UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

FACULTAD DE DERECHO

“Origen, retos y prospectiva del Derecho a la Protección de Datos Personales a 20 años de su constitucionalización”

TRABAJO TERMINAL DE GRADO

QUE PARA OBTENER EL GRADO DE MAESTRO EN DERECHO PARLAMENTARIOPRESENTA EL:

Lic. en D. Iván Aureliano Peña Zarco

DIRECTOR

DR. FÉLIX DÓTTOR GALLARDO

CO-DIRECTORA
DRA. ANGÉLICA GARCÍA MARBELLA

TUTOR ADJUNTO
DR. HIRAM RAÚL PIÑA LIBIEN

CIUDAD UNIVERSITARIA, TOLUCA DE LERDO NOVIEMBRE DE 2024

DEDICATORIAS

INDICE

RESUMEN

El trabajo titulado “Origen, retos y prospectiva del Derecho a la Protección de Datos Personales a 20 años de su constitucionalización” se centra en analizar la efectividad de las acciones gubernamentales en México para proteger el derecho a la protección de datos personales. Este derecho, consagrado en la Constitución mexicana hace dos décadas, cobra relevancia en la era digital, donde el flujo de información y la capacidad para recopilar y procesar datos personales han crecido exponencialmente.

La investigación revisa la historia del derecho a la protección de datos personales en México y el marco normativo desarrollado para regularlo, en especial a través de derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). También se comparan los avances y desafíos de México frente a otros países, especialmente en Europa, donde existe una normativa más consolidada, como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea.

El autor plantea que, a pesar de los avances legislativos y las reformas constitucionales, las acciones del gobierno mexicano aún enfrentan desafíos significativos en cuanto a la implementación y efectividad. Entre los objetivos, se busca proponer mejoras para fortalecer el marco jurídico y las estrategias institucionales, alineándolas con estándares internacionales para garantizar una protección efectiva de los datos personales en beneficio de la población mexicana.

Metodológicamente, se emplean análisis documental y cuestionarios aplicados a sujetos obligados en materia de protección de datos. La investigación combina enfoques cualitativos y cuantitativos y explora teorías sobre derechos humanos y privacidad. Finalmente, el estudio sugiere que aún se requieren mejoras en los mecanismos estatales y las políticas públicas para responder adecuadamente a los avances tecnológicos y las demandas de privacidad de los ciudadanos.

INTRODUCCIÓN

El presente trabajo de investigación tiene como propósito analizar la eficacia de las acciones gubernamentales implementadas para el reconocimiento, ejercicio, salvaguarda y restitución del derecho fundamental a la protección de datos personales en México, a veinte años de su consagración en la Constitución Política de los Estados Unidos Mexicanos.

En la era digital actual, la protección de los datos personales se ha convertido en una necesidad imperiosa, dado el vertiginoso incremento en el flujo de información y la capacidad de recopilar, almacenar y procesar dichos datos. Este derecho humano busca equilibrar la dinámica entre el acelerado avance tecnológico, el acceso a la información pública y la transparencia gubernamental, manteniendo a la vez la privacidad e intimidad de los individuos como pilares fundamentales.

Por medio de un análisis documental exhaustivo y la aplicación de un cuestionario a diversos sujetos obligados en materia de protección de datos personales, este estudio pretende identificar tanto los logros alcanzados, como los retos y áreas de oportunidad en la implementación de políticas y acciones gubernamentales encaminadas a garantizar el ejercicio efectivo de este derecho en el contexto nacional. Asimismo, se revisarán los antecedentes internacionales y la evolución normativa a nivel federal y local, con el fin de comprender el marco de referencia en el que se desarrolla la protección de datos personales en nuestro país.

El objetivo final de esta investigación es presentar una propuesta de mejora que permita fortalecer el marco jurídico y las estrategias institucionales, a fin de garantizar de manera más efectiva y acorde a los estándares internacionales el derecho a la protección de datos personales, en beneficio de todos los habitantes del territorio nacional.

Para ello, el presente estudio se encuentra organizado de la siguiente manera:

CAPÍTULO PRIMERO. Historia de la protección de datos personales; en este apartado se analizarán los antecedentes históricos del derecho a la protección de datos personales, abordando su desarrollo a nivel internacional, nacional, y específicamente en el Estado de México.

CAPÍTULO SEGUNDO. El derecho humano a la protección de datos personales, en este capítulo se centra en el contenido teórico y conceptual, explicando los conceptos fundamentales necesarios para comprender el ámbito de los datos personales, además de abordar la Teoría de los Derechos Humanos y la Teoría del Garantismo.

CAPÍTULO TERCERO. Regulación de la protección de datos personales desde la perspectiva jurídica y comparada, aquí se presenta un análisis jurídico y comparado de la regulación en materia de protección de datos personales, comparando los ordenamientos jurídicos de Europa y México.

CAPÍTULO CUARTO. Eficacia de las acciones gubernamentales en la protección de datos personales, en este en este apartado se evaluará la hipótesis de la investigación para determinar la efectividad de las acciones gubernamentales, marcos normativos y mecanismos en la protección de datos personales y en el ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

PROTOCOLO DE TRABAJO TERMINAL DE GRADO
UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO
FACULTAD DE DERECHO

Toluca, México a 27 de marzo del 2023. IV

COORDINADORA DE ESTUDIOS AVANZADOS
DE LA FACULTAD DE DERECHO
P R E S E N T E

Título: "Origen, retos y prospectiva del Derecho a la Protección de Datos Personales a 20 años de su Constitucionalización".

Modalidad: Trabajo terminal de grado.

Área de evaluación: Cuerpo Académico: Estudios Gubernamentales

Línea de Generación y aplicación del conocimiento: La función gubernamental.

Palabras Clave: Protección, datos personales, derechos humanos, derecho a la Intimidad, reforma constitucional, promoción y/o difusión, obligatoriedad.

Antecedentes (Estado de conocimiento)

Los datos personales, son la información que progresivamente ha cobrado gran relevancia social y económica. (Remolina Angarita, 210), ello debido a que en los últimos años los datos personales se han convertido en moneda de cambio ante instituciones de carácter público y privado, ya que forman parte de sistemas de datos personales y son insumos de información.

En 1980, debido al rápido desarrollo tecnológico y económico, surgieron las directrices de la OCDE, de las cuales emanan principios como la transparencia, la limitación de

recopilación, la calidad de los datos, la especificación de propósito, la limitación de uso, la salvaguarda de la seguridad, la participación individual y la responsabilidad.

Inicialmente, en la Declaración Universal de los Derechos Humanos, en el Pacto Internacional de Derechos Civiles y Políticos, en el Convenio para la Protección de los Derechos y Libertades Fundamentales y en la Convención Americana sobre Derechos Humanos se reconoce el derecho al respeto de la vida privada y familiar, así como de la honra y la dignidad personal, estableciendo la prohibición de injerencias arbitrarias por parte de la autoridad pública y velando por la protección de los datos personales, aun de manera implícita.

Pero es hasta el año 2000 que, en la Carta de los Derechos Fundamentales de la Unión Europea, se reconoce expresamente el derecho de toda persona al respeto de su vida privada y familiar, de su domicilio y comunicaciones, además del derecho de protección de los datos personales que le conciernen, según los principios difundidos por las Directrices de la OCDE.

A partir del año 2002 y con la expedición de la Ley Federal de Transparencia, se incorporó el derecho a la protección de datos personales como límite o contrapeso al derecho de acceso a la información en la transparencia, con algunas escuetas menciones a lo largo del articulado.

Así, esta reforma incluyó la protección constitucional de la privacidad. Una reforma posterior, fechada en 2009, modificó el artículo 16 de la Constitución Federal para dar carta de existencia a los derechos de acceso, rectificación, cancelación y oposición de los datos personales (ARCO), que son prerrogativas de los particulares respecto del manejo de los datos personales por parte del Estado y otras instituciones.

En nuestra entidad, mediante el decreto 44, publicado el 30 de abril de 2004 en el Periódico Oficial “Gaceta del Gobierno”, se reformó el artículo 5º de la Constitución

estatal, para adicionarle dos párrafos ligados con el reconocimiento y garantía de los derechos de acceso a la información pública y protección de los datos personales.

Por lo tanto, el 1º de mayo de 2004, entró en vigor la Ley de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, con la cual esta entidad fue una de las primeras en sumarse al esfuerzo de asegurar y promover el ejercicio de ambas prerrogativas.

Este ordenamiento jurídico se reformó, posteriormente, el 28 de diciembre de 2004 y en 2006, 2007, 2008, 2011 y 2012. En consecuencia, el organismo garante estatal fue revestido de autonomía constitucional aun antes que el organismo garante federal, lo cual contribuyó a que, en el Estado de México, los procedimientos de acceso a la información pública y protección de los datos personales se consolidaran de modo gradual.

Asimismo, el 13 de agosto de 2012, la Legislatura local aprobó la Ley de Protección de Datos Personales del Estado de México, a fin de separar esta materia de la propia transparencia.

Con dicha acción, la entidad mexiquense se convirtió en uno de los primeros estados de los 11 que habrían de aprobar sus respectivas legislaciones antes de la LGPDPPSO. En distinto sentido, el 8 de junio de 2015, en el Periódico Oficial “Gaceta del Gobierno”, se publicó el decreto 437, mediante el cual se reformó el artículo 5º, párrafos décimo sexto y décimo séptimo de la Constitución estatal.

Por otra parte, en lo que respecta a investigaciones referentes a la protección de datos personales se identificó la siguiente tesis para obtener el título de licenciado en derecho denominada: ***“Estudio comparado de las regulaciones jurídicas sobre la protección de datos personales de España y México” de Oscar, Suárez Rueda***” y en este trabajo se investigación se realizó un estudio comparado de legislaciones de protección de datos personales entre México y España, así como de las instituciones

gubernamentales facultadas para proteger a los titulares de la información. El estudio comparado contempla su enfoque señalando sus puntos más importantes en los siguientes parámetros: 1. Selección de un sistema jurídico 2. Sujeto materia de comparación 3. Delimitación del nivel de comparación 4. Identificación de similitudes y diferencias El presente estudio permitió señalar que en México existen algunas fallas del sistema jurídico cuyo objetivo es proteger la información personal y a sus titulares, por ello se necesita contemplar algunos puntos establecidos por la legislación de España, con el fin de proteger la intimidad de las personas al realizar un tratamiento de datos personales.

En este sentido, también se encontró el artículo publicado en la revista Universita Ciencia, denominado: ***"El derecho fundamental a la protección de datos personales de las personas con calidad de servidores públicos" de Hugo Edgar Chaparro Campos";*** aquí el autor expuso un estudio de caso en que se analizó el marco jurídico nacional e internacional del derecho al acceso a la información pública, en torno a la protección de la dignidad humana pretendiendo proponer la protección de datos personales de servidores públicos en calidad de sujetos obligados con el objeto de evitar su posible vulneración.

Asimismo, de la investigación de temas relacionados con la protección de datos personales, se encontró la tesis para obtener el título de licenciado en Ciencias Políticas y Administración Pública identificado con el título: ***"Protección de datos personales en redes sociales digitales" de Edgar Guijosa Delgado;*** en este trabajo de investigación aborda la privacidad y la protección datos personales en el ciberespacio, en específico las redes sociales digitales. La forma de uso de estas plataformas tecnológicas puede generar riesgos para la privacidad y los datos personales de los usuarios, se reflexiona sobre posibles mecanismos de protección y autorregulación de la información personal en la red social digital de mayor alcance en el mundo, Facebook. Este trabajo busca entender qué son las redes sociales digitales, qué alcance tienen en el país, qué usos se les pueden dar, qué tipo de información se sube y comparte, así como observar los posibles riesgos a la privacidad, a fin de

encontrar mecanismos de protección de datos, pero partiendo del hecho de que en el ciberespacio y las redes sociales no se puede ni debe regular el comportamiento e interacciones de los usuarios, quienes son personas en el mundo real, poseedoras de una personalidad y derechos.

En este tenor, también se encontró y se analizó la tesis para obtener el título de licenciado en Informática Administrativa bajo el título ***"La seguridad informática en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares" de Alma Irais Barreiro Neyra;*** en dicho trabajo de investigación se analizó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, para garantizar la implementación y el cumplimiento de la misma, así como investigar la función de la seguridad de la información de los particulares mediante la consideración de la importancia que se debe dar a la información privada de terceros, no solo para el cumplimiento satisfactorio de la Ley, sino porque la inseguridad aumenta día con día y si se da un uso inadecuado a la información que voluntariamente se confía a un empresa se pone en riesgo la integridad de las personas.

Por último y después de hacer una análisis a la literatura, podemos concluir que es necesaria la debida salvaguarda, ejercicio y protección de datos personales, toda vez que es un derecho humano esencial que da sustento a la dignidad humana, y que la vida privada únicamente le concierte a la persona y que debe respetarse y limitarse por los demás, tal como lo refiere los artículos 14 y 16, los cuales en sustancia refieren que ninguna persona puede ser molestado en su persona, siendo, la consecuencia de la individualidad, de la autonomía y de la libertas que se admite como propias de todo ser humano, siempre y cuando no afecte derecho o esferas de otra persona.

Originalidad y relevancia

El presente trabajo es una investigación original pues si bien aborda el tema de la protección de datos personales en México, también lo es que su enfoque no coincide

con el de otras investigaciones, como las mencionadas en el apartado de antecedentes.

Como se puede observar después de realizar una revisión a la literatura descrita en el apartado de antecedentes, no se encontraron coincidencias con el trabajo de estudio que se pretende desarrollar, el objeto es distinto, en esta investigación se analizaran entre otras cosas, cuáles han sido los alcances jurídicos de la protección de datos personales en México y hasta qué punto las acciones gubernamentales han sido suficientes para garantizar su protección y reconocimiento.

En este sentido estimamos que la investigación propuesta reviste gran relevancia al ser un tema actual y frecuente en la práctica jurídica, por lo que es de transcendencia indagar y exponer lo que ha pasado con los alcances de las reformas constitucionales en materia de protección de datos personales, para analizar los resultados de las estrategias, mecanismos y políticas públicas que ha implementado el Estado en su actuar gubernamental, ya que no basta únicamente con publicar y difundir la cultura de la protección de datos personales, sino que se tiene que analizar la operación de la función gubernamental para que se reconozca, ejerza y se respete el derecho a protección de datos personales de forma plena.

Planteamiento del problema.

