglamentarias, de investigación, cooperación y promoción.

Organización para la Cooperación y el Desarrollo Económicos

a) Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales. Su objetivo es instaurar líneas para el sector público y privado sobre la forma en que procesan datos personales, debido al riesgo que esto presenta a la privacidad por el uso de las TIC en distintos aspectos de la vida económica y social, y por el incipiente procesamiento automatizado de datos.[77]

Cada una de las normas señaladas con antelación, está dirigida a regular algún aspecto específico vinculado con la protección de datos personales, ya sea enfocándose en los ficheros automatizados, al sector en el que será aplicable, los principios que son resguardados, a un espacio geográfico o una situación específica del tratamiento.

Un acierto de la regulación en el territorio europeo es que contempla a la cooperación internacional y el compromiso entre naciones, pues es parte fundamental para la debida ejecución de los instrumentos, y si bien disponen normas orientadoras, alcances y limitaciones sobre el tratamiento de la información personal, dejan algunas excepciones para que en el derecho interno puedan regularse acorde a las necesidades de la nación.

Algunas de las disposiciones son más generales que otras, pues no prevén supuestos específicos sobre situaciones que se desarrollan en la materia, como el otorgamiento del consentimiento por los titulares o sobre la transferencia de datos. Por lo tanto, aunque su contenido es diverso, la constante que presentan es la libertad otorgada a la persona de decidir sobre el ejercicio de su información y el esfuerzo encaminado a la protección de la vida privada, la intimidad y los datos personales.

De la misma manera, cuando se trata de la transferencia de datos personales en la que un destinatario que no es Parte del documento, la mayoría de las normas

[77] Organización para la Cooperación y el Desarrollo Económicos, *Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*, París, 2002, *https://www.oecd.org/sti/ieconomy/15590267.pdf*.

incluyen como salvaguarda la obligación de que la organización o país que reciba la información para el posterior tratamiento de los datos personales deba garantizar que cumple con los estándares adecuados para su debido resguardo y trato, tal y como se requieren dentro del territorio europeo.

Al respecto, es destacable la prohibición generalizada que estipulan los documentos normativos en cuanto a la posibilidad de compartir la información con otros países u organizaciones siempre y cuando los receptores cuenten con el mismo nivel de protección que quien remite los datos.

Finalmente, si bien es cierto que las disposiciones incluyen algunas prohibiciones, alcances y excepciones, también lo es que son genéricos y no profundizan en algunos puntos técnicos, como las finalidades del tratamiento, el otorgamiento del consentimiento, mecanismos de aceptación o no de la transferencia o imposición de sanciones.

La excepción de lo antes afirmado es el Reglamento (UE) 2016/679 que sí posee apartados específicos en los que además de establecer los principios, alcances e incluso sanciones que se deberán aplicar por el tratamiento de datos en el caso de su transmisión a otro país, aporta un marco regulatorio novedoso y el reconocimiento de derechos como el del olvido y la portabilidad de datos personales.

2.1.2 Latinoamérica

El cúmulo de leyes que se han expedido y que actualmente se encuentran vigentes en la mayoría de los países latinoamericanos, medularmente se centran en los principios y supuestos ya previstos en las leyes europeas o en el convenio 108 y en la Ley Orgánica 5/1992.

Esto refiere que, los países sudamericanos han retomado en gran medida el espíritu de las disposiciones europeas para replicarlas en su régimen legal interno, ello en parte por la similitud de los sistemas jurídicos.

A diferencia del sistema europeo en el ámbito regional americano no se ha consumado un régimen formal de cooperación internacional o de asistencia mutua entre los países de Latinoamérica. Es decir, entre los países que integran, por ejemplo, la Organización de los Estados Americanos (OEA) no se ha pactado un

Convenio o instrumento jurídico internacional que regule el tratamiento de datos personales que se comparte entre las naciones.

Sin embargo, la Asamblea General de la OEA solicitó al Comité Jurídico Interamericano que propusiera métodos de regulación sobre la protección de datos personales, incluso un proyecto de Ley Modelo en la que se adoptaran los estándares internacionales ya establecidos en la materia. Fue así como, en el 2015 dicho Comité aprobó la Guía Legislativa sobre Privacidad y Protección de Datos Personales.[78]

La Guía se fundamentó en los 12 principios previamente adoptados por el Comité en el año 2012, pero amplió sus alcances orientadores con la finalidad de otorgar a los Miembros facilidades para la creación e implementación de las leyes locales y las normas sobre la materia en términos de los elementos descritos en la guía.

Se destaca que, de igual forma que en los documentos jurídicos europeos, se contempla a la cooperación internacional como un componente fundamental para la promoción de la transferencia transnacional de datos y la limitación de cargas adicionales que restrinjan la libre circulación de información, con lo cual se brinde un nivel regional de protección de los datos en términos de los principios previstos en la Guía.[79]

Sin embargo, como se advierte no hay un insumo jurídico internacional que establezca los parámetros del tratamiento de datos que se comparten entre los países latinoamericanos, esto puede ser debido a la diferencia de desarrollo tecnológico existente entre los países, como por falta de un interés colectivo regional por implementar reglas en la materia.

Ahora bien, por cuanto hace a las legislaciones locales, en Argentina se promulgó la Ley 25.326 de protección de los datos personales el 30 de octubre de 2000. La cual dispone que, con la finalidad de amparar el derecho al honor y la

[78] Organización de los Estados Americanos, “Ley Modelo Interamericana sobre Protección de Datos Personales (en elaboración)”, *https://www.oas.org/es/sla/ddi/proteccion_datos_personales_ley_modelo.asp*.

[79] Comité Jurídico Interamericano, *Guía Legislativa sobre la privacidad y la protección de datos personales en las Américas*, 2015, *https://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_Guia_Legilsativa_CJI.pdf*.

intimidad de las personas, se protegerá de forma integral los datos personales que estén registrados en medios que traten datos, ya sean públicos o privados.[80]

La ley establece que para la formación de los archivos se deberán de atender los principios de licitud, calidad, información, consentimiento, como también los deberes de seguridad y confidencialidad; y para tal efecto, se incluyen las disposiciones específicas que se deben de observar para su debido cumplimiento.

En esta norma se incluyen los supuestos en los que los datos personales pueden ser cedidos para hacer efectivos ciertos fines, pero de igual manera, prevé los casos en los que puede darse una transferencia internacional y las excepciones en las que puede operar sin la necesidad de que el país receptor no proporcione parámetros de protección suficientes.

Como derechos de los titulares se reconocen el derecho a la información (conocer los registros o bases de datos, sus finalidades y la identidad de los responsables); de acceso (conocer y obtener su información personal); de contenido de la información (la información debe otorgarse de forma clara, decodificada y con lenguaje accesible) y de rectificación o supresión (los datos sean corregidos o eliminados).

Por otro lado, se determinó la creación de un órgano de control encargado de realizar las gestiones correspondientes para el cumplimiento de los objetivos de la ley. Si bien es cierto forma parte del Poder Ejecutivo se le brindó de autonomía funcional y de atribuciones para otorgar asesoría, emitir reglamentación, de control y sancionatorias.

Por último, se prevé un apartado que regula la acción de protección de los datos personales o de habeas data, para lo cual se disponen los casos en los que procederá, la legitimación que se tendrá, la competencia, el procedimiento, trámite y los requisitos de la demanda.

La Ley N° 18.331 Protección de datos personales y acción de “Habeas Data”, publicada en Uruguay el 18 de agosto de 2008, tiene como objetivo la protección de datos personales que sean usados en los ámbitos público o privado; no obstante,

[80] Congreso de la Nación Argentina, *Ley 25.326*, Argentina, 2000, artículo 1, *https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto*.

separa la regulación que tendrán las bases de datos de titularidad pública y de titularidad privada y dicta el procedimiento de la acción de protección de daos personales.[81]

Un año después, se publicó el Decreto N° 414/2009 protección de datos personales -acción de "Habeas Data"- reglamentación en la que se norma el funcionamiento de la Unidad Reguladora y de Control de Datos Personales, y se amplía sobre las atribuciones del Consejo Ejecutivo, la inscripción del Registro de Bases de Datos y las normas de actuación.[82]

Por su parte, en Colombia se decretó la Ley estatutaria 1581 de 2012 por la cual se dictan disposiciones generales para la protección de datos personales.

Esta al ser una ley más reciente, desde su artículo primero estipula que su objeto es *… desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma*.[83]

En dicha norma, como en las de los países ya mencionados, se establece un ámbito de aplicación para el sector público y privado; se retoma la obligación de la observancia de los principios y deberes; se reconocen los derechos y las condiciones para el tratamiento de la información personal con algunas precisiones; se disponen procedimientos para hacer efectivos los derechos; mecanismos de vigilancia y sanción; como también se regulan las transferencias transfronterizas de datos.

Una distinción que se advierte de esta norma es la clasificación del tipo de datos según el habeas data, dicha categorización es: datos públicos (no están

---

[81] Asamblea General República Oriental de Uruguay, *Ley N° 18.331 Protección de datos personales y acción de "Habeas Data",* República Oriental de Uruguay, 18 de agosto de 2008, artículos 2 y 3, *http://www.oas.org/es/sla/ddi/docs/U4%20Ley%2018.331%20de%20Protecci%C3%B3n%20de%20Datos%20Personales%20y%20Acci%C3%B3n%20de%20Habeas%20Data.pdf*.

[82] Presidencia de la República, *Decreto N° 414/2009*, Uruguay, 15 de septiembre de 2009, *https://www.impo.com.uy/bases/decretos/414-2009#:~:text=El%20derecho%20a%20la%20protecci%C3%B3n%20de%20los%20datos%20personales%20se,tipo%20que%20refiera%20a%20ellas.*

[83] Congreso de Colombia, *LEY ESTATUTARIA 1581 DE 2012*, Colombia, artículo 1, *https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49981*.

clasificados en otras categorías); datos privados (los que el titular no da su consentimiento para tratarlos); datos semiprivados (reservados a uso exclusivo del administrador del registro) y datos sensibles (de protección especial por su potencial discriminatorio).[84]

Finalmente, y de la misma manera que en Argentina, se crea la autoridad de protección de datos mediante una delegatura adscrita a la Superintendencia de Industria y Comercio. Así, se configura dentro del Gobierno Nacional una nueva autoridad encargada de la vigilancia y cumplimiento de la normativa en la materia.

En general, las leyes nacionales que se han emitido durante las últimas décadas muestran que han existido esfuerzos por parte de los países regionales americanos en establecer medidas regulación en la materia de protección de datos personales. En su mayoría, retomando los principios y disposiciones previamente adoptadas en la comunidad europea.

Sin embargo, cada país consideró que para un efectivo cumplimiento de las leyes que emanaron de su poder legislativo, era necesaria la creación de una autoridad dependiente del Gobierno que tuviera atribuciones para supervisar, controlar y hacer efectivo el derecho de la protección de datos personales en sus respectivas competencias.

También se resalta la incorporación de la acción de protección de datos personales o hábeas data y su regulación, pues es por medio de este mecanismo que se les otorga a los titulares una forma eficiente para hacer valer los derechos que les son reconocidos en las leyes.

2.1.3 Estados Unidos de América (EUA)

El sistema jurídico norteamericano a diferencia del europeo, latinoamericano y mexicano pertenece al *common law* o derecho común, el cual se conforma por la aplicación de los precedentes judiciales, las sentencias y razonamientos dictados por los jueces. La aplicación de la ley se subordina a la determinación de los

[84] Torres Llantén, Edgar, “La Protección de datos personales en Europa y en Colombia similitudes y diferencias”, p. 5, *https://repository.usc.edu.co/bitstream/handle/20.500.12421/2937/LA%20PROTECCION%20DE%20DATOS.pdf?sequence=1&isAllowed=y*.

tribunales, con lo que se genera el derecho, es decir, el derecho norteamericano es jurisprudencial.[85]

Si bien cuentan con una Constitución que es considerada la norma suprema, una Suprema Corte de Justicia y tribunales federales, cada estado tiene la facultad y competencia de determinar sus propias leyes, adoptan sus propios precedentes y sentencias judiciales con las que se va moldeando su derecho interno, por lo que, el derecho entre un estado y otro puede variar.

En gran medida, la concepción que se tiene de la privacidad en Estados Unidos de América, su interpretación, límites, alcances y protección se ha definido por la doctrina y las decisiones judiciales emitidas por los tribunales, más que por la emisión de leyes que regulen la materia.

Para efecto de comprender la connotación actual que tiene la privacidad en el país vecino, es necesario reiterar lo señalado en el artículo *The Right to Privacy* de Samuel D. Warren y Louis D. Brandeis, considerado como la fuente doctrinal jurídica más influyente en dicho país sobre la protección de la privacidad.

No pasa desapercibido que previo al artículo antes mencionado, el juez Thomas M. Cooley en su Tratado sobre el derecho de los agravios afirmó que las garantías de la Tercera, Cuarta y Quinta Enmiendas son medios de protección de la esfera individual, de la persona, la propiedad y de la documentación personal. Por otro lado, fue este juez quien acuñó la famosa expresión *the right to be alone* o el derecho a estar solo.[86]

Ahora bien, en el artículo *The Right to Privacy* al momento de discutir sobre la naturaleza de la privacidad, se expresa que inicialmente el *common law* asegura a cada persona el derecho de determinar ordinariamente hasta qué punto sus pensamientos, sentimientos y emociones son compartidos con otros, pero manifiesta que la protección de estos derechos son una instancia de aplicación

[85] Márquez Piñero, Rafel, *Cuadernos Constitucionales México-Centroamérica 13. El sistema jurídico de los Estados Unidos de América*, México, Universidad Nacional Autónoma de México, Corte de Constitucionalidad de Guatemala, 1994, p. 26, *https://archivos.juridicas.unam.mx/www/bjv/libros/1/206/1.pdf*.

[86] Saldaña Díaz, María, "El derecho a la privacidad en los Estados Unidos aproximación diacrónica a los intereses constitucionales en juego", *Teoría y realidad constitucional*, núm. 28, 2011, pp. 282-283, *https://dialnet.unirioja.es/servlet/articulo?codigo=3883001*.

vinculada con el derecho del individuo a que se le deje en paz, y que el principio que protege a la información privada de ser publicada no es el de propiedad, sino el que involucra a la personalidad.[87]

Así, los autores comienzan a poner de manifiesto la necesidad de brindar a las emociones, sensaciones y pensamientos la misma protección que se da a las conversaciones, actitudes, escritos o conductas, y ello mediante el derecho a la privacidad. No obstante, también reconocen que este derecho debe presentar restricciones y alcances.

En ese sentido, indican que la privacidad no puede prohibir que se publiquen los asuntos de interés público o general, la comunicación de un tema privado cuando la publicación sea en circunstancias de comunicación privilegiada; precisan que de ser divulgada la información por parte del titular o con su consentimiento, este derecho cesa y no se generaría alguna reparación.[88]

Como se advierte, hace más de cien años en el sistema jurídico norteamericano ya comenzaba a considerarse a la privacidad como un derecho inherente a la persona, como una facultad del individuo para ejercerla conforme a su albedrío o como una libertad, pero no como un derecho de propiedad como las que se otorgaban a otras prerrogativas intangibles.

María Saldaña alude que fue hasta la década de los sesenta que en la jurisprudencia inicia una interpretación de la Cuarta Enmienda centrándose en el derecho a la privacidad, pues refiere que en 1961 el Tribunal Supremo en el caso *Mapp v. Ohio* dictó que dicha enmienda genera un derecho a la privacidad, que no es menos importante que otro derecho y que es exigible al Estado.[89]

Asimismo, destaca que la interpretación que se comienza en esta época resulta ser un giro trascendente para la jurisprudencia de EUA, debido a que el

[87] Brandeis Louis D. y Warren, Samuel D., "The Right to Privacy", *Harvard Law Review*, vol. 4, núm. 5, 15 de diciembre de 1890, p. 205, *https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf*.
[88] *Ibidem*, p. 215-218.
[89] Saldaña Díaz, María, "El derecho a la privacidad en los Estados Unidos aproximación diacrónica a los intereses constitucionales en juego",… *op. cit.*, p. 286.

reconocimiento constitucional del derecho a la privacidad se basa en la toma de decisiones para el desarrollo de la personalidad del individuo.[90]

Posterior a diversos pronunciamientos por los tribunales y de la emisión de algunas leyes encaminadas a regular las invasiones a la privacidad, en 1974 se aprobó el *Privacy Act of 1974* o Ley de privacidad de 1974, misma que dispone una serie de reglas sobre el almacenamiento, obtención, uso y divulgación de información personal que es mantenida en las bases de datos de las agencias federales.[91]

De igual manera, establece el aviso público de sus sistemas de registro por medio de un Registro Federal y prevé las prohibiciones de la difusión de un registro sin el consentimiento expreso otorgado por el titular. Por otra parte, esta ley también reconoce un mecanismo para el acceso y rectificación de sus registros.

No obstante, como se ha mencionado, cada estado tiene la libertad de promulgar la normativa interna que los regula, por lo que, respecto a la materia han publicado diversas normas con el objetivo de proteger la información personal de los individuos. Pero fue por motivo de la entrada en vigor del Reglamento (UE) 2016/679, que diversos estados aprobaron nuevas leyes de protección de datos personales o modificaros las ya existentes para adecuarse a los términos de dicho reglamento.

Por ejemplo, el estado de Alabama emitió su primera Ley de notificación de violación de datos en el año 2018, dirigida a proteger a los consumidores, exige que las entidades notifiquen cuando exista un acceso no autorizado a información personal confidencial almacenada de forma electrónica.[92]

En el estado de Louisina con la finalidad de proveer protección a la información personal y de notificación sobre violaciones; para implementar prácticas

---

[90] *Ibidem*, p. 289

[91] Department of justice, Privacy Act of 1974, pp. 53-66, *https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf*.

[92] Alabama Senate, *Alabama Data Breach Notification Act of 2018*, Alabama, 13 de febrero de 2018, *https://legiscan.com/AL/text/SB318/2018*.

y procedimientos de seguridad; y proporcionar medidas en relación con vulneraciones se modificó la *Database Security Breach Notification Law*.[93]

Por último, en California se emitió el *California Consumer Privacy Act (CCPA)* o Ley de Privacidad del Consumidor de California de 2018, misma que proporciona a las personas un mayor control sobre los datos personales que son recabados por las empresas; como también establece nuevos derechos como el de eliminar información, el de excluirse a la venta de sus datos, el de no discriminación y el derecho a saber.[94]

A diferencia de México y el continente europeo, la legislación norteamericana es más flexible al momento de establecer parámetros, restricciones y alcances sobre la privacidad y la protección de datos personales. Esto debido a que su sistema jurídico se conforma por precedentes y determinaciones judiciales, pero también se debe a la fuerte intromisión del poder empresarial que existe en el país en la materia.

2.2 México

La LFTAIPG decretada el 11 de junio de 2002, es el primer precedente normativo en el país que regulaba la protección de datos personales a nivel federal dentro del sector público. Pero debido a que la competencia de la protección de este derecho en el sector público se dividió entre el sector federal y estatal, un año después en el estado de Colima se publicó la Ley de Protección de Datos Personales del Estado de Colima, convirtiéndose en la primera norma estatal reglamentaria en la materia existente en México.

Así pues, se tiene que la normativa que existía en la materia estaba dirigida a controlar y asegurar el debido tratamiento de la información personal por parte del sector público. Sin embargo, fue hasta el año 2009 que se reconoce al derecho de la protección de datos personales como un derecho fundamental en México al

[93] Louisiana Senate, *Act. No. 382*, Louisiana, 2018, *https://www.legis.la.gov/legis/ViewDocument.aspx?d=1101149*.
[94] State of California Department of Justice, *California Consumer Privacy Act (CCPA)*, California, *https://oag.ca.gov/privacy/ccpa*.

reformarse el artículo 16 constitucional, al introducir los derechos de acceso, rectificación, cancelación y oposición, conocidos como derechos ARCO.

Posteriormente, en el año 2010 se promulgó la LFPDPPP con el objetivo de garantizar la protección de los datos personales pero que estén en posesión de los particulares, es decir, del sector privado. En esta norma se retoman los principios y deberes que se prevén en la legislación europea, pero se abundan en los alcances y restricciones que se tendrá sobre el tratamiento de la información por parte de los responsables.

El siguiente año, para efecto de facilitar y reglamentar las disposiciones de la LFPDPPP, se emite su reglamento en el que se clarifican y profundizan cuestiones sobre el otorgamiento del consentimiento, excepciones, plazos de conservación, términos sobre la relación entre el responsable y el encargado, remisión de información personal, subcontratación de servicios, medidas de seguridad, transferencia de datos, autorregulación vinculante, certificaciones, procedimientos de queja, procedimientos de verificación e imposición de sanciones.

Después de la reforma constitucional del año 2014 se llevaron a cabo diversos cambios estructurales y legales como la consolidación del sistema nacional de transparencia y anticorrupción; la instauración del órgano constitucional autónomo competente para garantizar los derechos de acceso a la información pública y protección de datos personales y, el origen de un nuevo marco legal que regulara, además de los derechos aludidos la transparencia y los archivos.

Por lo que hace al Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de datos Personales (SNT), *… se integra por el conjunto orgánico y articulado de sus miembros, procedimientos, instrumentos y políticas, con el objeto de fortalecer la rendición de cuentas del Estado mexicano*.[95]

Este SNT conforme a la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), es considerado la instancia de coordinación y deliberación que tiene como finalidad la organización de los esfuerzos de promoción, difusión, articulación, colaboración y cooperación en materia de

[95] Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, "¿Qué es el Sistema Nacional de Transparencia?", *https://snt.org.mx/?page_id=431*.

transparencia, acceso a la información y protección de datos personales. Se indica es el espacio para generar una política pública integral con el objetivo de garantizar los derechos antes señalado por medio del fomento de una educación y cultura cívica.[96]

El Sistema Nacional Anticorrupción (SNA) por su parte se conforma por un Comité Coordinador y se integra por los titulares de la Auditoría Superior de la Federación, la Fiscalía Especializada en Combate a la Corrupción, la secretaría del Ejecutivo Federal responsable del control interno, el presidente del Tribunal Federal de Justicia Administrativa, el presidente del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y un representante del Consejo de la Judicatura y del Comité de Participación Ciudadana.[97]

Dicho SNA es la instancia de coordinación entre las autoridades competentes de todos los órdenes de gobierno para la prevención, detección y sanción de actos de corrupción y responsabilidades administrativas, como de la fiscalización y control de recursos públicos.[98]

En cuanto al órgano constitucional autónomo encargado de garantizar los derechos fundamentales de acceso a la información y protección de datos personales,[99] cabe destacar que, antes de la reforma constitucional en la que se instruye su creación, se contaba con el Instituto Federal de Acceso a la Información Pública y Protección de Datos, órgano administrativo del Poder Ejecutivo que velaba por el debido cumplimiento tanto de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG) para el sector público federal, y la LFPDPPP en toda la nación.

Derivado de la reforma constitucional ya señalada, ahora el INAI, es la autoridad competente y responsable de salvaguardar los derechos de privacidad y protección de datos personales en el país.

---

[96] *Idem*.
[97] Cámara de Diputados, *Constitución Política de los Estados Unidos Mexicanos*,… *op. cit.,* artículo 113, fracción I.
[98] *Ibidem*, artículo 113, párrafo primero.
[99] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, “Qué es el INAI", *https://home.inai.org.mx/?page_id=1626*.

A esta Institución se le otorgaron facultades reglamentarias, por lo tanto, ha publicado una serie de normas para regular aspectos específicos en relación con el derecho fundamental, las cuales serán mencionadas en el siguiente capítulo pues en ellas se establecen diversas obligaciones que son las que se pretenden resaltar en este proyecto.

En cuanto al marco legal generado por motivo de la reforma se decretaron diversas leyes, en materia de acceso a la información: la LGTAIP, que efectúa la homologación de normas estatales y federales y tiene como objeto establecer principios, bases y procedimientos para garantizar el derecho de acceso a la información en posesión de sujetos obligados[100] y la Ley Federal de Transparencia y Acceso a la Información Pública (LFTAIP) cuyo objetivo es salvaguardar el derecho de acceso a la información pública.

En materia de archivos, se decretó la Ley General de Archivos que es de orden público y de observancia general en todo el territorio general, la cual tiene como finalidad instaurar los principios y bases para la preservación, conservación, administración y organización de los archivos que estén en posesión de cualquier institución pública, órgano autónomo, partido político, fideicomiso, fondo público, persona física, moral o sindicato que reciba recursos públicos o ejerza actos de autoridad.[101]

En materia de protección de datos personales, la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGPDPPSO), expedida el 26 de enero de 2017, está dirigida a reglamentar los artículos 6 y 16 constitucional en materia de protección de la información personal en el sector público federal.

Con esta LGPDPPSO se separa la regulación de los derechos de acceso a la información pública y protección de datos personales dentro del sector público, ya que, hasta antes de la entrada en vigor de esta ley, en la LFTAIPG se establecían

[100] Cámara de Diputados, Ley General de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*, México, 04 de mayo de 2015, última reforma publicada 20 de mayo de 2021, artículo 1, *https://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP_200521.pdf*.
[101] Cámara de Diputados, Ley General de Archivos, *Diario Oficial de la Federación,* México, 15 de junio de 2018, última reforma publicada 05 de abril de 2022, artículo 1, *https://www.diputados.gob.mx/LeyesBiblio/pdf/LGA.pdf*.

los parámetros para la sustanciación de asuntos en materia de datos personales en posesión de los sujetos obligados.

Sin embargo, se respeta la competencia de la defensa de este derecho entre la federación y los estados para el sector público; como también se mantiene la división la regulación de la materia entre el sector público y privado.

Un punto que subrayar de la LGPDPPSO es que, a diferencia de la LFPDPPP y la propia Constitución Política de los Estados Unidos, introduce a los derechos ARCOP, al reconocer el derecho de acceso, rectificación, cancelación, oposición y adicionalmente al de portabilidad, pues en su artículo 57 dispone que cuando los datos personales obren en electrónico en un formato estructurado comúnmente utilizado, el titular tendrá el derecho de acceder a una copia de su información personal en formato electrónico que le brinde oportunidad de seguir utilizándolos.[102]

Ahora bien, el cuerpo jurídico mexicano en relación con la protección de datos personales ha evolucionado durante las dos últimas décadas, pues pasó de regular cuestiones relativas a los datos personales a reconocer a la protección de datos personales como un derecho fundamental.

De igual forma, se creó un órgano constitucional autónomo con personalidad jurídica y patrimonio propio, que cuenta con facultades reglamentarias, administrativas, procedimentales y sancionatorias para hacer valer los derechos que se vinculan con la protección de datos personales.

No obstante, a diferencia de países latinoamericanos, en México para efecto de hacer efectivo el derecho humano comentado, se instauraron procedimientos administrativos que son resueltos por el Instituto y no por el Poder Judicial, aunque las determinaciones adoptadas por el órgano constitucional autónomo pueden ser impugnadas ante dicho Poder, los medios de queja son administrativos.

Por lo que hace a las similitudes del marco jurídico mexicano con los documentos legales europeos, se puede afirmar que en principio se crearon tomando como base las disposiciones del continente europeo, sin embargo, se cuentan con algunos contrastes.

---

[102] Cámara de Diputados, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *Diario Oficial de la Federación*, Ciudad de México, 26 de enero de 2017, artículo 57, *https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf*.

Un ejemplo de dichas diferencias es que en México sí es posible efectuar transferencias internacionales con terceros independientemente de si el país destino cuenta con un nivel de protección de datos alto o del mismo nivel que se tiene en México.

Como se observa, las leyes mexicanas tienen la característica de adoptar algunas de las directrices de los instrumentos internacionales, pero también desarrollan parámetros en cuestiones específicas como en temas de obtención de consentimiento o de excepciones aplicables al mismo.

En específico por lo que hace a la LFPDPPP un punto a destacar es que si bien retomó medidas de documentos internacionales y al momento de que entró en vigor pudo ser vanguardista y cumplía con las necesidades que el tratamiento de información personal representaba en ese momento, se estima que actualmente ya no atiende a las situaciones jurídicas que se presentan en la materia.

Lo anterior se estima así pues, en primer lugar, la tecnología ha avanzado a gran medida que algunas de sus disposiciones ya no son suficientes para regular el tratamiento de datos mediante las TIC, es decir, las situaciones legales que se presentan han superado el marco normativo; y en segundo, no ha retomado la restructura y renovación que implicó la reforma constitucional del año 2014 ya mencionada, esto es que, no refleja la creación de sistemas, órgano constitucional o nuevas determinaciones legales.

Para efecto de aludir a algunos ejemplos de lo señalado, el primero consiste en que la LFPDPPP no ha adoptado el derecho de portabilidad como se hizo referencia en párrafos anteriores; y el segundo, refiere a que no ha reflejado los cambios en relación con los procedimientos de impugnación que proceden en contra de los fallos emitidos por el INAI.

Sobre el segundo ejemplo, se trae a colación la jurisprudencia emitida por la segunda Sala de la Suprema Corte de Justicia de la Nación, en la que falló que en materia de protección de datos personales en posesión de particulares no procede

el juicio contencioso administrativo federal en contra de las determinaciones emitidas por el INAI.[103]

La Suprema Corte de Justicia de la Nación fijó que, si bien el artículo 56 de la LFPDPPP prevé que en contra de las resoluciones del Instituto pueden promoverse ante el Tribunal Federal de Justicia Fiscal y Administrativa juicios de nulidad, lo cierto es que derivado de la reforma constitucional del año 2014 la única vía procedente para impugnarlas es por medio del juicio de amparo.[104]

Ante ello, señaló que el artículo 56 aludido de la LFPDPPP debe tenerse por derogado, ya que deviene contrario a lo dispuesto en la Constitución Política de los Estados Unidos, pues uno de los objetivos principales de la mencionada reforma constitucional fue la posibilidad de impugnar las resoluciones del INAI únicamente por la vía del juicio de amparo.[105] Con esto se refleja que algunas disposiciones de la ley deben actualizarse.

Por último y como se indica en los párrafos anteriores, los marcos normativos existentes en México sobre la materia de protección de datos personales separan las normas aplicables al sector público y al privado, así como las que aplican a nivel federal y estatal dentro del sector público. No obstante, el desarrollo del presente proyecto se centrará en el estudio de la LFPDPPP al ser la que norma la materia en el sector privado, misma que se analizará en el siguiente capítulo.

[103] Tesis 2a./J.31/2020 (10a.), *Seminario Judicial de la Federación*, Décima Época, octubre de 2020, *https://sjf2.scjn.gob.mx/detalle/tesis/2022203*.
[104] *Idem.*
[105] *Idem.*

Capítulo 3.

Las obligaciones derivadas de la Ley Federal de Protección de Datos Personales en Posición de Particulares y la situación de su cumplimiento en México

Capítulo 3. Las obligaciones derivadas de la Ley Federal de Protección de Datos Personales en Posición de Particulares y la situación de su cumplimiento en México.

La dignidad humana es la base de donde se crean derechos y libertades que dan al individuo las herramientas y pautas para desenvolverse tal y como lo desea dentro de la sociedad.[106] La privacidad y la protección de datos personales son derechos humanos que derivan de esta, puesto que permiten a las personas desarrollar su personalidad.

Esto es que, la protección de datos personales y la privacidad al tratarse de derechos vinculados de forma directa con la dignidad humana y al ser intrínsecos del ser humano, se vuelven derechos necesarios para que el individuo pueda realizarse, por lo que, las autoridades se ven obligadas a respetarlos y garantizarlos en todo momento.

Por lo anterior y como se expuso en el capítulo segundo del presente proyecto, los gobiernos y organizaciones internacionales han creado normas dirigidas a proteger la privacidad y la protección de datos personales. Para ello, se han instituido convenios, estatutos, reglamentos, leyes, protocolos, así como otro tipo de documentos normativos en los que se establecen alcances, competencias, y mecanismos dirigidos a garantizar dichos derechos.

En ese sentido, debido al impacto que tiene la tecnología en los datos personales y por su utilización desmedida mediante la misma, se ha reconocido por gobiernos e instituciones en las últimas décadas la importancia que tiene el salvaguardar la información personal de los titulares por medio de las tecnologías y dentro de éstas.

Tal como lo indica Emercio José Aponte, por motivo de los avances tecnológicos y la posibilidad de almacenar grandes cantidades de datos personales, se han creado diversos marcos normativos para proteger ese derecho, ya que al ser

[106] Lefranc Weegan, Federico, *Holocausto y Dignidad Significado y fin de la invocación a la dignidad humana en el Preámbulo de la Declaración Universal de Derechos Humanos,… op. cit.*, p. 101.

conscientes de la relevancia de la informática para la actividad comercial se busca lograr un balance entre la protección de los datos personales y la utilización de la tecnología.[107]

El amparo de la protección de datos personales se torna aún más relevante actualmente debido a la afluencia de información personal que transita en Internet, redes sociales o entre los sistemas de las empresas, el uso masivo de la TIC y el tratamiento masivo y profundo que se hacen de los datos.

Por ello, es necesario que las empresas o responsables del tratamiento de datos personales tomen en cuenta que tiene la obligación de velar por la garantía de los derechos humanos, ya que, como se profundizará en páginas posteriores, las empresas por sus relaciones comerciales deben observar principios para prevenir o mitigar consecuencias adversas sobre los derechos humanos.

En tal tenor, derivado de la importancia que tiene la protección de datos personales para el sector privado en el mundo y en México, como también por la falta de herramientas con las que se socialicen las obligaciones que tienen los responsables sobre el cumplimiento de este derecho, es que se propone el presente proyecto, en tanto que, se estima que con su aplicación aumentarán los niveles de la salvaguarda de la prerrogativa señalada.

Es por lo anterior que, en el presente capítulo, se mencionarán cuáles son las obligaciones principales que los responsables deben atender para respetar los principios de licitud, responsabilidad, información, proporcionalidad, calidad, lealtad, consentimiento, finalidad, los deberes de seguridad y confidencialidad y, en consecuencia, garantizar el derecho de la protección de datos personales.

Se incluye un resumen de las acciones que los responsables deben realizar para cumplir con cada uno de los principios y deberes, el artículo del que se deriva tal obligación y se refieren los diversos mecanismos, guías, lineamientos y capacitaciones brindados por el INAI, que otorgan a los responsables un cúmulo de insumos para estar en aptitud de atender lo previsto en la LFPDPPP.

---

[107] Aponte Núñez, Emercio José, “La importancia de la protección de datos de carácter personal en las relaciones comerciales. Aproximación al Derecho venezolano”, *Revisa de Derecho Privado*, Colombia, Universidad Externado de Colombia, núm. 12-13, enero-diciembre 2007, p. 110, *https://www.redalyc.org/articulo.oa?id=417537588004*.

Asimismo, se citan estadísticas y estudios emitidos por el sector privado y público, de los que se infiere cuál es el nivel de cumplimiento en materia de protección de datos personales en México, la evolución de su acatamiento, los motivos o razones que se estiman son los que obstaculizan la observancia de la LFPDPPP y las áreas de oportunidad que en las que se pueden realizar mejoras.

En este capítulo se pretende resaltar que, si bien los responsables tienen a su alcance diversa documentación e instrumentos que les otorga información para acatar la LFPDPPP, lo cierto es que se requiere de una herramienta digital que les facilite conocer de forma sencilla y clara, si son responsables en términos de dicha norma y, en consecuencia, saber cuáles son las responsabilidades que tienen para así estar en posibilidad de atenderlas.

Ahora bien, previo a referir las estadísticas aludidas y desarrollar las causas más recurrentes de infracción de los responsables, es conducente partir de la identificación de quiénes son responsables de cumplir con la LFPDPPP y cuáles son las obligaciones que deben atender para con ello cumplir con el derecho de la protección de datos personales.

La LFPDPPP dispone que la persona física o moral de carácter privado que decide sobre la obtención, acceso, uso, aprovechamiento, divulgación, almacenamiento, transferencia, manejo o disposición de datos personales, realiza el tratamiento de estos y, por lo tanto, tiene el carácter de responsable.[108]

Además, establece que quien tiene dicho carácter, el de responsable, debe velar por los principios de consentimiento, calidad, lealtad, responsabilidad, licitud, proporcionalidad, información y finalidad, así como de los deberes de confidencialidad y seguridad.[109]

No obstante, la citada ley también es clara en señalar quiénes no se considerarán responsables del tratamiento de datos y no están conminados a seguir los parámetros dispuestos por la norma. Estos sujetos son las sociedades de información crediticia y las personas que recolecten o almacenen información

[108] Cámara de Diputados, *Ley Federal de Protección de Datos Personales en,… op. cit.*, artículo 3, fracciones XIV y XVIII.
[109] *Ibidem*, artículo 6.

personal para uso exclusivamente personal y sin fines de divulgación o utilización comercial.[110]

3.1 Obligaciones de responsables en materia de protección de datos personales

Una vez establecido quiénes están obligados a cumplir con las disposiciones en materia de protección de datos personales en México, conviene referir de forma básica qué es lo que deben de prever para observar la legislación.

Algunas de las obligaciones impuestas al responsable dependerán del tipo de dato personal que se usa o almacena (de identificación, patrimonial o sensible), como del manejo que haga de la información personal, por ejemplo, si la transfiere a otras empresas o si realiza cómputo en la nube.

Sin embargo, las obligaciones principales que deben velarse por todos los responsables independientemente de la categoría de dato que se trate, consisten en *… informar a los titulares de los datos, la información que se recaba de ellos y con qué fines, a través de su aviso de privacidad;*[111] como también la consecución del consentimiento del titular para el tratamiento de sus datos.

Parta efecto de acatar lo antes mencionado, la LFPDPPP instaura que el responsable debe crear un documento en el que se señale el alcance, términos y condiciones del tratamiento que se dará a la información personal, esto es, las características principales del manejo que tendrán los datos personales. [112] A este documento se le denomina aviso de privacidad.

El aviso de privacidad es el documento más importante y que por antonomasia todos los responsables deben de generar y poner a disposición de sus clientes o de los titulares de los datos personales, pues además de dar a conocer el uso que se dará a la información, en éste también se brindan los mecanismos para el ejercicio de los derechos ARCO y las opciones para limitar el uso o divulgación de los datos.

---

[110] *Ibidem*, artículo 2.
[111] *Ibidem*, artículo 15.
[112] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *El ABC del Aviso de Privacidad*, *http://abcavisosprivacidad.ifai.org.mx/#seccion1_02P*.

Las disposiciones normativas en la materia reconocen tres modalidades de aviso de privacidad, que de acuerdo con el "ABC del Aviso de Privacidad" son los siguientes:[113]

- Integral: contiene todos los elementos que se establecen el artículo 16 de la LFPDPPP o en la sección III de la guía. Se utiliza generalmente cuando se recaban los datos directamente del titular.
- Simplificado: cuenta con algunos de los elementos del aviso de privacidad integral, como la identidad y domicilio del responsable, las finalidades del tratamiento, los mecanismos para manifestar la negativa del tratamiento y los mecanismos para que el titular conozca la modalidad integral. Se utiliza generalmente cuando se obtienen los datos por medio de Internet o vía telefónica.
- Corto: contempla la identidad y domicilio del responsable, las finalidades del tratamiento y los mecanismos para conocer la modalidad integral. Se utiliza para espacios limitados o mínimos, como mensajes de texto o cupones, por lo que, tiene elementos mínimos que deben darse a conocer.

Debido a que el presente trabajo solo pretende referir a las obligaciones que los responsables deben cumplir, si se desea profundizar sobre la elaboración, especificaciones y ejemplos de los modelos de avisos de privacidad, se sugieren revisar los documentos siguientes: "Lineamientos del Aviso de privacidad",[114] "Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares",[115] y "Guía para la elaboración del Aviso de Privacidad en el área de recursos humanos".[116]

---

[113] *Ibidem*, sección III.
[114] Secretaría de Economía, *Lineamientos del Aviso de Privacidad*, México, D.F.,17 enero de 2013, *https://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013#gsc.tab=0*.
[115] 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*, junio de 2016, pp. 91, *https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_obligaciones_lfpdppp_junio2016.pdf*.
[116] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Guía para la elaboración del Aviso de Privacidad en el área de recursos humanos*, Ciudad de México, mayo 2022, 1a. ed., pp. 47, *https://home.inai.org.mx/wp-content/uploads/GuiaElaboracion_AvisoPrivacidad_Area_RH.pdf*.

En cuanto a la obtención del consentimiento, aunque hay excepciones, por regla general una vez que se da a conocer el aviso de privacidad al titular de los datos, se debe recabar su anuencia de forma tácita o expresa para que el tratamiento pueda realizarse.[117]

El otorgamiento del consentimiento mediante manifestación expresa sucede cuando el titular de forma verbal, por escrito, a través de medios electrónicos, ópticos, por cualquier otra tecnología o por signos inequívocos, señala estar conforme con el tratamiento de su información.[118]

Este tipo de consentimiento se recaba cuando se tratan datos de las categorías de carácter financiero, patrimonial y sensible, con la precisión de que para el caso de datos sensibles se requiere además que sea otorgado por escrito.[119]

Al respecto y sobre la creación de bases de datos personales de carácter sensibles, la LFPDPPP prohíbe su realización salvo si su creación está justificada y es para finalidades concretas, legítimas y acordes a las actividades que persigue el responsable.[120]

Es importante resaltar que la información personal que se obtenga solo debe utilizarse para fines legales y atendiendo al marco normativo de la materia. Por lo tanto, existen prohibiciones específicas para el tratamiento, por ejemplo: que los datos sean recabados por medio de dolo, mala fe o negligencia; que se quebrante la confianza del titular o que en el aviso de privacidad no se den a conocer todas las finalidades para las que se tratarán los datos.[121]

Por otro lado, el responsable debe procurar que la información personal que almacene en sus bases de datos sea pertinente, correcta y actualizada en relación con los fines para los que se obtuvieron. No obstante, en caso de que dichos datos ya no sean necesarios para el cumplimiento de las finalidades, pueden ser cancelados y eliminados una vez que transcurra un plazo de 72 meses.[122]

---

[117] Cámara de Diputados, *Ley Federal de Protección de Datos Personales en,… op. cit.*, artículo 8.
[118] *Idem.*
[119] *Idem.*
[120] *Ibidem*, artículos 8 y 9.
[121] *Ibidem*, artículo 7.
[122] *Ibidem*, artículo 11.

De la misma manera, el manejo de los datos debe ser adecuado, relevante y necesario de acuerdo con las finalidades establecidas en el aviso de privacidad; para ello, resulta primordial que se obtengan el menor número de datos personales y que el uso al que sean sometidos sea entorno a los propósitos necesarios. Además, cuando sean datos personales sensibles su tratamiento debe ser por un periodo razonable.[123]

Cabe destacar que, para cumplir con los principios de la LFPDPPP y lo dispuesto en el aviso de privacidad, el responsable debe aplicar las medidas necesarias y suficientes para garantizar que los mismos sean respetados por sí mismo como por los terceros con los que tenga un vínculo jurídico.[124]

Así pues, independientemente de la categoría de datos en la que encuadre la información tratada, de la forma en la que se recaba, como del medio o formato en el que se encuentren, la norma establece obligaciones de hacer y no hacer en relación con la adquisición y uso que den a la información personal.

Adicionalmente prevé la observancia de dos deberes, en específico, en materia de seguridad y confidencialidad. Por lo que hace al deber de seguridad, es menester resaltar que *La seguridad es un aspecto crítico para poder garantizar la privacidad, y al mismo tiempo no hay seguridad sin privacidad*.[125]

En tal tenor, resulta esencial que los responsables dispongan y mantengan medidas de seguridad administrativas, físicas y técnicas con las que se ampare la información personal frente a su destrucción, pérdida, alteración, daño, uso o acceso no autorizado. No obstante, si se cuentan con tales medidas y se da el caso de una vulneración de seguridad a datos patrimoniales o morales se debe informar al titular.[126]

En ese mismo sentido, para prevenir una afectación a los titulares de los datos, tanto el responsable como los terceros involucrados en el tratamiento de la

---

[123] *Ibidem*, artículo 13.
[124] *Ibidem*, artículo 14.
[125] Centro de Investigación y Docencia Económicas A.C., *Lineamientos de Protección de Datos en el Cómputo en la Nube: Parámetros para su elaboración*, México, 2014, p. 46, *https://cidecyd.files.wordpress.com/2014/09/white-paper-lineamientos-proteccion-datos-computo-nube-mx-18-sept-14-def.pdf*.
[126] Cámara de Diputados, *Ley Federal de Protección de Datos Personales en,… op. cit.*, artículos 19 y 20.

información, deben mantener secreto sobre la misma. Para esto, se debe realizar lo necesario para evitar que los datos sean divulgados, incluso aún finalizada la relación contractual entre las partes.[127]

Ahora bien, y por lo que respecta a las acciones que se deben realizar para dar atención a los derechos ejercicios por los titulares. Los responsables deben dar trámite a las solicitudes de acceso, rectificación, cancelación u oposición de datos personales y hacerlos efectivos salvo que aplique una causal de excepción o limitación prevista en la LFPDPPP.[128]

En suma, para revisar a profundidad las obligaciones que los responsables deben cumplir y dar cabalidad a cada uno de los principios y deberes, se sugiere revisar la "Guía para cumplir con los principios y deberes de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares",[129] en la que de forma clara y exhaustiva se explican las acciones a realizar para observar la ley.

Sin embargo, a manera de resumen y para conjuntar las obligaciones principales que se tienen en la materia, se inserta la siguiente tabla (Tabla 1):

Tabla 1 Obligaciones, principios, deberes y fundamento

Acciones para cumplir con las obligaciones	Principio, deber o derecho que se garantiza	Disposición normativa de la que emana
Elaborar y poner a disposición del titular el aviso de privacidad (modalidad integral, simplificado o corto).	Principio de Información	Artículo 15 LFPDPPP
Requerir el consentimiento tácito para el tratamiento de datos personales.	Principio de consentimiento	Artículo 8 LFPDPPP
Requerir el consentimiento expreso para el tratamiento de datos personales, cuando se usen datos patrimoniales o financieros,	Principio de consentimiento	Artículos 8 y 9 LFPDPPP

[127] *Ibidem*, artículo 21.
[128] *Ibidem*, artículos 28 y 34.
[129] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Guía para cumplir con los principios y deberes,… op. cit.*, p. 91.

además de por escrito cuando sean de la categoría de sensibles.		
Establecer mecanismos y procedimientos para la revocación del consentimiento.	Principio de consentimiento	Artículo 8 LFPDPPP
Obtener y utilizar los datos del titular de forma lícita.	Principio de licitud	Artículo 7 LFPDPPP
Mantener la confianza con el titular al utilizar la información personal conforme lo acordado.	Principio de lealtad	Artículo 7 LFPDPPP
Informar todas las finalidades para las que se obtienen o usarán los datos personales y limitar el tratamiento al cumplimiento de las mismas.	Principio de lealtad	Artículo 7 LFPDPPP
Obtener los datos personales de forma auténtica y veraz.	Principio de lealtad	Artículo 7 LFPDPPP
Procurar que los datos personales almacenados sean correctos, pertinentes y actualizados.	Principio de calidad	Artículo 11 LFPDPPP
Obtener, usar y almacenar datos personales únicamente para cumplir con las finalidades que se informan mediante el aviso de privacidad al titular.	Principio de finalidad	Artículo 12 LFPDPPP
Incluir en el aviso de privacidad todas las finalidades para las que se obtienen y usan los datos personales.	Principio de finalidad	Artículo 15 LFPDPPP
Usar solo los datos personales que sean relevantes, adecuados y necesarios para cumplir con las finalidades para las que se recabaron.	Principio de proporcionalidad	Artículo 13 LFPDPPP

Aplicar las medidas necesarias y suficientes para cumplir con los principios y el aviso de privacidad.	Principio de responsabilidad	Artículo 14 LFPDPPP
Implementar o desarrollar medidas de seguridad físicas, técnicas o administrativas que protejan datos personales ante su destrucción, pérdida, alteración, daño o uso no autorizado.	Deber de seguridad	Artículo 19 LFPDPPP
Informar a los titulares de los datos patrimoniales o financieros en caso de vulneraciones de seguridad.	Deber de seguridad	Artículo 20 LFPDPPP
Guardar la confidencialidad o secreto respecto de los datos personales que son tratados por el responsable o terceros que intervengan en cualquier fase del tratamiento.	Deber de confidencialidad	Artículo 21 LFPDPPP
Guardar la confidencialidad o secreto respecto de los datos personales que son tratados aún después de concluida la relación con el titular.	Deber de confidencialidad	Artículo 21 LFPDPPP
Dar trámite a las solicitudes y hacer efectivo el ejercicio de derechos de acceso, rectificación, cancelación u oposición.	Derechos ARCO	Artículo 28 LFPDPPP

Fuente: elaboración propia

3.2 Nivel de cumplimiento de los responsables en la materia de protección de datos personales

Una vez establecidas las obligaciones y acciones principales que el responsable debe atender para cumplir con los principios, deberes y derechos establecidos en la LFPDPPP, es conveniente mencionar algunos estudios que ponen en relieve cómo se encuentra el nivel de cumplimiento México en relación con la protección de

datos personales en el sector privado y qué tanto ha avanzado la defensa de este derecho humano desde el año 2010.

Dos años después de la entrada en vigor de la LFPDPPP, la Asociación Mexicana de Internet (AMIPCI) emitió el Estudio de Protección de Datos Personales entre Usuarios y Empresas, cuyo objetivo fue contar con una fotografía en la que se identificaran las áreas de oportunidad de las empresas en la materia para con ello generar conciencia sobre la importancia del derecho y establecer corresponsabilidad entre los usuarios y responsables.

Para efecto de lo anterior, se evaluaron a 187 empresas y 734 usuarios de los 32 estados del país, arrojando como resultados que el 44% de las evaluadas no tenían conocimiento sobre las obligaciones que emanaban de LFPDPPP y solo el 12% señaló conocerlas completamente; que el 32% desconocían las acciones que deben realizar para atender la norma y solo el 6% contaba con una persona especializada en la materia entre sus filas, mientras que 5 de cada 10 empresas carecían de conocimiento suficiente sobre los derechos ARCO.[130]

De igual forma, se obtuvo que *El principal obstáculo para implementar acciones concretas para cumplimentar la ley, es el desconocimiento parcial y total en la materia con 41% y 22% respectivamente*.[131] Ante esto, se exhibió que el 74% de las empresas coincidió en que no se había divulgado sobre el impacto que la ley pueda tener en los responsables.[132]

Los datos mencionados muestran que, los responsables del tratamiento de datos personales no contaban con insumos ni conocimientos suficientes para dar una debida atención a las disposiciones en la materia, pero es entendible que a tan corto plazo de la entrada en vigor de la ley no se presentara una robusta observancia.

Si bien es cierto que hace diez años no se tenían avances concretos y visibles en relación con en el acatamiento de la norma, también lo es que la introducción de

---

[130] Asociación Mexicana de Internet, *Estudio de Protección de Datos Personales entre Usuarios y Empresas*, México, 2012, *https://www.asociaciondeinternet.org.mx/es/component/remository/func-startdown/19/lang,es-es/?Itemid=*.
[131] *Idem*.
[132] *Idem*.

un cuerpo normativo novedoso que debe ser atendido implica tiempo, trabajo continuo y la aplicación de recursos económicos y humanos, por lo que, para el 2012 era comprensible el nivel de cumplimiento que se tenía en la materia.

No obstante, posterior a la creación del INAI, órgano constitucional autónomo encargado de velar por la protección de datos personales en México, en convenio con el Instituto Nacional de Estadística y Geografía (INEGI) emitieron dos encuestas con el objetivo de saber el grado de conocimiento de la población sobre los derechos de acceso al a información, protección de datos personales y los mecanismos para ejercerlos.

Así, en el año 2016 se formuló la Encuesta Nacional de Acceso a la Información Pública y Protección de datos Personales (ENAID), en la que se cuestionó a una población de 18 años o más, de un tamaño de muestra nacional de 14,400 viviendas ubicadas en cuatro regiones del país de domino urbano alto.[133]

Por lo que hace al tipo de datos y su flujo en Internet, la encuesta reveló que el 89.4% que tiene cuenta en alguna red social dio a conocer su nombre y algún apellido en la misma, mientras que el 95.6% divulgó ese mismo dato, pero en alguna red profesional.[134]

En específico, sobre las obligaciones de las empresas en la materia, la encuesta reveló que al 31.6% de la población la contactaron para ofrecerle un servicio sin haber cedido a la empresa sus datos personales, como también que a nivel nacional a solo el 32.7% de la población se le dio a conocer un aviso de privacidad. No obstante, en cuanto a la presentación de quejas por el uso indebido de datos personales únicamente el 1.4% interpuso una queja.[135]

En el 2019, el INEGI publicó la siguiente ENAID que en adición a lo que se analizó en la previa encuesta, ésta tuvo como objetivo el detectar las actitudes, experiencias y percepciones que tienen injerencia en el ejercicio de los derechos de

[133] Instituto Nacional de Estadística y Geografía, *Encuesta Nacional de Acceso a la Información Pública y Protección de datos Personales*, 2016, *https://www.inegi.org.mx/contenidos/programas/enaid/2016/doc/ENAID_2016_Principales_resultados.pdf*.
[134] *Ibidem*, pp. 7.2a, 7.2b.
[135] *Ibidem*, pp. 7.8, 7.11, 7.14.

acceso y protección de datos personales. Para esto, se tomó como muestra a 17,600 viviendas y una población de 18 años y más de todo el país.[136]

En cuanto a la información personal que fluye en plataformas de Internet, la encuesta mostró que el 89.7% de la población que cuenta con una red social dio a conocer su nombre y algún apellido, con lo que se advierte un mínimo aumento a diferencia del estudio previo. Misma situación acontece para la población que cuenta con una red profesional pues se arroja que el 95.7% dio a conocer el mismo tipo de dato personal.[137]

Asimismo, al 41.8% de la población le dieron a conocer un aviso de privacidad; a un 43.5% de la población se le contactó para ofrecer un servicio sin haber concedido sus datos personales; mientras que, sobre las quejas presentadas por uso indebido de información personal, un 3.9% de la población presentó una; de lo anterior sobre estos tópicos se observa un aumento en el porcentaje a comparación con la previa encuesta.[138]

De los resultados obtenidos se colige que, en los últimos años, el cúmulo de datos personales que ha fluido en Internet es inmenso, pues aún y cuando no todas las personas tienen acceso a la red y no cuentan con un dispositivo electrónico, la mayoría que sí hace uso de estas tecnologías comparte su información personal en las redes o plataformas digitales.

Las evidencias exhiben que, del año 2016 al 2019 sí hubo un avance en el cumplimiento de una de las obligaciones en la materia, debido a que a un mayor número de personas de la población se le dio a conocer un aviso de privacidad, con lo que se deduce que las responsables acataron en mayor medida con el principio de información.

No obstante, no pasa desapercibido que, si bien el nivel de atención a la obligación de poner a disposición el aviso de privacidad al titular se incrementó y

---

[136] Instituto Nacional de Estadística y Geografía, *Encuesta Nacional de Acceso a la Información Pública y Protección de datos Personales*, 2019, p. 6, *https://www.inegi.org.mx/contenidos/programas/enaid/2019/doc/enaid_2019_principales_resultados.pdf*.
[137] *Ibidem*, pp. 71, 72.
[138] *Ibidem*, pp. 85, 88, 91.

fue mayor para el año 2019, el porcentaje de cumplimiento seguía manteniéndose por debajo del 50%.

Otro resultado no alentador fue la disminución en la salvaguarda del principio de consentimiento, ya que el porcentaje de personas a las que se les contactó sin haber conferido sus datos personales se acrecentó, es decir, se dio tratamiento a su información personal sin adquirir previamente su consentimiento de forma tácita o expresa.

Debido a lo antes mencionado, se afirma que dos de las obligaciones principales en la materia, como lo son la puesta a disposición del aviso de privacidad y la obtención del consentimiento del titular para tratar sus datos personales, seguían sin garantizarse a nivel nacional en gran medida.

Por otra parte, se recuerda que el INAI es la institución que resuelve sobre las solicitudes de protección de derechos, quien verifica el debido acatamiento de los principios, deberes y derechos previstos en la LFPDPPP y es la autoridad facultada para imponer sanciones en caso de que un responsable vulnere alguno de los principio, deberes o disposición normativa.

En ese sentido, el INAI en sus informes de labores ha dado a conocer la cantidad de asuntos que tramita, las infracciones y los motivos que los responsables cometen de forma más recurrentes. En ese orden de ideas, con el objetivo de mostrar las obligaciones que más se incumplen se traen a colación información y algunos datos estadísticos que ha reportado.

De acuerdo con la Dirección General de Investigación y Verificación del Sector Privado del INAI, de los años del 2017 al 2021 se tiene que, dentro de los procedimientos de verificación, los motivos más recurrentes por los cuales el Pleno del Instituto ordenó iniciar un procedimiento de imposición de sanciones por el presunto incumplimiento a alguna disposición de la LFPDPPP fueron los siguientes (Tabla 2):[139]

[139] Dirección General de Investigación y Verificación del Sector Privado, *Oficio: INAI/SPDP/DGIVSP/0290/22*, INAI, Ciudad de México, 2022, *https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=330031322000179&coleccion=2*.

Tabla 2 Motivos recurrentes de infracción a la LFPDPPP

Ejercicio	Motivos recurrentes
2017	El Responsable no acreditó la puesta a disposición del aviso de privacidad.
	Irregularidades en el Aviso de Privacidad del Responsable.
	Divulgación indebida de los Datos Personales del Denunciante.
2018	Obtención de Datos Personales sin consentimiento del Denunciante.
	Uso indebido de los Datos Personales del Denunciante.
2019	El Responsable no acreditó la puesta a disposición del aviso de privacidad.
	Obtención de Datos Personales sin consentimiento del Denunciante.
2020	El responsable no acreditó la puesta a disposición del aviso de privacidad.
	Divulgación indebida de los Datos Personales del Denunciante.
	Uso indebido de los Datos Personales del Denunciante.
2021	Divulgación indebida de los Datos Personales del Denunciante.
	Uso indebido de los Datos Personales del Denunciante.

Fuente: Dirección General de Investigación y Verificación del Sector Privado, Oficio: INAI/SPDP/DGIVSP/0290/22, INAI, Ciudad de México, 2022, https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=330031322000179&coleccion=2.

Derivado de lo anterior, se colige que las conductas más frecuentes que se cometen por los responsables y ocasionan la transgresión de una disposición normativa son: la omisión de la puesta a disposición del titular del aviso de privacidad; la obtención de datos personales sin consentimiento del titular; el uso y divulgación indebida de datos personales.