Si bien es cierto que en el año 2002 se creó la Ley de Protección de Datos Personales, también es cierto que ésta se creó por la necesidad que tenía en ese momento el Estado Mexicano, de seguir perteneciendo a la Red Iberoamericana de Protección de Datos Personales, sin embargo la generación de esta ley no fue por una necesidad de los gobernados, sino más bien por una revolución global de que ya se venía trabajando en interior de Europea.

Entonces tenemos que como no fue una necesidad de los gobernados, sino más bien fue realizada como un requisito para seguir perteneciendo a la Red Iberoamericana de

Protección de Datos Personales, fue como se creó esta ley, sin embargo, durante el proceso de esta investigación se analizará si los mecanismos utilizados hasta el momento por parte de las autoridades competentes para salvaguardar este derecho humano han sido eficaces para el reconocimiento, salvaguarda y protección de los datos personales.

En esencia, el planteamiento del problema consiste en establecer si las normas y mecanismos implementados a la luz de las reformas constitucionales en materia de protección de datos personales son eficaces para consagrar y salvaguardar de forma completa el derecho a la protección de datos personales.

Preguntas de investigación

- ¿Son eficaces las acciones gubernamentales para el reconocimiento, ejercicio, salvaguarda y restitución del Derecho a la Protección de Datos Personales desde su institucionalización Constitucional?

Justificación del problema

El proporcionar información de acceso público en muchas ocasiones puede colisionar con el derecho de protección a datos personales y ello implicaría que el entregarla podría poner en evidencia información que pudiera afectar la esfera más íntima de una persona lo que es objeto de la protección de datos personales y la vida privada, que si bien es cierto que hay servidores públicos que deben transparentar sus actos y sus actividades, también es cierto que son personas y que se debe respetar sus datos personales, tal y como lo refieren los artículo 6 y 16 párrafo segundo de nuestra máxima carta magna, el cual refiere que se debe respetar la vida privada y que toda persona tiene derecho a la salvaguarda y protección de sus datos personales, así como al Acceso, Rectificación, Cancelación y Oposición(ARCO).

Delimitación del problema

1. Delimitación temporal.- **2002-2023**
2. Delimitación espacial.- **Nacional**
3. Delimitación Humana.- **Derechos humanos (protección de datos personales)**

Orientación Teórico Metodológica

En la presente investigación, se realizará una orientación teórico-metodológica, en donde se aplicarán los diversos métodos de investigación.

En este orden de ideas, para la presente investigación se tomará en cuenta el enfoque de la investigación mixta, es decir, cualitativa y cuantitativa.

En este sentido, utilizaremos el enfoque cuantitativo y cualitativo, porque se consideran necesarios para el desarrollo de nuestros objetivos, como ejemplo para:

1. Consultar el marco jurídico de la protección de datos personales.
2. Conocer las teorías en torno a los conceptos de privacidad, intimidad, derecho al honor, y a la protección de datos personales.
3. Buscar antecedentes
4. Estadísticas

Derivado de ello, es importante destacar algunos de los métodos científicos que coadyuvan al desarrollo del trabajo de investigación que se propone.

a) Positivismo: este método científico se orienta a la observación y análisis de los hechos como elementos de la realidad actual y a partir de ahí se construye no solo un conocimiento teórico sino también el conocimiento empírico.

b) **Racionalismo crítico:** tal y como lo refiere Karl R. Popper, destaca que en el conocimiento científico lo más importante es la comprensión lógica del conocimiento, lo que implica destacar cómo se conoce, y qué se conoce.

c) **Método comparativo:** en este, se tiene la ventaja de que estudia las similitudes y diferencia entre las diferentes estructuras tanto sociales, políticas, económicas, administrativas y gubernamentales.

Hipótesis

- No resultan suficientes los instrumentos normativos, así como los mecanismos para la protección de datos personales en nuestro país, toda vez que la realidad aparentemente refleja la imperiosa necesidad de acciones estaduales para un adecuado reconocimiento, ejercicio y salvaguarda de dicho derecho.

Objetivo General

- Determinar si a la luz de las reformas constitucionales en materia de protección de datos personales en México son eficaces las acciones gubernamentales para el reconocimiento, ejercicio y salvaguarda de este derecho.

Objetivos Específicos

1. Reconocer los antecedentes internacionales y nacionales del derecho a la protección de datos personales.
2. Reseñar la teoría de los Derechos Humanos.
3. Identificar los conceptos básicos relacionados con la Protección de Datos Personales.
4. Reconocer la regulación en materia de Protección de Datos Personales.
5. Conocer cuáles han sido los alcances que han tenido las reformas constitucionales en materia de protección de datos personales.

6. Establecer la suficiencia de las acciones públicas para el cabal reconocimiento, ejercicio y salvaguarda en la Protección de Datos Personales.

TÉCNICAS DE INVESTIGACIÓN

a) Técnica documental.

Hernández y Sampieri (2014) señala que la revisión de la literatura implica detectar, consultar y obtener la bibliografía (referencias) y otros materiales que sean útiles para los propósitos del estudio, de donde se tiene que extraer y recopilar la información relevante y necesaria para enmarcar nuestro problema de investigación. Esta revisión debe ser selectiva, puesto que cada año se publican en el mundo miles de artículos en revistas académicas y periódicos, libros y otras clases de materiales sobre las diferentes áreas del conocimiento.

Si al revisar la literatura nos encontramos con que en el área de interés hay 5 000 posibles referencias, es evidente que se requiere seleccionar sólo las más importantes y recientes, y que además estén directamente vinculadas con nuestro planteamiento del problema de investigación.

TÉCNICAS (GRUPO FOCAL, ENTREVISTA PROFUNDA)

Entrevistas no estructuradas[1]

Las entrevistas se dividen en estructuradas, semiestructuradas y no estructuradas o abiertas (Díaz-Bravo, , Torruco-García, Martínez-Hernández, , & Varela-Ruiz, , 2013) En las primeras, el entrevistador realiza su labor siguiendo una guía de preguntas

[1] Corbetta (2007) clasifica las entrevistas, según su grado de estandarización, en tres tipos básicos: entrevistas estructuradas, semiestructuradas y no estructuradas. En la entrevista estructurada las preguntas planteadas por el entrevistador se establecen de antemano, tanto en la forma como en el contenido; en la entrevista semiestructurada se establece de antemano el contenido, pero no la forma de las preguntas; por último, en la entrevista no estructurada, ni siquiera el contenido de las preguntas se fija previamente, y éste puede variar en función del sujeto.

específicas y se sujeta exclusivamente a ésta (el instrumento prescribe qué cuestiones se preguntarán y en qué orden). Las entrevistas semiestructuradas se basan en una guía de asuntos o preguntas y el entrevistador tiene la libertad de introducir preguntas adicionales para precisar conceptos u obtener más información. Las entrevistas abiertas se fundamentan en una guía general de contenido y el entrevistador posee toda la flexibilidad para manejarla.

TRABAJO TERMINAL DE GRADO[2]:

I. VINCULACIÓN CON EL ÁREA DE INVESTIGACIÓN

La vinculación del derecho parlamentario con el trabajo de investigación denominado “Origen, retos y prospectiva del derecho a la protección de datos personales a 20 años de su Constitucionalización”, en la actualidad es un tema de gran relevancia en el contexto actual de la gobernanza democrática y la protección de este derecho fundamental.

En un primer momento, es importante traer a colación que el Derecho Parlamentario, se refiere al conjunto de normas y principios que regulan el funcionamiento de los órganos legislativos y la relación entre sus integrantes, este derecho, asegura la representación, la participación y la transparencia en el proceso legislativo.

En un segundo momento, el derecho a la protección de datos personales, es un derecho fundamental que protege la intimidad, y la privacidad de los individuos frente al tratamiento de los datos personales. Con la constitucionalización de este derecho se ha establecido un marco jurídico que obliga a las instituciones públicas o privadas a garantizar la protección de la información personal de los ciudadanos.

Luego entonces, después de analizar por separado al Derecho Parlamentario y al Derecho a la Protección de Datos Personales, se tiene que la vinculación, relación, intersección de estos derechos es crucial, ya que por un lado los parlamentos deben legislar sobre la protección de datos personales, teniendo en cuenta las necesidades de seguridad y la privacidad. Por otro lado, la recopilación y el tratamiento de datos en el ámbito parlamentario deben realizarse en estricto apego al marco jurídico, respetando el derecho a la privacidad de sus ciudadanos.

[2] Estructura de acuerdo al artículo 56 del Reglamento de Estudios Avanzados de la UAEM.

II. OBJETO DE APLICACIÓN DEL CONOCIMIENTO

Actualmente, el objeto de aplicación del derecho a la protección de datos personales se puede analizar desde diversas perspectivas, entre ellas, el derecho a la privacidad, regulación y normatividad, impacto tecnológico, responsabilidad de las organizaciones y conciencia y educación.

En la primera perspectiva (derecho a la privacidad), la protección de datos personales se fundamenta en el derecho a la privacidad, que resguarda la vida personal y familiar de los individuos. Esto implica que cualquier tratamiento de datos debe ser realizado con el consentimiento del titular y bajo principios de legalidad, transparencia y finalidad.

Por lo que respecta a la regulación y normatividad, se han generado e implementado leyes y regulaciones específicas que establecen los lineamientos para el manejo de datos personales, tanto en el ámbito público y privado.

Tocante al impacto tecnológico, se advierte que esta ha aumentado y ha cambiando su manejo de manera drástica ya que la digitalización y el uso de la internet ha facilitado la recopilación, almacenamiento y procesamiento de la información, lo que ha llevado a la necesidad de adaptar el marco jurídico de la protección de datos personales, y con ello abordar los nuevos desafíos que se han ido presentando.

Ahora bien, con relación a la responsabilidad de las organizaciones, estas son entidades que manejan datos personales y que están sujetas a responsabilidades legales, incluyendo la obligación de implementar medidas de seguridad adecuadas, que garanticen la protección de datos personales es su posesión.

Por último, es imperante promover la concienciación sobre la importancia de la protección de datos personales tanto a nivel individual como organizacional. La

educación en este ámbito permite a los ciudadanos ejercer sus derechos y a las organizaciones cumplir con sus obligaciones legales.

III. METODO DE TRABAJO

Para la realización de la investigación fue necesario una orientación teórico-metodológica, en donde se aplicaron los diversos métodos de investigación.

En este orden de ideas, para la presente investigación se tomará en cuenta el enfoque de la investigación mixta, es decir, cualitativa y cuantitativa.

En este sentido, utilizaremos el enfoque cuantitativo y cualitativo, porque se consideran necesarios para el desarrollo de nuestros objetivos, como ejemplo para:

1. Consultar el marco jurídico de la protección de datos personales.
2. Conocer las teorías en torno a los conceptos de privacidad, intimidad, derecho al honor, y a la protección de datos personales.
3. Buscar antecedentes
4. Estadísticas

Derivado de ello, es importante destacar algunos de los métodos científicos que coadyuvan al desarrollo del trabajo de investigación que se propone.

a) Positivismo: este método científico se orienta a la observación y análisis de los hechos como elementos de la realidad actual y a partir de ahí se construye no solo un conocimiento teórico sino también el conocimiento empírico.

b) Racionalismo crítico: tal y como lo refiere Karl R. Popper, destaca que en el conocimiento científico lo más importante es la comprensión lógica del conocimiento, lo que implica destacar cómo se conoce, y qué se conoce.

c) **Método comparativo:** en este, se tiene la ventaja de que estudia las similitudes y diferencia entre las diferentes estructuras tanto sociales, políticas, económicas, administrativas y gubernamentales.

IV. RESULTADOS

Al terminar la investigación se evidenció que si bien es cierto ya se cuenta con una amplia literatura, un marco normativo con relación a la protección de datos personales, empero, aún se identifican desafíos para la salvaguarda de este derecho, ya que, como todo derecho, es cambiante y se tiene que actualizar conforme a las necesidades de la sociedad, presente y futura.

DISCUSIÓN

CAPÍTULO PRIMERO
ORÍGENES Y EVOLUCIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

El presente apartado da cuenta de la revisión de la literatura especializada sobre el derecho a la protección de datos personales tanto en el orden internacional como en el nacional, lo que permitirá identificar los orígenes y evolución de la protección de datos personales; se expondrán algunas consideraciones que los autores acerca de este derecho fundamental.

1.1 Orígenes del derecho a la protección de datos personales

Los datos personales hoy en día se han vuelto un tema que inciden en todos los aspectos de la vida diaria, desde las cosas más comunes hasta las más complejas, y al ser de gran impacto, los gobiernos han dirigido sus esfuerzos para garantizar su debida protección, es común que en muchas ocasiones sin otorgar nuestro consentimiento, se recaben y se transfieran datos personales tanto a entes públicos como privados, lo que vulnera la privacidad y pone en riesgo la intimidad, dignidad, honor, honra e integridad de los titulares.

La intimidad y la vida privada de las personas es un derecho humano que debe garantizarse respecto de injerencias arbitrarias o ilegales, desde mi perspectiva jurídica conlleva un grado especial de protección, pues una intromisión o vulneración de la esfera más íntima de la persona puede poner en peligro la vida, la libertad y la seguridad, en primera instancia, pero también puede llegar afectar el honor, la honra, la reputación y dignidad de una persona.

Cuando se habla de protección de datos personales surge la necesidad de crear elementos de prevención y regulación a partir de importantes factores de riesgo como lo son la amenaza derivada del uso de las tecnologías de la información en perjuicio de la intimidad y privacidad de las personas por parte de terceras personas

y la afectación producida por el uso ilícito de estos a partir de conductas perjudiciales por parte de los responsables de las bases de datos.

Por ello es importante hacer un pequeño recorrido por los orígenes de los datos personales, para entender su concepción como un derecho humano reconocido por ordenamientos jurídicos internacionales, en esta virtud y desde la perspectiva universal, el 2 de mayo de 1948 en la Declaración Americana de los Derechos y Deberes del Hombre, en su artículo V “Derecho a la protección a la honra, la reputación personal y la vida privada y familiar” precisaba que, “Toda persona tiene derecho a la protección de la ley contra los ataques abusivos en su honra, a su reputación y a su vida privada y familiar” (Comisión Interamericana de Derechos Humanos , 2023).

Además, en su artículo 12 refiere que “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataque a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley entre tales injerencias o ataques” (Declaración Universal de los Derechos Humanos, 2023).

De esta manera se garantiza primeramente el reconocimiento a la protección de la vida privada, es el instrumento internacional que sirve de base para la generación de otros instrumentos que de manera específica y con mayor profundidad abordaran el tema, y no someramente sino con un mayor grado de profundidad.