En esta relatoría, respecto las sanciones impuestas en los procedimientos de imposición de sanciones a responsables derivadas de los procedimientos de verificación, por no cumplir con sus obligaciones al vulnerar los principios y deberes establecidos en la LFPDPPP, se tienen los números siguientes:

En el periodo de octubre 2015 a septiembre 2016 se instauraron 66 procedimientos de imposición de sanciones en los cuales se determinó que hubo un incumplimiento a las conductas previstas en el artículo 63 de la LFPDPPP, por lo que se impuso un total de multas que oscilaron a los 92 millones 771 mil 204 pesos.[140]

Las conductas más recurrentes por que los responsables fueron sancionados en el periodo aludido: en mayor medida se localiza la contravención de principios; seguido por la obstrucción de actos de verificación; obtención o transferencia de datos personales sin consentimiento expreso del titular; la omisión de uno o todos los elementos requeridos en el aviso de privacidad y el cambio sustancial de la finalidad originaria por la que se recabaron los datos para el tratamiento.[141]

Para el periodo de octubre 2016 a septiembre de 2017 se advirtió un aumento en el número de procedimientos de imposición de sanciones, con un registro de 85 expedientes, de los cuales se obtuvo un total de multas por la cantidad redondeada de 81 millones 740 mil 420 pesos.[142]

De forma similar al año previo que el antes indicado, las conductas más frecuentes por las que los responsables fueron acreedores a sanciones consistieron en: transgredir los principios de la norma; obstruir actos de verificación de la autoridad y obtener o transmitir datos personales sin el consentimiento expreso del titular.[143]

En el informe de labores del 2018, que contempla los meses de octubre de 2017 a septiembre de 2018, se reportó que hubo un aumento del 17.6% de procedimientos de imposición de sanciones al tramitarse 100 expedientes, derivado

[140] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Informe de labores 2016*, México, enero de 2017, pp. 156-160, *https://micrositios.inai.org.mx/informesinai/?page_id=425*.
[141] *Ibidem*, p. 163.
[142] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Informe de labores 2017*, México, diciembre 2017, pp. 146-147, *https://micrositios.inai.org.mx/informesinai/?page_id=385*.
[143] *Ibidem*, p. 148.

de los cuales se impuso un monto total de multas a las acreedoras por la cantidad redondeada de 89 millones 533 mil 240 pesos.[144]

Se destaca que, de las 18 conductas que la ley de la materia contempla por las que se puede sancionar a un responsable por incumplimiento, las más recurrentes fueron las siguientes: contravenir los principios de la legislación; omitir en el aviso de privacidad uno o todos los elementos que son requeridos; obstruir actos de verificación por parte de la autoridad y obtener o transmitir datos personales sin el consentimiento expreso del titular.[145]

En el siguiente periodo de octubre 2018 a septiembre 2019, se reportó la tramitación de 758 procedimientos de imposición de sanciones, registrándose un aumento del 658% a comparación con el año inmediato anterior. En consecuencia, también incrementó la cantidad total de las multas impuestas ascendiendo a 112 millones 397 mil 139 pesos.[146]

Las conductas más frecuentes por las que se sancionaron a los responsables, a diferencia de años previos, se centraron en tres rubros: por tratar datos personales vulnerando los principios de la ley; omitir alguno o todos los elementos requeridos en el aviso de privacidad y recabar o transferir datos personales sin el consentimiento expreso del titular.[147]

Por último, para el periodo de octubre 2019 a septiembre 2020 se impusieron a los responsables que incumplieron con la ley un total de multas que osciló en la cantidad de 56 millones 771 mil 662 pesos, pues el número de procedimientos de imposición de sanciones tramitados a diferencia con el año anterior decreció sustancialmente a 75 expedientes.[148]

---

[144] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Informe de labores 2018*, México, diciembre 2018, pp. 215-216, *https://micrositios.inai.org.mx/informesinai/?page_id=372*.
[145] *Ibidem*, 219
[146] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Informe de labores 2019*, México, diciembre 2019, p. 191, *https://micrositios.inai.org.mx/informesinai/?page_id=15*.
[147] *Ibidem*, p. 193.
[148] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Informe de labores 2020*, México, diciembre 2020, p. 188, *https://micrositios.inai.org.mx/informesinai/?page_id=519*.

En cambio, los motivos más recurrentes por los que se impuso una multa a responsables no tuvieron gran variación, pues se reiteraron las conductas de incumplimiento siguientes: tratamiento datos personales en contravención a los principios de la ley; obstruir actos de verificación de la autoridad y obtener o transmitir datos personales sin el consentimiento expreso del titular.[149]

De forma similar que en los procedimientos de verificación, los motivos recurrentes por los que se han impuesto sanciones a los responsables derivado del incumplimiento de sus obligaciones en los últimos años son repetitivas, es decir, se observa que las conductas por las que se multan a los responsables son generalmente las mismas.

Dichas razones consisten en: contravenir los principios de la ley (en el que se contempla la falta de la puesta a disposición del aviso de privacidad); omitir alguno o todos los elementos requeridos en el aviso de privacidad; obstruir actos de verificación; obtener y transferir datos personales sin el consentimiento expreso del titular y cambiar sustancialmente la finalidad originaria por la que se obtuvieron los datos para el tratamiento.[150]

Como se observa, en gran parte el incumplimiento de la norma por parte de los responsables se limita a ciertas acciones u omisiones, que se estima son básicas y de relativa sencilla atención, pues incluso una de las faltas más recurrentes consiste en la omisión de no poner a disposición de los titulares de los datos personales el aviso de privacidad.

Parece ser una acción fácil de cumplir, pues lo único que se requiere por parte de los responsables es la elaboración del documento para posteriormente hacerlo de conocimiento del titular. Sin embargo, sigue siendo una de las causas principales por las que se vulnera uno de los principios amparado por la norma.

---

[149] *Ibidem*, p. 190.

[150] De los informes de labores emitidos por el INAI correspondientes a los años 2016, 2017, 2018, 2019 y 2020 se tiene que la ubicación de los infractores se concentra principalmente en la Ciudad de México. Asimismo, se tiene registro que las infractoras se localizan en otras entidades federativas, en su mayoría en estados ciudades con un gran número de población como Nuevo León y Jalisco, excepcionalmente para el año 2020, además de ubicarse la mayoría en la Ciudad de México, la segunda ubicación en la que se concentró el mayor número de sancionados fue en Michoacán.

De la misma manera, el no adquirir el consentimiento del titular para almacenar o hacer uso de su información personal, se considera es una de las obligaciones primordiales que se deben de atender, en cambio es una de las acciones que con frecuencia no se efectúa.

3.3 Motivos o razones del incumplimiento de las obligaciones

A más de una década de la entrada en vigor de la LFPDPPP, como se infiere de las estadísticas y estudios citados, en México se sigue presentado un alto grado de incumplimiento de las obligaciones que los responsables tiene en relación con la ya mencionada ley.

Ante esto, es imprescindible hacer los siguientes cuestionamientos ¿cuáles son las razones o motivos por las que los responsables incumplen con sus obligaciones? ¿qué les impide llevar a cabo las gestiones para desempeñar su función dentro del marco de la LFPDPPP? ¿existen suficientes herramientas, guías o documentos que en la práctica les facilite el cumplimiento de sus obligaciones? De existir los documentos y herramientas necesarios ¿aumentaría la protección de datos personales de los titulares en México?

Es importante señalar que no existe un estudio, estadística, análisis, informe o documento técnico que muestre claramente cuál es la situación actual del nivel de cumplimiento de las obligaciones de los responsables en materia de protección de datos personales en México o la evolución que ha tenido esta en poco más de una década. Tampoco se localizó un documento similar que ponga en relieve cuáles son los motivos reales del por qué se siguen cometiendo las mismas infracciones.

Lo anterior, resulta ser relevante, ya que, si se contara con un documento en el que se identifiquen las razones por las que se ocasiona la conducta indebida, el trabajo y esfuerzo de las autoridades, del sector privado y la academia, podrían dirigirse específicamente a solventar las causas de la problemática, y así evitar vuelvan a ocurrir o al menos disminuir su frecuencia.

Desde esta perspectiva, se estima que existen varios factores que influyen en que los responsables cometan esas acciones u omisiones que vulneran los

principios y deberes previstos en el cuerpo normativo, tales motivos se desarrollan a continuación:

a) El desconocimiento de las obligaciones por parte de los responsables

Es posible que los propietarios de las pequeñas y medianas empresas que tratan datos personales no tengan conocimiento de la existencia de una ley que los hace responsables del uso que le den a la información de sus clientes y mucho menos que conozcan qué es lo que deben realizar para cumplir con la norma.

En esa tesitura, en principio, es necesario contar con un estudio que específicamente muestre si una de las situaciones que se enfrentan en México, por la que se tiene un bajo nivel de cumplimiento del derecho a la protección de datos personales, es el desconocimiento de la LFDPPP, o en su caso que exhiba que el problema sea otro.

Al respecto, se trae a colación que desde su creación el INAI ha hecho labores de difusión y promoción en la materia; han pactado convenios con el sector privado para realizar trabajos a favor de la protección de datos; han implementado diversas campañas, capacitaciones y cursos dirigidos a socializar no solo la importancia de este derecho sino la forma de cómo pueden garantizarlo.

En ese sentido, con la finalidad de difundir y facilitar la protección de datos personales en el sector privado, el INAI también ha emitido una serie de lineamientos, guías, documentos y herramientas digitales dirigidas a orientar a los responsables sobre la atención de sus responsabilidades en términos de la legislación.

Dichos documentos van desde una guía para cumplir con los principios y deberes de la ley hasta metodologías para el análisis de riesgos. No obstante, de una revisión a estos apoyos normativos y de orientación, se considera que pueden llegar a ser, en cierto grado, documentos técnicos que para su entendimiento se requieren conocimientos básicos en el tópico, lo cual puede desincentivar a las personas en continuar con su revisión o instrumentación.

Por otro lado, dentro de las herramientas digitales existentes en la materia, se localizó un generador de aviso de privacidad, el cual permite a los responsables generar el documento legal con los elementos mínimos que se requieren para

cumplir con una de las obligaciones previstas la legislación. Sin embargo, esta plataforma únicamente permite la creación del aviso de privacidad, mas no brinda otros elementos para atender el resto de los principios u obligaciones.

El INAI oferta capacitaciones, cursos y talleres los responsables, pues cuenta con cursos en la modalidad presencial y en línea sobre temas como: "Introducción a la LFPDPP", "Aviso de Privacidad", "Atención a las solicitudes de derechos ARCO", "Autorregulación en Materia de Protección de Datos Personales", "Designación de la Persona o Departamento de Datos Personales", "Curso en materia de Medidas de Seguridad", o "Tratamiento de datos biométricos y manejo de incidentes de seguridad de datos personales".[151]

Sobre lo referido, el informe de labores del año 2020 observa que, de las 76 acciones de capacitación sobre los temas mencionados en el párrafo anterior, se tuvo un total de 3 mil 682 participantes.[152] De esto se colige que, los esfuerzos de la autoridad competente han tenido resultados positivos al aumentarse el número de personas que participan para adquirir conocimientos en la materia, pero a su vez se presenta un área de oportunidad y de mejora, ya que podría estimarse insuficiente el número de personas capacitadas.

Lo anterior se afirma así pues, si se toma en cuenta que para el año 2019 existían 4.9 millones de establecimientos micro, pequeños y medianos del sector privado y paraestatal,[153] comparándose con el número de establecimientos que podrían ser responsables de cumplir con la LFPDPPP y con el de personas capacitadas en el tema, el impacto de la difusión o conocimientos sobre el cumplimiento de las obligaciones puede ser mínimo, por ende, se sustenta el supuesto de la falta de conocimiento de la materia.

No obstante, el desconocimiento de la materia no puede deberse solo por la falta de suficiente difusión y promoción por parte del INAI o las instituciones de gobierno. Existen otros sectores como el privado y la academia que podrían no estar

---

[151] Dirección General de Capacitación, *INAI/SE/DGC/039/22*, INAI, 17 de febrero de 2022, *https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=330031322000232&coleccion=5*.
[152] *Ibidem*, p. 267.
[153] Instituto Nacional de Estadística y Geografía, *Comunicado de Prensa núm. 790/21*, diciembre de 2021, *https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/EDN/EDN_2021.pdf*.

haciendo lo necesario para tener un impacto positivo en que las empresas conozcan sus obligaciones, pero ¿qué han hecho en este ámbito?

Dentro del sector privado, en el año 2015, la Confederación Patronal de la República Mexicana (COPARMEX) celebró un convenio de colaboración con el INAI, para de manera conjunta coordinar la elaboración y ejecución de estrategias y actividades con el objetivo de fortalecer la cultura sobre el acceso a la información pública, la transparencia, la rendición de cuentas y la protección de datos personales.[154]

Aparte del convenio aludido no se localizó alguno otro similar por parte de otro grupo empresarial dedicado a impulsar la cultura en la materia. Es posible advertir que, sí existe participación del sector privado a través de la colaboración de sus representantes en conferencias o eventos públicos, pero esto se limita normalmente a personal de grandes empresas y las empresas ubicadas en el área metropolitana.

Por lo tanto, se afirma que no hay una intervención activa o profunda por parte de las empresas o los responsables para, en primer término, conocer cuáles son sus obligaciones en la materia, es decir, se advierte una falta de asistencia para que en el sector se difundan sus responsabilidades o ha sido mínima.

En cambio, dentro de la academia se tiene registro que cada vez más instituciones, universidades públicas y privadas insertan dentro de sus programas de estudios alguna materia, curso, diplomado, especialidad o posgrado relacionado con la protección de datos personales. Algunos de los que se imparten o se han ofrecido son los que se incluyen en la tabla siguiente (Tabla 3):

[154] Confederación Patronal de la República Mexicana e Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Convenio General de Colaboración*, p. 4, *https://home.inai.org.mx/wp-content/documentos/Convenios/OA-09-2015%20Confederaci%C3%B3n%20Patronal%20de%20la%20Republica%20Mexicana%20COPARMEX.pdf*.

Tabla 3 Protección de datos personales en la academia

Institución o Universidad	Programa en materia de protección de datos personales	Fuente de consulta
Universidad Nacional Autónoma de México (UNAM)	▪ Maestría en Derecho a la Información. Dirigida a servidores públicos integrantes del INAI, Órganos Internos de Control, Sistema Nacional de Transparencia, Comités y Unidades de Transparencia. ▪ TIC Aplicables al Derecho (Facultad de Estudios Superiores Acatlán). Dirigida a estudiantes de licenciatura en derecho. ▪ Asignatura Transparencia, Derecho a la Información y Protección de Datos Personales (Facultad de derecho). Dirigida a estudiantes de licenciatura en derecho. ▪ Especialización en derecho de la información (Facultad de derecho división de estudios de posgrado). No se precisa el perfil a quien se dirige. ▪ Diplomado en Contratación Pública. Módulo VII Transparencia en la contratación Pública (Instituto de Investigaciones Jurídicas). Dirigido a servidores públicos encargados de realizar contrataciones públicas en los 3 niveles de gobierno, a integrantes del sector privado que quieran vender sus servicios o realizar obra pública con el	▪ https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=330031922000231&coleccion=5 ▪ https://www.juridicas.unam.mx/actividades-academicas/2716-diplomado-encontratacion-publica-2021-3a-edicion ▪ https://archivos.juridicas.unam.mx/diplomados/temario/Ge9d3RtXsNQtEwbF1EzPSlFNXDq6d64coxDa2l4j.pdf

	estado, legisladores, jueces y magistrados en materia administrativa. ▪ Diplomado Poderes Tradicionales y Órganos Constitucionales Autónomos. Módulo XV Institutos de Transparencia y Acceso a la Información (Instituto de Investigaciones Jurídicas). Dirigido a alumnos de licenciaturas de ciencias sociales, servidores públicos de los tres poderes del estado y órganos constitucionales autónomos. ▪ Diplomado Dr. Jorge Carpizo en "Derechos Humanos Eje Temático III. "Seminario de derechos en particular". XXVIII. Derechos de acceso a la información y a la protección de datos (Instituto de Investigaciones Jurídicas). Dirigido a personas que cuenten por lo menos con 70% de créditos de alguna licenciatura. ▪ Diplomado en Derecho Digital, 2021. Módulo II. Protección de datos personales y sus retos en el entorno digital (Instituto de Investigaciones Jurídicas). Dirigido a funcionaros del gobierno, abogados de empresas, litigantes, de corporativos, oficiales de privacidad, consultores de empresas, profesionales y empresarios de TIC o digitales.	▪ https://www.juridicas.unam.mx/actividades-academicas/2581-diplomado-drjorge-carpizo-en-derechos-humanos-6ta-edicion-2021 ▪ https://www.juridicas.unam.mx/actividades-academicas/2610-diplomado-enderecho-digital-2021

Universidad de Guadalajara	• Maestría en Transparencia y Protección de Datos Personales. Se dirige a servidores públicos que laboran en el área de transparencia, a ciudadanos que recaben información y periodistas especializados en medios de comunicación. • Diplomado en Protección de Datos Personales. Dirigido a personas con nivel licenciatura integrantes de instituciones públicas o privadas, o de quienes acrediten experiencia mínima de dos años en tratamiento de datos personales.	• https://www.udgvirtual.udg.mx/mtpdp • https://www.udg.mx/es/convocatorias/diplomado-en-proteccion-de-datos-personales-dirigido-una-generacion-2019
Centro de Investigación y Docencia Económicas (CIDE)	• Materia optativa “Derecho y Tecnología” en Licenciatura Derecho. Dirigido a alumnos de la licenciatura de derecho. • Materia optativa “Privacidad, Regulación y Gobernanza de Datos” en Licenciatura Derecho. Dirigido a alumnos de la licenciatura de derecho. • Diplomado en Privacidad, Regulación y Gobernanza de Datos. No se precisa el perfil a quien se dirige.	• https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=330004922000044&coleccion=5
INFOTEC, Centro de Investigación e Innovación en Tecnologías de	• Maestría en Derecho de las Tecnologías de la Información y Comunicación. Dirigida a egresados de licenciaturas vinculadas con las disciplinas afines al derecho y TIC.	• https://www.infotec.mx/es/Infotec/Maestria-en-Derecho-de-las-Tecnologias-

la Información y Comunicación	• Especialidad en Derecho de la Protección de Datos Digitales (EDPDD). No se precisa a quién se dirige.	de-Informacion-y-Comunicacion • https://www.infotec.mx/Esp-Derecho-Proteccion-Datos
Universidad Anáhuac	• Diplomado de Datos Personales. Dirigido a profesionales del área de compilación en iniciativa privada, a dedicados al tratamiento de datos personales, a servidores públicos de las Unidades de Transparencia, abogados postulantes y miembros de asociaciones civiles relacionados con el tema.	• https://online.anahuac.mx/diplomados-en-linea/derecho/proteccion-datos-personales/
Universidad Iberoamericana	• Curso sobre la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Dirigido a funcionarios públicos.	• https://ibero.mx/prensa/ibero-impulsa-proteccion-de-datos-personales-con-capacitacion-instituciones-publicas
Universidad Panamericana	• Curso en línea: Privacidad y Protección de Datos Personales en México. No se indica al perfil de personas al que se dirige.	• https://hipodec.up.edu.mx/shop/product/curso-en-linea-

		privacidad-y-proteccion-de-datos-personales-en-mexico-1#attr=
Fundación de Investigación para el Desarrollo Profesional (FINDES)	• Curso de Ley de Protección de Datos (El temario es en específico sobre la LFPDPPP). No se indica a qué personas se dirige el curso.	• https://www.findes.org/cursos/finanzas/curso-de-ley-de-proteccion-de-datos/

Fuente: elaboración propia

Del listado aludido se colige lo siguiente: sí existen programas educativos que enseñen y den a conocer la protección de datos personales en México; algunos de ellos se imparten a través de asignaturas a nivel de licenciatura otros por medio de posgrados especializados; los impartidos por las universidades públicas son gratuitos, mientras que los diplomados, cursos o maestrías brindados por las instituciones o por escuelas privadas tienen un costo.

Sobresale que varios de estos programas se centran a la enseñanza de la protección de datos dentro del sector público, aunado a que en algunos no se contempla dentro de su temario el estudio de las obligaciones que los responsables del sector privado tienen en la materia, salvo los otorgados, por ejemplo, por el FINDES, la Universidad Panamericana y el INFOTEC.

La oferta académica está orientada a funcionarios públicos de los sujetos obligados o en especial a integrantes de las Unidades de Transparencia, a estudiantes de la licenciatura en derecho, a abogados que desean incrementar sus conocimientos en la materia o ingenieros que desean tener las bases relacionadas con el derecho aludido, como el caso del Diplomado en Protección de Datos Personales ofertado por la Universidad de Guadalajara que es dirigido a personas con nivel licenciatura integrantes de instituciones públicas o privadas, o de quienes acrediten experiencia mínima de dos años en tratamiento de datos personales.

Sin embargo, la mayoría de estos programas se dirige a personas que ya tienen un conocimiento técnico o jurídico previo en el tópico, pocos de estos cursos o diplomados pueden ser tomados por alguna persona que no tenga una base previa en el tema o que simplemente esté interesada en saber cuáles son sus obligaciones en la materia.

La oferta académica de las universidades públicas en su mayoría se inclina a los alumnos de las licenciaturas de derecho. Situación similar se presenta en los posgrados que son ofrecidos por la UNAM, la Universidad de Guadalajara y el INFOTEC, pues el posgrado se circunscribe a personas con un perfil afín a la carrera de derecho o vinculado a las TIC.

Derivado de lo anterior, se concluye que la mayoría de los programas relacionados con la materia de protección de datos personales, están delimitados a

personas con un perfil en el área del derecho o de las TIC. Esto es que, alumnos o personas con perfiles diversos no tienen la facilidad de adquirir estos conocimientos con los que les sea posible cumplir con la protección de datos personales de sus clientes.

Al respecto, si los temarios de otras profesiones diversas a de derecho no incorporan alguna materia o curso en el que se dé a conocer la importancia y el valor de los datos personales, así como su responsabilidad al momento de tratar la información personal de sus clientes, es posible que por esta vía no lleguen a tener en cuenta sobre sus responsabilidades en la materia.

Se observa la existencia de aportaciones académicas, cursos y diplomados sobre la enseñanza de las obligaciones que tienen los responsables en relación con los principios y deberes previstos en la LFPDPPP, empero, para acceder a algunas de ellas se requiere del desembolso de una cantidad pecuniaria o tener un perfil específico, con lo que se limita la oferta educativa.

Adicionalmente, se desprende que los responsables pierden de vista que por el incumplimiento a sus responsabilidades, además de las grandes pérdidas económicas que les puede acarrear la imposición de una sanción, también puede generar desconfianza a sus clientes, desprestigio de su marca y una desventaja competitiva frente a otros responsables que sí cumplan las obligaciones lo que se traduciría en pérdida de clientes.

Por último, se deduce que gran parte de la población desconoce las consecuencias negativas que puedes traerles el ser acreedores de una sanción por transgredir la LFPDPPP, pues en caso de conocerlas, podrían ser un aliciente para mantenerse y actuar dentro del marco jurídico.

b) Baja promoción de la cultura de protección de datos personales

Como punto de partida, es menester establecer qué se entiende por cultura de protección de datos personales. Aristeo García González señala es *… el conjunto de conocimientos, opiniones, prácticas o conductas que una persona tiene*

sobre el tratamiento y la protección de su información personal (datos personales).[155]

Asimismo, indica que la cultura en materia de protección de datos personales atiende a una doble perspectiva: la jurídica, referente a los conocimientos sobre el marco normativo y los componentes principales de su contenido; y la social, que contempla la expresión de las opiniones, prácticas o conductas que se expresan en red.[156]

La cultura de protección de datos personales refiere a aquellos conocimientos que son adquiridos por la sociedad en relación con los datos personales, su relevancia, su tratamiento, los principios y deberes por los que se rige su tratamiento, el uso adecuado que puede darse sobre de ellos y los derechos vinculados que permiten garantizar el derecho humano.

De igual forma, apunta a los conocimientos que tienen los responsables y servidores públicos encargados del tratamiento de los datos personales, los titulares de la información personal, los académicos, los niños, niñas y adolescentes.

En ese sentido, la cultura de la protección de datos personales no se limita a un solo sector, es decir, debe desarrollarse dentro de todos los sectores de la población, es y debe ser para todos, ya que se busca que todas las personas involucradas cuenten con los insumos e información necesaria para que exista una efectiva garantía del derecho.

Al respecto, en México ¿cuál es el nivel de la cultura en protección de datos personales? Si traemos a colación las estadísticas y reportes señalados en el apartado anterior, se afirma que, dentro del sector privado existe una carencia en este tema. Mientras que por lo que hace a las personas o titulares de los datos personales, también se muestra que desconocen cuáles son sus derechos o de conocerlos no los ejercen.

En el área de la academia, algunas universidades e instituciones han abonado en el tema incluyendo en sus programas o cursos específicos

---

[155] García González, Aristeo, “Hacia una cultura en materia de protección de datos personales”, *Hechos y Derechos*, núm. 14, *https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/6816/8752*.
[156] *Idem*.

especializados en la materia, pero se trata de instituciones ubicadas principalmente en zonas metropolitanas, lo que deja al resto de regiones del país sin un avance sobre la promoción o difusión de la defensa de este derecho humano.

En este punto, es importante mencionar qué es lo que se está haciendo para enseñar y promocionar la multireferida cultura en México. El INAI difunde y fomenta la protección de datos personales, realiza continuamente conferencias, conversatorios, publica infografías, cuenta con micrositios, realiza asesorías, atiende consultas y emite anuncios publicitarios o spots de radio dirigidos a todos los sectores de la población.

Sin embargo, como se reportó en la ENAID 2019, el porcentaje de quejas presentadas por la vulneración de su derecho en la encuesta más reciente no alcanza a llegar a un 4% de la población que fue cuestionada.[157] De lo que se infiere que las personas no conocen que pueden ejercer el derecho o desconocen la importancia de sus datos personales, lo cual está vinculado con el nivel de cultura en la materia que existe en México.

En el área académica, como se alude en el estudio del apartado del inciso a, se están incorporando materias optativas en las licenciaturas de derecho, se ofrecen programas de posgrado, cursos, especialidades o diplomados sobre el tema; y en el sector privado, se cuenta con una mayor participación por parte de las empresas para que su personal se capacite.

Aún y con los esfuerzos de las autoridades y de la sociedad interesada en el incremento del nivel de la protección de datos personales en México, como de su cultura jurídica, se estima que se requiere de una mayor visualización sobre la utilidad de este derecho, que se difunda a los titulares y los responsables dueños de negocios cuál es su relevancia, incluso éstos últimos al contar con esta información podrían verse incentivados para realizar las gestiones necesarias para cumplir con la LFPDPPP.

Por ende, se advierte un área de oportunidad en relación con la cultura de la protección de datos personales, pues la carencia de conocimientos por parte de

[157] Instituto Nacional de Estadística y Geografía, *Encuesta Nacional de Acceso a la Información Pública y Protección de datos Personales*, 2019 … *op. cit*, p. 91.

quiénes deben de cumplir con las obligaciones previstas por ley y de los titulares, afecta directamente la garantía y salvaguarda de este derecho humano.

c) El bajo interés de los responsables para cumplir con sus obligaciones en la materia

Partiendo de la idea de que los responsables buscan en todo momento atender el marco jurídico, en los apartados de los incisos a y b anteriores, se adujo que el incumplimiento de las obligaciones en la materia deriva del desconocimiento de éstas y por la baja promoción y difusión de la cultura de protección de datos personales en México.

No obstante, es posible que se dé el escenario en el que el responsable sí conozca cuáles son sus responsabilidades en términos de la LFPDPPP, la existencia de este derecho y las acciones o gestiones que debe llevar a cabo para salvaguardarlo. En ese sentido, si tienen conocimiento sobre sus obligaciones ¿por qué es que no las cumplen?

La protección de datos personales es un derecho fundamental que ha sido incorporado en el cuerpo normativo mexicano en años recientes, es un área jurídica poco explorada por los abogados o de la que no existen muchos especialistas en el país a comparación con otras disciplinas.

Conforme lo anterior, una de las causas de incumplimiento puede ser la falta de personal capacitado para dar el debido tratamiento a los datos personales, es decir, los responsables no cuentan con recursos humanos preparados para llevar a cabo las gestiones suficientes con las que se brinde atención a las obligaciones y derechos.

En ese tenor, los responsables se ven en la necesidad de contratar despachos jurídicos o especialistas en la materia, implicando un gasto de recursos económicos de su presupuesto que, por ser ahorrados o invertidos en otras áreas del negocio, se opta por no contratarlos.

Lo anterior, trae a colación otro de los posibles motivos de inobservancia, siendo la no identificación de un beneficio tangible a favor de su negocio o empresa por razón de la tutela del derecho, es decir, no se aprecia el valor de la información

personal, la ventaja competitiva que les traería frente a otros negocios o la posición que les daría en el mercado al resguardarlo.

Otro punto que considerar es que tomando en cuenta que los niveles de interposición de quejas son muy bajos, los responsables deciden esperar a ser denunciados por el incumplimiento a la LFPDPPP y pagar la multa que se les impone después del largo proceso administrativo y judicial, en lugar de invertir en realizar las gestiones necesarias para atender la norma.

Los procesos administrativos para la imposición de sanciones son largos y pueden extenderse aún más derivado de los procedimientos jurisdiccionales que se tramiten, esto implica que se opte por acudir a los procedimientos legales pues el resultado que se adquiere es el aplazamiento del pago de la multa.

De igual forma, puede considerase que es más barato dilucidar las controversias legales ante los tribunales o autoridades competentes, que desembolsar cantidades de dinero para atender lo que marca la LFPDPPP, pues el monto para la tramitación de los procedimientos puede ser menor que lo que se tenga que invertir para el cumplimiento de obligaciones o que el propio pago de la sanción.

Se reitera que el número de interposición de quejas por el indebido tratamiento de datos personales es bajo, lo que permite inferir que la falta de participación ciudadana es otro de los elementos que confabulan para el desinterés de las empresas en la atención de la norma, ya que, de existir una mayor participación de su parte en la que ejerza los mecanismos de protección que tiene a su alcance detonaría una mayor observancia.

Aunado a lo antes mencionado, el INAI es la autoridad competente para la tramitación de los procedimientos a través de los cuales se imponen sanciones a responsables por motivo de infracciones a la LFPDPPP, pero no es esta autoridad quien ejecuta las multas, sino la Tesorería de la Federación, lo cual implica que el cobro de la sanción se dilate en tiempo aún más pues se requiere de otro procedimiento administrativo para el cobro.

Otra de las razones por las que las empresas no se ven forzadas a atender la disposición, puede ser la baja cantidad de procedimientos que se ventilan ante el

INAI. Es cierto que la cantidad de denuncias presentadas por las personas es bajo, pero también lo es el número de procedimientos de verificación por vulneraciones a la LFPDPPP iniciados de oficio, tal como se muestra a continuación (Tabla 4):[158]

Tabla 4 Procedimientos iniciados de oficio por el otrora IFAI e INAI

Ejercicio	Total de procedimientos de verificación iniciados de oficio
2011 (a partir del 01 de julio de 2011)	1
2012	0
2013	0
2014	2
2015 (incluye periodo del IFAI e INAI)	4
2016	3
2017	38
2018	16
2019	24
2020	2
2021	50
Ejercicio 2022 (hasta el 06 de abril de 2022)	10

Fuente: Dirección General de Investigación y Verificación del sector privado, Oficio: INAI/SPDP/DGIVSP/1398/22, INAI, Ciudad de México, 2022, https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=330031322000755&coleccion=5.

Desde que el órgano federal asumió facultades para ejercer la verificación de oficio sobre el acatamiento de deberes y principios de la LFPDPPP, del 01 de julio de 2011 hasta principios del mes de abril del año 2022, el entonces IFAI y ahora INAI han iniciado 150 procedimientos de verificación oficiosamente. Se puntualiza

[158] Dirección General de Investigación y Verificación del sector privado, *Oficio: INAI/SPDP/DGIVSP/1398/22*, INAI, Ciudad de México, 2022, *https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=330031322000755&coleccion=5*.

que de la totalidad de procedimientos de oficio la mayoría fueron activados durante el periodo del órgano constitucional autónomo, INAI.

Es posible que el número de procedimientos oficiosos iniciados por el INAI sea bajo, pero esto puede deberse a varios factores como el presupuesto asignado al órgano constitucional autónomo, la cantidad de personal asignado en las áreas correspondientes, la capacidad de recursos técnicos y el alcance que pueda llegar en toda la República.

No debe pasar desapercibido que independientemente de la capacidad de llevar a cabo estos procedimientos, si la autoridad ejerciera en mayor medida su facultad de iniciar dichos procedimientos oficiosos de forma aleatoria en toda la República mexicana, las empresas se verían forzadas a acatar el cuerpo normativo y, en consecuencia, aumentar los niveles de la protección de datos personales.

Es decir, si las empresas por sí solas no se ven motivadas a atender la LFPDPPP, se requiere de una participación activa del INAI con la que se fuerce a los responsables a observarla, que sea por el temor de ser sometidos a una verificación que la atiendan y que su alcance sea en aquellas entidades federativas o ciudades en las que normalmente no se realizan verificaciones a los responsables.

Adicionalmente, la falta de un marco jurídico que otorgue más atribuciones al Instituto para hacer efectivas las multas, en el que se incluyan otras obligaciones a cargo de los responsables como la de notificarle al INAI las vulneraciones de seguridad en sus sistemas o en el que se incorporen las situaciones novedosas que representa el uso de las TIC, da a lugar al comportamiento laxo de las responsables frente a sus responsabilidades.

Ahora bien, parece ser que las empresas o negocios pierden de vista que deben garantizar los derechos humanos de sus clientes o usuarios. Ante esto, se retoma lo dispuesto por los Principios Rectores sobre las Empresas y los Derechos Humanos, documento que aplica para todos los derechos humanos y que establece el impacto que las empresas pueden tener en todo el espectro de los derechos humanos, así como la responsabilidad que tienen de respetarlos.[159]

[159] Naciones Unidas, *Principios Rectores sobre las empresas y los derechos humanos*, Nueva York y Ginebra, 2011, p. 15, *https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_sp.pdf*

Los Principios disponen que las empresas por sus propias actividades o por sus relaciones comerciales pueden estar relacionadas en las consecuencias negativas que tengan los derechos humanos. Para tal efecto, en el Principio Rector 19 se instaura que las empresas en sus acciones u omisiones y en sus relaciones comerciales deben prevenir o mitigar las consecuencias antes aludidas.[160]

En suma, de la revisión a las estadísticas y estudios que se han señalado se infiere que, los responsables desconocen cuáles son sus obligaciones para cumplir con los principios y deberes que emanan de la LFPDPPP. No tienen conocimiento de qué acciones deben realizar para atender las disposiciones, como tampoco tienen en cuenta qué es lo que no deben efectuar para evitar vulnerarlas.

Por otra parte, si bien existen motivos por los cuales los responsables consideren es más barato incumplir con la ley, también lo es que se sitúan en una posición transgresora de derechos humanos, lo cual debería ser de primordial atención en términos de la protección de los datos personales, la privacidad y lo dispuesto por los Principios.

Asimismo, el INAI durante la última década ha realizado capacitaciones, cursos, talleres, guías y generado documentos que faciliten a los responsables el cumplimiento de sus obligaciones. Sin embargo, como las estadísticas lo exponen, aún y con los insumos mencionados existe un gran camino por recorrer para que los niveles de protección de datos personales en el país aumenten.

De igual forma, se colige que falta un análisis específico que muestre cuál ha sido la evolución del cumplimiento de las obligaciones de los responsables desde la entrada en vigor de la LFPDPPP hasta el día de hoy, es necesario un estudio o informe que dé a conocer cuál es la situación actual de los niveles de cumplimiento en la materia en México.

Esto es así, pues una vez identificadas las faltas o los puntos débiles por los que se siguen cometiendo las mismas conductas por las que se sancionan a los infractores, se podrían crear herramientas específicas que ayuden a subsanar tales problemáticas y, por consiguiente, aumentar la defensa del derecho, o en todo caso,

[160] *Ibidem*, p. 17.

se sabría las razones específicas y reales de la falta de cumplimiento para con ello presentar políticas públicas concretas que ataquen la situación.

En tal tenor, se presenta un área de oportunidad y de mejora para incrementar los niveles de cumplimiento de las obligaciones. Además de lo que ya se lleva a cabo por el INAI, se deben buscar otras formas y medios con los que se facilite y oriente a los responsables conocer qué es lo que deben hacer para respetar la LFPDPPP.

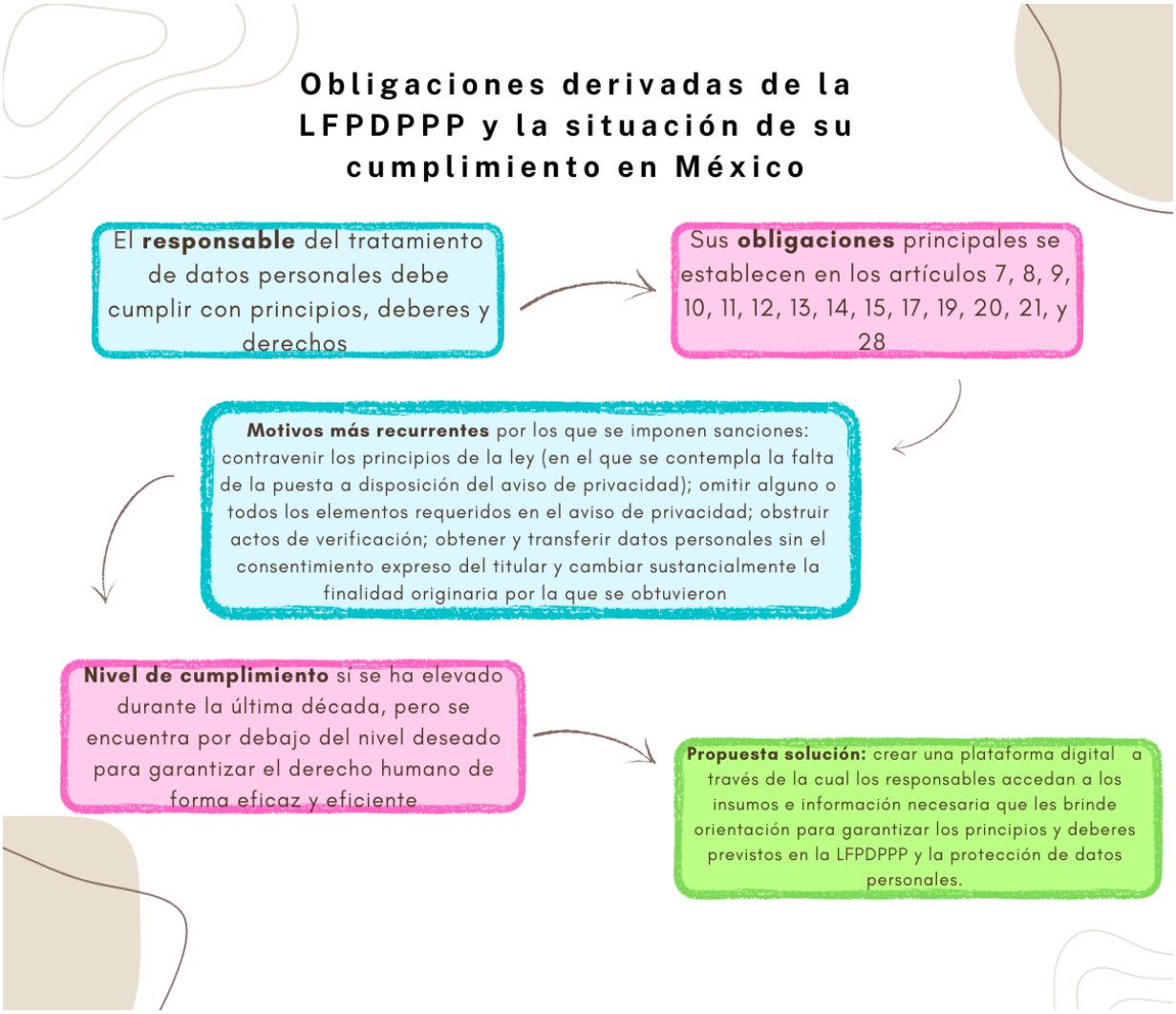
Pues como se indica, si bien se brindan capacitaciones a los responsables y tienen a su alcance diversa documentación sobre lo que deben hacer para obedecer la ley, lo cierto es que ha quedado evidenciado que año tras año se siguen presentando las mismas conductas ilegales, por lo tanto, se deben contar con otras herramientas que faciliten de forma sencilla y clara cuáles son las obligaciones que se tienen y la forma de observarlas.

Con el objetivo de aumentar los niveles de protección de datos personales de los titulares que otorgan su información a los responsables, se considera que debe implementarse, además de los documentos y plataformas ya existentes, otra que facilite a los responsables conocer cuáles son sus obligaciones en la materia.

En conclusión, se estima que sí se ha elevado el nivel de cumplimiento de la protección de datos personales en el sector privado en México en años recientes, sin embargo, se encuentran por debajo del nivel esperado para garantizar un eficaz y eficiente defensa del derecho humano, y es justamente con la implementación de la página web, de la cual se proponen delimitar sus elementos, que se busca enseñar las disposiciones de la LFPDPPP, que se busca alcanzar ese nivel deseado.

Finalmente, con la finalidad de ilustrar un resumen del presente capítulo, es que a continuación, se incluye un diagrama de flujo que contiene una síntesis en la que se resaltan los puntos más importantes que condensan lo desarrollado en este apartado (Diagrama 1):

Diagrama 1 Resumen capítulo 3



Fuente: elaboración propia

Capítulo 4.

Propuesta para el diseño de una plataforma digital interactiva para promover y facilitar el cumplimiento de las obligaciones en materia de protección de datos personales en posesión de particulares

Capítulo 4. Propuesta para el diseño de una plataforma digital interactiva para promover y facilitar el cumplimiento de las obligaciones en materia de protección de datos personales en posesión de particulares.

En el capítulo anterior se demostró la importancia y la necesidad de que en México se cuente con una plataforma digital a través de la cual los responsables del tratamiento de datos personales accedan a los insumos e información necesaria que les brinde orientación para garantizar de forma eficaz y eficiente los principios y deberes previstos en la LFPDPPP.

De la misma manera, como se indicó, el incumplimiento a la disposición normativa puede ser por los supuestos siguientes: 1. Existe desconocimiento por parte de los responsables sobre sus obligaciones en materia de protección de datos personales; 2. No se cuenta con una cultura de protección de datos personales en México; 3. No existe voluntad por parte de los responsables para la observancia de la LFPDPPP o 4. No existe una participación activa coercitiva por parte del INAI.

La inobservancia referida trae como resultado que los responsables sean acreedores a sanciones pecuniarias impuestas por la autoridad competente derivado de la infracción acreditada, lo que además de causarles perjuicios económicos, los sitúa en desventaja competitiva frente a otras empresas al darles una imagen negativa.

Por lo tanto, se advierte un área de oportunidad y de mejora en el ámbito de la protección de datos personales, misma que consiste en aplicar instrumentos o mecanismos que permitan el aumento del nivel de protección de datos personales en México en el sector privado. Aquí es donde se muestra la vinculación de las TIC con la materia señalada, es decir, se recurre a la utilización de éstas como uno de los métodos de solución para la problemática planteada.

Se reitera en este punto que, la aplicación de las TIC ha acarreado nuevos retos o paradigmas que se enfrentan o chocan con distintos ámbitos de la sociedad, significan un riesgo en alguna área, como en este caso, se presenta en el ámbito

del derecho, en específico, en relación con los derechos de protección de datos personales y privacidad.

Pues como se ha indicado, en los últimos años la utilización de tecnologías ha originado que las empresas adquieran grandes cantidades de datos personales y los utilicen para fines comerciales; se ha creado el término de tratamiento intensivo de información personal debido a la inmensa cantidad de información personal utilizada, con lo que se pone en riesgo al titular al vulnerarse sus derechos por el indebido tratamiento de sus datos personales.

No obstante, para el presente estudio, se concluye que las TIC no son el origen de los bajos niveles de atención de la LFPDPPP, si bien puede ser parte del problema no son el principal elemento que los causa. En cambio, se apelan a sus beneficios para convertirse en la solución a la problemática.

Es decir, se acude a las TIC como un recurso que colabore en la resolución a la situación planteada. Por ello, es que se propone la determinación de los elementos para la creación de un sitio digital a través de la cual se otorguen a los responsables en términos de la LFPDPPP insumos adicionales a los ya existentes para asistir en subsanar las faltas que cometen.

En ese sentido, la necesidad de contar con una plataforma digital que facilite a los usuarios conocer si son responsables y saber cuáles son sus obligaciones en la materia, se sustenta porque la página permitiría orientar y guiar a los responsables sobre cómo pueden atender sus responsabilidades y, en consecuencia, se podrían aumentar los niveles de protección de datos personales de los titulares en el país.

En consecuencia, para efecto de acreditar la vinculación de la propuesta del trabajo recepcional con las TIC, en este capítulo, se contrastarán algunas de las herramientas digitales similares y que han servido a sus usuarios para mejorar el tratamiento de datos personales y se desarrollará una de las posibles soluciones a la problemática planteada mediante el uso de un instrumento digital, es decir, se desplegará el bosquejo, las características y diagramas que indican cómo sería la aplicabilidad de la tecnología como un método de solución.

4.1 Plataformas digitales

Una plataforma digital vista desde el punto académico, según Anayda Fernández y Miguel Rivero, es una *… aplicación informática diseñada para facilitar la comunicación pedagógica entre los participantes en un proceso pedagógico*.[161] Corresponde a un software que otorga la logística para formación en línea y constituye la arquitectura tecnológica sobre la que se sustenta la teleformación.[162]

Como se apunta, la plataforma digital es aquella que permite el aprendizaje sobre un tema por medio del uso de tecnología.

En consecuencia, es conveniente referir a las herramientas digitales existentes en el campo de la protección de datos personales que brindan información a los usuarios sobre cómo garantizarlos, para así tener una base comparativa sobre el tipo de plataformas que son utilizadas, conocer sus características, similitudes, diferencias y los beneficios que otorgan a la sociedad.

Para efecto de lo anterior, se eligieron y contrastaron diversas plataformas propiedad de empresas privadas y de instituciones públicas, con presencia internacional y nacional, que se relacionan con la protección de datos personales. A continuación, se mencionan algunos ejemplos y sus elementos:

a) BigID

Es una compañía con sede en Nueva York y oficinas en el resto del mundo que ofrece a las empresas conocer los datos que utilizan y las medidas que pueden adoptar sobre privacidad, seguridad informática y gobierno de datos. Cuenta con una plataforma inteligente con la cual se apoya a los clientes a conocer, administrar, salvaguardar y potencializar el valor de los datos personales.[163]

Dentro de sus plataformas cuenta con la de descubrimiento, que permite conocer los datos personales y confidenciales que el cliente posee, catalogarlos, analizarlos y realizar un estudio de información de datos; la de privacidad, que va a

---

[161] Fernández, Anayda y Rivero, Miguel, "Las plataformas de aprendizajes, una alternativa a tener en cuenta en el proceso de enseñanza aprendizaje", *Revista Cubana de Informática Médica*, Ciudad de la Habana, vol. 6, núm. 2, jul-dic 2014, *http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592014000200009#:~:text=Una%20plataforma%20virtual%20no%20es,participantes%20en%20un%20proceso%20pedag%C3%B3gico.*

[162] *Idem.*

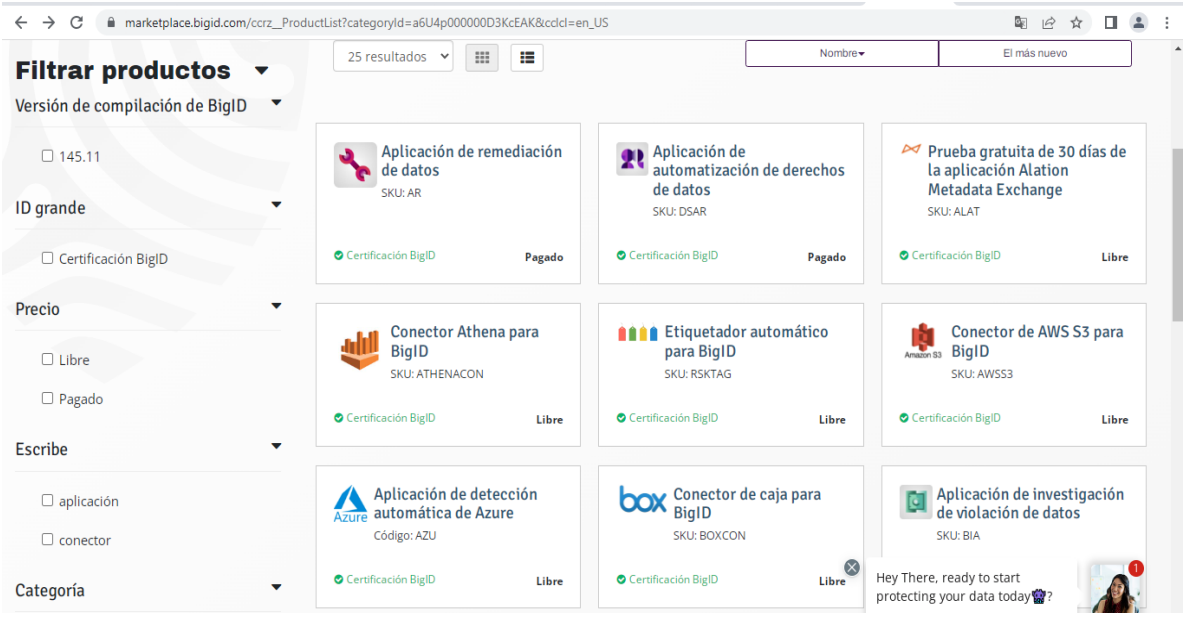
[163] BigID, "Sobre BigID", *https://bigid.com/es/company-spanish/*.

la automatización y cumplimiento de la privacidad en torno a los datos; la de seguridad, que brinda la remediación, inteligencia, riesgo, investigación de violación y etiquetado de datos y la de gobernanza, con la que se optimizan los datos y la gobernanza con inteligencia artificial de datos.[164]

La compañía ofrece una serie de productos y servicios a los usuarios relativos al tratamiento, remediación o automatización de datos personales, entre otros, pero solo algunos de estos otorgan certificaciones, son de libre acceso previo al registro del usuario o son de pago.

Sus servicios se dividen por aplicaciones o conectores, tipo de categoría e industrias. Para mostrar un ejemplo de la forma en que se ofertan los más de 100 servicios y productos, en seguida se inserta un extracto de su página web (Figura 1):[165]

Figura 1 Productos BigID



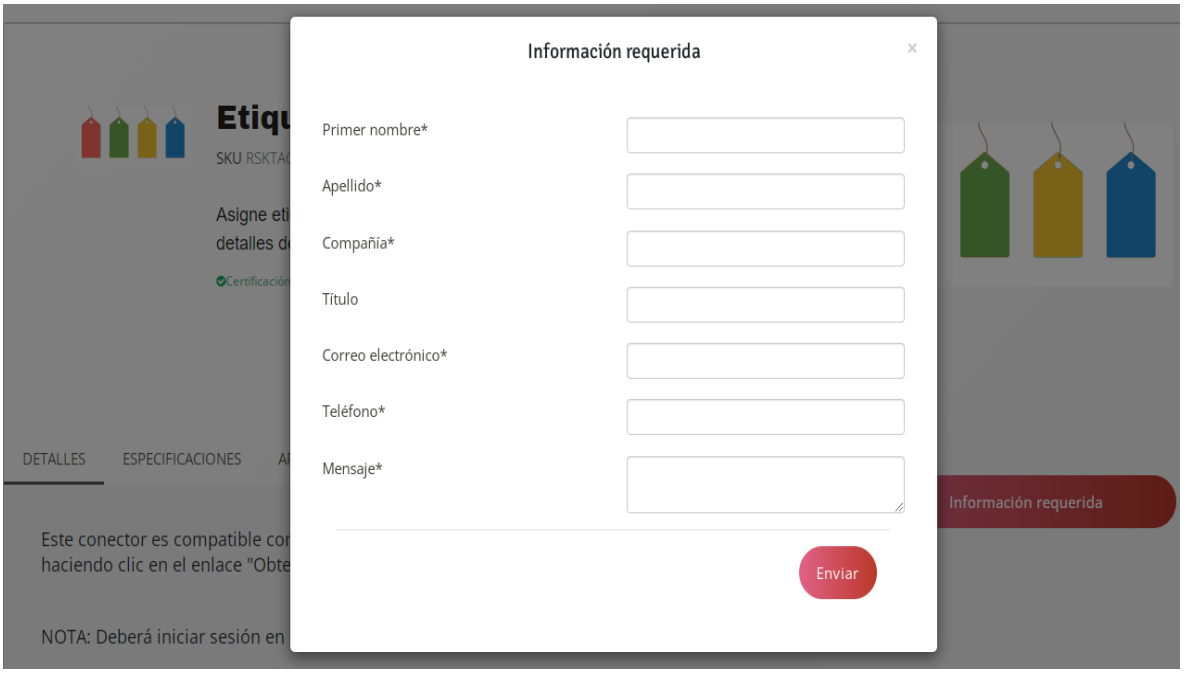
Fuente: tomada de página web BigID

A fin de efectuar un ejercicio con el espacio web, se seleccionó el producto gratuito denominado “Etiquetador automático para BigID” para verificar sus

[164] BigID, “Plataforma de inteligencia de datos BigID”, *https://bigid.com/data-intelligence-platform/*.
[165] BigID, “Productos”, *https://marketplace.bigid.com/ccrz__ProductList?categoryId=a6U4p000000D3KcEAK&cclcl=en_US*.

características y su funcionamiento, no obstante, para acceder a la información de este se requiere llenar un formulario con los datos de nombre, apellido, compañía, título, correo electrónico, teléfono y mensaje, tal como se muestra (Figura 2):[166]

Figura 2 Etiquetador automático para BigID



Fuente: tomada de página web BigID

Para el producto denominado “Aplicación de remediación de datos”, si se desea obtener más información sobre su funcionamiento se necesita llenar un formulario y solicitar la información. Asimismo, se hace referencia a sus especificaciones y detalles, empero, si se quiere observar una demostración de la aplicación debe agendarse, una muestra de ello es la siguiente figura (Figura 3):[167]

[166] BigID, “Información requerida”, *https://marketplace.bigid.com/ccrz__ProductDetails?sku=RSKTAG&cclcl=en_US*.
[167] BigID, “Remediación de datos que funciona para usted”, *https://bigid.com/protection/data-remediation-app/*.

Figura 3 Remediación de datos que funcionan para usted

Fuente: tomada de página web BigID

Esta empresa, como se indica, ofrece aplicaciones, plataformas y servicios para el tratamiento de datos personales, algunas con costo y otras de libre acceso, pero para conocer más información sobre ellos se solicitan una serie de datos personales de la persona interesada, es decir, no se advierte el funcionamiento específico y de forma inmediata.

En caso de que se desee una demostración del funcionamiento de las aplicaciones y productos se debe agendar con la empresa una cita para la exposición del servicio y las particularidades, por lo tanto, no es posible conocer las características directas que tengan.

b) Informatica

Es una compañía con oficinas en diversos países como España, Hong Kong, Ecuador, Suiza, Nueva Zelanda, Corea, entre otros, que ofrecen herramientas de integración de datos, innovaciones basadas en datos, soluciones a la gestión de datos, modernización, privacidad, gobierno de datos y cómputo en la nube. Sobre el tema específico de privacidad, emitieron una guía para principiantes con la finalidad de que se conozca cómo implementar una solución sobre el tema.

La guía referida se denomina *Data Privacy for Dummies* en la que se incluye información sobre cómo evolucionan las necesidades de privacidad de datos, qué

se necesita para garantizarla a escala, cómo se afrontan los desafíos reales y claves para la implementación de soluciones de privacidad de datos inteligente. El acceso a esta guía digital es por medio del llenado de un formulario con datos personales del interesado, para que posteriormente se envíe el documento a su correo electrónico.[168]

Dentro de sus productos también se cuenta con la plataforma de nube denominada *Intelligent Data Management Cloud*, la cual otorga servicios relacionados con el cómputo para la gestión de datos como importación, exportación replicación o sincronización de datos en cualquier aplicación, herramientas basadas en la nube para el mapeo e integración en tiempo real de datos y para la integración de todas sus aplicaciones, como se muestra en seguida (Figura 4):[169]

Figura 4 Plataforma Informatica

Fuente: tomada de página web Informatica

De lo observado, no es posible acceder a las características específicas de la plataforma del servicio de cómputo en relación con el tratamiento de datos personales, empero, se reitera que sí es posible acceder a su servicio durante un

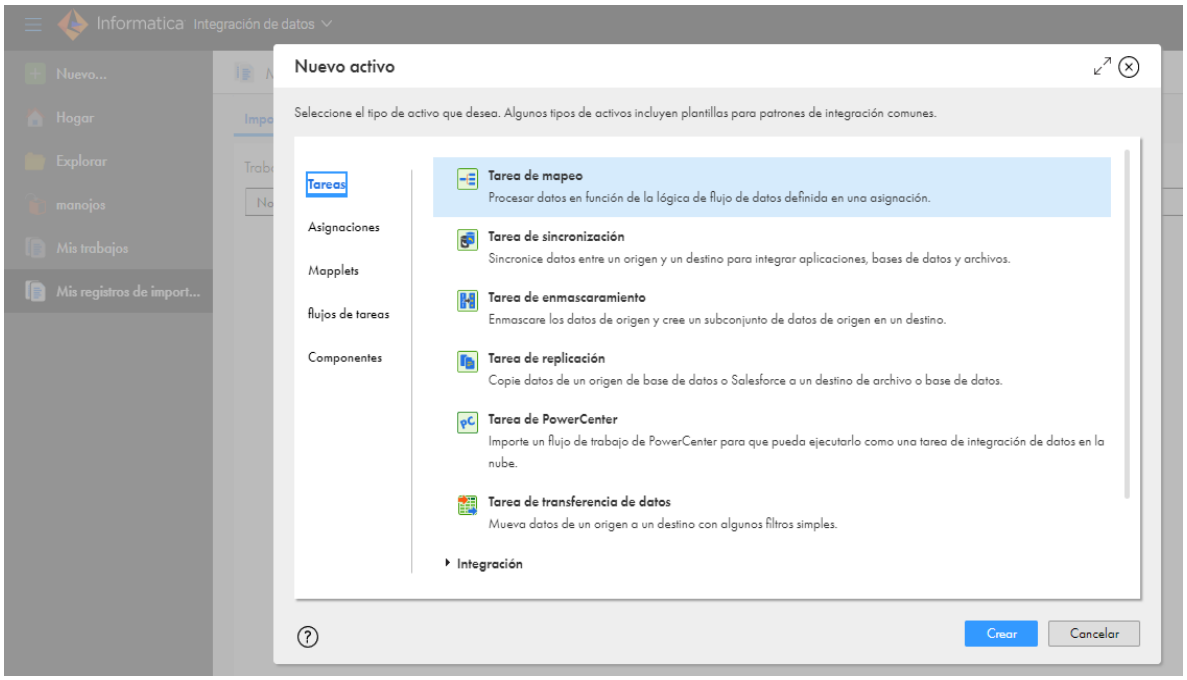
[168] Informatica, "Data Privacy for Dummies", *informatica.com/mx/lp/data-privacy-for-dummies_3600.html?formid=9270&programName=20Q1-M-DPDS-ESO-DGP-NS-NP-NI-IF-EBK-DataPrivacyDummiesMexico-0-PT3600-D&&_bt=580497307819&_bk=privacidad%20de%20datos&_bm=p&_bn=g&_bg=134235174858&gclid=EAIaIQobChMI_e3Ds_mc-AIVlhPUAR2HRwnSEAMYASAAEgJdd_D_BwE&gclsrc=aw.ds*.
[169] Informatica, "Prueba de Cloud", *https://www.informatica.com/mx/trials/informatica-cloud.html*.

periodo gratuito de 30 días, posterior a ello debe pagarse una cantidad la cual no se publica.

También se realizó el ejercicio de utilizar la prueba gratuita y una vez insertados los datos en el formulario y verificada la cuenta de usuario, se permitió el acceso a muestras de algunos sistemas, en tal tenor, se seleccionó el producto denominado “Primeros pasos con el diseñador de mapas”, mismo que permite realizar un mapeo y transformación de datos con *“Informatica Cloud Data Integration”*.