Años más tarde, en 1966 el Pacto Internacional de Derechos Civiles y Políticos y al cual se suscribió México en el año 1981, se reconoce en el artículo 17 que:

> “1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de los ataques ilegales a su honra y reputación.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques" (Pacto Internacional de Derechos Civiles y Políticos, 2023).

Este pacto reviste de gran importancia porque fue adoptado por la Asamblea General de las Naciones Unidas el 16 de diciembre de 1966 y entró en vigor el 23 de marzo de 1976. En 2012 este pacto ya había sido ratificado por 167 estados; el pacto desarrolla los derechos civiles y políticos y las libertades recogidas en la Declaración Universal de los Derechos Humanos.

En la consecución de los hechos, encontramos que en el año de 1969 en la Convención Americana sobre Derechos Humanos (Pacto de San José), reconoce en su artículo 11 refiere a la Protección de la Honra y la Dignidad y señala en sus numerales 1, 2 y tres lo siguiente:

"1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques" (Convención Americana sobre Derechos Humanos, 2023)

Este pacto reafirma el respeto a la honra y el reconocimiento de la dignidad la privacidad y la reputación, elementos esenciales para una correcta protección de los datos personales son los primeros indicios de un reconocimiento de esa figura jurídica.

De igual modo, dentro de los datos internacionales de la protección de datos personales particularmente en Europa, se encontró que, para el tratamiento y flujo

de datos transfronterizos, se realizaron documentos necesarios para la protección de los datos personales, entre ellos el Convenio N° 108 del Consejo de Europa.

El 28 de enero de 1981, se promulgó el Convenio N° 108 del Consejo de Europa, dicho instrumento reconoce por primera vez el derecho a la vida íntima, a la vida familiar; específicamente en la protección de las personas con respecto al tratamiento sistematizado de datos personales, aunque no incluye expresamente la protección de los datos personales, dicho ordenamiento, es considerado uno de los primeros instrumentos que tiene el carácter de vinculatorio en materia de protección de datos personales, esto, debido al vertiginoso procesamiento electrónico de la información personal y de las primeras apariciones de las bases de datos que era utilizadas por grandes compañías y algunos gobiernos estatales.

> "…en el territorio de cada parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto a sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona"[3].

Recalcar que este convenio no era exclusivamente para regular el flujo transfronterizo de datos de carácter personal, sino también contemplaba las obligaciones que de él derivan; en este sentido el artículo cuarto del citado ordenamiento establece que los Estados parte de ese convenio, optarán en su régimen interno, "…las medias necesarias de seguridad en materia de protección de datos personales para que sean efectivos los principios básicos en materia de protección de datos personales" (Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2011)

[3] Artículo 1. Objeto y Fin. Convenio 108 del Consejo de Europa.

Cabe mencionar que dicho Instrumento fue fortalecido a través de la resolución 45/95 por parte de las Naciones Unidas, adoptada el 14 de diciembre de 1990, en el cual establece los “principios rectores para la reglamentación de los ficheros computarizados de datos personales” (Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2011).

Otro significativo instrumento normativo es la Directiva 95/46/CE, del 24 de octubre de 1995, emitida por el Parlamento y el Consejo de la Unión Europea, relativa a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y su libre circulación, es el principal instrumento legislativo en materia de protección de los datos personales en la Unión Europea, establece condiciones generales para el legal tratamiento de datos personales y define los derechos de los interesados, al tiempo que prevé la designación de autoridades nacionales de control independientes. De conformidad con la Directiva, el tratamiento de los datos personales está supeditado al consentimiento explícito del interesado, quien ha de ser informado antes de que se proceda a dicho tratamiento.

Por otra parte, el desarrollo del derecho a la protección de los datos personales ha mostrado, en todo el mundo, la marca de la experiencia europea, por ejemplo, en 1980, debido al rápido desarrollo tecnológico y económico, surgieron las Directrices de la Organización para la Cooperación y el Desarrollo Económico (OCDE), de las cuales emanan principios como la transparencia, la limitación de recopilación, la calidad de los datos, la especificación de propósito, la limitación de uso, la salvaguarda de la seguridad, la participación individual y la responsabilidad.

Luego entonces, se tiene que, si bien existen ya ordenamientos jurídicos, estos se tienen que ir adecuando a las necesidades cambiantes de la sociedad, y que realmente sean aplicados para la debida protección y salvaguarda de datos personales.

Por su parte la Carta de los Derechos Fundamentales de la Unión Europea, del 07 de diciembre del 2000, se gesta con la plena convicción del porvenir pacífico basado en valores comunes, fundada en productos indivisibles y universales como: la dignidad humana, la libertad, la igualdad y la solidaridad, y se basa en los principios de la democracia y del Estado de Derecho (Europeas, 2000), esta unión busca fomentar un desarrollo equilibrado y sostenible y garantiza la libre circulación de personas, bienes, servicios y capitales, así como la libertad de establecimiento.

Esta Carta, refuerza la protección de los derechos fundamentales al tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos (Europeas, 2000), respetando las competencias y misiones de la Comunidad y de la Unión; el disfrute de tales derechos origina responsabilidades y deberes respecto de los demás como de la comunidad humana y de las futuras generaciones. En consecuencia, la Unión reconoce los derechos, libertades y principios relacionados con el respeto a la vida privada y la protección de datos particularmente los artículos 7 y 8 que a la letra señalan:

> *"…*
> *Artículo 7 Respeto de la vida privada y familiar*
>
> Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones.
>
> *Artículo 8 Protección de datos de carácter personal*
>
> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente…” (Europea, 2024)

Merece especial reconocimiento este precepto, pues aquí ya es claro el respeto a la vida privada y a la protección de los datos personales como derechos independientes, si bien es cierto que se relacionan con otros derechos como el de acceso a la información, también lo es que logra su independencia, individualidad y protagonismo propio; después de años de tratar de ubicar el lugar que merece dentro de la normativa jurídica como un derecho fundamental.

En esta carta se considera el tratamiento leal y adecuado y no solo eso, se vislumbra el derecho de acceso y rectificación de los datos personales, aunque no establece el procedimiento para ello, deja abierta la puerta abierta para las autoridades regulen al respecto.

Para concluir con este aparatado, nos referiremos al Reglamento General para la Protección de Datos Personales del Consejo Europeo que se creó en Bruselas el 27 de abril de 2016 y entró en vigencia el 25 de mayo de 2018, mismo que contemplaba los principios y la normatividad relacionada con la protección de datos personales y a su tratamiento que todos los estados miembros debían llevar a cabo.

Este Reglamento General de Protección de Datos (RGPD) responde a una larga evolución sobre la protección de datos personales en la Unión Europea de más de 40 años, que ha influenciado en otras regiones del mundo, entre ellas Latinoamérica. La aplicación directa del RGPD y su alcance extraterritorial hacen que instituciones públicas y privadas de todo el mundo deban cumplir con las obligaciones en él establecidas, incluidas las latinoamericanas.

Como se ha visto en líneas anteriores, los gobiernos han tenido la necesidad de salvaguardar la intimidad de todas las personas, creando instrumentos jurídicos que dotan de seguridad en el uso y manejo de los datos personales proporcionados a

entidades públicas y privadas, pero es la última década en la que ha tenido un mayor auge debido al uso masivo de las tecnologías de la información, para ser exactos de la Internet. En este sentido, se observa un camino largo, considerando que únicamente un instrumento jurídico no protegerá ni garantizará el uso adecuando, responsable y comprometido de los datos personales, sino que también falta crear conciencia de los riesgos que puede sufrir cualquier persona al ser vulnerado sus datos personales, aunado a que las personas que tienen a su cargo el tratamiento de datos personales deben actuar con probidad, ética y sobre todo responsabilidad para garantizar y salvaguardar el derecho a la protección de datos personales.

1.2 Surgimiento en América Latina

Una vez referidos los orígenes internacionales, daremos paso a los orígenes del derecho a la protección de datos personales en América Latina, para conocer cuáles fueron las causas de su incorporación en los ordenamientos legales latinoamericanos, sí se debió a los instrumentos jurídicos supranacionales o bien a las necesidades propias de cada país; en este sentido, la protección de datos personales tuvo su primer acercamiento en la relación comercial que existe entre los países miembros de la Unión Europea y la cual fue una condicionante para seguir con estas relaciones económicas razón por la cual se comenzó a su normativización en América Latina, posteriormente y con el paso del tiempo las entidades latinoamericanas se dieron cuenta de que el Derecho a la Protección de Datos Personales fue tomando importancia y se vieron en la necesidad de crear y modificar la legislaciones que rigen la materia.

En América, el primer antecedente surgió en Estados Unidos de América en el año de 1974 para ese entonces la Unión Americana contaba con dos legislaciones en materia de protección de datos personales, una de estas legislaciones era para el sector público denominada “Ley de Privacidad” y otra para el sector privado “*Fair*

Infromation Practice y Safe Harbor". (Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2011)

La Ley de Privacidad contemplaba experiencias para regular la recolección, mantenimiento, uso y difusión de los datos personales en poder de autoridades gubernamentales, y para ello era necesario informar al titular que sus datos personales debían estar inscritos en un registro, así que era necesario informar el nombre y ubicación del sistema, la categoría de datos que se recaban, las categorías de los registros, accesos diarios a los sistemas, políticas y prácticas de la agencia respecto al almacenamiento, recuperación, controles de acceso, retención y eliminación de registros y, en su caso, los procedimientos por los que el titular de los datos personales podía hacer una solicitud de notificación.

Esta circunstancia es lo que consideramos actualmente en la legislación mexicana como el Aviso de Privacidad, es el documento en el que se informa a los titulares cual será el tratamiento que se dará a sus datos personales, para su tiempo resulta una ley innovadora con grandes aportaciones para las normativas siguientes.

Para el caso de Estados Unidos de América a pesar de que ya se refirió una ley de carácter privado, no cuenta con una legislación específica sobre la protección de datos personales en posesión de los particulares como en otras Naciones, empero cuenta con una legislación que es la *Fair Information Practice Principals (FIP´s*), está básicamente, es el resultado final de un análisis a los procedimientos electrónicos de recolección, almacenamiento y tratamiento que se les da a los datos personales, asimismo, establece garantías mínimas para tratar de salvaguardad la protección de datos en posesión de particulares, pues se reitera, en ese país no se cuenta con una legislación específica para regular el tratamiento de datos personales en posesión de los particulares.

Por su parte, Brasil en 1997 tuvo un primer acercamiento a la protección de datos personales el cual se vio materializado en su Constitución, y específicamente en su artículo 5, fracción LXXII, el cual menciona que se concederá “habeas data”:

a) “Para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público:
b) Para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo.” (García González, 2007)

Para el año 2018, se fortaleció su normatividad y hoy en día es una de las más actuales y completas en materia de protección de datos personales, ya que llego a conjuntarse con autoridades estatales que crearon un marco unificado, garantizando un enfoque global y para el año 2020 se creó la Autoridad Nacional de Protección de Datos Personales, la cual más adelante se analizará de manera detallada.

Siguiendo con el análisis de los orígenes latinoamericanos del derecho a la protección de datos personales, se tiene que Chile en el año de 1999, adoptó una ley para regular la protección de datos personales, y para el año que 2024, a través de su Congreso se aprobó la creación de la Agencia de Protección de Datos Personales, institución que es independiente del derecho de acceso a la información y transparencia.

Para el año 1999 en la Constitución de la República Bolivariana de Venezuela, se estableció en su artículo 60 que: “…toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática” (Sánchez Pérez & Rojas González, 2018)

Otro antecedente en América Latina es Argentina, para el año 2000 específicamente en el artículo 43 de su Constitución, el cual refiere:

> “Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que conste en registros o bancos públicos, o privados destinados a proveer informes, y en su caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquellos.” (Contituyente, 2023)

Aunado a lo anterior, es sustancial manifestar que en Argentina se cuenta con una Dirección Nacional de Protección de Datos Personales, institución que al igual que en Chile es la encargada de salvaguardar el derecho a la protección de datos personales independientemente de cualquier otro derecho como el de acceso a la información pública y a la política pública de transparencia.

En Perú, en el año 2011 en su Constitución, se estableció en su artículo 2 incisos 6 y 7 que:

> “Toda persona tiene derecho:
>
> 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.
>
> 7. Al honor y a la buena reputación, a la intimidad personal y familiar, así como a la voz y a la imagen propias.
>
> Toda persona afectada por afirmaciones inexactas o agraviada en cualquier medio de comunicación social tiene derecho a que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley.” (República, 2023)

En este caso la situación normativa refiere únicamente a servicios informáticos que puedan afectar la intimidad de una persona, que repercutan en su honor, reputación e imagen; su precepto se basa medularmente en cualquier afectación producida por la libertad de prensa, lo que a mi parecer cuenta con un alcance limitado.

Importante señalar que Colombia en el año 2012 también estipulo en el artículo 15 de su Constitución que:

> “Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tiene derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución” (Colombia, 2023)

Cuando Colombia reconoció el derecho a la protección de datos ya contaba con referentes jurídicos internacionales, mismo que ya se ven reflejados en su texto constitucional, lo que otorga mayor certeza a los titulares.

Ecuador, también reguló la protección de dato personal y quedo consagrado en el artículo 66 incisos 19 y 20 de su Constitución, el cual refiere:

> “Se reconoce y garantizará a las personas:
>
> 19. El derecho a la protección de datos personales, que incluye el acceso y la decisión sobre información y datos de este carácter y su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

20. El derecho a la intimidad personal y familiar.” (Constituyente, 2023)

Las leyes de protección de datos personales empiezan a surgir a partir de los años 2000´s. Estas leyes fueron influenciadas por la visión sobre el derecho a la vida privada de la Unión Europea, plasmadas específicamente en la Directiva Europea 95/46/EC y a partir de la entrada en vigor del RGPD el 25 de mayo del 2018, casi todos los países latinoamericanos entraron en un proceso de reforma de sus leyes de protección de datos para adherirse con el RGPD, lo que, desde mi perspectiva, esto convierte a Latinoamérica en un aliado estratégico de la Unión Europea en esta área.

Dicho Reglamento General de Protección de Datos Personales encuentra su fundamento en la gestión de riesgos, un lenguaje universal para el sector de la seguridad de la información. De esta forma se observa que uno de los mayores desafíos es el enfoque de la gestión de riesgos, pues la han aplicado tradicionalmente la gran mayoría de las empresas latinoamericanas desde el punto de vista de la protección de sus activos y no desde el punto de vista de la protección de derechos y libertades.

Por lo tanto, las empresas latinoamericanas deben adaptar sus procedimientos y modelos de gestión del riesgo a partir de este nuevo enfoque y no solo buscar adherirse a estos ordenamientos con mira económico sino en realidad proteger los datos personales, sus derechos y sus limitaciones.