Al acceder al tutorial de la muestra de dicho producto, se pueden realizar acciones como tareas de mapeo, de sincronización, enmascaramiento, recopilación, de transferencia de datos o importe de flujo, lo anterior se observa a continuación (Figura 5):[170]

Figura 5 Informatica Integración de datos



Fuente: tomada de página web Informatica

La utilización de esta herramienta requiere de conocimientos previos en la materia para obtener resultados derivado de su uso, por otro lado, se deben de cumplir una serie de procesos previos, como el llenado de un formulario, la

[170] Informatica, “Integración de datos”, *https://usw5.dm-us.informaticacloud.com/diUI/products/integrationDesign/main/MyOieJobs*.

aceptación de envío de propagando e información de mercadotecnia por parte de la empresa, la creación de una cuenta como usuario y la validación de la cuenta para acceder al tutorial.

c) SealPath

Es una empresa con sede en Bilbao, España, con socios en más de 25 países, que brinda servicios para reducir el riesgo de fuga de datos, garantizar la seguridad de información confidencial y proteger los activos de datos en cualquier lugar que se encuentren resguardados.[171]

Señalan contar con una cartera de más de 250 clientes con un porcentaje de satisfacción del 98%. Dentro de esos usuarios, se encuentran Siemens Gamesa, Claro y el Banco de España y entre los servicios que prestan se encuentra un software con herramientas nativas diseñadas para integrarse en las empresas con la característica de ser interoperables.[172]

Ofrecen una protección a los datos por medio de un control granular de permisos, la utilización de instrumentos habituales, la sencillez para compartir, un exhaustivo control de accesos, la automatización de la protección, la integración con sistemas corporativos y una evaluación.

A manera de ejemplo, se revisó el apartado de protección automática para servidores de ficheros, pero solo se puede solicitar un demo como en seguida se advierte (Figura 6):[173]

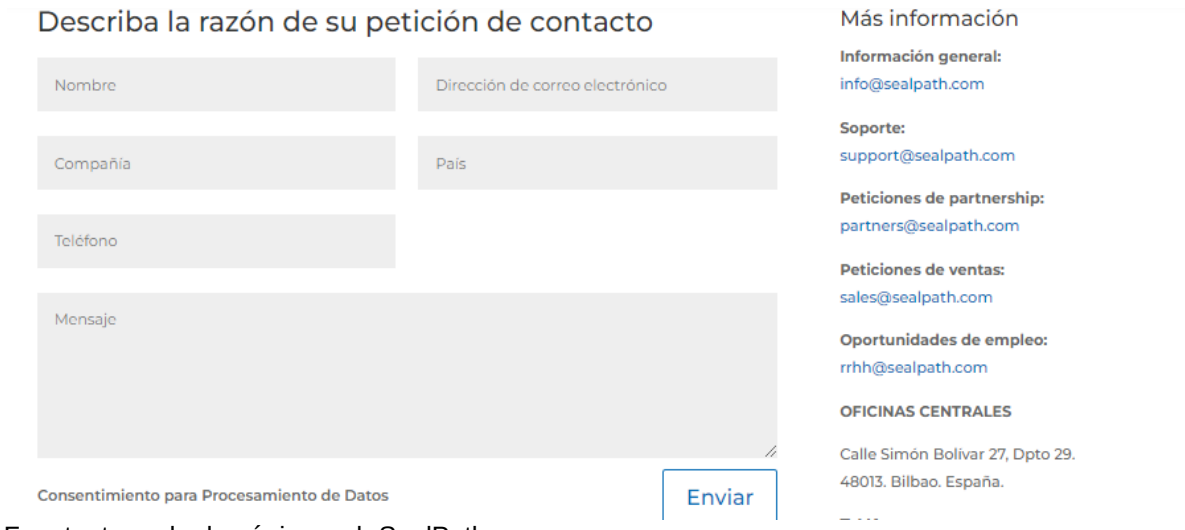
[171] SealPath, “Seguridad de Datos Inteligente”, *https://www.sealpath.com/es/sobre-nosotros/*.
[172] *Idem.*
[173] SealPath, “Automatización de la protección”, *https://www.sealpath.com/es/automatizacion-proteccion/*.

Figura 6 Automatización de la protección

Fuente: tomada de página web SealPath

En el apartado se señalan los tipos de protección automática que se ofrecen para cada herramienta, sistema o servicio y se da la opción de descargar una ficha técnica con la que se obtendría más información, no obstante, de la misma forma que cuando se solicita la demostración que se observa en la figura anterior, se debe llenar un formulario con la que se cedan datos personales conforme lo siguiente (Figura 7):[174]

Figura 7 SealPath Petición de Contacto



Fuente: tomada de página web SealPath

[174] SealPath, “Contacta con SealPath”, *https://www.sealpath.com/es/contactar/*.

No es posible conocer las características específicas de las plataformas o los servicios que ofrece la empresa, pues incluso para tener acceso a las fichas técnicas de algunos de los productos se debe llenar el formulario anterior y esperar a que sea remitida la información al correo electrónico del solicitante.

d) Agencia Española de Protección de datos (AEPD)

La AEPD es la autoridad pública independiente en España que tiene como función principal el garantizar la privacidad y la protección de datos personales de los ciudadanos españoles.[175]

Es la encargada de proteger los derechos de acceso, rectificación, limitación, supresión (derecho al olvido), oposición, portabilidad y oposición al tratamiento de decisiones automatizadas y ofrece una serie de mecanismos para garantizarlos. Asimismo, tiene atribuciones para verificar que los responsables del tratamiento de datos personales en España cumplan con los principios y deberes que están obligados a respetar.[176]

Para efecto de lo anterior, la AEPD ha creado diversos documentos básicos de consulta que ayudan a los responsables a cumplir con los requisitos previstos en la disposición normativa como lo es la "Guía para profesionales del sector sanitario", la "Guía de gestión del riesgo y evaluación de impacto en tratamiento de datos personales, o la "Guía para la notificación de brechas de datos personales".[177]

También ha generado diversas herramientas digitales para facilitar a los responsables el cumplimiento normativo como lo son: "Facilita RGPD", que indica qué hacer con el tratamiento de datos de escaso nivel de riesgo; "Canal del DPD", que atiende las consultas planteadas antes los delegados de protección de datos; "Gesgiona EIPD", asiste para el análisis de riesgo y evaluaciones de impacto; "Facilita Emprende", ayuda a las *"startups"* tecnológicas a cumplir con la norma; "Comunica-Brecha RGDP", brinda valoración para la toma de decisiones sobre la

[175] Agencia Española de Protección de datos, "Bienvenida a la Agencia", *https://www.aepd.es/es/la-agencia/bienvenida-la-agencia*.
[176] Agencia Española de Protección de datos, "¿En qué podemos ayudarte?", *https://www.aepd.es/es/la-agencia/en-que-podemos-ayudarte*.
[177] Agencia Española de Protección de datos, "Guías", *https://www.aepd.es/es/guias-y-herramientas/guias?combine=&sort_bef_combine=field_advertise_on_value_1%20DESC&sort_by=field_advertise_on_value_1&sort_order=DESC&page=0*.

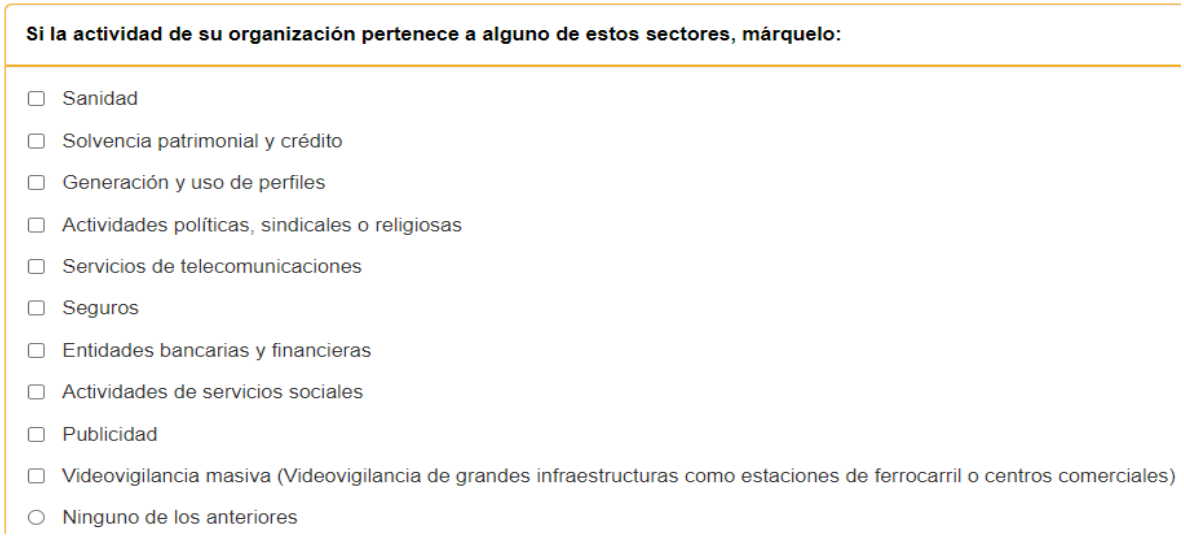
comunicación a las personas afectadas por brecha de seguridad y “Evalúa-Riesgo RGPD”, para el análisis de la necesidad de una Evaluación de Impacto.[178]

La herramienta “Facilita 2.0” o “Facilita RGPD” fue creada para orientar a las empresas que efectúan un tratamiento datos personales de escaso nivel de riesgos y no aplica para todas las empresas, pues cada una puede tener su particularidad, como el tratar datos personales de alto riesgo.

Para las empresas que tratan datos personales de escaso nivel de riesgo, la herramienta resulta ser benéfica, pues los documentos resultantes de la ejecución del programa pueden ser válidos en la medida en la que las respuestas sean ciertas y cumplan con los mínimos para facilitar el cumplimiento del Reglamento General de Protección de Datos.[179]

Al ingresar, en primer lugar, se requiere seleccionar si la actividad de la empresa no corresponde a algunos de los sectores de escaso nivel de riesgos, como se muestra en las siguientes figuras (Figura 8):[180]

Figura 8 Formulario Herramienta Facilita 2.0



Fuente: tomada de página web AEPD

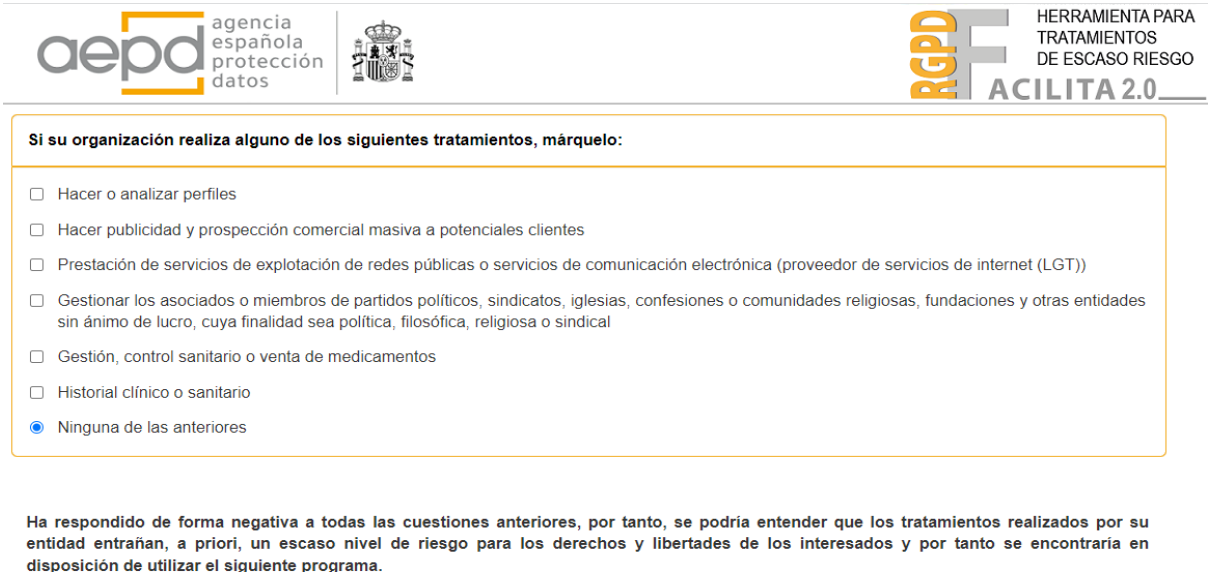
[178] Agencia Española de Protección de Datos, “Herramientas”, *https://www.aepd.es/es/guias-y-herramientas/herramientas*.

[179] Agencia Española de Protección de Datos, “Facilita 2.0”, *https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDQxMjQ4NzExNjU1MTc3MjUxNzY4?updated=true*.

[180] Agencia Española de Protección de Datos, “Facilita 2.0. Herramienta para Tratamientos de Escaso Riesgo”, *https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDQxMjQ4ODgxNjU1MTgwNDU3Mzk2*.

En seguida, se debe señalar si trata datos personales sensibles o si realiza tratamiento de datos personales de alta intromisión, tal como el extracto siguiente lo exhibe (Figura 9):

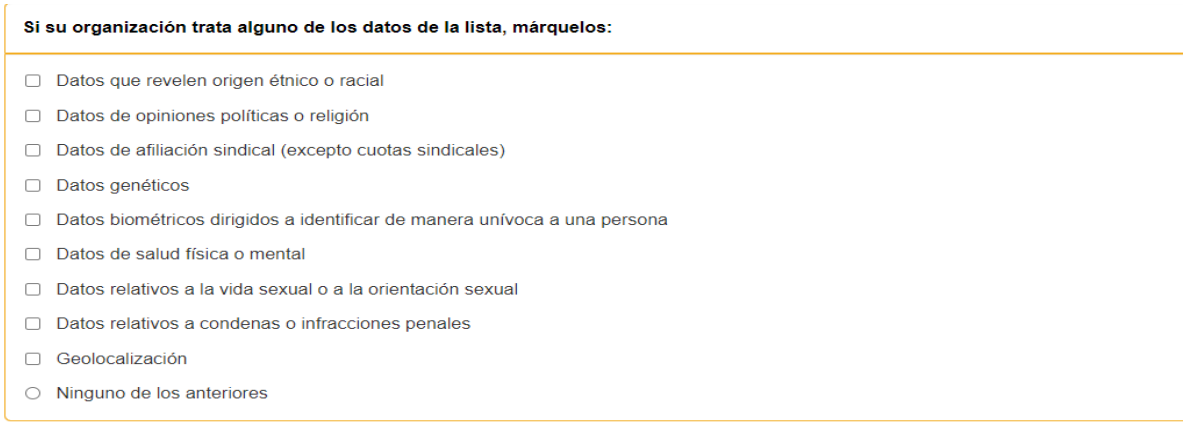
Figura 9 Datos a incorporar al programa Facilita 2.0



Fuente: tomada de página web AEPD

Posterior a la selección de las casillas en las que se señala que la empresa no pertenece al sector que hace tratamiento de datos de medio o alto riesgo, que no se tratan datos personales sensibles y no efectúan ciertas acciones indicadas, se comienza a llenar un diverso formulario cuya información será la base para la elaboración de los documentos, se inserta un ejemplo (Figuras 10 y 11):[181]

Figura 10 Llenado de formulario Facilita 2.0 II



Fuente: tomada de página web AEPD

[181] *Idem.*

Figura 11 Llenado de datos formulario Facilita 2.0 III

Fuente: tomada de página web AEPD

Una vez concluido el llenado del formulario con los datos se generan varios documentos de forma automática y adaptados a la empresa, como lo son cláusulas informativas en los formularios de obtención de datos personales, cláusulas contractuales para incluir en los contratos de encargado de tratamiento, el registro de actividad de tratamiento y un anexo con medidas de seguridad orientativas y mínimas.[182]

e) Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

El INAI es el órgano constitucional autónomo que con fundamento en el artículo 6, Apartado A, fracción VIII de la Constitución Política de los Estados Unidos Mexicanos se creó para garantizar los derechos humanos de acceso a la información pública y la protección de datos personales.[183]

Tiene como misión el promover y consolidar una cultura del debido tratamiento de datos personales para conformar una sociedad incluyente y

[182] Agencia Española de Protección de Datos, "Facilita RGPD", *https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd#:~:text=La%20herramienta%20genera%20diversos%20documentos,un%20anexo%20con%20medidas%20de*.

[183] Cámara de Diputados, *Constitución Política de los Estados Unidos Mexicanos*,… *op. cit.,* artículo 6, Apartado A, fracción VIII.

participativa; su visión es ser una Institución eficaz y eficiente que promueva el ejercicio del derecho de protección de datos personales como base para la participación democrática y, por lo tanto, uno de sus objetivos es el garantizar el cumplimiento óptimo de ese derecho.[184]

Para efecto de lo anterior, el INAI ha creado diversas guías y herramientas dirigidas a sujetos obligados, responsables y a la ciudadanía con la finalidad de orientar en el cumplimiento de las obligaciones y el ejercicio del derecho de protección de datos personales. En específico, sobre los instrumentos interactivos que ofrece en la materia, tanto para el sector público como privado se advierten las siguientes:

El **Registro de Esquemas de Autorregulación y Mejores Prácticas** se divide entre el sector público y el privado. Consiste en el registro por parte de responsables o encargados del esquema de autorregulación vinculante en materia de protección de datos personales, en complemento a los estándares establecidos en la ley y su reglamento.[185] Sin embargo, en la página del Instituto solo se advierte una serie de vínculos que redirigen a más información sobre el tema para obtener el registro y certificación correspondiente.

El **Evaluador de Vulneraciones** es un medio que permite a responsables de ambos sectores, público y privado, registrar y documentar las medidas de seguridad con las que cuentan y de las que carecen, con el objetivo de minimizar la ocurrencia y el impacto de vulneraciones de seguridad.[186]

---

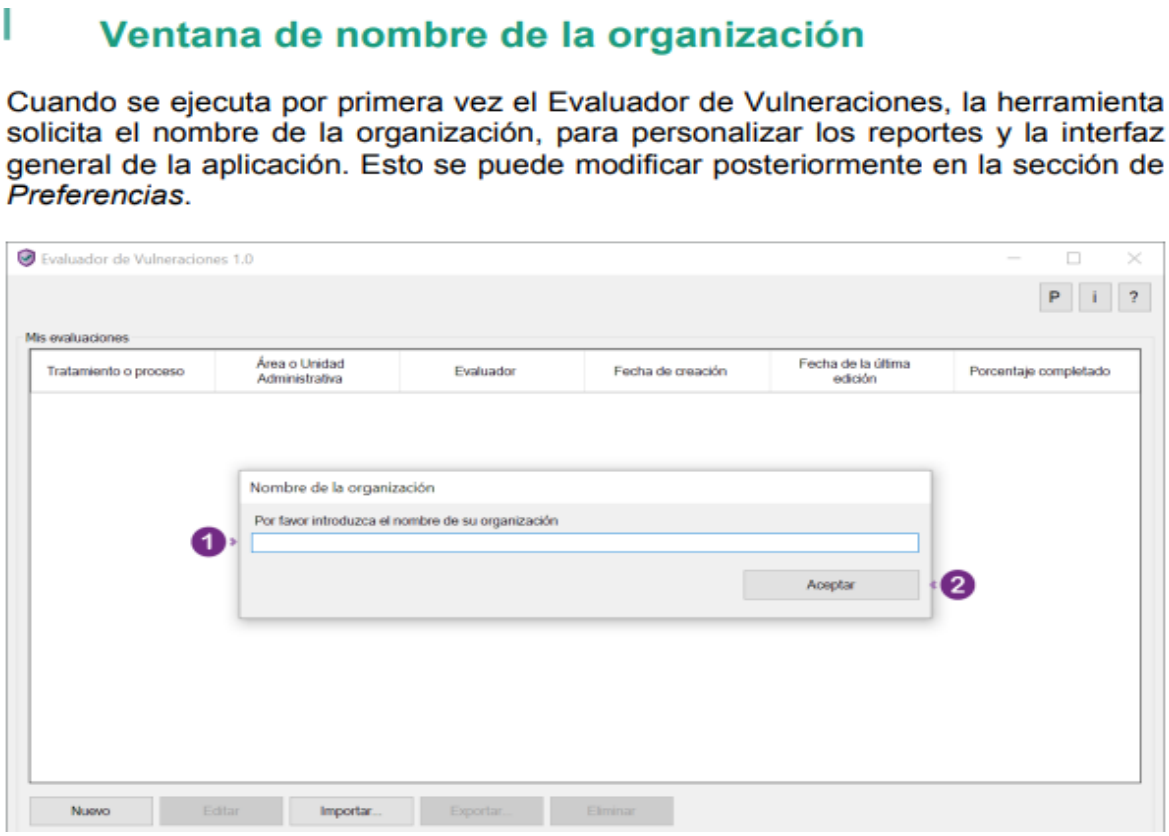
[184] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Qué es el INAI",… *op. cit.*, *https://home.inai.org.mx/?page_id=1626*.

[185] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Registro Esquemas de Autorregulación Vinculante. Sector Privado", *https://registro-esquemas.inai.org.mx/?page_id=177&a=2&b=2*.

[186] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, *Evaluador de Vulneraciones. Manual de Usuario,* p. 3, *http://inicio.inai.org.mx/EvaluadorVulneracionesDocs/Manual%20de%20Usuario.pdf*.

Se proporciona un Manual de Usuario para la utilización de la plataforma pues si bien no requiere de instalación ni de configuración de algún componente, sí se presenta en un archivo único ejecutable “Evaluador de Vulneraciones.exe”, para sistemas operativos Microsoft Windows 7 (SP2), 8, 8.1 y 10.[187] En seguida se muestra un ejemplo del momento en que se ejecuta por primera vez el evaluador (Figura 12):[188]

Figura 12 Evaluador de Vulneraciones Primera Ejecución

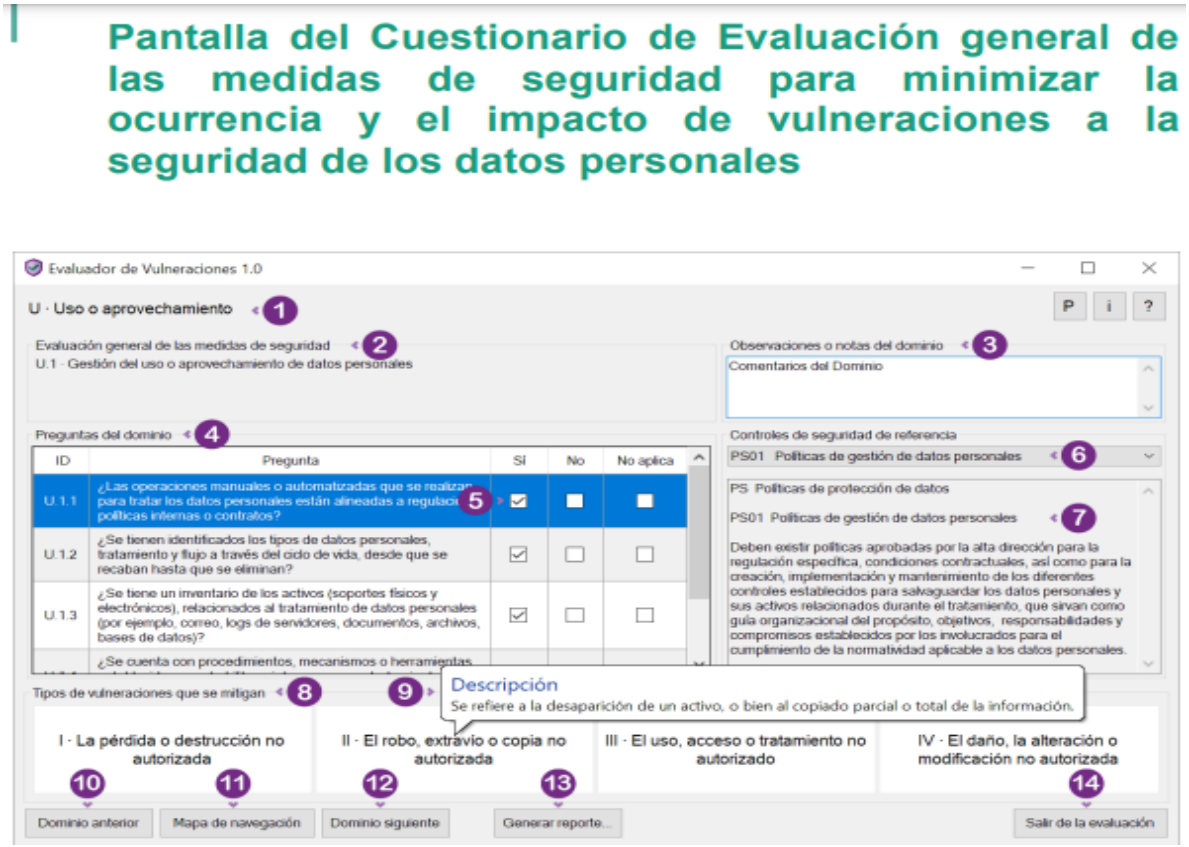


Fuente: tomada de “Evaluador de Vulneraciibes.exe”

Una vez completado el cuestionario de evaluación en la interfaz de trabajo en relación con las medidas de seguridad y de impacto de vulneraciones, se genera el reporte de la evaluación en archivos TXT, HTML, Excel y Word, para que el usuario lo utilice en cualquier formato. Un ejemplo de la pantalla de cuestionario de evaluación general se muestra en seguida (Figura 13):[189]

[187] *Ibidem*, p. 6.
[188] *Ibidem*, p. 7.
[189] *Ibidem*, p. 19.

Figura 13 Cuestionario de Evaluación general



Fuente: tomada de “Evaluador de Vulneraciibes.exe”

La herramienta digital es dinámica, flexible, entendible y fácil de usar. El llenado del cuestionario y la generación del reporte no implica poseer previamente conocimientos en la materia, por lo que, puede ser utilizada por cualquier persona. Se destaca que no se necesitan de requerimientos técnicos para su uso, sino únicamente el llenado de la información de la responsable.

La plataforma está dirigida a auxiliar a los responsables en el cumplimiento del deber de seguridad y varios principios, como lo pueden ser el de responsabilidad y licitud. No obstante, no se dirige a una protección integral de los principios o deberes, como tampoco para el cumplimiento de todas las obligaciones que son exigibles.

El **CORPUS IURIS en materia de protección de datos personales** es una plataforma impulsada por la Red Iberoamericana de Protección de Datos que conglomera documentos, normas y precedentes que hacen latente el desarrollo

que, como derecho humano, ha tenido la protección de datos personales, sus avances, las direcciones que ha adoptado y las áreas que deben fortalecerse.[190]

Al existir la colaboración de diversos entes y países la plataforma se compone de dos secciones, la de documentos internacionales y documentos nacionales de los diversos países que integran la antes mencionada Red. A la fecha en que se consulta, para ambas secciones se tiene un total de 113,153 visitas. A continuación, se muestra un ejemplo de la sección del ámbito internacional (Figura 14):[191]

Figura 14 Corpus Iuris Internacional

Fuente: tomada de página CORPUS Iuris

En cada una de las secciones que integran esta herramienta se pueden buscar documentos conexos, jurisprudencia de órganos jurisdiccionales, criterios derivados de informes, criterios de órganos cuasi jurisdiccionales emitidos en diversos ámbitos como el europeo o asiático y por distintos órganos, como el Tribunal Europeo de Derechos Humanos en el ámbito internacional o la Suprema Corte de Justicia de la Nación en el nacional.

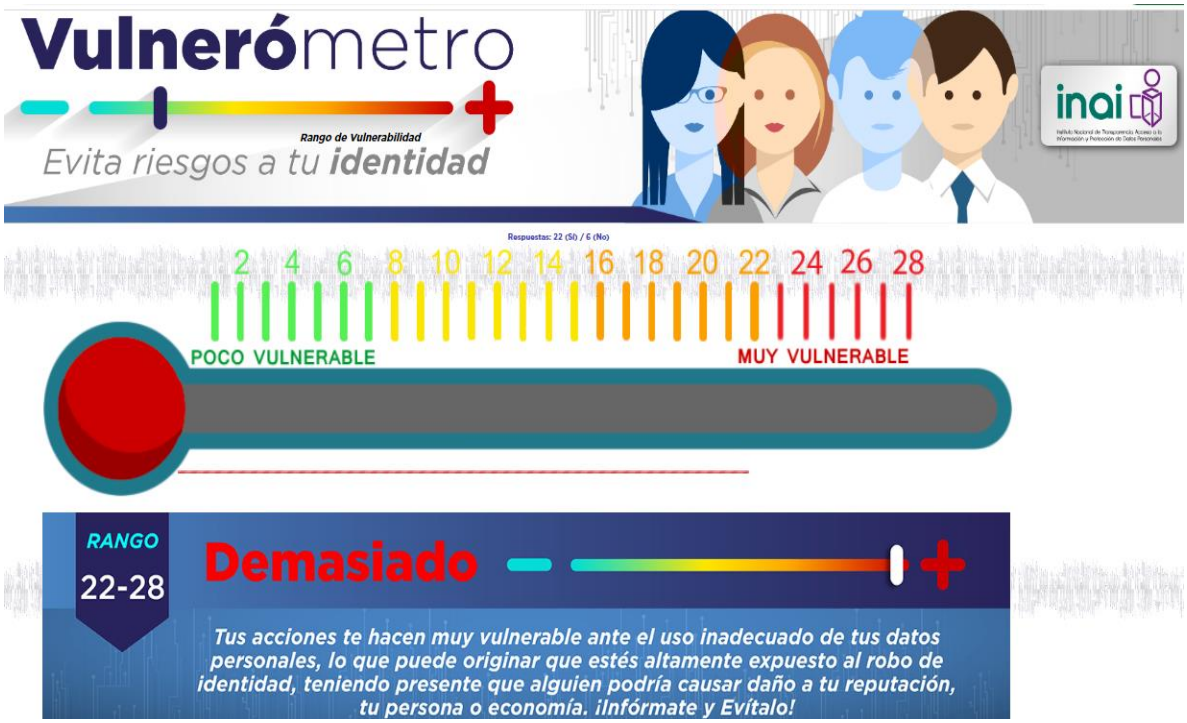
---

[190] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Corpus Iuris Internacional y Nacional", *http://corpusiurispdp.inai.org.mx/Pages/home.aspx*.
[191] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Corpus Iuris en materia de Protección de Datos Personales. Documentos Internacionales", *http://corpusiurispdp.inai.org.mx/Pages/Inicio.aspx*.

El **Vulnerómetro** consiste en un espacio digital dirigido a los ciudadanos, con la finalidad de que conozcan cuál es el rango de vulnerabilidad que tiene su información personal y así puedan evitar riesgos de robos de identidad a través de dispositivos electrónicos.

La persona debe llenar un cuestionario sobre los hábitos de seguridad que tiene con su información personal y, posteriormente, se da el resultado del rango de vulnerabilidad que presenta. La plataforma ha sido visitada en 11,431 ocasiones a la fecha de consulta y, a manera de ejemplo, se hizo la selección de las casillas de forma que se eligiera la mayor cantidad de respuestas afirmativas dando como resultado el siguiente (Figura 15):[192]

Figura 15 Vulnerómetro



Fuente: tomada de página del INAI

Derivado del ejercicio efectuado, se obtuvo que los datos personales en relación con los hábitos de seguridad que se seleccionaron son demasiados vulnerables, por lo tanto, se indica que se efectúa un uso inadecuado de datos

[192] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, "Vulnerómetro", *https://micrositios.inai.org.mx/vulnerometro/resultados.php*.

personales y que se está altamente expuesto al robo de identidad, en consecuencia, se invita a consultar la Guía para prevenir el robo de identidad.

Por último, se trae a colación el sistema **Generador de Avisos de Privacidad**, primera herramienta interactiva creada por el IFAI y la más utilizada por los usuarios. A través de esta plataforma se facilita a los responsables del tratamiento de datos personales del sector público y privado la creación de avisos de privacidad.

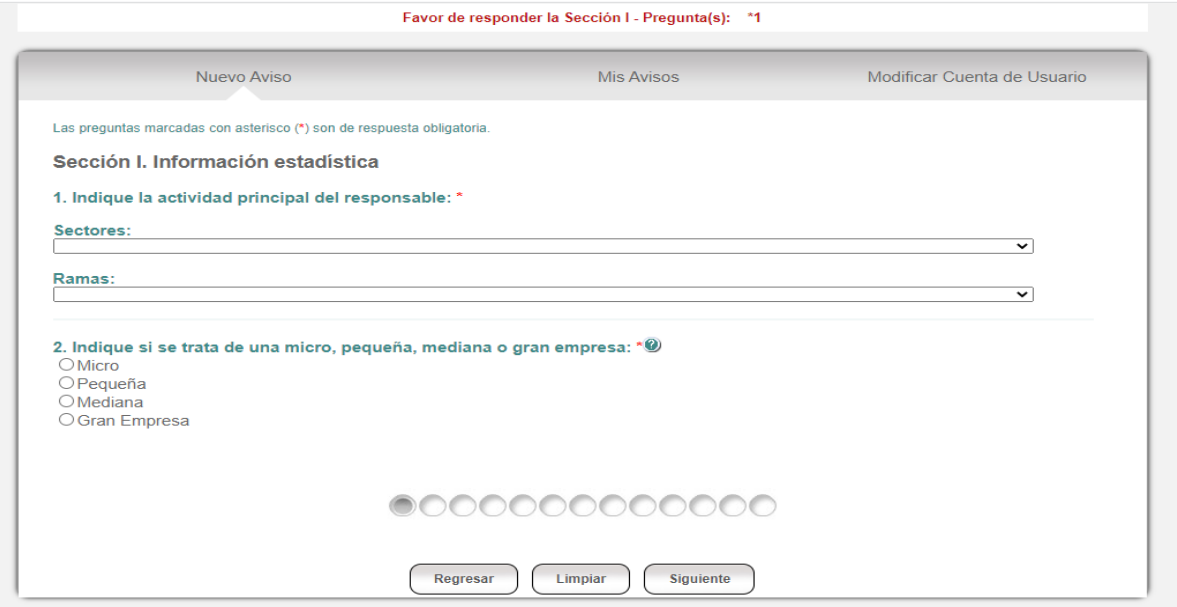
Este entorno digital busca que los responsables cumplan con una de las obligaciones principales que tienen en materia de protección de datos personales, esto es, crear y dar a conocer a los titulares de los datos los parámetros y condiciones del tratamiento al que será sometida su información personal.

Para la utilización de la plataforma, inicialmente se debe seleccionar el sector para el cual se requiere generar el aviso de privacidad, esto es, si es público o privado. Así, para efectos de este proyecto se ingresó al Generador de Avisos de Privacidad del sector privado, en el cual se localizó un Manual de Usuario y el documento denominado “ABC del Aviso de Privacidad”, éste último, ya citado con antelación.

En la plataforma se establece que el servicio del generador es gratuito, pero para su utilización se debe crear una cuenta con un usuario y contraseña. Una vez concluida la creación de la cuenta, se ingresa al generador para originar el aviso de privacidad, para lo cual, se requiere contestar una serie de preguntas por secciones, como a continuación se muestra (Figura 16):[193]

[193] Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, “Generador de Avisos de Privacidad. Sector Privado”, *https://generador-avisos-privacidad.inai.org.mx/policies/myAdd?v=1*.

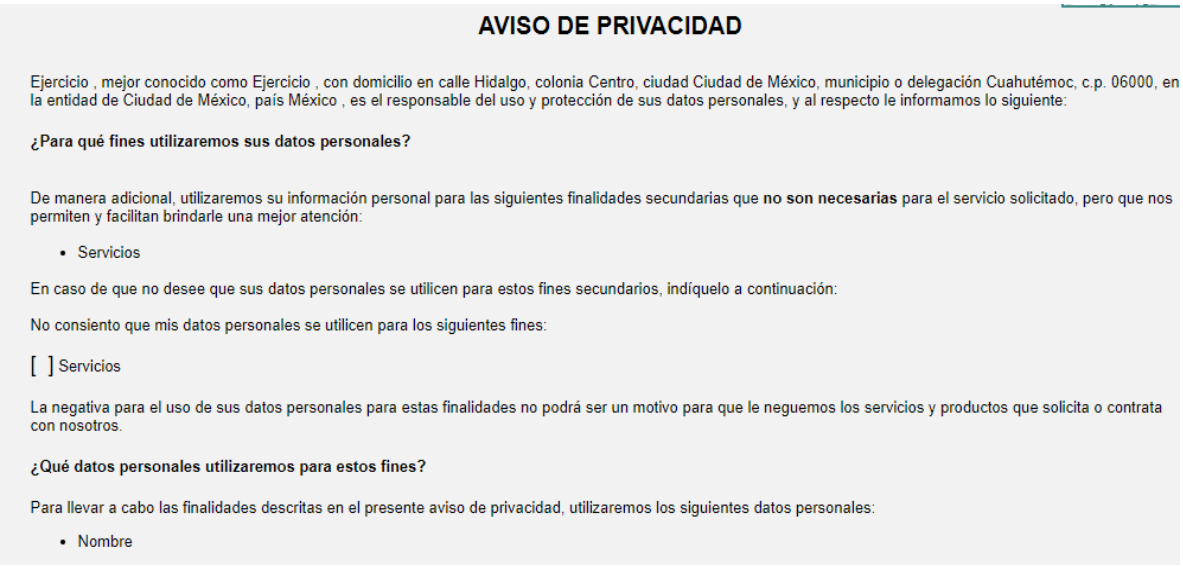
Figura 16 Generador de Avisos de Privacidad



Fuente: tomada de página de generador de avisos de privacidad

Una vez que se cumple con la primera sección, se procede a elegir el tipo de aviso de privacidad que se desea generar, integral, simple o corto, posteriormente, se continúa con la selección de casillas y brindando información que van dando contenido al aviso de privacidad para generarse de la siguiente forma (Figura 17):[194]

Figura 17 Ejemplo Aviso de Privacidad



AVISO DE PRIVACIDAD

Ejercicio , mejor conocido como Ejercicio , con domicilio en calle Hidalgo, colonia Centro, ciudad Ciudad de México, municipio o delegación Cuahutémoc, c.p. 06000, en la entidad de Ciudad de México, país México , es el responsable del uso y protección de sus datos personales, y al respecto le informamos lo siguiente:

¿Para qué fines utilizaremos sus datos personales?

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

- Servicios

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

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

[ ] Servicios

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

¿Qué datos personales utilizaremos para estos fines?

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

- Nombre

Fuente: tomada de página de generador de avisos de privacidad

[194] *Ibidem.*

El aviso de privacidad generado puede ser modificado o actualizado en el momento que desee y conforme a las necesidades específicas que tenga el usuario. Puede descargarse de tal forma que pueda ser puesto a disposición de los titulares en diversos formatos o en distintos sitios.

Sin embargo, esta plataforma sirve para dar cumplimiento a algunas de las obligaciones que son exigibles a los responsables, como lo son la creación del aviso de privacidad y su puesta a disposición, pero no para la totalidad de los principios o deberes, aunado a que se asume que el usuario que utiliza la página tiene certeza de ser responsable conforme la LFPDPPP.

En cuanto a la utilización del sistema, la Dirección General de Prevención y Autorregulación del INAI dio a conocer el número de avisos de privacidad generados para el sector privado dentro del periodo del 01 de enero de 2013 al 06 de abril de 2022, siendo los siguientes (Tabla 5):[195]

Tabla 5 Avisos de privacidad generados

Años	Cifras
2013	16510
2014	26901
2015	12860
2016	13003
2017	14409
2018	12950
2019	12334
2020	13925
2021	12444
2022 (hasta 6/04/22)	3405

Fuente: Dirección General de Prevención y Autorregulación, *OFICIO No. INAI/SPDP/DGPA/066/2022* INAI, Ciudad de México, 2022, p, 3,

[195] Dirección General de Prevención y Autorregulación, *OFICIO No. INAI/SPDP/DGPA/066/2022*, INAI, Ciudad de México, 2022, p. 3, *https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=330031322000754&coleccion=5*.

https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=330031322000754&coleccion=5.

Desde su creación este instrumento ha sido utilizado frecuentemente por los usuarios, quienes se benefician al contar con el documento que les permite cumplir con una de las obligaciones que les son exigibles en términos de la legislación mexicana, esto es, contar y poner a disposición de los titulares el aviso de privacidad.

Ahora bien, del análisis que se hizo a las plataformas citadas con antelación, se colige que existe una variedad de opciones y aplicaciones creadas para orientar a los usuarios y responsables sobre el cumplimiento de sus obligaciones en términos de las legislaciones que les son aplicables, como también para brindarles asesorías con el objetivo de aumentar los niveles de seguridad de sus bases de datos y la automatización de los datos personales.

Los espacios de las empresas de consultoría privada ofrecen sus servicios y productos en específico a los responsables interesados en aumentar los niveles de seguridad de sus bases de datos, automatizar sus procesos, gestión de datos o de cómputo en la nube, pero en la mayoría de los casos solo se brinda una breve referencia sobre lo que se puede adquirir del producto sin conocer en específico su funcionamiento.

Asimismo, la finalidad de estas aplicaciones es que la empresa que oferta el servicio sea quien se encargue de la gestión y operación de los productos y no directamente el responsable, es decir, éste deja a cargo de la empresa lo relacionado con el tratamiento de los datos personales, aunado a que en su mayoría todos los servicios tienen un costo o para acceder a ello se requiere otorgar la información personal del usuario.

La utilización de los entonos web gratuitos como las de BigID están más dirigidos a la gestión y automatización de procesos que ayuden a los usuarios al procesamiento, almacenamiento o utilización de los datos personales que resguardan, pero no están enfocadas a atender, como objetivo principal, los principios o deberes de la legislación.

Por lo que hace a las herramientas de las instituciones públicas, a diferencia de las del sector privado, se encaminan a guiar a los responsables a atender las

obligaciones que por ley les son exigibles. Por ejemplo, “Facilita RGPD” de la AEPD, ayuda a que los responsables cumplan con algunas de las disposiciones del Reglamento General de Protección de Datos.

El sistema aludido es gratuito, flexible, de fácil acceso, no se requieren conocimientos técnicos previos para el llenado del formulario y permite la generación de documentos que son necesarios para los usuarios con los que se pueda garantizar el derecho de la protección de datos personales.

En el ámbito nacional, desde la creación del IFAI y con la continuación del INAI como autoridad competente dentro del sector privado para garantizar la protección de datos personales, se han emitido guías y herramientas para orientar a los responsables en la atención de sus obligaciones.

De igual forma, todas las plataformas el Instituto ofrece son de servicio gratuito y en algunas de ellas solo se requiere crear una cuenta con un usuario y contraseña para utilizarlas. Los sistemas son fáciles de usar, flexibles, entendibles y no se requiere tener conocimiento técnico sobre la materia para generar los documentos a través de ellas.

No obstante, estos instrumentos tienen finalidades específicas, por ejemplo, el generador del aviso de privacidad tiene como objetivo que el responsable cuente con un documento con el que pueda dar a conocer a sus usuarios o clientes los términos en que se dará tratamiento a los datos personales, esto es, para cumplir con algunas de las disposiciones de la LFPDPPP, pero no todas las obligaciones.

En sentido similar se encuentra el evaluador de vulneraciones, que sirve, como su nombre lo señala, para evaluar las medidas de seguridad que tienen los responsables y con dicho informe se puedan minimizar los riesgos de posibles incidentes o afectaciones en sus bases de datos, pero tampoco brinda atención a la totalidad de las normas.

Los sitios web estudiados tanto de las empresas consultoras privadas como de las instituciones públicas, en general, sirven de apoyo para que los responsables tengan insumos e información para atender algunas de sus obligaciones como para mejorar los procesos internos que tienen al interior de sus empresas.

Asimismo, los beneficios que traen a la sociedad son latentes, en virtud de que siguen siendo utilizadas por parte de la sociedad, tal es el caso del generador de avisos de privacidad que, desde su creación a la fecha reportada en párrafos anteriores (del 01 de enero de 2013 al 06 de abril de 2022) ha emitido 138,741 avisos de privacidad, facilitando así a un gran número de responsables la observancia de la norma.

Por otro lado, se resalta que son espacios de sencillos de usar, explican claramente lo que se puede obtener al utilizarlas, los pasos a seguir dentro de ellas son fáciles y no necesitan conocimientos técnicos en la materia. Sin embargo, se requiere que la persona que las usará conozca cuál es el producto o servicio que va a adquirir.

Con lo anterior se colige que, la persona que desea atender una disposición o mejorar algún elemento de su empresa tiene una idea de lo que está buscando, es decir, ya tiene información de que tiene una obligación que observar y, por lo tanto, es que trata de allegarse de los insumos que le ayudarán a conseguir ese objetivo.

En ese sentido, la finalidad que se busca alcanzar con la plataforma, de la cual se propone establecer sus elementos en este proyecto, se encuentra un paso antes de los objetivos que se logran con los instrumentos mencionados en este apartado. Esto es que, brindaría la información previa y necesaria para conocer, en primer lugar, el usuario que la utiliza si es responsable conforme la LFPDPPP y, en segundo, qué es lo que se debe cumplir y cómo lo puede hacer.

Una vez conociendo los datos básicos, la recomendación sería la utilización del resto de sistemas ya existentes, que son complementarias o de apoyo para el seguimiento de la atención de las disposiciones jurídicas en la materia.

Ahora bien, se estima necesario mencionar cuáles son las características que una página web tiene y cómo debe ser su diseño para que el usuario pueda utilizarla con facilidad y los objetivos que se buscan alcanzar con la misma se logren. Para tal efecto, en el siguiente apartado se desarrollarán las particularidades, elementos y diseño que conformarían la página web.

4.2 Características y diseño de la plataforma

En México no existe una página web que contemple los elementos para que los responsables tengan conocimiento de las obligaciones que emanan de la LFPDPPP, lo cual genera incertidumbre e inconvenientes en el acceso a la información para el cumplimiento de la normatividad y, por consiguiente, ante la falta de observancia se transgreden derechos humanos de los particulares y los entes obligados se vuelven acreedores de sanciones.

En virtud de lo anterior, es que el espacio web que se propone en el presente proyecto está dirigido a orientar a los responsables del tratamiento de datos personales en términos de la LFPDPPP, sobre cuáles son sus obligaciones y cómo pueden cumplirás.

Es decir, como punto de partida se busca dar a conocer a los usuarios si son o no responsables en términos de la LFPDPPP, de igual manera, está dirigido a todas aquellas personas físicas o morales consideradas responsables para que conozcan de forma sencilla la información básica que les oriente y facilite la atención de las disposiciones normativas.

El espacio web además de ser un instrumento orientador sobre la atención de una norma, también funcionaría como un medio educativo tanto para responsables como para titulares de los datos personales, pues las personas de igual forma podrían saber qué deben realizar las empresas para garantizar sus derechos.

Asimismo, tomando en cuenta que uno de los objetivos es facilitar el conocimiento sobre la materia, es que este entorno digital se convierte en una herramienta que, de forma paralela a la ayuda de la atención de la LFPDPPP, colabora en el aumento de la cultura en materia de protección de datos personales.

Ahora bien, en cuanto a quién desarrollaría la página web o en qué sectores podría aplicarse, se pueden considerar tres vertientes:

- Institución pública (sector público): en la que una autoridad pública adopte la propuesta y la incluya dentro de su propio sitio web y solo se desarrolle como un elemento más de la misma, pero en la que se contemplen las características y diseño que aquí se propone.

El INAI, al ser la autoridad en México encargada de garantizar la protección de datos personales en el sector privado, podría acoger esta propuesta y desarrollarla como una herramienta más de las que ofrece entre su catálogo de opciones.

- Institución educativa (sector académico): una universidad o institución educativa pública con el objetivo de impulsar a la cultura de protección de datos personales, así como para fomentar una educación en la materia, podría también incluir entre sus instrumentos digitales esta propuesta.
- Consultoría o despacho (sector privado): alguna empresa que esté interesada en ofrecer servicios legales y técnicos en la materia de protección de datos personales y que quiera atraer clientes, podría utilizar esta plataforma como una forma de brindar un servicio gratuito para posteriormente interesar a los responsables en utilizar su asistencia.

Al respecto, para la creación del espacio podría utilizarse un software que se adapte al presupuesto de la institución o consultoría que desee utilizarlo, ello mediante una página que ofrezca servicios de gestión de contenidos y sea adecuada para crear sitios con un bajo costo.

El alojamiento del espacio web puede realizarse en mediante otro que ofrezca este tipo de servicio. Existen diversas opciones y variedades, pero se encuentran algunos que se dirigen a alojar páginas web de pequeños y medianos negocios, o para proyectos individuales que tiene un costo bajo, lo cual puede utilizarse para el caso de esta propuesta.

Una vez determinado el medio que se utilizará para la creación de la herramienta y para el alojamiento de esta, se procedería a originar el nombre de dominio y a su registro en alguna de las empresas que ofrecen este servicio, para que el entorno digital cuente con su URL y pueda ser identificado de forma rápida y sencilla, a manera de ejemplo dicho nombre puede ser: “protecciondatos.com.mx”.

Las características específicas que conformarían la página web se basan en las recomendaciones brindadas por Gustavo B. creador de sitios web quien se

enfoca en la aplicación de estrategias SEO en Hostinger para España y Latinoamérica.[196] Así, las características del espacio serían las siguientes:

- Se crearía una sola sección de inicio en la que se encuentre la información y elementos básicos de la página, esto es, se señalaría cuál es el objetivo de la herramienta, qué obtendrían los responsables al usarla y la opción de ingresar a realizar un formulario.
- Se generaría una página de inicio de ventana única en la que se localice toda la información y se contaría con otra sección que sea la que directamente remita al llenado del cuestionario.
- La jerarquía visual partiría incluyendo el título de la página web, continuando con el objetivo de esta, las preguntas que se buscan resolver con su utilización, la opción de ingresar al formulario y finalmente un apartado en el que se pueda observar el contador de visitas, lo anterior alternado con imágenes que visualmente sean atractivas.
- La organización de la estructura sería de forma lógica para que el usuario localice sencillamente la sección que permita acceder al cuestionario, por lo tanto, se utilizaría una estructura de sitio plana en la que las funciones de la página se limiten a uno o dos clics para ingresar al formulario.
- Los elementos de diseño serían simples, pues únicamente se incluirían dos imágenes que refieran a la protección de datos personales, con lo que se busca mantener la facilidad de uso, la armonía visual y la optimización del sistema y velocidad de carga de la información, imágenes y formulario.
- El tamaño y tipo de letra se seleccionarán de forma que sea legible la información y lo que se ofrece.
- Los colores que se utilizarían son morado, rosa, azul y verde en tonos suaves para mantener un balance en la plataforma y sea fácil visualizar la información.
- Atendiendo al método de indexación “dispositivos móviles primero” de la empresa Google y en virtud de que estos equipos son los que se usan en

[196] B. Gustavo, “Cómo diseñar una página web en 10 pasos”, 2022, *https://www.hostinger.mx/tutoriales/como-disenar-una-pagina-web/*.

mayor medida por los usuarios para acceder a las búsquedas,[197] es que el diseño y configuración de la página se haría de tal forma que se ajuste a dispositivos móviles, tabletas, equipos portátiles y computadoras de escritorio.

- Se utilizaría una configuración que permita realizar ajustes a las herramientas, funcionamiento y diseño conforme se utilice la página. En este sentido, se agregaría un contador de visitas en el que se muestre las consultas que ha tenido, para medir los niveles de uso que tiene y de impacto. En su caso, se agregaría la fecha de última actualización del espacio en caso de haber alguna.
- Para atender las recomendaciones de Google sobre el tiempo de carga del sitio web, se buscaría que esta no supere los 500 KB, por lo que, su tamaño y diseño se mantendrían simples.
- Se utilizaría un tema y diseño que funcione correctamente con los navegadores principales como Firefox, Google Chrome y Safari.

En resumen, las características de diseño de la página web serían las siguientes: visualización simple en primera plana o ventana con una sola sección de inicio; letras de color y tamaño legible; se incluiría la información básica con la que se advierta cuál es el objetivo del espacio y sus beneficios; el diseño de visualización se mantendría sencillo para facilitar el acceso simple al formulario y las imágenes se adaptarían a la jerarquía visual.

La configuración del espacio web se concretizaría en lo siguiente: el acceso al formulario será de forma que no implique dar más de dos clics; se buscaría que no supere los 500 KB de peso; su funcionamiento sería con los navegadores principales y en dispositivos electrónicos como computadoras de escritorio y portátiles, tables y móviles y se permitirá ir ajustándola conforme se vaya utilizando.

De acuerdo con los elementos indicados con antelación, se tiene un resultado inicial de diseño para computadora y móvil que sería el que se muestra y describe en los siguientes párrafos y figuras.

---

[197] Google, “Prácticas recomendadas para la indexación "dispositivos móviles primero”, *https://developers.google.com/search/mobile-sites/mobile-first-indexing*.

Al ingresar al vínculo electrónico que direcciona a la página web, inicialmente se desplegaría una parte de la plataforma en la que se observe el título “Protege los datos personales de tus clientes y usuarios”, así como una imagen que se relacione con la protección de datos personales y que llame la atención de quien visita la página (Figura 18):

Figura 18 Desplegado inicial de la página web

Fuente: elaboración propia

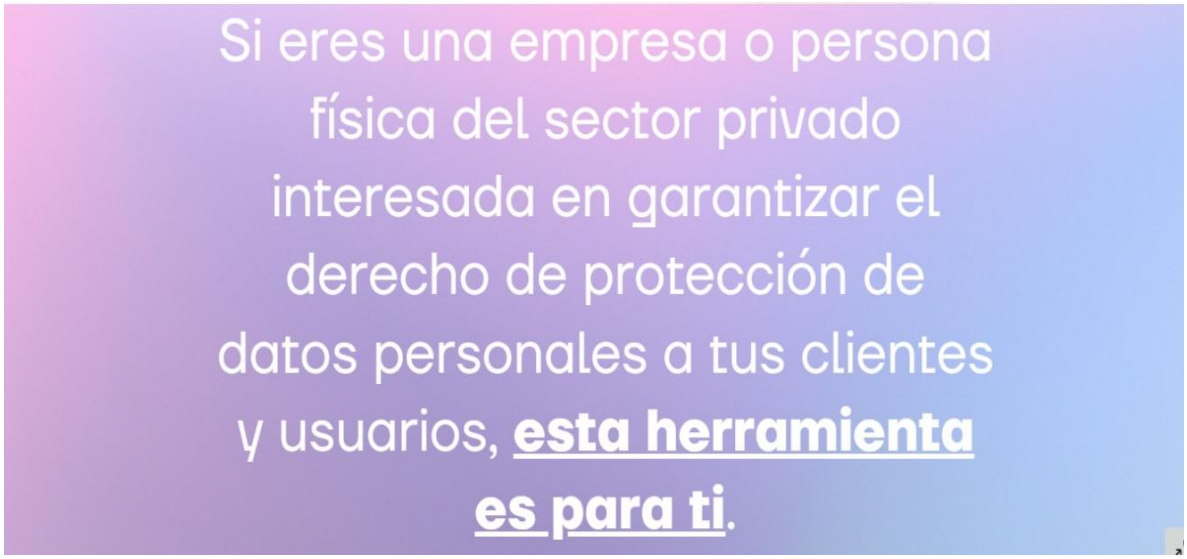
En seguida, se incluirían algunas preguntas con las que se busca llamar la atención de los visitantes, para que se interesen en responder el formulario. Las preguntas que se incluyen son “¿Soy responsable de cumplir las obligaciones de la LFPDPPP”, “¿Qué debo hacer para cumplirlas?” y, finalmente, para resaltar la importancia de que la protección de datos personales se trata de un derecho humano se incorpora el cuestionamiento “¿Sabías qué?” (Figura 19):

Figura 19 Apartado de preguntas

Fuente: elaboración propia

Al continuar con la navegación en el entorno digital, se resalta que si la persona que visita el sitio es una persona física o parte de una empresa del sector privado que esté interesado en garantizar la protección de datos personales de sus clientes o usuarios, esta herramienta podrá servirle (Figura 20):

Figura 20 ¿A quién se dirige la página web?



Fuente: elaboración propia.

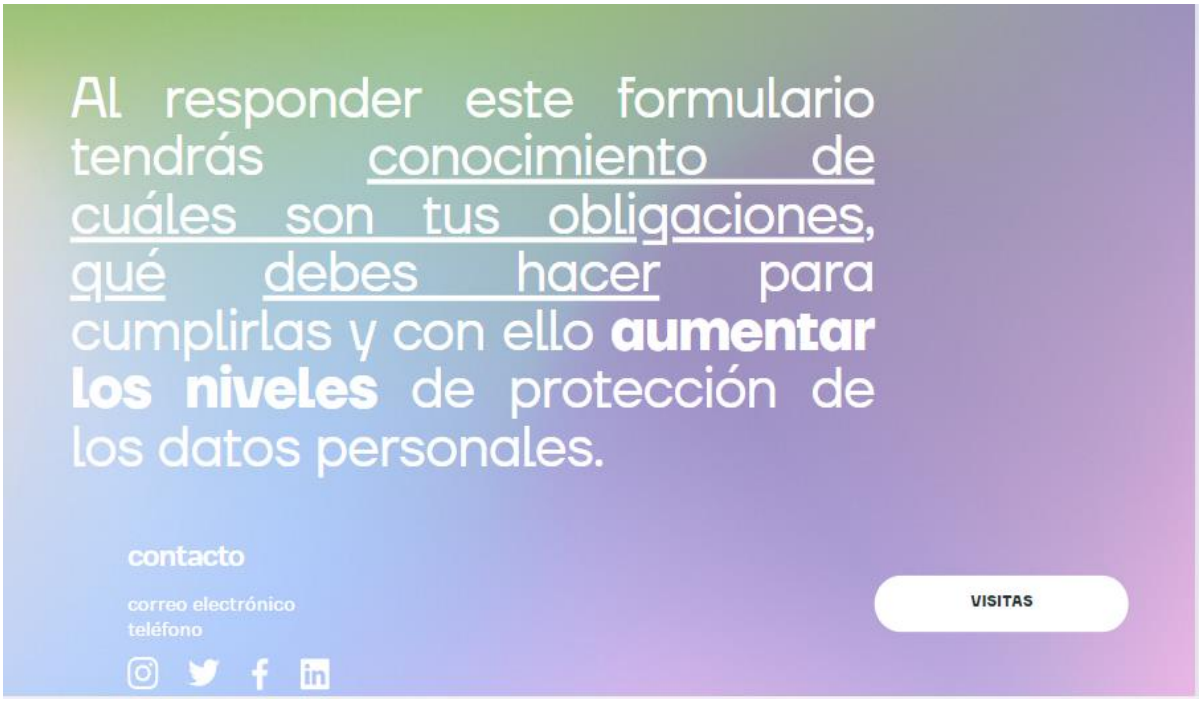
A continuación, se incluye el apartado específico en el que se localiza el botón que dirigirá a la persona a la interfaz en la que se podrá llenar el formulario. Se incluye una imagen que indica datos personales en color que contrasta con el botón de “Formulario” (Figura 21):

Figura 21 Formulario

Fuente: elaboración propia.

En la parte final de la página web se incluye un breve texto que explica qué es lo que se espera al llenar el cuestionario, los datos de contacto de quien administra el sitio y el número de visitas que ha tenido ésta (Figura 22):

Figura 22 Contacto, visitas y contexto



Fuente: elaboración propia

Asimismo, se muestra cómo sería el resultado del diseño del instrumento en los dispositivos móviles (Figura 23):

Figura 23 Visualización en dispositivos móviles

Fuente: elaboración propia

El diseño del sitio web se realizó mediante la plataforma digital denominada Canva, que permite previsualizar el resultado de la página antes de publicarla en versión para computadora y móvil, que es lo que se muestra con anterioridad.

Por otro lado, una vez seleccionado el botón “formulario”, se remita directamente a la contestación del cuestionario. Dicho cuestionario permitirá que el usuario seleccione diversas casillas que vayan dando ciertas respuestas y que le ayuden a conocer, en primer lugar, si es responsable de cumplir con las obligaciones de la LFPDPPP y, en segundo, que la selección de ciertas casillas le vayan dando ciertos resultados cobre cuáles son las obligaciones que tiene.