Considero, que en América Latina no existe aún un proceso de integración jurídica en esta área, las disposiciones establecidas en el RGPD pueden tener muchas variantes. Los ejemplos incluyen el principio de protección de la privacidad desde el diseño y por defecto, las certificaciones, las notificaciones de violaciones de datos, el rol del Oficial de Protección de Datos o las sanciones administrativas por incumplimiento independientemente de las acciones civiles o penales que a las que pueda ser sujeto por incumplimiento a la Ley de Protección de Datos Personales, si

bien es cierto ya existe la Red Iberoamericana de Protección de Datos Personales (RIPD), cuyo objetivo es motivar la creación, modificación y adopción de leyes que garanticen el derecho a la protección de datos personales y a la vida privada de los ciudadanos que integran las naciones miembros, sin embargo, si no se tiene la voluntad de garantizar el derecho a la protección de datos personales, no se logrará la salvaguarda.

Para finalizar este apartado, se puede concluir que la Unión Europea ha sido un factor para que los países latinoamericanos hayan optado por seguir el modelo europeo de protección de datos personales, sobre todo cuando se trata del respeto a la vida privada, honra, honor, dignidad y acaso más cuando se refiere a transferencias de datos personales, empero, se considera homologar los diferentes criterios sobre la protección de datos personales y con ello garantizar una adecuada salvaguarda al derecho fundamental de la Protección de Datos Personales.

1.3 Evolución de los datos personales en México.

Ahora bien, es momento de referir la evolución histórica de este derecho en México; el primer antecedente en nuestro país para la protección de datos personales, data de 1857 (Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, 2011), y estaba consagrado en nuestra Constitución específicamente en el artículo 16 el cual refiere “nadie puede ser molestado en su persona, familia, domicilio, papeles y posesiones, sino en virtud de mandamiento escrito de la autoridad” (Nacional, 2023)

Sin embargo, no fue hasta el año 2000 donde se promocionaron varios proyectos legislativos en el Congreso de la Unión para legislar sobre esta materia y el resultado derivó en la publicación en el Diario Oficial de la Federación el 11 de junio de 2002 de la Ley de Transparencia y Acceso a la Información Pública Gubernamental.

Ahora bien, una vez que se creó la Ley de Transparencia y Acceso a la Información Pública Gubernamental, tuvo que ser modificado el artículo 16 Constitucional en el sentido de hacer más específico la protección de datos personales al decir que, todas las personas tienen derecho de proteger sus datos personales. Este derecho está ratificado y asentado en el cuerpo normativo de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (Cámara de diputados del H. Congreso de la Unión, 2010) aprobada por el Congreso de la Unión en 2010, reconociéndolo mediante derechos ARCO relativos al acceso, rectificación o corrección de los datos personales obtenidos de los individuos, así como el derecho de oponerse a que se recaban (Derechos ARCO: Acceso, Rectificación, Cancelación u Oposición).

Ya en el marco del nuevo paradigma constitucional que se modificó desde el año 2011 hasta el 2014 tuvo verificativo la más significativa reforma en materia de transparencia. Una vez aprobada la modificación, está dio paso a la amplia variedad de la información determinada como: pública, confidencial y reservada, que se encuentra en posesión de "órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal"[4]

En el mismo sentido, esta reforma transformó la naturaleza del órgano garante del derecho de acceso a la información pública, para transitar del Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), concebido como "un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica, de gestión,

[4] Artículo 23. Son sujetos obligados a transparentar y permitir el acceso a su información y proteger los datos personales que obren en su poder: cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en los ámbitos federal, de las Entidades Federativas y municipal. (Ley General de Transparencia y Acceso a la Información Pública)

capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna" (INAI, s.f.)

Atendiendo el mandato contenido en el artículo tercero transitorio de la Ley General de Transparencia Acceso a la Información Pública el cual refiere en sustancia "…en tanto no se expida la ley general en materia de datos personales en posesión de sujetos obligados, permanecerá vigente la normatividad federal y local de la materia, en sus respectivos ámbitos de aplicación"

Fue así que el Congreso de la Unión aprobó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el Diario Oficial de la Federación el 26 de enero de 2017, esta ley fue producto del trabajo intenso para incorporar en su marco normativo este derecho humano; con la intención de crear una Ley General de Protección de Datos Personales que de manera independiente y autónoma a cualquier otro derecho, empodere a los titulares del derecho frente al Estado Mexicano para garantizar el control sobre su información personal.

Si bien es cierto que esta iniciativa fue presentada por el entonces Instituto Federal de Acceso a la Información y Protección de Datos; también es cierto, que los organismos garantes, órganos especializados, la docencia, la investigación y las aportaciones de organizaciones de la sociedad civil, fueron clave para la reforma constitucional; para dotar de contenido al derecho de protección de datos personales, y la urgencia de la legislación secundaria en la materia, así como la creación de las legislaciones estatales y sus respectivos órganos garantes.

Demostrando que, aunque es cierto que hay instrumentos necesarios para regir la protección de datos personales acorde a los de la Unión Europea, aún se requiere voluntades de los entes involucrados (sociedad-gobierno) para que la implementación de esta ley alcance los objetivos planteados.

CAPÍTULO SEGUNDO
EL DERECHO HUMANO A LA PROTECCIÓN DE DATOS PERSONALES DESDE SU CONCEPCIÓN CONCEPTUAL

La presencia de las tecnologías de la información en nuestros días sin duda le ha permitido a la sociedad avanzar en la generación de conocimientos y herramientas que le permiten al hombre gozar de mayores beneficios personales y sociales, sin embargo, el avance en la protección y cuidado de las garantías constitucionales frente a estos nuevos esquemas es lento y paulatino de tal manera que el avance tecnológico deja muy atrás el reconocimiento efectivo de nuevos derechos.

Mediante el análisis hermenéutico la normativa constitucional y de la revisión de la interpretación jurisprudencial, se analizará si la forma en la que actualmente se protegen los datos personales es efectiva.

Proteger los datos relativos a las personas no es producto de la casualidad o la desidia, los datos personales son la representación tangible de nuestro paso por la vida, reflejan características, opiniones, debilidades, intereses, gustos, son la fotografía perfecta de un individuo. El tratamiento adecuado de los datos personales es un reclamo sentido y vibrante de la dignidad y del libre desarrollo de la personalidad; el permitir que otras personas conozcan información sobre un individuo que no tiene intención de revelarla, afecta drásticamente la intimidad de una persona, es decir, la forma en la que habrá de conducirse ante su círculo más cercano, familia, amigos, compañeros de trabajo y ante la sociedad.

La vorágine tecnológica produce una explosión masiva y riegos de la información personal, su origen se ubica en el nacimiento de este mundo globalizado y tecnificado, en el que la inteligencia artificial con solo un par de indicadores crea perfiles perfectos de personalidad atentando no solo contra la privacidad sino con otros derechos fundamentales.

El derecho a la protección de datos personales tiene su origen en la intimidad, ambos derechos están vinculados pero que no son iguales, y ambos se encuentran reconocidos en la Declaración de Derechos Humanos, al amparo de la dignidad humana. El derecho a la protección de datos está íntimamente ligado al de la intimidad y a la privacidad, pero goza de autonomía propia, empero es necesario revisar minuciosamente cada uno de ellos.

Este reconocimiento de los derechos fundamentales se plasma en el Derecho positivo, Luigi Ferrajoli manifiesta que son fundamentales los derechos “que no se pueden comprar ni vender”, esto es, aquellos derechos subjetivos que corresponden de manera universal a “todos” los seres humanos que sea dotados del status de personas, de ciudadanos o de sujetos con capacidad de obrar.

Por su parte, son “derechos subjetivos” todas las expectativas positivas (de prestaciones) o negativas (de no sufrir lesiones) adscritas a un sujeto por una norma jurídica y en razón de su status o condición de tal, prevista asimismo por una norma jurídica positiva, “como presupuesto de su idoneidad para ser titular de situaciones jurídicas y/o autor de los actos que son ejercicio de estas”. (Ferrajoli, 2004)

De lo anterior se desprende que un individuo adquiere valores en razón de su ser que lo hacen completamente distinto a cualquier otro y que reflejan en tanto su esencia, su intimidad, así llegamos a la definición de que los derechos fundamentales son aquellos “derechos que están adscritos universalmente a todos en cuanto personas, o en cuanto ciudadanos o personas con capacidad de obrar, y que son por tanto indisponibles e inalienables”. (Carbonell, 2007)

2.1 La intimidad de los datos personales

Los derechos a la privacidad y a la intimidad guardan esas características, y por tanto los consideraré para efectos de este escrito como derechos fundamentales, pero a que se refiere intimidad, etimológicamente, intimidad proviene del latín

“intimus” superlativo de interior y significa “lo que está más adentro, lo más interior, el fondo”, la Real Academia de la Lengua Española señala que íntimo, ma es el adjetivo que se refiere a lo más interior o interno; y como sinónimo de privado, personal, particular, reservado y familiar.

Por su parte el Diccionario del Español de México puntualiza que la intimidad es la parte más interna o personal de un ser humano, sus sentimientos e ideas; vida privada, familiar o de un pequeño círculo de amistades cercanas: en la intimidad de nuestro corazón.

Ante este contexto amplio es indubitable que la intimidad no es otra cosa más que el aspecto del ser humano más personal, en que se descansan sus sentimientos, anhelos, ideas y su esencia.

Ahora bien, desde el punto de vista de la doctrina jurídica el derecho a la intimidad es sin lugar a dudas un elemento *sine qua non* de la libertad personal instituido por el derecho a la protección de datos personales que corresponde a una parte de esa ejecución plena de las libertades otorgadas.

La intimidad como derecho fundamental protege la esfera más privada del individuo, esta revestida de información reservada que posibilita o no compartirse mediante autorización.

Para algunos doctrinarios los términos intimidad y privacidad, tienen la misma connotación no hay diferencia alguna es como si se trataran de dos términos similares; sin embargo, se considera que ambas concepciones son completarías y no tan diferentes.

La intimidad se puede conceptualizar como “la esfera personal que está exenta del conocimiento generalizado de tercero y la privacidad es la posibilidad irrestricta de realizar acciones privadas (que no dañen a otros) que se cumplan a la vista de los

demás y que sean conocidas por estos" (Bidart y Carnota, 1998); al ser considerada como un bien jurídico protegido, y más aún un derecho fundamental mantiene una gama de protección singularizada y complementaria con la privacidad.

Por su parte, la privacidad presenta un alcance que se entiende compatible con la intimidad, sin llegar a la premisa de que son diferentes, hasta el punto de generar como conclusión un silogismo de premisas mayores y menores: "los asuntos íntimos son privados, pero no todos los asuntos privados pueden tener carácter de íntimos" (Villalba, 2017)

Andrea Villalba refiere que, cuando se vulnera la intimidad, que engloba áreas muy concretas de la vida de una persona, se ha vulnerado a la vez a la privacidad o aspectos generales referentes a una persona; pero cuando se ha vulnerado la privacidad, no necesariamente significa que se ha atentado contra la intimidad sin perjuicio de que efectivamente pueda llegar a producirse.

El antecedente más próximo dentro del derecho positivo de la intimidad se ubica en el artículo "The Right of Privacy", en el cual surgió el concepto de la intimidad como un derecho, y por tanto un bien jurídico tutelable y de propiedad inherente a las personas, cuya importancia generó el estudio y aplicación de medidas para que este sea debidamente protegido.

El derecho a la intimidad personal se encuentra protegido constitucionalmente, e incluso se podría considerar que esta tutela del derecho es irrenunciable, inalienable e imprescriptible por la naturaleza jurídica que contiene; por tanto, la renuncia a este derecho es inconsistente. Sin embargo, es esencial recordar que este derecho como tal no es de carácter absoluto; lo mismo sucede con la protección de datos: estas son prerrogativas que deben ejercerse dentro de límites razonablemente impuestos en consonancia de los derechos de los demás.

Partiendo de la premisa, y tomando en cuenta que el derecho a la intimidad se vincula a la esfera más reservada de las personas, es decir, al ámbito que constituye un secreto para los demás y que se aleja totalmente del conocimiento público, ámbito aquel que el propio individuo desea mantener oculto a los demás por pertenecer a su esfera más privada, que además se encuentra vinculado con la dignidad y el libre desarrollo de la personalidad. Es por tanto un derecho innato de las personas sin importar proveniencia, nacionalidad o autodeterminación, ya que de esta forma el derecho a un núcleo inaccesible de intimidad se reconoce incluso a las personas más expuestas al público.

Ahora es momento de dar paso a otro concepto de gran importancia en este trabajo, la privacidad, aquí se podrá entender cuál es la diferencia entre uno y otro concepto.

2.2. Privacidad concepto mecánico de la vida privada

La era digital ha transformado irreversiblemente la forma en que las sociedades procesan la información. Cada día, se generan gran cantidad de datos derivados de transacciones electrónicas, interacciones en redes sociales, monitoreo de salud, entre otros. A medida que el volumen de datos crece exponencialmente, también lo hace la preocupación sobre cómo estos datos son recolectados, almacenados, procesados y compartidos. En este contexto, surgen conceptos que permiten proteger a los individuos como lo es el de privacidad.

La privacidad se puede entender como el “ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.” (Española, 2024) Por su parte, el derecho a la privacidad es el derecho de las personas para separar aspectos de su vida privada del escrutinio público, es decir, el derecho de las personas para desarrollar en un espacio reservado ciertos aspectos de la vida personal. Este derecho tiene dos componentes esenciales: el derecho de aislarse y el derecho de controlar la información de carácter personal. (Isabel Davara F. de Marcos, 2024)

El concepto “privacidad” es un concepto que contiene varias connotaciones, el Tribunal Europeo de Derechos Humanos, considera a la privacidad como un concepto amplío, no susceptible de una definición exhaustiva. La Suprema Corte de Justicia de la Nación (SCJN) ha establecido que la privacidad es útil en la medida en que no se tomen de manera descontextualizada, surjan de un análisis cuidadoso del contexto jurídico en el que la idea de privacidad entra en juego y no se pretenda derivar de ellas un concepto mecánico de vida privada, de referentes fijos e inmutables. Lo único que estas resoluciones permiten reconstruir, en términos abstractos, es la imagen general que evoca la idea de privacidad en nuestro contexto cultural. (INAI, 2023).