En ese sentido, en el siguiente apartado, a manera de ejemplo, se incluirán una serie de diagramas, que formarían el bosquejo del contenido del formulario de

la herramienta digital que se propone, pues mediante dichos diagramas se podrían conocer cuáles son los resultados que ofrecería la página web.

4.3 Bosquejo y diagrama del formulario de la plataforma

Fernando Anciniega, programador web y diseñador gráfico, indica que los diagramas son mecanismos esenciales para representar bocetos de espacios web y su arquitectura de información. Resalta que esta técnica permite que el costo de producción disminuya, además, es beneficiosa pues de ser necesario hacer modificaciones es más sencillo y económico cambiar el diseño sobre papel que en el producto ya implementado y programado.[198]

Por su parte, la empresa IBM establece que se pueden utilizar esquemas de página para diseñar sus aplicaciones basadas en la web y los requerimientos del cliente. Dicho esquema es un diagrama de línea simple o esquemático para realizar una maqueta de interfaces de usuario o entornos web.[199]

En tal tenor, el diagrama de flujo de la página web es un instrumento de planificación que permite organizar y aclarar el contenido existente y eliminar el innecesario o repetido, por lo tanto, también ayuda a que el espacio se mantenga centrada en el usuario y en los objetivos que se buscan alcanzar por medio de esta, pues la finalidad es que no se confunda al usuario cuando navega por el espacio o al interactuar con el contenido.[200]

---

[198] Anciniega, Fernando, “Tipos de diagramas para representar sitios web”, *https://fernandoarciniega.com/tipos-de-diagramas-para-representar-sitios-web/*.

[199] IBM, “Esquemas de página”, 09 marzo 2021, *https://www.ibm.com/docs/es/elm/6.0.4?topic=requirements-wireframes*.

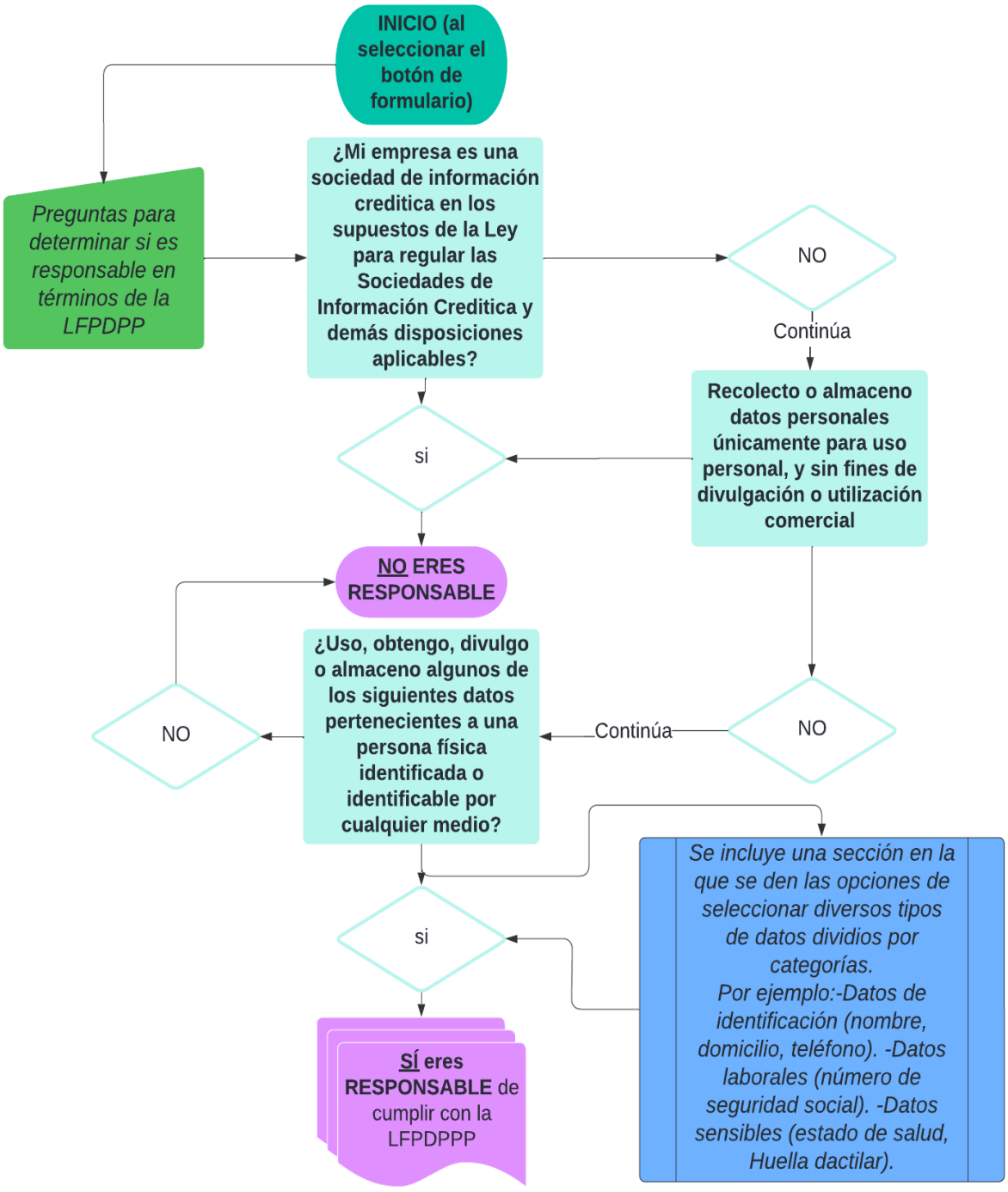
[200] Miro, “Plantilla de diagrama de flujo para un sitio web”, *https://miro.com/es/plantillas/diagrama-flujo-para-sitio-web/*.

En este orden de ideas, a continuación, se incluirán algunos ejemplos de diagramas basados en selección de casillas de opción sí o no y múltiples, que se podrían utilizar para el diseño de la herramienta digital que se propone en el presente proyecto y que darían cuenta de cómo funcionaría la página web. Para clarificar y poner en relieve qué significa cada recuadro que contiene la información de los diagramas, se inserta la siguiente simbología (Diagrama 2):

Diagrama 2 Simbología

Fuente: elaboración propia

Diagrama 3 ¿Soy Responsable?



Fuente: elaboración propia

En el diagrama anterior se muestran las preguntas que se efectuarían y el procedimiento que se seguiría para determinar, en principio, si el usuario que utiliza la herramienta digital es responsable o no del tratamiento de datos personales en términos de la LFPDPPP.

Lo anterior es relevante, puesto que, si el resultado a las preguntas iniciales arroja que el usuario no es responsable, en consecuencia, no tiene que cumplir con las obligaciones exigibles en términos de la disposición jurídica y, por lo tanto, no tendría que seguir con el llenado del resto del cuestionario.

En seguida, se incluyen algunas muestras de los resultados del llenado del formulario si se determina que el usuario es o no responsable conforme la LFPDPPP (Figura 24):

Figura 24 Resultado: no eres responsable

Fuente: elaboración propia

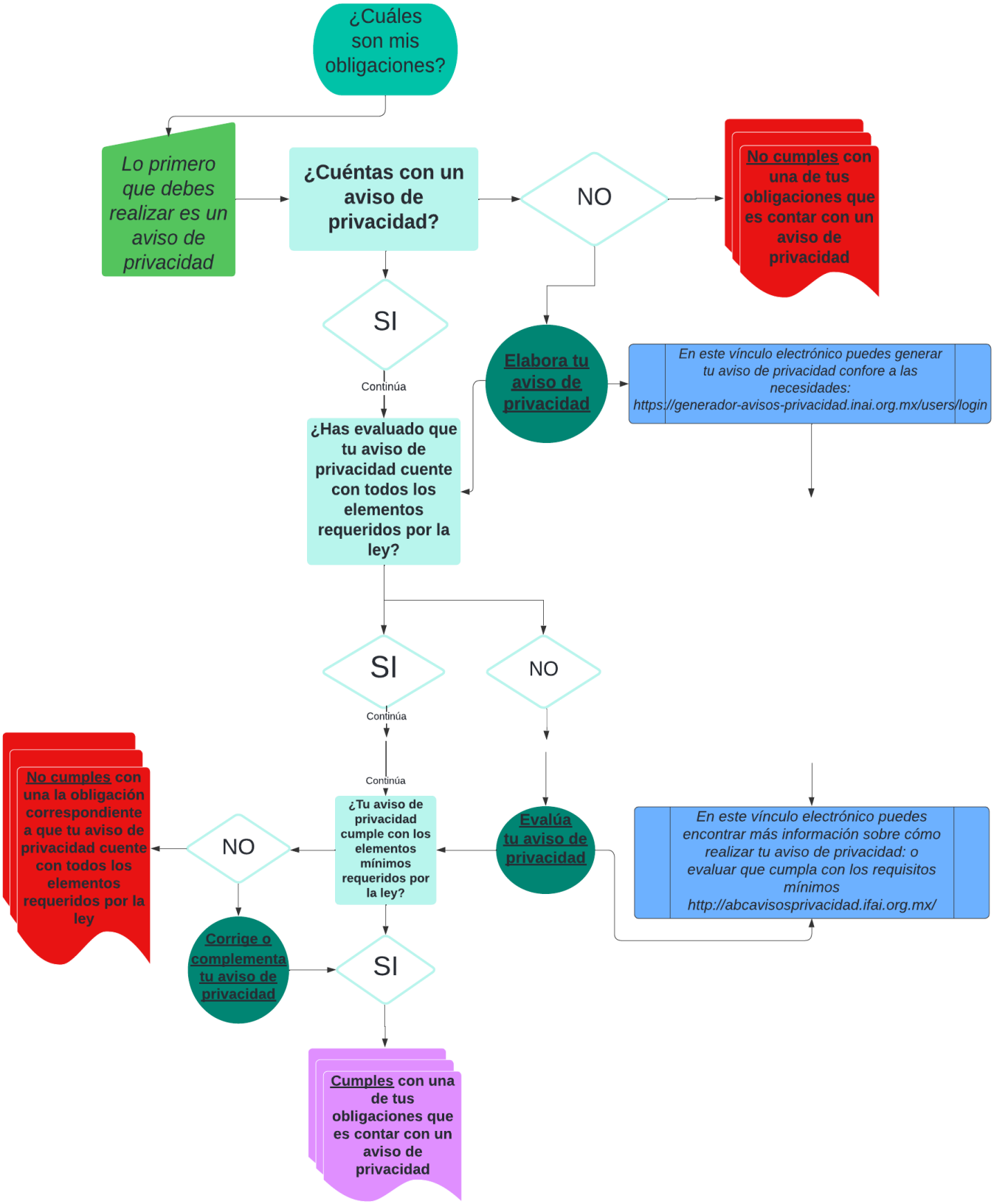
Si del llenado a la primera parte del formulario el resultado que se obtiene es que el usuario seleccionó las casillas que advierten que trata datos personales de los titulares, se observaría el siguiente resultado (Figura 25):

Figura 25 Resultado: sí eres responsable

Fuente: elaboración propia

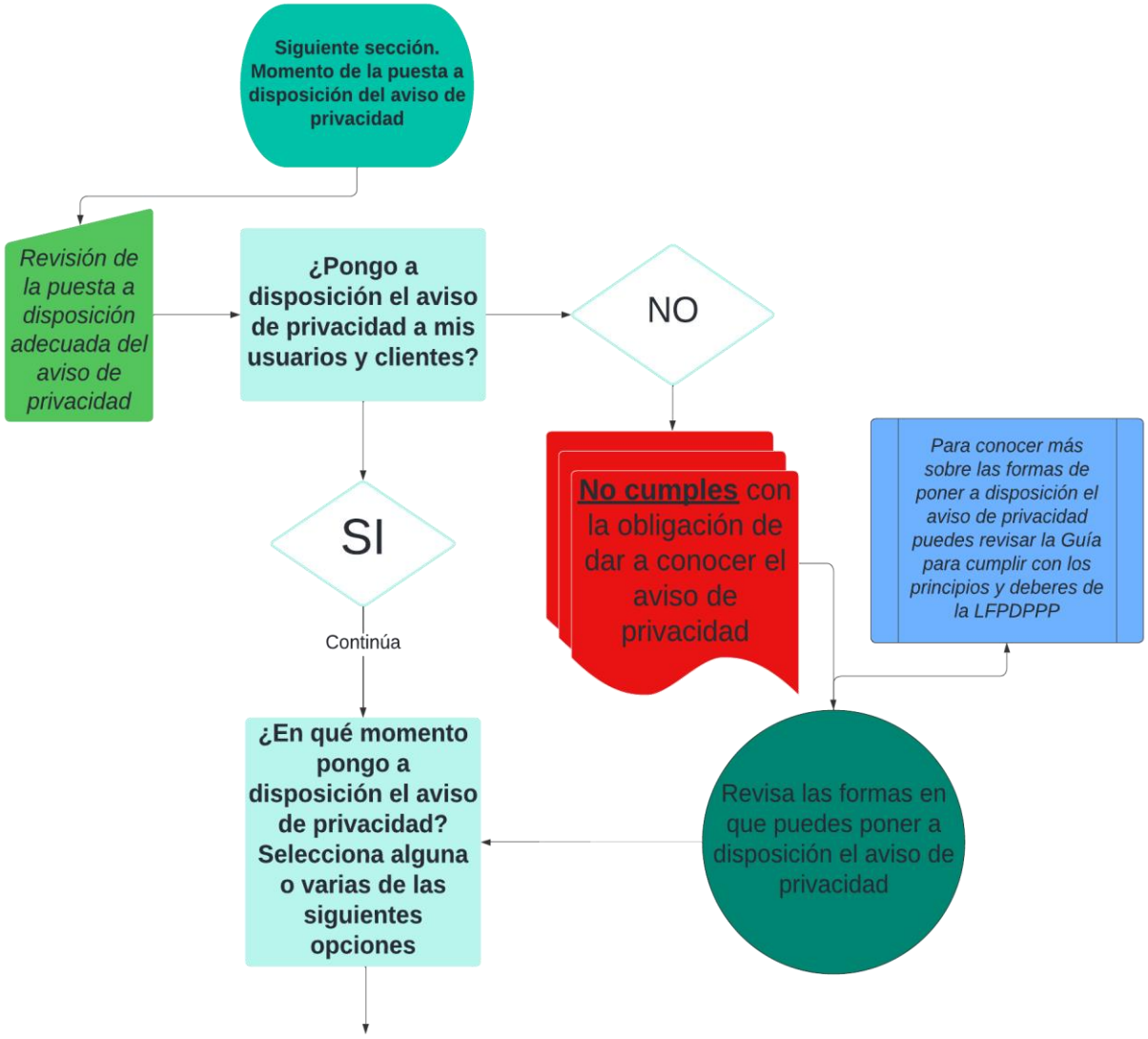
Ahora bien, si el usuario resulta ser responsable conforme lo dispuesto en la LFPDPPP, y desea seguir con el cuestionario para conocer cuáles son sus obligaciones, a continuación, se incluyen algunas de las siguientes secciones y procedimientos sobre tales responsabilidades (Diagrama 4):

Diagrama 4 Aviso de privacidad



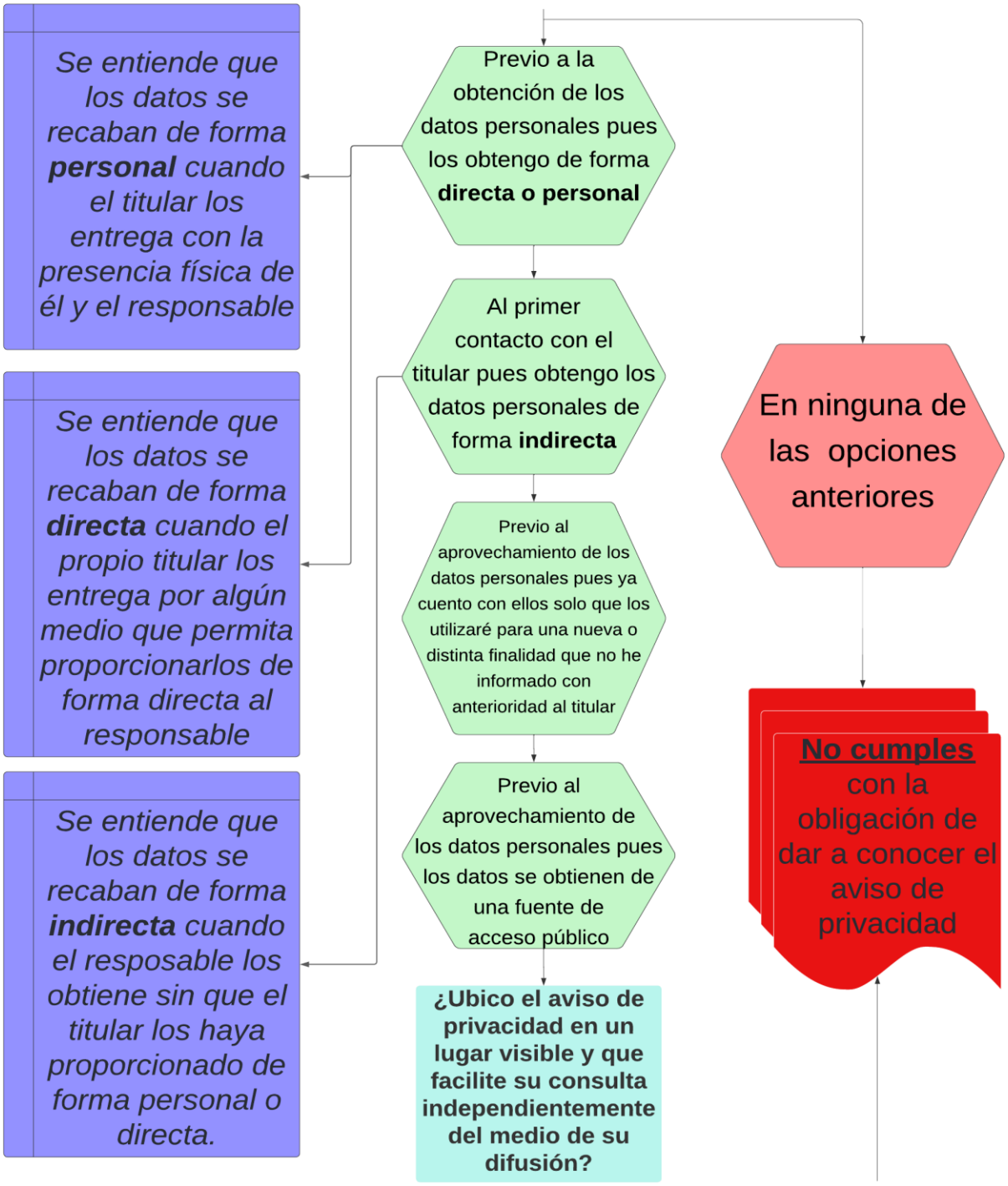
Fuente: elaboración propia

Diagrama 5 Puesta a disposición del aviso de privacidad



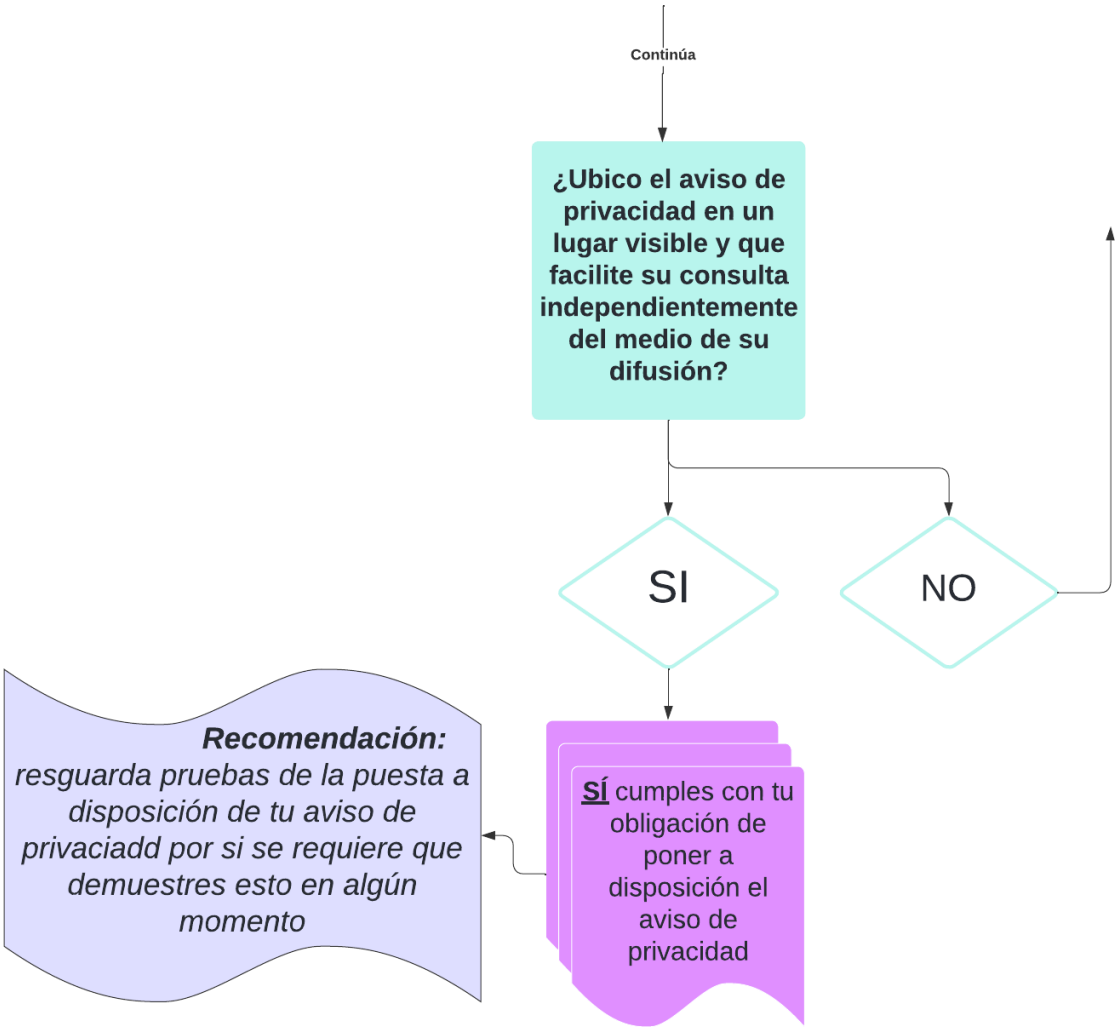
Fuente: elaboración propia

Diagrama 6 Momento de la puesta a disposición del Aviso de Privacidad I



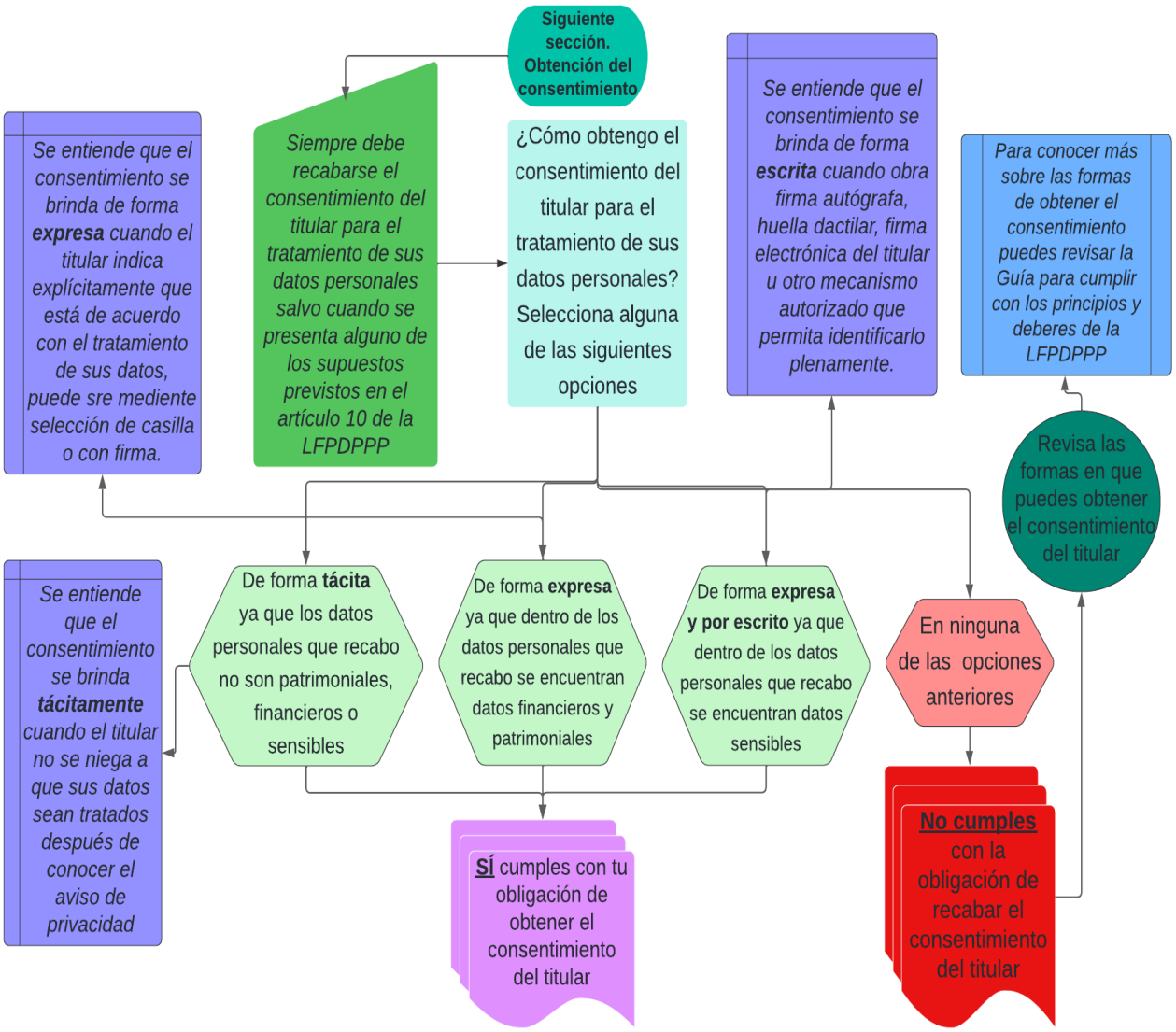
Fuente: elaboración propia

Diagrama 7 Momento de la puesta a disposición del Aviso de Privacidad II



Fuente: elaboración propia

Diagrama 8 Obtención del consentimiento



Fuente: elaboración propia

Los diagramas que se insertan con antelación son un ejemplo de los procesos que se seguirían para configurar las opciones, resultados de cumplimiento o incumplimiento, recomendaciones, sugerencias, acciones a realizar, que dan contenido al formulario de la página web.

Como se indicó, la finalidad de la herramienta es que de forma sencilla los usuarios que la utilicen puedan responder las preguntas que los guíen a conocer si cumplen o no con las obligaciones exigibles en términos de la ley de la materia, es

por ello, que las opciones a seleccionar se mantendrían en las mínimas, reducidos clics y las respuestas serían categóricas.

De igual forma, para no saturar de información las secciones que se abrirían en cada parte del formulario, se limitaría a señalar la recomendación de revisar algunos documentos o vínculos electrónicos que brindan más información al usuario para efecto de conocer cuáles son sus obligaciones y cómo atenderlas.

Se recuerda que el objetivo principal es que los usuarios conozcan, en primer lugar, si son responsables y, en segundo, cuáles son las obligaciones básicas que deben de atender, por lo que, las preguntas y selecciones son simples.

Conclusiones

Conclusiones

La privacidad al otorgar al titular la facultad de decidir qué información de su vida privada hace pública y comparte con el resto de las personas y la protección de datos personales al otorgar la potestad al titular de decidir sobre el flujo y control de su información personal, son considerados derechos intrínsecos al ser humano

Ambos se encuentran dentro de la categoría de derechos humanos al vincularse directamente con la dignidad humana y al ser elementos necesarios para el desarrollo de la personalidad de cada individuo. Además, su reconocimiento se contempla directa o indirectamente en textos internacionales y nacionales que les brindan tal calidad.

Por ello, es que es sumamente importante que el Gobierno, las empresas y todos aquellos que puedan estar involucrados en la garantía de estos derechos, efectúen las gestiones necesarias y apliquen los mecanismos que se requieran para en todo momento salvaguardar su defensa.

Por su parte, las TIC durante las últimas décadas se han situado como instrumentos indispensables para llevar a cabo casi cualquier actividad, se han sumergido en la mayoría de los ámbitos de la sociedad y su aplicación ha generado nuevos retos o desafíos. Sin embargo, al mismo tiempo se han convertido en elementos para la disolución de conflictos.

En ese sentido, este proyecto opta por proponer una solución a un área de oportunidad localizada mediante el uso de las TIC, es decir, utilizarlas como un recurso para solventar una situación, la cual consiste en incrementar los niveles de protección de datos personales en México dentro del sector privado, al facilitar a los usuarios el conocimiento sobre cómo cumplir con la LFPDPPP.

La propuesta se sustenta jurídicamente en los documentos internacionales que dan fundamento a la privacidad y a la protección de datos personales, así como en el cuerpo jurídico mexicano que ampara la protección de datos personales como derecho fundamental y la LFPDPPP que reglamenta los alcances y límites de su garantía.

En México, la protección de datos personales se divide su regulación entre el sector público y privado, pero en este caso se enfocó el estudio para el ámbito privado. En ese tenor, se identificaron las obligaciones específicas que los responsables en términos de la LFPDPPP deben acatar, así como los documentos y guías que sirven de apoyo para atender la norma.

Asimismo, se revisaron estudios y estadísticas que mostraron que, si bien en los últimos años ha aumentado el nivel de cumplimiento del derecho de la protección de datos personales en el sector privado en México, este incremento no se encuentra en un nivel deseado con el que se garantice una eficaz y eficiente defensa del derecho.