Aunado a lo anterior, el acelerado desarrollo tecnológico presenta desafíos hacía el ámbito privado en la vida de los individuos, verbigracia correos electrónicos, mensajería instantánea, dispositivos de localización y geolocalización. En este sentido los términos privacidad y derecho a la privacidad no necesariamente refieren a lo mismo: la privacidad es un elemento consustancial a la dignidad humana y por ende debe ser protegido por el derecho y el derecho a la privacidad es aquél que todo individuo tiene a separar aspectos de su vida privada del escrutinio público.

Por otro lado, la protección de datos personales ha sido vista como una necesidad práctica y como un derecho fundamental. Según Soria (2019), la protección de datos personales puede conceptualizarse como una herramienta técnica o jurídica y como una manifestación contemporánea de los derechos humanos. A medida que el entorno digital se vuelve más intrincado, la individualidad y la privacidad de las personas pueden verse amenazadas por sistemas ante la pérdida, robo, uso o extravío de datos personales ante las entidades que tienen la capacidad de recolectar, analizar y, en ocasiones, malversar dichos datos (Martínez, 2020).

Acorde con González (2018), la magnitud y el alcance de la recolección de datos han propiciado debates sobre la ética de la privacidad y la autodeterminación informativa. Las consecuencias de un manejo inadecuado de datos pueden ser

vastas, desde la manipulación de comportamientos hasta la discriminación basada en análisis de datos (Pérez, 2021). En este sentido, el derecho a la protección de datos personales emerge como una respuesta a los desafíos inherentes de una sociedad hiperconectada.

No obstante, la interpretación y aplicación de este derecho varía considerablemente de un país a otro. Mientras algunos ven la protección de datos como una extensión lógica de los derechos a la privacidad y a la libertad de expresión, otros enfatizan su naturaleza autónoma (Ramírez, 2017). A pesar de estas divergencias, existe un consenso creciente acerca de la necesidad de contar con un marco normativo que salvaguarde la integridad y privacidad de los datos personales de los individuos.

Por lo que en este capítulo se tiene el propósito de explorar el Derecho Humano a la Protección de Datos Personales, ofreciendo una perspectiva profunda y actualizada sobre su evolución, sus desafíos y su relevancia en el siglo XXI. Utilizando una variedad de fuentes académicas y estudios recientes, se pretende arrojar luz sobre las implicaciones y responsabilidades que conlleva el manejo de datos en el mundo digital contemporáneo.

La normativa sobre protección de datos enfrenta retos ante un escenario complejo de tratamientos de datos desproporcionados en el sector público y privado, en los que el Big Data y el Internet de las cosas juegan un papel muy relevante con el impulso de los legisladores para crear leyes adecuadas al tiempo y al contexto.

En México existe una apremiante necesidad de reformar la legislación en materia de protección de datos personales, con su adhesión al Convenio 108 del Consejo de Europa y con la búsqueda de su incorporación al Convenio 108+, pero no cuenta con los niveles adecuados de protección de datos, lo que le impide alcanzar el objetivo; que necesita además de ello, normas equiparables a las del esquema europeo, pero sobretodo la certeza de contar con una base sólida para la tutela del

derecho. En este sentido expondré los conceptos básicos para comprender de mejor manera sus orígenes y alcances.

Para tener claridad en el tema, es necesario referirnos al término "datos personales" que ha evolucionado a medida que la sociedad ha transitado hacia la era digital, convirtiéndose en un pilar esencial en las discusiones sobre privacidad y derechos humanos en el siglo XXI.

Según la definición proporcionada por la Reglamento General de Protección de Datos (RGPD) de la Unión Europea (2018), los datos personales se refieren a "cualquier información relacionada con una persona física identificada o identificable". “Una persona identificable es aquella que puede ser identificada, directa o indirectamente, en particular mediante referencia a un identificador como un nombre, un número de identificación, datos de ubicación, un identificador en línea o a uno o más factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de dicha persona” (Reglamento UE 2016/679 del Parlamento Europeo y del Consejo, 2016).

Esta definición es reflejo de la diversidad de información que, en el contexto digital actual, puede utilizarse para identificar a un individuo. No se trata únicamente de información directamente identificativa, como el nombre o la dirección, sino que también puede incluir elementos que cuando se combinan, pueden llevar a la identificación de una persona. Por ejemplo, una combinación de preferencias, historial de navegación y ubicaciones geográficas frecuentes, aunque no contenga un nombre explícito, puede ser suficiente para identificar a un individuo en ciertos contextos (Martínez, 2019).

Los datos personales, por lo tanto, no solo se limitan a la información que tradicionalmente consideraríamos como identificativa. En el entorno digital actual, casi cualquier pieza de información puede convertirse en un dato personal si se usa junto con otras piezas para identificar a un individuo. Esta expansión del concepto

subraya la creciente complejidad del paisaje de protección de datos y la necesidad de salvaguardar adecuadamente esta información en una era donde la digitalización y el análisis de datos están en el centro de muchas actividades humanas (García, 2020).

En el contexto de la protección de datos personales, es imperativo entender primero una serie de conceptos básicos que proporcionan la base y el entendimiento necesario para profundizar en este complejo tema.

El concepto **"dato personal"** se refiere a: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información (Obligados, 2024). Esto puede incluir, pero no se limita a, nombres, fechas de nacimiento, direcciones, números de teléfono, direcciones de correo electrónico y más. En un contexto digital, esta definición también abarca identificadores electrónicos como direcciones IP o identificadores de dispositivos.

Por otro lado los "**datos personales sensibles**", de acuerdo a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, son aquellos "a los referentes de la esfera de su titular cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste" (Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, 2023), en este orden de ideas también refiere de manera enunciativa, más no limitativa, algunos datos personales sensibles como son: el origen étnico o racial, el estado de salud física o mental presente o futura, información genética, creencias religiosas, fisiológicas y morales, así como las opiniones políticas y preferencias sexuales.

Otro concepto, transcendental para este trabajo de investigación, encontramos el **"honor"**, el cual debemos precisar que no es lo mismo que la honra, ello obedece

a que la honra, es la estima y respeto de la dignidad propia, es decir, al respetarse a sí mismo a su persona.

Otro concepto valioso es el de la **“honra”,** este concepto básicamente consiste en la cualidad moral que nos lleva al más severo cumplimiento de nuestros deberes respecto del prójimo y de nosotros mismos, es decir, que es la aptitud que tienen las personas para hacer lo correcto en cumplimiento a los derechos y deberes propios y de otras personas.

Como se puede observar, todos estos conceptos están relacionados entre sí, porque mi parecer se encarga de la dignidad humana, de la esfera más próxima a la íntima de la persona y el individuo, para ello es oportuno traer a colación dos teorías que en particular reforzaran este dicho la Teoría de las Esferas y la Teoría de los Mosaicos.

2.3 Teoría de las esferas

La teoría de las esferas de privacidad, desarrollada por el alemán Heinrich Hubmann en 1957 y citada por (Piña Libien, 2024), es un enfoque conceptual para entender y proteger la privacidad de las personas. Esta teoría se enfoca en dividir la vida de un individuo en varias esferas o ámbitos, cada uno con diferentes niveles de privacidad y accesibilidad diferente.

La teoría de las esferas plantea que las personas tienen diferentes capas o áreas de su vida, como el trabajo, la familia, la salud, las finanzas, entre otras. Cada una de estas esferas puede contener información sensible y personal. Sin embargo, cuando se combinan diferentes esferas, se puede revelar información mucho más detallada y personalizada, lo que puede afectar la privacidad de una persona.

En otras palabras, la premisa es que la información obtenida de diferentes fuentes puede ser correlacionada y utilizada para inferir información personal y sensible.

Esto puede ocurrir incluso si cada fuente individualmente no contiene información suficiente para identificar a una persona.

Por lo tanto, la teoría de las esferas destaca la importancia de establecer salvaguardias y protecciones adecuadas para garantizar la privacidad y la protección de datos personales en un entorno donde la combinación de diferentes fuentes de información puede representar un riesgo para la privacidad de las personas.

La teoría de las esferas se basa en el reconocimiento de que las personas tienen diferentes áreas de su vida que son independientes entre sí, pero que juntas pueden revelar información más detallada y personalizada. Estas esferas pueden incluir aspectos como la salud, las finanzas, las relaciones personales, la ubicación, las preferencias, entre otros.

La premisa subyacente es que, aunque cada esfera individualmente puede contener información que no es necesariamente identificable, cuando se combinan diferentes esferas, se puede extraer conclusiones más precisas y detalladas sobre una persona. Por ejemplo, si se combina la información sobre la ubicación de una persona con sus compras en línea, se puede inferir información sobre sus hábitos de consumo y preferencias personales.

A continuación, se describe en detalle esta teoría:

En esta teoría, se distinguen primeramente tres esferas distintas:

- Esfera Íntima, es el círculo más cercano a la intimidad de una persona y contiene la información más privada y personal, como pensamientos, sentimientos y relaciones íntimas. Es la esfera con el mayor nivel de protección.

- Esfera Privada: es el segundo círculo que incluye datos personales que uno comparte con un círculo limitado de personas, como amigos y familiares.

- Esfera Pública: es el tercer círculo que según el autor Heinrich Hubmann es la información accesible públicamente, como la información disponible en redes sociales públicas o registros públicos.

Es de desatacar que dentro de esta teoría cada esfera requiere diferentes niveles de protección y control sobre quién puede acceder a la información contenida en ella. La teoría sostiene que las personas deben tener la capacidad de controlar quién tiene acceso a qué tipo de información en cada esfera.

Siguiendo con el análisis de esta teoría, es dable reconoce que las esferas no son completamente independientes, sino que hay interacción y acoplamiento entre ellas, y que la información puede moverse de una esfera a otra, lo que requiere mecanismos adecuados para gestionar estos flujos de información.

La teoría de las esferas proporciona un marco útil para entender y gestionar la privacidad en la era digital. Al dividir la vida en diferentes esferas con distintos niveles de protección y accesibilidad, esta teoría permite un enfoque más matizado y adaptable a la protección de datos personales. Sin embargo, la implementación efectiva de esta teoría requiere un esfuerzo coordinado entre legisladores, diseñadores de tecnología y usuarios.

2.4 Teoría de los mosaicos

Esta teoría fue creada por Fernando Madrid Conesa en 1984, la teoría de los mosaicos para el jurista Hiram Raúl Piña Libien, citada en la Obra Diálogos Jurídicos entre España Y México, al igual que otras interpretaciones de la teoría de los mosaicos en el contexto de la protección de datos personales, trata sobre la idea de que datos aparentemente inocuos o no identificables, cuando se combinan con otros

datos, pueden revelar información sensible o identificable sobre una persona. Esta teoría subraya la importancia de considerar la re-identificación y el contexto en el manejo de datos personales.

De manera enunciativa más no limitativa, se agregan algunos ejemplos:

1. **Datos de Salud:**

Datos médicos anonimizados pueden no identificar a una persona por sí solos. Sin embargo, si estos datos se combinan con registros de seguros, historiales de medicación y otras bases de datos, pueden permitir la identificación de individuos y revelar información médica sensible.

2. **Datos de Geolocalización:**

Los datos de ubicación por sí solos pueden parecer inofensivos, pero cuando se combinan con otros datos (como patrones de movilidad y datos de redes sociales), pueden identificar a una persona y rastrear sus movimientos.

3. **Datos de Navegación en Internet:**

Historiales de navegación, cookies y datos de comportamiento en línea pueden no ser identificables individualmente, pero combinados con datos de cuentas de usuario y otras bases de datos, pueden reconstruir perfiles detallados de usuarios.

La teoría de los mosaicos resalta la complejidad de la protección de datos en un entorno donde la información está fragmentada, pero puede ser combinada para formar perfiles completos de individuos. Esta teoría enfatiza la importancia de adoptar un enfoque holístico en la protección de datos, considerando no solo los datos individuales sino también sus combinaciones potenciales. Para implementar efectivamente esta teoría, es esencial una combinación de políticas robustas,

diseño de tecnologías seguras y educación continua sobre los riesgos y mejores prácticas en la protección de datos personales.

Y al tratarse de la protección de datos personales considerados como un derecho humano se vinculan adicionalmente dos teorías la Teoría de los Derechos Humanos y la Teoría del Garantismo.

2.5 Teoría de los Derechos Humanos

La protección de datos personales, si bien es un tema contemporáneo, no puede separarse de la discusión más amplia sobre los derechos humanos. Para entender completamente este derecho en particular, es esencial examinar la teoría general de los derechos humanos, que ha evolucionado a lo largo de siglos de debate, conflicto y consenso.

Desde el inicio de la civilización, las sociedades han luchado con la noción de derechos inalienables: derechos que pertenecen a todos los seres humanos, independientemente de cualquier circunstancia de nacimiento, origen, identidad o estatus (Donnelly, 2017). La Declaración Universal de Derechos Humanos, adoptada en 1948, establece que todos los seres humanos nacen libres e iguales en dignidad y derechos (Asamblea General de las Naciones Unidas, 1948). Esta declaración, aunque no es vinculante legalmente, ha sentado las bases para muchos tratados y convenios internacionales que buscan proteger y promover los derechos humanos.

Los derechos humanos, según Nickel (2018), pueden clasificarse en varias categorías, incluidos los derechos civiles, políticos, económicos, sociales y culturales. Estos derechos no son mutuamente excluyentes y a menudo están interrelacionados. Por ejemplo, el derecho a la libertad de expresión (un derecho civil y político) puede influir en el derecho a participar en la cultura de la comunidad (un derecho cultural).

En el centro de la teoría de derechos humanos se alberga el principio de la dignidad humana. Según Arendt (1958), la dignidad se refiere a la valoración intrínseca de la humanidad, independientemente de sus contribuciones, capacidades o circunstancias. Cada individuo, por el simple hecho de ser humano, tiene derecho a ser tratado con respeto y a no ser objeto de violaciones a su integridad física o moral.

Uno de los debates centrales en la teoría de derechos humanos es la universalidad frente a la relatividad. Mientras algunos argumentan que los derechos humanos son universales y aplicables a todas las culturas y sociedades (Sen, 2019), otros sostienen que estos derechos están moldeados por contextos culturales y, por lo tanto, pueden variar (Engle, 2020). A pesar de estos debates, hay un reconocimiento general de que ciertos derechos, como el derecho a la vida, son fundamentales y no deben ser violados en ninguna circunstancia.

En la era digital, el derecho a la protección de datos personales emerge como un nuevo derecho humano, enraizado en principios más antiguos de privacidad y autodeterminación (Richards, 2019). Si bien el debate sobre la protección de datos es relativamente nuevo en el panorama de los derechos humanos, refleja la continua adaptación de estos principios fundamentales a las realidades cambiantes de la sociedad.