Al respecto, para dar cuenta de la problemática que se busca solucionar mediante el uso de las TIC, se señalaron y describieron algunas de las causas por las cuales se estima el nivel de cumplimiento no ha aumentado en gran medida o que influyen en que los responsables transgredan los principios y deberes establecidos en las disposiciones normativas.

Las razones de incumplimiento aludidas consisten en: el desconocimiento de ser responsable en términos de la ley y sobre sus obligaciones en materia de protección de datos personales; el no contar con una cultura de protección de datos personales en el país; la apatía de los responsables para cumplir con las obligaciones; la no suficiente participación activa coercitiva por parte del INAI y la baja cantidad de procedimientos iniciados de parte o de oficio por la denuncia de violación de principios o deberes.

En sentido similar, se observaron cuáles son los motivos más recurrentes por los que se les ha iniciado un procedimiento de imposición de sanciones o se ha impuesto una sanción a los responsables, estos corresponden a: quebrantar los principios de la ley; omitir alguno o todos los elementos requeridos en el aviso de privacidad; obstruir actos de verificación; obtener o transferir datos personales sin el consentimiento expreso del titular y cambiar sustancialmente la finalidad originaria por la que se adquirieron los datos para el tratamiento.

Se advierte que si bien las acciones que deben realizar los responsables para atender lo que le es exigible en términos de la norma parecen ser sencillas, lo cierto

es que en los últimos años se han repetido las acciones u omisiones que transgreden las disposiciones jurídicas.

De lo anterior, se advierte un área de oportunidad y de mejora consistente en aumentar los niveles de cumplimiento de las obligaciones en materia de protección de datos personales en el sector privado y, en consecuencia, el derecho fundamental consagrado en la Constitución Política de los Estados Unidos Mexicanos, a través del uso de las TIC, esto es, por medio del establecimiento de los elementos que conformarían una plataforma digital que otorgue a los responsables los insumos e información necesaria para conocer si son responsables y cuáles son sus obligaciones, para así estar en aptitud de atenderlas.

Esta propuesta deviene del análisis que se efectuó a otras herramientas digitales de empresas privadas y de instituciones públicas, se contrastaron oros instrumentos similares de los cuales se observó tienen impactos positivos para los responsables, puesto que a través de estas se ayuda a las empresas a mejorar los procesos internos para garantizar el derecho, como también, en la creación de los documentos que les permitan alcanzar ese objetivo.

Por lo tanto, se propone la determinación de los elementos para la creación de un sitio web que oriente a las responsables del tratamiento de datos personales sobre cuáles son sus obligaciones y cómo pueden cumplirlas, es decir, que se les informe de forma sencilla y simple de la información básica para la atención de las disposiciones jurídicas.

Adicionalmente, fungiría como una herramienta educativa que de forma paralela impulsaría la cultura en materia de protección de datos personales pues cualquier persona podría utilizarla de forma gratuita y conocer si quien utiliza o recaba su información personal debe o no garantizar su derecho humano.

En tal tenor, se propone fijar los elementos para crear una página web mediante un software adaptable al presupuesto de la empresa o institución que desee utilizarlo, sus características se conformarían de elementos básicos como ventana plana, con jerarquía visual y estructura lógica en la que no se requieran más de dos clics para ingresar al formulario.

En cuanto su diseño, sería simple, con letras y colores que permitan que la información sea legible, pocas imágenes para que el peso de la misma no sobrepase los 500 KB recomendados y se configuraría de forma tal que el entorno digital se ajuste a dispositivos móviles, equipos portátiles, tabletas y computadoras de escritorio.

Referencias bibliográficas

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Bienvenida a la Agencia", *https://www.aepd.es/es/la-agencia/bienvenida-la-agencia*.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "¿En qué podemos ayudarte?", *https://www.aepd.es/es/la-agencia/en-que-podemos-ayudarte*.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Facilita 2.0", *https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDQxMjQ4NzExNjU1MTc3MjUxNzY4?updated=true*.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Facilita RGPD", *https://www.aepd.es/es/guias-y-herramientas/herramientas/facilita-rgpd#:~:text=La%20herramienta%20genera%20diversos%20documentos,un%20anexo%20con%20medidas%20de*.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Facilita 2.0. Herramienta para Tratamientos de Escaso Riesgo", *https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDQxMjQ4ODgxNjU1MTgwNDU3Mzk2*.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Guía del derecho fundamental a la protección de datos de carácter personal*, 2004, pp. 35, *https://datos.redomic.com/Archivos/GuiasUtiles/G33.pdf*.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Guías", *https://www.aepd.es/es/guias-y-herramientas/guias?combine=&sort_bef_combine=field_advertise_on_value_1%20DESC&sort_by=field_advertise_on_value_1&sort_order=DESC&page=0*.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, "Herramientas", *https://www.aepd.es/es/guias-y-herramientas/herramientas*.

ALABAMA SENATE, *Alabama Data Breach Notification Act of 2018*, Alabama, 13 de febrero de 2018, *https://legiscan.com/AL/text/SB318/2018*.

ANCINIEGA, Fernando, “Tipos de diagramas para representar sitios web”, *https://fernandoarciniega.com/tipos-de-diagramas-para-representar-sitios-web/*.

ARAYA, Manuel y CALANDRA, Pedro, *Conociendo las TIC*, Santiago, Universidad de Chile, 2009, pp. 173, *https://repositorio.uchile.cl/bitstream/handle/2250/120281/Calandra_Pedro_Conociendo_los_TIC.pdf?sequence=1*.

ASAMBLEA GENERAL DE LA ONU, Principios Rectores para la Reglamentación de los Ficheros Computarizados de Datos Personales, 14 de diciembre de 1990, *http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/OTROS%2015.pdf*.

ASAMBLEA GENERAL DE LA REPÚBLICA ORIENTAL DE URUGUAY, Ley N° 18.331 Protección de datos personales y acción de “Habeas Data”, República Oriental de Uruguay, 18 de agosto de 2008, pp. 31, *http://www.oas.org/es/sla/ddi/docs/U4%20Ley%2018.331%20de%20Protecci%C3%B3n%20de%20Datos%20Personales%20y%20Acci%C3%B3n%20de%20Habeas%20Data.pdf*.

ASOCIACIÓN MEXICANA DE INTERNET, “Estudio de Protección de Datos Personales entre Usuarios y Empresas”, México, 2012, *https://www.asociaciondeinternet.org.mx/es/component/remository/func-startdown/19/lang,es-es/?Itemid=*.

APONTE NÚÑEZ, Emercio José, “La importancia de la protección de datos de carácter personal en las relaciones comerciales. Aproximación al Derecho venezolano”, *Revisa de Derecho Privado*, Colombia, Universidad Externado de Colombia, núm. 12-13, enero-diciembre 2007, pp. 109-214, *https://www.redalyc.org/articulo.oa?id=417537588004*.

AYALA ÑIQUEN, Evelyn y GONZÁLEZ SÁNCHEZ, Santiago, *Tecnologías de la Información y la Comunicación*, Perú, Universidad Inca Garcilasco de la Vega, Fondo Editorial, 2015, pp. 76, *http://repositorio.uigv.edu.pe/bitstream/handle/20.500.11818/1189/Libro%20TIC%20%282%29-1-76%20%281%29.pdf?sequence=1&isAllowed=y*.

BIGID, “Información requerida”, *https://marketplace.bigid.com/ccrz__ProductDetails?sku=RSKTAG&cclcl=en_US*.

BIGID, “Sobre BigID”, *https://bigid.com/es/company-spanish/*.

BIGID, “Plataforma de inteligencia de datos BigID”, *https://bigid.com/data-intelligence-platform/*.

BIGID, “Productos”, *https://marketplace.bigid.com/ccrz__ProductList?categoryId=a6U4p000000D3KcEAK&cclcl=en_US*.

BIGID, “Remediación de datos que funciona para usted”, *https://bigid.com/protection/data-remediation-app/*.

BRANDEIS, Louis D. y WARREN, Samuel D., “The Right to Privacy”, *Harvard Law Review*, vol. 4, núm. 5, 15 de diciembre de 1890, pp. 193-220, *https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf*.

CÁMARA DE DIPUTADOS, Constitución Política de los Estados Unidos Mexicanos, *Diario Oficial de la Federación*, México, 5 de febrero de 1917, última reforma publicada 28 de mayo de 2021, pp. 354, párrafo segundo, *https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf*.

CÁMARA DE DIPUTADOS, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *Diario Oficial de la Federación*, México, 05 de julio de 2010, pp. 18, *http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf*.

CÁMARA DE DIPUTADOS, Ley General de Archivos, *Diario Oficial de la Federación,* México, 15 de junio de 2018, última reforma publicada 05 de abril de 2022, pp. 40, *https://www.diputados.gob.mx/LeyesBiblio/pdf/LGA.pdf*.

CÁMARA DE DIPUTADOS, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, *Diario Oficial de la Federación*, Ciudad de México, 26 de enero de 2017, pp. 52, *https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf*.

CÁMARA DE DIPUTADOS, Ley General de Transparencia y Acceso a la Información Pública, *Diario Oficial de la Federación*, México, 04 de mayo de 2015, última reforma publicada 20 de mayo de 2021, pp. 70, *https://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP_200521.pdf*.

CARREÓN GALLEGOS, Ramón Gil, “Derechos humanos, garantías individuales y derechos fundamentales. Problema terminológico o conceptual”, Universidad Autónoma de Coahuila, Poder Judicial del Estado de Coahuila, Comisión de los Derechos Humanos del Estado de Coahuila, Editora Laguna, S.A. de C.V., 2012, pp. 133-134, *https://archivos.juridicas.unam.mx/www/bjv/libros/7/3171/7.pdf*.

CENTRO DE INVESTIGACIÓN Y DOCENCIA ECONÓMICAS A.C., *Lineamientos de Protección de Datos en el Cómputo en la Nube: Parámetros para su elaboración*, México, 2014, pp. 76, *https://cidecyd.files.wordpress.com/2014/09/white-paper-lineamientos-proteccion-datos-computo-nube-mx-18-sept-14-def.pdf*.

CERDA SILVA, Alberto, “Mecanismos de control en la protección de datos en Europa”, *Ius et Praxis*, Chile, Universidad de Talca, vol. 12, núm. 2, 2006, pp. 221-251, *https://www.redalyc.org/pdf/197/19712209.pdf*.

COBO ROMANÍ, Juan Cristóbal, “El concepto de tecnologías de información. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento”, *ZER: Revista de Estudios de Comunicación = Komunikazio Ikasketen Aldizkaria*, vol. 14, núm. 27, pp. 295-318, *https://ojs.ehu.eus/index.php/Zer/article/view/2636*.

COMITÉ JURÍDICO INTERAMERICANO, *Guía Legislativa sobre la privacidad y la protección de datos personales en las Américas*, 2015, *https://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_Guia_Legilsativa_CJI.pdf*.

CONFEDERACIÓN PATRONAL DE LA REPÚBLICA MEXICANA E INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Convenio General de Colaboración*, pp. 11, *https://home.inai.org.mx/wp-content/documentos/Convenios/OA-09-2015%20Confederaci%C3%B3n%20Patronal%20de%20la%20Republica%20Mexicana%20COPARMEX.pdf*.

CONGRESO DE LA NACIÓN ARGENTINA, *Ley 25.326*, Argentina, 2000, *https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto*.

CONSEJO EUROPEO, *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, Estrasburgo, 20 de enero de 1981, pp. 34, *http://www.oas.org/es/sla/ddi/docs/u12%20convenio%20n%20108.pdf*.

CONSEJO DE EUROPA, *Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, Luxemburgo, 24 de octubre de 1995, *https://www.boe.es/doue/1995/281/L00031-00050.pdf*.

CONSEJO DE EUROPA, *Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE*, Estrasburgo, 15 de marzo de 2006, *https://www.boe.es/doue/2006/105/L00054-00063.pdf*.

CONSEJO EUROPEO, *Protocolo adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos*, Estrasburgo, 08 de noviembre de 2001, pp. 34, *http://www.oas.org/es/sla/ddi/docs/u12%20convenio%20n%20108.pdf*.

CONSEJO DE EUROPA, *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 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 y por el que se deroga la Directiva 95/46/CE*, Bruselas, 27 de abril de 2016, *https://www.boe.es/doue/2016/119/L00001-00088.pdf*.

DAVARA, Isabel, CERVANTES, Padilla, *et. al.*, “Protección de datos personales”, en Davara, Isabel (coord.), *Diccionario de Protección de Datos Personales Conceptos fundamentales*, México, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, primera edición, noviembre de 2019, pp. 898, *https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf*.

DEPARTMENT OF JUSTICE, *Privacy Act of 1974*, pp. 53-66, *https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf*.

DIRECCIÓN GENERAL DE CAPACITACIÓN, *INAI/SE/DGC/039/22*, INAI, 17 de febrero de 2022, *https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=330031322000232&coleccion=5*.

DIRECCIÓN GENERAL DE INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PRIVADO, *Oficio: INAI/SPDP/DGIVSP/0290/22*, INAI, Ciudad de México, 2022, *https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=330031322000179&coleccion=2*.

DIRECCIÓN GENERAL DE INVESTIGACIÓN Y VERIFICACIÓN DEL SECTOR PRIVADO, *Oficio: INAI/SPDP/DGIVSP/1398/22*, INAI, Ciudad de México, 2022, *https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=330031322000755&coleccion=5*.

DIRECCIÓN GENERAL DE PREVENCIÓN Y AUTORREGULACIÓN, *OFICIO No. INAI/SPDP/DGPA/066/2022*, INAI, Ciudad de México, 2022, *https://buscador.plataformadetransparencia.org.mx/web/guest/buscadornacional?buscador=330031322000754&coleccion=5*.

ECHAVARRÍA, Stephania y ROCHA Jenny, “Importancia de las T.I.C.s en el ambiente empresarial”, Bogotá, Universidad de La Salle, 2017, pp. 20, *https://ciencia.lasalle.edu.co/cgi/viewcontent.cgi?article=2482&context=administracion_de_empresas*.

FERNÁNDEZ, Anayda y RIVERO, Miguel, “Las plataformas de aprendizajes, una alternativa a tener en cuenta en el proceso de enseñanza aprendizaje”, *Revista Cubana de Informática Médica*, Ciudad de la Habana, vol. 6, núm. 2, jul-dic 2014, *http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1684-18592014000200009#:~:text=Una%20plataforma%20virtual%20no%20es,participantes%20en%20un%20proceso%20pedag%C3%B3gico.*

FLORES SALGADO, Lucerito Ludmila, *Temas actuales de los derechos humanos de última generación*, Puebla, México, Benemérita Universidad Autónoma de Puebla, 2015, pp. 171, *https://archivos.juridicas.unam.mx/www/bjv/libros/9/4304/13.pdf*.

GARCÍA GONZÁLEZ, Aristeo, “Hacia una cultura en materia de protección de datos personales”, *Hechos y Derechos*, núm. 14, *https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/6816/8752*.

GOOGLE, “Prácticas recomendadas para la indexación "dispositivos móviles primero”, *https://developers.google.com/search/mobile-sites/mobile-first-indexing*.

GONZÁLEZ, Guadalupe, “Legado tecnológico de la Segunda Guerra Mundial”, *Prisma Tecnológico*, Universidad Tecnológica de Panamá, Editorial Tecnología, vol. 9, núm. 1, diciembre 2018, pp. 46, *https://revistas.utp.ac.pa/index.php/prisma/article/view/2067/pdf*.

HIDALGO RIOJA, Ileana, *Derecho a la protección de datos personales*, México, Instituto Nacional de Estudios Históricos de las Revoluciones de México, Instituto de Investigaciones Jurídicas, pp. 56, *https://inehrm.gob.mx/recursos/Libros/DerProtectDatos.pdf*.

IBM, “Esquemas de página”, 09 marzo 2021, *https://www.ibm.com/docs/es/elm/6.0.4?topic=requirements-wireframes*.

INFORMATICA, “Data Privacy for Dummies”, *informatica.com/mx/lp/data-privacy-for-dummies_3600.html?formid=9270&programName=20Q1-M-DPDS-ESO-DGP-NS-NP-NI-IF-EBK-DataPrivacyDummiesMexico-0-PT3600-D&&_bt=580497307819&_bk=privacidad%20de%20datos&_bm=p&_bn=g&_bg=134235174858&gclid=EAIaIQobChMI_e3Ds_mc-AIVlhPUAR2HRwnSEAMYASAAEgJdd_D_BwE&gclsrc=aw.ds*.

INFORMATICA, “Integración de datos”, *https://usw5.dm-us.informaticacloud.com/diUI/products/integrationDesign/main/MyOieJobs*.

INFORMATICA, “Prueba de Cloud”, *https://www.informatica.com/mx/trials/informatica-cloud.html*.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, “Corpus Iuris en materia de Protección de Datos Personales. Documentos Internacionales”, *http://corpusiurispdp.inai.org.mx/Pages/Inicio.aspx*.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, “Corpus Iuris Internacional y Nacional”, *http://corpusiurispdp.inai.org.mx/Pages/home.aspx*.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *El ABC del Aviso de Privacidad*, *http://abcavisosprivacidad.ifai.org.mx/#seccion1_02P*.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Evaluador de Vulneraciones. Manual de Usuario*, pp. 22, *http://inicio.inai.org.mx/EvaluadorVulneracionesDocs/Manual%20de%20Usuario.pdf*.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, “Generador de Avisos de Privacidad. Sector Privado”, *https://generador-avisos-privacidad.inai.org.mx/policies/myAdd?v=1*.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Guía para la elaboración del Aviso de Privacidad en el área de recursos humanos*, Ciudad de México, mayo 2022, 1a. ed., pp. 47, *https://home.inai.org.mx/wp-content/uploads/GuiaElaboracion_AvisoPrivacidad_Area_RH.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*, junio de 2016, pp. 91, *https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Guia_obligaciones_lfpdppp_junio2016.pdf*.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Informe de labores 2016*, México, enero de 2017, pp. 419, *https://micrositios.inai.org.mx/informesinai/?page_id=425*.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Informe de labores 2017*, México, diciembre 2017, pp. 374, *https://micrositios.inai.org.mx/informesinai/?page_id=385*.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Informe de labores 2018*, México, diciembre 2018, pp. 476, *https://micrositios.inai.org.mx/informesinai/?page_id=372*.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Informe de labores 2019*, México, diciembre 2019, pp. 385, *https://micrositios.inai.org.mx/informesinai/?page_id=15*.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, *Informe de labores 2020*, México, diciembre 2020, pp. 178, *https://micrositios.inai.org.mx/informesinai/?page_id=519*.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, "Qué es el INAI", *https://home.inai.org.mx/?page_id=1626*.

INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA, *Encuesta Nacional de Acceso a la Información Pública y Protección de datos Personales*, 2016, *https://www.inegi.org.mx/contenidos/programas/enaid/2016/doc/ENAID_2016_Principales_resultados.pdf*.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, "Registro Esquemas de Autorregulación Vinculante. Sector Privado", *https://registro-esquemas.inai.org.mx/?page_id=177&a=2&b=2*.

INSTITUTO NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN Y PROTECCIÓN DE DATOS PERSONALES, "Vulnerómetro", *https://micrositios.inai.org.mx/vulnerometro/resultados.php*.

INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA, *Comunicado de Prensa núm. 790/21*, diciembre de 2021, *https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/EDN/EDN_2021.pdf*.

INSTITUTO NACIONAL DE ESTADÍSTICA Y GEOGRAFÍA, *Encuesta Nacional de Acceso a la Información Pública y Protección de datos Personales*, 2019, pp. 95, *https://www.inegi.org.mx/contenidos/programas/enaid/2019/doc/enaid_2019_principales_resultados.pdf*.

KUBLI-GARCÍA, Fausto, "Componentes del derecho a la privacidad", *Revista del Posgrado en Derecho de la UNAM*, nueva época, año 4, núm. 7, julio-diciembre 2017, pp. 25,-49 *http://revistaderecho.posgrado.unam.mx/index.php/rpd/article/view/109/118*.

LEFRANC WEEGAN, Federico, *Holocausto y Dignidad Significado y fin de la invocación a la dignidad humana en el Preámbulo de la Declaración Universal de Derechos Humanos*, México, UBIJUS Editorial pp. 255, *http://movaprinting.com/HOLOCAUSTO_Y_DIGNIDAD.pdf*.

LOUISIANA SENATE, *Act. No. 382*, Louisiana, 2018, *https://www.legis.la.gov/legis/ViewDocument.aspx?d=1101149*.

MAGALLANES MARTÍNEZ, Víctor Hugo, “Derecho a la protección de datos personales. Su diseño constitucional”, *Estudios en Derecho a la Informática*, núm. 2, julio-diciembre 2016, pp. 25-45, c*https://revistas.juridicas.unam.mx/index.php/derecho-informacion/article/view/10486/12651*.

MÁRQUEZ PIÑERO, Rafel, *Cuadernos Constitucionales México-Centroamérica 13. El sistema jurídico de los Estados Unidos de América*, México, Universidad Nacional Autónoma de México, Corte de Constitucionalidad de Guatemala, 1994, pp. 57, *https://archivos.juridicas.unam.mx/www/bjv/libros/1/206/1.pdf*.

MENDOZA ERÍQUEZ, Olivia, “Privacidad”, en Davara, Isabel (coord.), *Diccionario de Protección de Datos Personales Conceptos fundamentales*, México, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, primera edición, noviembre de 2019, pp. 898, *https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf*.

MENDOZA ENRÍQUEZ, Olivia Andrea, “Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento”, *Revista IUS*. 2018, vol. 12, núm. 41, Puebla, enero-junio, pp. 267-291, *http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472018000100267*.

MIRO, “Plantilla de diagrama de flujo para un sitio web”, *https://miro.com/es/plantillas/diagrama-flujo-para-sitio-web/*.

NACIONES UNIDAS, *Principios Rectores sobre las Empresas y los Derechos Humanos*, Nueva York y Ginebra, 2011, pp. 43, *https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_sp.pdf*.

ORGANIZACIÓN DE LAS NACIONES UNIDAS, *Declaración Universal de Derechos Humanos*, 10 de diciembre 1948, *https://www.humanium.org/es/ddhh-texto-completo/*.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, *Convención Americana sobre Derechos Humanos*, San José, Costa Rica, pp. 30, *https://www.cndh.org.mx/sites/default/files/doc/Programas/TrataPersonas/MarcoNormativoTrata/InsInternacionales/Regionales/Convencion_ADH.pdf*.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, "Ley Modelo Interamericana sobre Protección de Datos Personales (en elaboración)", *https://www.oas.org/es/sla/ddi/proteccion_datos_personales_ley_modelo.asp*.

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS, *Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*, París, 2002, *https://www.oecd.org/sti/ieconomy/15590267.pdf*.

PESCHARD, Jacqueline, "Cien años del derecho a la privacidad en la Constitución", *Cien ensayos para el centenario*, Instituto de Investigaciones Jurídicas, tomo 2, núm. 786, México, 2017, pp. 539, *https://archivos.juridicas.unam.mx/www/bjv/libros/9/4319/23.pdf*.

PRESIDENCIA DE LA REPÚBLICA, *Decreto N° 414/2009*, Uruguay, 15 de septiembre de 2009, *https://www.impo.com.uy/bases/decretos/414-2009#:~:text=El%20derecho%20a%20la%20protecci%C3%B3n%20de%20los%20datos%20personales%20se,tipo%20que%20refiera%20a%20ellas.*

RITCHER, Marcelo, "La protección de datos de carácter personal como derecho humano", *Revista Auctoritas Prudentium*, Guatemala, año VII, núm. 12, primer semestre del 2015, pp. 18-29, *https://dialnet.unirioja.es/servlet/articulo?codigo=5002034*.

SADURNÍ, J.M., "Virginia Hall, la espía más peligrosa de los aliados", 21 agosto de 2020, *https://historia.nationalgeographic.com.es/a/virginia-hall-espia-mas-peligrosa-aliados_15606*.

SALDAÑA DÍAZ, María Nieves, "El derecho a la privacidad en los Estados Unidos aproximación diacrónica a los intereses constitucionales en juego", *Teoría y realidad constitucional*, núm. 28, 2011, pp. 704, *https://dialnet.unirioja.es/servlet/articulo?codigo=3883001*.

SALDAÑA, María Nieves, “The Right to Privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis”, *UNED. Revista de Derecho Político*, núm. 85, septiembre-diciembre 2012, pp. 195-240, *http://revistas.uned.es/index.php/derechopolitico/article/view/10723/10242*.

SÁNCHEZ RAMÍREZ, María Cristina, “La protección y el tratamiento de datos personales. El derecho humano a la privacidad y a la intimidad”, *Mirada Legislativa*, Ciudad de México, núm. 201, abril 2021, *http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/5234/ML%20201.pdf?sequence=1&isAllowed=y*.

SÁNCHEZ ROJO, Alberto, “El derecho humano a la privacidad desde el enfoque de las capacidades: una reflexión educativa”, *EDETANIA*, Madrid, España, julio 2017, pp. 158-170, *https://riucv.ucv.es/bitstream/handle/20.500.12466/574/113-Texto%20del%20art%c3%adculo-306-1-10-20171109.pdf?sequence=1&isAllowed=y*.

SEALPATH, “Automatización de la protección”, *https://www.sealpath.com/es/automatizacion-proteccion/*.

SEALPATH, “Contacta con SealPath”, *https://www.sealpath.com/es/contactar/*.

SEALPATH, “Seguridad de Datos Inteligente”, *https://www.sealpath.com/es/sobre-nosotros/*.

SECRETARÍA DE ECONOMÍA, *Lineamientos del Aviso de Privacidad*, México, D.F., 17 enero de 2013, *https://www.dof.gob.mx/nota_detalle.php?codigo=5284966&fecha=17/01/2013#gsc.tab=0*.

SILVA GARCÍA, Fernando, *Jurisprudencia Interamericana sobre derechos Humanos Criterios esenciales*, México, 2011, pp. 389, *https://www.corteidh.or.cr/tablas/r28946.pdf*.

SISTEMA NACIONAL DE TRANSPARENCIA, ACCESO A LA INFORMACIÓN PÚBLICA Y PROTECCIÓN DE DATOS PERSONALES, “¿Qué es el Sistema Nacional de Transparencia?”, *https://snt.org.mx/?page_id=431*.

STATE OF CALIFORNIA DEPARTMENT OF JUSTICE, *California Consumer Privacy Act (CCPA)*, California, *https://oag.ca.gov/privacy/ccpa*.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Tesis 1a. CCXIV/2009, *Semanario Judicial de la Federación y su Gaceta, Novena Época*, diciembre 2009, p. 277, *https://sjf2.scjn.gob.mx/detalle/tesis/165823*.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Tesis 1a. XLIII/2010, *Semanario Judicial de la Federación y su Gaceta*, Novena época, t. XXXI, marzo de 2010, p. 928, *https://sjf2.scjn.gob.mx/detalle/tesis/164992*.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Tesis 1a. CCXV/2013 (10a.), *Seminario Judicial de la Federación y su Gaceta*, Décima época, t. I, julio de 2013, p. 557, *https://sjf2.scjn.gob.mx/detalle/tesis/2003975*.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Tesis 2a./J.31/2020 (10a.), *Seminario Judicial de la Federación*, Décima Época, octubre de 2020, *https://sjf.scjn.gob.mx/SJFSem/Paginas/DetalleGeneralV2.aspx?ID=2022203&Clase=DetalleTesisBL*.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Tesis I.10o.A.6 CS (10a*.), Gaceta del Semanario Judicial de la Federación*, Décima época, t. III, septiembre de 2019, p. 2200, *https://sjf2.scjn.gob.mx/detalle/tesis/2020564*.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Tesis I.4o.A.9 K (10a.), *Semanario Judicial de la Federación y su Gaceta*, Décima época, t. III, abril de 2013, p. 2254, *https://sjf2.scjn.gob.mx/detalle/tesis/2003350*.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Tesis I.4o.A.70 K, *Semanario Judicial de la Federación y su Gaceta*, Novena época, t. XXIV, agosto 2006, p. 2346, *https://sjf2.scjn.gob.mx/detalle/tesis/174338*.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Tesis P./J. 20/2014 (10a.), *Seminario Judicial de la Federación*, 25 de abril de 2014, *https://sjf.scjn.gob.mx/SJFSem/Paginas/Reportes/ReporteDE.aspx?idius=2006224&Tipo=1*.

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN, Tesis P./J. 21/2014 (10a.), *Seminario Judicial de la Federación,* 25 de abril de 2014, *https://sjf.scjn.gob.mx/SJFSem/Paginas/Reportes/ReporteDE.aspx?idius=2006225&Tipo=1*.

SKERIGES RIKSDAG, *Datalag (1973:289)*, Justitiedepartementet L6, 1973, *https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/datalag-1973289_sfs-1973-289*.

TELLO LEAL, Edgar, "Las tecnologías de la información y comunicaciones (TIC) y la brecha digital", *Revista de Universidad y Sociedad del Conocimiento*, vol. 4, núm. 2, 2007, pp. 8, *https://rusc.uoc.edu/rusc/es/index.php/rusc/article/download/v4n2-tello/305-1221-2-PB.pdf*.

TENORIO ADAME, Manuel, "La protección de datos personales desde el derecho al acceso al a información y como derecho fundamental autónomo, el caso mexicano", *Revista Internacional de Protección de Datos Personales*, Colombia, núm. 1, julio-diciembre de 2012, pp. 12, *https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/5_-Manuel-Tenorio_FINAL.pdf*.

TRIBUNAL CONSTITUCIONAL DE ESPAÑA, *Sentencia 292/200*, Madrid, 30 de noviembre 2000, *http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276*.

TORRES LLANTÉN, Edgar, "La Protección de datos personales en Europa y en Colombia similitudes y diferencias", pp. 8, *https://repository.usc.edu.co/bitstream/handle/20.500.12421/2937/LA%20PROTECCION%20DE%20DATOS.pdf?sequence=1&isAllowed=y*.

UNIÓN EUROPEA, *Reglamento general de protección de datos*, 26 de marzo de 2021, *https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_es.htm*.