2.6. Teoría del Garantismo

El garantismo es una ideología jurídica, que intenta representar, comprender, interpretar y explicar el derecho. La Teoría General del Garantismo se ha vinculado estrechamente con la Teoría del Estado Constitucional, desde el punto de vista normativo, y con el llamado neoconstitucionalismo, desde el punto de vista teórico.

Una de las principales ideas del garantismo es la desconfianza hacia todo tipo de poder, público o privado, nacional o internacional. El garantismo no se hace falsas

ilusiones acerca de la existencia de poderes buenos que den cumplimiento espontáneo a los derechos y prefiere verlos vinculados siempre sujetos, a vínculos jurídicos que los acoten y que preservan los derechos subjetivos sobre todo si tienen carácter de derechos fundamentales.

El garantismo tiene por nación central y articuladora precisamente la de la garantía. Ferraioli define en términos generales a una garantía como cualquier técnica normativa de tutela de un derecho subjetivo. Aunque el concepto de garantía tiene un origen vinculado al derecho civil, en el que existen garantías de tipo real y personal, su utilización se ha extendido a otras ramas del derecho y en particular al derecho constitucional. (Ferrajoli, 2006)

Precisando el concepto general que se ha citado, por garantía puede entenderse toda obligación correspondiente a un derecho subjetivo, entendiendo por derecho subjetivo toda expectativa jurídica positiva de prestaciones, o negativa de no lesiones.

Si el derecho subjetivo se traduce en una obligación de abstención por parte de uno o más sujetos, se configura entonces una garantía negativa, que obliga abstenciones a los sujetos obligados; en cambio si el derecho subjetivo se traduce en una obligación de hacer, se estaría frente a una garantía positiva, qué obliga o comisiona a los sujetos obligados.

Existe también en la categorización de Ferrajoli garantías primarias o sustanciales y garantías secundarias o jurisdiccionales, las primeras corresponden a las conductas en forma de obligaciones de hacer o prohibiciones, señaladas por los derechos objetivos garantizados, la segunda son las obligaciones que tiene el órgano jurisdiccional para sancionar o declarar la nulidad cuando conste en actos ilícitos.

A mayor abundamiento es preciso traer a colación las principales aportaciones de su teoría a fin de encontrar la vinculación con la protección de datos personales.

Empezaré por la concepción de la democracia como el marco en cual convergen los derechos fundamentales, Ferrajoli (2008) establece que la fuente de legitimación democrática de los poderes públicos es únicamente la autonomía, esto es, la libertad positiva que consiste en “gobernarse por sí mismo” y “en que la regulación de la propia conducta no dependa de otros, sino de uno”.

Esta es la versión de democracia la cual denomina formal o procedimental, puesto que la identifica con las formas y procedimientos adecuados, precisamente, para garantizar que las decisiones alcanzadas sean expresión, directa o indirecta, de la voluntad popular. La democracia, tiene que ver con el quién (el pueblo o sus representantes) y el cómo (la regla de la mayoría) de las decisiones, pero sería independiente de qué se decide, es decir, de los contenidos, aunque estos fueran antiliberales, antisociales e incluso antidemocráticos.

Dicho de otra manera, la palabra democracia indica un mundo posible, es decir, una de las formas políticas en las cuales puede ser organizada la convivencia social pero tal forma no corresponde necesariamente a la del mundo político real.

Ferrajoli (2008), establece cuatro aporías en la concepción puramente procedimental de la democracia:

1. La *primera razón* es la falta de alcance empírico, y por consiguiente, de capacidad explicativa, de una definición de democracia limitada a sus connotaciones formales, esto es, a las condiciones en las que las decisiones políticas expresan directa o indirectamente, la voluntad popular.

   En efecto, la novedad que el constitucionalismo introduce en estructura de las democracias es que también el supremo poder legislativo se

encuentra jurídicamente regulado y limitado, no sólo en lo que respecta a las formas, que garantizan a la afirmación de la voluntad de la mayoría, sino también a la sustancia de su ejercicio, vinculado al respecto de normas constitucionales específicas, como el principio de igualdad y los derechos fundamentales.

2. La *segunda razón* consiste en la escasa consistencia teórica de un concepto de democracia solamente formal que pretende ser consecuente consigo mismo. En teoría siempre es posible que con métodos democráticos se supriman, por mayoría, los principios y métodos democráticos: no sólo los derechos de libertad y los derechos sociales, sino también los derechos políticos, el pluralismo político, la división de los poderes, la representación, en otras palabras, todo el sistema de reglas que constituyen la democracia política.

3. La *tercera razón* consiste en el nexo indisoluble, que las concepciones puramente formales de la democracia ignoran entre soberanía popular, democracia política y todos los derechos fundamentales que el autor denomina “sustanciales” y que operan como límites o vínculos a la voluntad, de otro modo absoluta de la mayoría. En primer lugar, los derechos de libertad. En efecto la voluntad popular se expresa auténticamente solo sí puede expresarse libremente. Que las libertades fundamentales por parte de todos y cada uno son la libertad de pensamiento, de prensa, de información, de reunión y de asociación, por eso no existe soberanía popular sin derechos de libertad individual.
   La omnipotencia de la mayoría no solamente amenaza la democracia política y la propia soberanía popular. No existe participación en la vida pública sin garantía de mínimos vitales, es decir, de derechos a la supervivencia, ni existe formación de voluntad consciente, sin educación e información.

4. La *cuarta razón* de la insuficiencia de una noción de democracia puramente formal está vinculada a una aporía de carácter filosófico-político. La concepción formal o procedimental se asienta, como se ha dicho, en la connotación de la democracia como "autonomía" o "autogobierno" o "autodeterminación" popular, es decir, como libertad positiva del pueblo a no someterse a otras decisiones y, por tanto, otros límites o vínculos, que no sean los acordados por el mismo.

Una vez dicho lo anterior es necesario comentar que Ferrajoli (2008) replantea de manera radical la relación entre pueblo y democracia, a partir de una redefinición de la noción de soberanía popular compatible con el actual paradigma constitucional de la democracia.

Establece que para que un sistema político sea democrático, es necesario que se sustraiga constitucionalmente a la mayoría del poder de suprimir o limitar la posibilidad de qué las minorías se convierta a su vez en mayoría. Y ello a través de límites y vínculos que establezcan lo que en varias ocasiones sea denominado la "esfera de lo no decidible (qué y qué no)".

Luego entonces, la democracia consistirá únicamente en un método, es decir, en reglas procedimentales que aseguran la representatividad popular, a través del sufragio universal y del principio de la mayoría. La soberanía al pertenecer a todo el pueblo no pertenece a nadie más y ninguna persona individual o grupo de personas puede apropiarse de ella. En un segundo sentido, la fórmula de soberanía popular pertenece al pueblo quiere decir, por tanto, que pertenece al conjunto de sus ciudadanos, a todas las personas que componen el pueblo. (Ferrajoli, 2008)

Cuando se establece que la soberanía del pueblo es ilimitada, se crea y se introduce en la sociedad humana un grado de poder tan grande que es un mal con independencia de a quien se entrega.

La soberanía del pueblo no es ilimitada; está circunscrita a los límites que establecen la justicia y los derechos de los individuos. La voluntad de todo un pueblo no puede convertir en justo lo que es injusto.

De aquí que expresa que los derechos fundamentales dan forma y contenido a la soberanía popular y a la voluntad popular, la cual no puede manifestarse de manera auténtica si no puede expresarse libremente, si no dispone de garantías no sólo para derechos políticos sino también para los derechos de libertad y para los derechos sociales.

Fórmula que la soberanía popular pertenece al pueblo, por tanto, pertenece al conjunto de sus ciudadanos, a todas las personas que lo componen. Esto significa, en concreto, que la soberanía popular no es otra cosa que la suma de poderes y contrapoderes de todos los derechos políticos, civiles, sociales y de libertad que la Constitución estipula como derechos fundamentales. Estos derechos, no son solo límites a la democracia política, sino que son la sustancia democrática, puesto que se refiere al pueblo en un sentido más concreto y vinculante que la propia representación política.

Es menester apuntar que la lógica de Ferrajoli permite entender que los derechos fundamentales son la esencia de la soberanía y la voluntad popular, y para que estas pueden expresarse libremente se debe disponer de garantías.

Así, las garantías constitucionales de los derechos fundamentales son también garantías de la democracia. Ferrajoli articula la noción de la democracia constitucional a partir de su relación con las cuatro clases de derechos en las cuales, a su vez, ha dividido la categoría de derechos fundamentales: la democracia política, asegurada por la garantía de los derechos políticos; la democracia civil, asegurada por la garantía de los derechos civiles; la democracia liberal asegurada por la garantía de los derechos de libertad; la democracia social, asegurada por la garantía de los derechos sociales.

El garantismo, explicado en sus cuatro dimensiones política, civil, liberal y social, dependiendo de la clase de los derechos garantizados, constituye el presupuesto jurídico de la democracia.

2.6.1. ¿Qué son las garantías?

Es así que llegamos al significado que le otorgó a las garantías de *obligaciones y prohibiciones,* que corresponden a las expectativas positivas y negativas establecidas normativamente, en este orden de ideas es pertinente referirnos a las garantías negativas las cuales designan las prohibiciones que corresponden a las expectativas negativas y de garantías positivas para designar a las obligaciones que corresponden a las expectativas positivas, además de señalar que las garantías primarias son la suma de las garantías positivas y de las negativas, y las garantías secundarias designan las garantías de justiciabilidad que intervienen en caso de vulneración de las expectativas normativas y de sus garantías primarias. (Ferrajoli, 2008).

Las garantías negativas consisten en la prohibición de derogar; las garantías positivas en la obligación de aplicar lo que las normas constitucionales disponen.

Las *garantías constitucionales negativas*, las que consisten en prohibiciones, son dos:

a) Las normas sobre la reforma constitucional, que excluyen toda la reforma o que sólo la permiten mediante procedimientos más gravosos que los previstos para las leyes ordinarias.
b) Las normas sobre el control jurisdiccional de constitucionalidad de los preceptos, por comisión u omisión, por razones de forma donde sustancia contrarios a las normas constitucionales. Consisten en la anulación de esa aplicación de las normas legales contrarias a las normas constitucionales y que violen, por tanto, su garantía negativa primaria.

Estas garantías constitucionales negativas, se refieren a las facultades que la propia constitución confiere al legislador a través del procedimiento legislativo agravado, la facultad de producir normas legales que violen o deroguen normas constitucionales. Las *garantías constitucionales negativas secundarias*, consisten en el control jurisdiccional de constitucionalidad, pueden ser más o menos incisivas. Desde el punto de vista histórico, se han desarrollado dos tipos de control de justicia sobre la legitimidad de las leyes:

a. El control difuso, que han expuesto en los Estados Unidos y en otros ordenamientos americanos y que consisten en la nueva aplicación en el caso concreto, aunque no esté en la anulación, de la norma inconstitucional.
b. El control concentrado, difundido en Italia y en otros muchos países europeos en la segunda posguerra, a partir del modelo que el Kelseniano.

Existe diferenciación de las garantías constitucionales negativas primarias y por otro lado siempre tenido lugar o no en ausencia de diseño teórico alguno.

Sería necesario extender a otros sujetos, además de a los jueces a que, la legitimación para elevar la cuestión de inconstitucionalidad. Pienso en la figura del juicio de amparo, presente en muchos ordenamientos latinoamericanos y en el español, y que puede ser activado por cualquier individuo contra cualquier medida que dañe un derecho constitucionalmente establecido.

Del otro lado de la moneda encontramos las garantías constitucionales positivas, estas garantías consisten en la obligación que tiene el legislador, como correlato de la estipulación de los derechos, de desarrollar una legislación de aplicación a los mismos.

Las normas existen si se han establecido o producido, y no debido a un arbitrario teórico como si la teoría pudiese desarrollar funciones legislativas. La obligación de una legislación de desarrollo consiste en la introducción de las garantías primarias y secundarias ausentes lo que completa la garantía constitucional positiva de los derechos constitucionalmente establecidos. Esta obligación de una legislación de aplicación precisamente es la garantía constitucional positiva primaria de los derechos constitucionalmente establecidos. Se trata, ciertamente, de una garantía débil bajo un doble aspecto. En primer lugar, por la dificultad de asegurar su eficacia a través de una garantía constitucional positiva secundaria como se dice control jurisdiccional de una constitucionalidad de las lagunas.

2.6.2. Derechos fundamentales

Como se ha señalado en líneas anteriores los derechos fundamentales dan forma y contenido a la soberanía popular y a la voluntad popular, así las garantías constitucionales de los derechos fundamentales son también garantías de la democracia; pero qué son los derechos fundamentales, Ferrajoli (2009) señala que son aquellos “derechos intrínsecos que corresponden universalmente a todos los seres humanos en cuanto dotados del status de personas, de ciudadanos o personas con capacidad de obrar; entendiendo por derecho subjetivo cualquier expectativa positiva (de prestaciones) o negativa (de no sufrir lesiones) adscrita a un sujeto por una norma jurídica.”

Apunta que son fundamentales los derechos adscritos por un ordenamiento jurídico a todas las personas físicas, en cuanto a su calidad de ciudadanos o en cuanto a su capacidad de obrar. (Ferrajoli, 2009) y agrega que los derechos fundamentales son derechos indisponibles, inalienables, inviolables, intransigibles, y personalísimos.

Bajo esta tesitura, los derechos al ser universales y al establecer que son de todos, constituyen elementos de distinción entre los derechos fundamentales y los que no son derechos fundamentales.

Refiere que la personalidad, ciudadanía y capacidad de obrar, son condiciones de la igual titularidad de todos los derechos fundamentales, son consecuentemente los parámetros tanto de la igualdad como de la desigualdad. La ciudanía y la capacidad de obrar han quedado hoy como las únicas diferencias de estatus que aún delimitan la igualdad de las personas humanas.

En cambio, la distinción entre derechos civiles, derechos políticos, derechos de libertad y derechos sociales hace referencia a su estructura: los derechos civiles y los políticos son, además de expectativas negativas (de su no lesión), poderes para realizar actos de autonomía en la esfera privada y en la esfera política, respectivamente.

En torno a su definición de derechos fundamentales esta sienta su base en cuatro tesis, esenciales para la teoría de la democracia constitucional.

La primera remite a la radical diferencia de estructura entre los derechos fundamentales y los derechos patrimoniales, concernientes los unos a enteras clases de sujetos y los otros a cada uno de sus titulares con exclusión de todos los demás.

La segunda tesis es que los derechos fundamentales, al corresponder a intereses y expectativas de todos, forman el fundamento y el parámetro de la igualdad jurídica y por ello de la que llamaré dimensión «sustancial» de la democracia, previa a la dimensión política o «formal» de ésta, fundada en cambio sobre los poderes de la mayoría.

La tercera tesis hace referencia al génesis supranacional de la mayoría de los derechos fundamentales. Se ha visto cómo nuestra definición proporciona los criterios de una tipología de tales derechos dentro de la que los «derechos de ciudadanía» forman solamente una subclase.

Finalmente, la cuarta tesis, quizá la más influyente, tiene que ver con las relaciones entre los derechos y sus garantías. Los derechos fundamentales, de la misma manera que los demás derechos, consisten en expectativas negativas o positivas a las que corresponden obligaciones (de prestación) o prohibiciones (de lesión).

Se trata de cuatro diferencias que prescinden del contenido de las dos clases de derechos y que únicamente tienen que ver con su forma o estructura.

Los derechos fundamentales son indisponibles, quiere decir que están sustraídos tanto a las decisiones de la política como al mercado. En virtud de su indisponibilidad activa, no son alienables por el sujeto que es su titular: no puedo vender mi libertad personal o mi derecho de sufragio y menos aún mi propia autonomía contractual.

Las necesidades protegidas por los derechos fundamentales son consecuencia de sus características de universalidad, igualdad, indisponibilidad, atribución *ex lege* y rango habitualmente constitucional y por ello *supra* ordenado a los poderes públicos como parámetros de validez de su ejercicio.

Los derechos fundamentales, a diferencia de los demás derechos, vienen a configurarse como otros tantos vínculos sustanciales normativamente impuestos en garantía de intereses y necesidades de todos estipulados como vitales, por eso fundamentales (la vida, la libertad, la subsistencia) tanto a las decisiones de la mayoría como al libre mercado.

El paradigma de la democracia constitucional no es otro que la sujeción al derecho generada por esa disociación entre vigencia y validez, entre mera legalidad y estricta legalidad, entre forma y sustancia, entre legitimación formal y legitimación sustancial o, si se quiere, entre la weberiana «racionalidad formal» y «racionalidad material».

Después del nacimiento de la ONU, y gracias a la aprobación de cartas y convenciones internacionales sobre derechos humanos, estos derechos son fundamentales no sólo dentro de los Estados en cuyas constituciones se encuentran formulados, son derechos supra-estatales a los que los Estados están vinculados y subordinados también en el plano del derecho internacional; no, pues, derechos de ciudadanía, sino derechos de las personas con independencia de sus diversas ciudadanías.

Un derecho existe si las normas que lo contemplen han sido producidas por el legislador siguiendo las reglas procesales y de competencia previstas para su producción. Si un derecho carece de garantías —si no lo tutelan o aplican las autoridades competentes, no hay una laguna o incumplimiento normativo.

En este caso considero que no podría definirse “letra muerta” el plasmar un derecho en un ordenamiento jurídico que no está dotado de mínimos necesarios para garantizar su ejecución.

La eficacia de las normas sobre su existencia o validez, se inclinan a declarar la inexistencia de un derecho fundamental, si resulta ineficaz.

Ferrajoli (2009), hace una distinción entre derechos de libertad y derechos de autonomía, entre libertad negativa y libertad positiva, que se remonta a Benjamin Constant y que han sido retomadas por Norberto Bobbio. La libertad negativa, es la libertad como no impedimento o no constricción, que es un predicado de la acción; la libertad positiva es la libertad como autodeterminación autonomía, que

es un predicado de la voluntad. La primera es la libertad de inmunidad o libertad de: el área, el ámbito en el que un hombre puede actuar sin ser obstaculizado; la segunda es la facultad o libertad que consiste en ser dueño de sí mismo.

Hablando de las dos libertades en términos homogéneos, con referencia en ambos casos del derecho positivo, es decir, en sentido jurídico, la libertad jurídicamente tutelada implica la autonomía también tutelada jurídicamente y viceversa. En otras palabras, las dos libertades coinciden jurídicamente. La distinción entre las dos libertades vale terreno moral pero no en el jurídico. Sólo en el plano moral pero no en el jurídico, no es redundante, afirmar tanto la una como la otra, del mismo modo que no es contradictoria afirmar una y negar la otra.

Existen, sin embargo, otros dos significados, bastante restringidos y específicamente jurídicos, tanto de la libertad negativa como de la positiva, que se distinguen por ser, ellos sí, independientes uno de otro. Es por un lado de esas libertades negativas que son los derechos fundamentales de libertad y quedan sustraídas en términos establecidos y universales, a la autonomía privada y, cuando gozan de rango constitucional, a la política.

Entendidos en este sentido, libertad y autonomía son figuras jurídicas distintas, no reducibles entre sí y susceptibles de subsistir con independencia una de otras.

La principal premisa del garantismo es que todo ejercicio del poder debe estar vinculado y limitado por normas y procedimientos que aseguren los derechos fundamentales de los individuos (Ferrajoli, 2007). El poder del Estado, o de cualquier entidad, no puede ser absoluto ni arbitrario, sino que debe ejercerse en un marco normativo que garantice los derechos y libertades de las personas.

El garantismo no sólo se enfoca en los derechos tradicionales, como los derechos civiles y políticos, sino que también subraya la importancia de garantizar derechos sociales, económicos y culturales. Estas garantías no son meras declaraciones de

intenciones, sino que deben tener mecanismos efectivos de protección y realización, lo que significa que el Estado tiene la obligación no sólo de respetar estos derechos, sino también de protegerlos y cumplirlos (Gargarella, 2010).

Un aspecto esencial del garantismo es la distinción entre norma y hecho. Mientras que las normas definen cómo deberían ser las cosas en un sistema jurídico ideal, la realidad a menudo se desvía de estos ideales. Por ello, el garantismo subraya la necesidad de mecanismos de control que aseguren que las normas se respeten en la práctica y que existan remedios efectivos cuando se violen (Zagrebelsky, 2012).

En el contexto de la protección de datos personales, el garantismo se manifestaría en la necesidad de garantizar que, más allá de las leyes y reglamentos que establezcan la protección de estos datos, existan mecanismos efectivos que aseguren su cumplimiento. Esto podría incluir la existencia de organismos de supervisión independientes, procedimientos claros para la denuncia de violaciones y sanciones efectivas para aquellos que no respeten las normas de protección de datos.

El garantismo jurídico de Ferrajoli propone una estructura de límites precisos para proteger las libertades individuales, y en el ámbito contemporáneo es una referencia esencial para entender las dinámicas entre poder, ley y derechos (Ferrajoli, 2007). Esta teoría se desarrolló inicialmente en el contexto penal, subrayando la necesidad de garantías procesales y sustantivas para los acusados. Sin embargo, su relevancia ha trascendido ese campo específico y ha informado debates en otros ámbitos del derecho y la justicia.

El principio garantista impone la noción de que la dignidad de la persona humana y sus derechos fundamentales deben ser siempre prioritarios y protegidos frente a cualquier acto de poder. Además, propugna por la máxima realización de derechos fundamentales y la mínima intervención punitiva, es decir, se debe buscar la máxima eficacia de los derechos y la mínima restricción de libertades (Bobbio, 2019).

En esta misma línea, el garantismo plantea que las normas no solo deben ser claras y precisas, sino que también deben ser justas y proporcionadas. Es decir, las leyes deben establecerse de manera que no limiten los derechos más allá de lo necesario para proteger otros derechos o intereses legítimos (Dworkin, 2018).

Con la llegada de las tecnologías de la información y la comunicación, y la creciente acumulación de datos personales por entidades tanto públicas como privadas, el garantismo encuentra un nuevo escenario en el que desplegar sus principios. El manejo de datos personales, en muchos casos, implica un ejercicio de poder que puede tener repercusiones significativas en los derechos de los individuos. En este contexto, la teoría garantista exige transparencia, responsabilidad y control en el manejo de datos, asegurando que los individuos no solo tengan acceso a la información sobre cómo se recopilan, almacenan y utilizan sus datos, sino también que tengan medios efectivos para controlar y, si es necesario, corregir o eliminar esa información (Pasquale, 2020).

El diálogo entre garantismo y protección de datos personales no solo refuerza la necesidad de una regulación estricta y mecanismos de control, sino también de una cultura de respeto a la privacidad y autodeterminación informativa. Las entidades, ya sean públicas o privadas, no solo deben adherirse a la letra de la ley, sino también adoptar una postura ética que priorice los derechos de los individuos por encima de intereses comerciales o gubernamentales (Rosen, 2021).

La protección de los derechos fundamentales en el marco garantista se proyecta como una barrera infranqueable frente a potenciales excesos y arbitrariedades. Esto es relevante cuando la información se ha convertido en mercancía y en una herramienta de poder. Las dinámicas actuales, caracterizadas por la interconexión global y el avance vertiginoso de la tecnología, demandan una revisión constante y adaptativa de las garantías (Zuboff, 2019).

El garantismo, en este contexto, también pone de manifiesto la relación entre el Estado de Derecho y el respeto a los derechos fundamentales. Es un recordatorio constante de que las leyes y normativas deben ser instrumentos de protección y no herramientas de opresión o control desmedido (Habermas, 2018). La democratización del acceso a la información y la capacidad de los individuos para decidir sobre sus propios datos personales son ejemplos concretos de cómo el garantismo puede materializarse en la era digital.

Además, esta teoría se alinea con la idea de que no solo se deben establecer leyes y regulaciones, sino también fomentar prácticas y comportamientos éticos. En el mundo de la protección de datos, esto implica que las empresas y organizaciones no solo cumplan con las regulaciones, sino que adopten una postura proactiva para garantizar que los derechos de los usuarios estén en el centro de sus operaciones y decisiones (O'Neil, 2017).

También mencionar que el garantismo propone un enfoque multidimensional y no se limita únicamente a garantías judiciales o legislativas, sino que se extiende a garantías sociales, culturales y educativas. La educación sobre derechos digitales y el conocimiento sobre cómo proteger la privacidad y la información personal se vuelven esenciales en este nuevo paradigma (Westin, 2017).

Las teorías de los Derechos Humanos y Derechos Fundamentales que se abordaron en el presente trabajo de investigación fueron tomados para su estudio debido a que el derecho a la protección de datos personales es un derecho fundamental consagrado en el artículo 16 párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, y de ella emana la protección de una persona a su integridad y a sus datos personales, y que el estado debe garantizar con las disposiciones normativas y la creación de Órganos Garantes capaces de proteger datos personales de toda persona que radique en México, independientemente de su origen étnico o racial. Situación que en el capítulo cuarto será abordada para saber si hasta el día de hoy y a veinte años de su

Constitucionalización, el estado mexicano a través de sus órganos de gobierno ha logrado una profunda protección de datos personales o aún falta por mejorar y aprender de otros países más avanzados, como en su momento México lo hizo al implementar las diferentes legislaciones que se ocupan de la protección de datos personales en la Unión Europea y hacer su propia legislación.

Es de reconocer, que se advierte que el legislador si bien es cierto creó una Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, también lo es que los legisladores no adaptaron o no se contempló su aplicabilidad en la sociedad mexicana.

CAPÍTULO TERCERO
REGULACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES

3.1 Naturaleza jurídica de los datos personales en la normativa internacional

El derecho internacional surge como respuesta a la necesidad de regular las relaciones entre los Estados, para evitar conflictos y obtener la mayor cantidad de beneficios, respecto de actividades fuera de las fronteras, y regular sobre temas de interés común relacionados, para el caso que nos ocupa aquellos que tienen que ver con la protección de datos personales.

El tránsito de las sociedades a sociedades tecnológicas requiere de regulaciones que favorezcan la protección de los datos personales, un tema que concierne a los Estados como entes particulares por el intercambio transfronterizo de datos personales. A continuación, se presentan los instrumentos internacionales que forman las bases de la protección de datos como Derechos Humanos.

3.1.1 Declaración Universal de los Derechos Humanos

La Declaración Universal de los Derechos Humanos es un documento adoptado por la Asamblea General de las Naciones Unidas en 1948, es un plan de acción universal para la libertad e igualdad, protegiendo los derechos inherentes a las personas.

Dicha declaración protege más 30 derechos y libertades, (Unidas O. d., 2023), dentro de estos, encontramos el marcado con el número 12, en el que se consagra el derecho a la privacidad, tal y como se aprecia:

> “Artículo 12. Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques

> a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."[5]

Con ello los Estados miembros cuentan con una base para legislar en la materia de protección de datos personales al interior de sus demarcaciones, este texto pretende resguardar la privacidad y los datos personales de cada persona, sin importar los bordes fronterizos. En dicha cita se garantiza que todas las personas del mundo alcancen la libertad, la igualdad y la dignidad y dentro de las cuales se encuentra el derecho a la protección de datos personales.

La declaración universal de los derechos humanos es el documento que garantiza la libertad, la justicia y la paz en el mundo, tienen por base el reconocimiento de la dignidad intrínseca y de los derechos iguales e inalienables de todos los miembros de la familia humana (Unidas O.d., 2023).

En esencia, este ordenamiento protege los derechos humanos por un régimen de Derecho, a fin de que el hombre este protegido de las extralimitaciones del propio hombre, en materia de protección de datos este es un gran paso, la comunidad internacional reconoce el derecho a la intimidad como un derecho fundamental, además de que le concede un valor agregado al ser vinculado con la dignidad, la honra y la reputación, y como se dijo en líneas anteriores es la puerta de entrada para que la comunidad internacional promueva el desarrollo de relaciones robustas que permitan un mejor manejo de datos personales.

Para fortalecer este entramado jurídico surgen otros ordenamientos como el Pacto Internacional de Derechos Civiles y Políticos.

[5] Declaración universal de los Derechos humanos. Véase en https://www.un.org/es/about-us/universal-declaration-of-human-rights

3.1.2 Pacto Internacional de Derechos Civiles y Políticos

En el año de 1948, se firmó el Pacto Internacional de los Derechos Civiles y Políticos, el cual pretende garantizar el derecho a la autodeterminación de los países, sin perjuicio a la protección de los derechos humanos. En este documento se otorgaba la prerrogativa de salvaguardar la vida privada de las personas y del núcleo familiar que rodea al o la titular de los datos personales, así como la reputación y honra de todas y cada una de las personas, tal como se aprecia en su artículo 17°, mismo que a continuación se transcribe:

> "Artículo 17°
>
> 1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
>
> 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques"[6]

De la interpretación armónica al artículo que antecede se aprecia que este ordenamiento jurídico internacional, retoma lo normado por la Asamblea General de las Naciones Unidas y da la pauta para que los Estados, dentro de sus soberanías, contemplen el derecho a la protección de los datos personales y a la privacidad de las personas.

Luego entonces, se tiene que el Derecho a la Protección de Datos Personales, Privacidad e Intimidad, es reconocido con anterioridad, y que al día de hoy con el avance tecnológico y social con mayor razón se debe salvaguardar.

---

[6] Pacto Internacional de Derechos Civiles y Políticos.- véase en https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

3.1.3 Convención Americana sobre Derechos Humanos (Pacto de San José).

Es notable hacer mención que el citado instrumento internacional entró en vigor el 23 de marzo de 1976, y ha sido ratificado por 173 países miembros (Unidas O. d., 2023), ello derivado de la evolución en el marco jurídico internacional con relación a la protección de los derechos humanos civiles y políticos, asimismo se tiene que los estados de Latinoamérica, no se quedaron atrás y fue así como en San José, Costa Rica, se aprobó la Convención Americana sobre Derechos Humanos cuyo propósito es consolidar un régimen de libertad personal y de justicia social que se fundó en el respeto de los derechos esenciales del hombre.(1948)

Es así que, a través de dicho ordenamiento particularmente en su artículo 11°, se considera el derecho a la protección de datos personales, a la honra y a la dignidad de las personas, tal y como se aprecia enseguida:

> "Artículo 11. Protección de la Honra y de la Dignidad
>
> 1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
>
> 2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
>
> 3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."

Con lo anterior, se observa que los estados Latinoamericanos con la finalidad de estar a la vanguardia normativa en materia de protección de datos personales y competir con ordenamientos internacionales de mayor jerarquía contempló la protección a los datos personales, no solo del titular sino también los de su familia,

el respeto a la vida privada de las personas y no solo eso, sino que fue más allá al considerar que el interceptar las comunicaciones, era una intromisión a la intimidad.

3.1.4 Convenio N° 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y Protocolo Adicional al Convenio para la Protección de las Personas

Este convenio nació el 01 de octubre de 1985, con la necesidad de establecer los principios y directrices sobre el tratamiento automatizado de datos personales. En este sentido, en el artículo primero de dicho convenio, se estableció que toda persona tiene derecho inherente a la protección de sus datos personales.

> "Artículo 1°. Derecho humano. - El derecho a la protección de datos personales es inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República"[7]

Dicho ordenamiento tiene por objetivo proteger, dentro de su territorio a cualquier persona física, sean cual sea su nacionalidad o su domicilio, así como a garantizar el respeto de sus derechos y libertades fundamentales, específicamente a su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondiente a dicha persona.

Este instrumento comprometía a los países firmantes a emanar leyes de la materia o a modificar su normatividad nacional para implementar y homologar dichos principios con todos los países miembros para recolectar y tratar con fines legítimos y no para otros propósitos.

[7] Convenio N° 108 del Consejo de Europa Para la Protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y protocolo adicional al Convenio para la protección de las personas.- véase en: http://www.oas.org/es/sla/ddi/docs/u12%20convenio%20n%20108.pdf

Este instrumento, sustancialmente refiere que solo se debe almacenar la información estrictamente indispensable y que su uso se hiciera con el fin para el que fueron recolectados, garantizando la confidencialidad de los datos sensibles; así como el acceso, rectificación de datos personales; sobre todo, a la protección en personas físicas con relación al tratamiento y a la libre circulación.

3.1.5. Red Iberoamericana de Protección de Datos Personales (RIPDP)

Esta red, surgió con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos Personales (EIPDP), celebrado en Guatemala allá por el año 2003, ante la presencia de 14 países iberoamericanos, entre ellos Canadá, México, Principado de Andorra, Reino de España, República de Argentina, República de Cabo Verde, República de Chile, República de Colombia, República de Costa Rica, República del Salvador, República de Guatemala, República Honduras, República Nicaragua, República de Panamá, República Ecuador, República Paraguay, República de Perú, República Democrática de Santo Tomé y Príncipe, República Dominicana, República Federativa de Brasil, República Oriental de Uruguay, República Portuguesa.

Cabe recordar que esta iniciativa fue el resultado del apoyo que tuvo la Declaración Final de la XIII Cumbre Iberoamericana de Jefes de Estado y De Gobierno, celebrado los días 14 y 15 de Noviembre, 2003, en donde a través de su punto 45, los Jefes de Estado y de Gobierno de los países iberoamericanos suscribieron que: “45. Asimismo, somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad.” (Bolivia, 2024), en dicha reunión se contemplaba al derecho a la protección de datos personales como un Derecho Fundamental.

La (RIPDP), se configura desde sus inicios como un foro integrador de diversos sectores, entre ellos públicos y privados con la finalidad de desarrollar proyectos relacionados con la protección de datos personales en Iberoamérica para fomentar, mantener un estrecho y permanente cambio de información y conocimientos necesarios para el desarrollo normativos y para garantizar una regulación acorde a los avances sociales y tecnológicos en materia de protección de datos personales.

De igual guisa y desde el año 2003, en colaboración con la (RIPDP), se han creado leyes generales en esta materia, en: Uruguay, México, Costa Rica, Perú, Nicaragua, Colombia, República Dominicana, Brasil y Panamá, Chile, Ecuador y El Salvador.

Por su parte, Argentina y Uruguay han obtenido el reconocimiento de la Comisión Europea como países con nivel de protección adecuada, a efectos de la transferencia de datos personales entre dichos países y la Unión Europea.

Algunos de los objetivos específicos de la (RIPD) son:

- Facilitar la cooperación entre las autoridades de protección de datos de los países iberoamericanos, promoviendo el intercambio de información y la realización de actividades conjuntas.

- Impulsar la armonización de las leyes y regulaciones de protección de datos en la región, con el fin de garantizar un nivel adecuado de protección para los derechos de las personas.

- Promover la difusión y concientización sobre los derechos y principios de protección de datos en la sociedad, a través de la realización de programas de formación y campañas de sensibilización.

- Apoyar el desarrollo de capacidades y la formación de los profesionales y funcionarios que trabajan en el ámbito de la protección de datos, con el fin de fortalecer la implementación efectiva de las leyes y regulaciones.

En este orden de ideas, y debido a la evolución de este derecho, derivan dos ideas relevantes, el primero de ellos el derecho al olvido y el derecho a la portabilidad.

El derecho al olvido es un concepto jurídico que se refiere al derecho de una persona a solicitar la eliminación o desindexación de información personal que ya no es relevante o que puede causarle perjuicio.

Para María Solage Maqueo Ramírez citado en el documento “El ejercicio del Derecho al Olvido” [el llamado derecho al olvido suele considerar el derecho de los individuos para borrar, limitar o alterar información pasada que puede conducir a errores, que resulte anacrónica o redundante, o que pueda contener datos irrelevantes, asociados a una persona.] (Guzman Camacho, 2024)

Luego entonces este derecho se basa en el principio de control sobre los propios datos personales y tiene como objetivo proteger la privacidad y la reputación de las personas. “El origen del derecho al olvido se encuentra en el marco legal y jurisprudencial de la Unión Europea, en particular en la sentencia del Tribunal de Justicia de la Unión Europea (TJUE)”, específicamente en el caso Google Spain vs. AEPD y Mario Costeja González en 2014. (Piña Libien, 2024)

En esencia, el caso se originó cuando Mario Costeja González, un ciudadano español, presentó una queja ante la AEPD contra Google y el diario La Vanguardia. Costeja González argumentó que cuando su nombre se buscaba en Google, los

resultados mostraban un anuncio de una subasta de bienes embargados de hace varios años, lo que consideraba que era una violación de su privacidad.

El (TJUE) determinó que los motores de búsqueda, como Google, son responsables del tratamiento de datos personales que aparecen en los resultados de búsqueda y, por lo tanto, deben cumplir con la legislación de protección de datos de la Unión Europea. El tribunal sostuvo que los individuos tienen el derecho a solicitar la eliminación de enlaces que contienen información personal que ya no es relevante o es inexacta. Esta sentencia tuvo un impacto significativo en el ámbito de la protección de datos y la privacidad en Internet.

Este derecho, aunque se originó en Europa, también ha sido objeto de debate y discusión en América Latina. Aunque no existe una legislación específica sobre el derecho al olvido en la mayoría de los países de la región, ha habido casos y discusiones relacionadas con la protección de datos personales y la privacidad en Internet.

A continuación, se presentan algunos antecedentes relevantes del derecho al olvido en América Latina:

- **Argentina**: En 2000, Argentina aprobó la Ley de Protección de Datos Personales, que establece los principios y las reglas para el tratamiento de datos personales. Aunque no menciona explícitamente el derecho al olvido, la ley reconoce el derecho de las personas a acceder, rectificar y suprimir sus datos personales.

- **México**: En México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, promulgada en 2010, garantiza a las personas el derecho a acceder, rectificar, cancelar y oponerse al tratamiento de sus datos personales. Aunque no se menciona específicamente el derecho al

olvido, se reconoce el derecho a cancelar o eliminar los datos personales cuando ya no sean necesarios para la finalidad para la cual fueron recabados.

- **Brasil**: En Brasil, la Ley General de Protección de Datos (LGPD), que entró en vigor en 2020, establece los principios y las reglas para el tratamiento de datos personales. La LGPD reconoce el derecho de los titulares de datos a solicitar la eliminación de datos personales que sean innecesarios, excesivos o tratados en violación de la ley. Aunque no se menciona explícitamente el derecho al olvido, se reconoce el derecho a la supresión de datos en determinadas circunstancias.

Es importante destacar que, a pesar de la ausencia de legislación específica sobre el derecho al olvido en la mayoría de los países de América Latina, los tribunales y las autoridades de protección de datos han abordado casos relacionados con la eliminación de información personal de motores de búsqueda y redes sociales. Estos casos se basan en los principios de protección de datos y privacidad establecidos en las leyes nacionales y los tratados internacionales de derechos humanos.

Ahora bien, por lo que respecta al derecho a la portabilidad, este encuentra su génesis en el marco de la "XXV Cumbre Iberoamericana de Jefes de Estado y de Gobierno", llevado a cabo en Cartagena de Indias, Colombia, durante los días 28 y 29 de octubre de 2016 y se puede definir como "Es el derecho del afectado a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado" (Personales, 2024).

El derecho a la portabilidad de los datos personales es otro derecho relacionado con la protección de datos. Este derecho permite a las personas solicitar que sus

datos personales sean transferidos de una organización a otra en un formato estructurado, de uso común y lectura mecánica.

El objetivo de este derecho es facilitar la movilidad de los datos y empoderar a los individuos para que puedan controlar y gestionar su información personal.

Para salvaguardar este derecho, la (RIPD), formuló y aprobó los “Estándares de Protección de datos para los países Iberoamericanos”, cuyo principal objetivo, es “establecer un conjunto de principios y derechos de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de garantizar un debido tratamiento de los datos personales y contar con reglas homogéneas en la región” [8]

Es así que este derecho quedó normado en dichos Estándares específicamente en sus artículos 30, 30.1, 30.2, 30.3 y 30.4, los cuales se insertan para su pronta referencia:

> “30. Derecho a la portabilidad de los datos personales
>
> 30.1. Cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera.
>
> 30.2. El titular podrá solicitar que sus datos personales se transfieran directamente de responsable a responsable cuando sea técnicamente posible.
>
> 30.3. El derecho a la portabilidad de los datos personales no afectará negativamente a los derechos y libertades de otros.

[8] Red Iberoamericana de Protección de Datos. Estándares de protección de datos para los países Iberoamericanos.

> 30.4. Sin perjuicio de otros derechos del titular, el derecho a la portabilidad de los datos personales no resultará procedente cuando se trate de información inferida, derivada, creada, generada u obtenida a partir del análisis o tratamiento efectuado por el responsable con base en los datos personales proporcionados por el titular, como es el caso de los datos personales que hubieren sido sometidos a un proceso de personalización, recomendación, categorización o creación de perfiles."

Sin embargo, el derecho a la portabilidad de los datos personales en América Latina está en desarrollo y varía significativamente entre países independientemente de que la (RIPD), obliga a los países miembros a cumplir con esta obligación para salvaguardar el derecho a la portabilidad de datos personales.

A continuación, se presentan algunos ejemplos de cómo se está implementando este derecho en los países de la región:

Argentina fue uno de los primeros países de América Latina en promulgar una ley de protección de datos, la Ley de Protección de los Datos Personales la Ley N° 25.326 en 2000. Si bien la ley original no incluía explícitamente el derecho a la portabilidad de datos, en años recientes se han realizado esfuerzos para actualizarla y alinearla más con el RGPD de la UE, incluyendo conceptos como la portabilidad.

Brasil promulgó la Ley General de Protección de Datos en 2018, que entró en vigor en 2020. La LGPD incluye el derecho a la portabilidad de datos, permitiendo a los individuos solicitar la transferencia de sus datos personales a otro proveedor de servicios o productos, de manera similar al RGPD.

México cuenta con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) desde 2010. La ley no incluye de manera explícita el derecho a la portabilidad, pero contempla derechos como el acceso, rectificación,

cancelación y oposición (derechos ARCO). La discusión sobre la inclusión de la portabilidad en futuras reformas está en curso.

En Chile, la Ley sobre Protección de la Vida Privada, Ley N° 19.628 de 1999 no contempla explícitamente el derecho a la portabilidad de datos. Sin embargo, se han presentado varias propuestas para reformar y modernizar la legislación de protección de datos, incluyendo la incorporación de derechos como la portabilidad.

Uruguay tiene una legislación avanzada en protección de datos con la Ley de Protección de Datos Personales (Ley N° 18.331) desde 2008. Al igual que en otros países de la región, la portabilidad no está explícitamente mencionada, pero hay un marco general que permite la protección y control de los datos personales.

Otros países de América Latina, como Colombia, Perú y Costa Rica, están en diferentes etapas de desarrollo y modernización de sus leyes de protección de datos. Estos esfuerzos a menudo incluyen discusiones sobre la incorporación de derechos modernos como la portabilidad de datos.

Ahora, dentro de este derecho se encuentran algunos desafíos y oportunidades, entre ellos:

Desafíos: Implementar el derecho a la portabilidad en América Latina enfrenta desafíos como la infraestructura tecnológica, la falta de estandarización y la necesidad de crear conciencia tanto entre los consumidores como en las empresas.

Oportunidades: La portabilidad de datos puede fomentar la competencia y la innovación en el mercado, dando a los consumidores más control sobre sus datos y permitiendo la creación de nuevos servicios.

Para finalizar, el derecho a la portabilidad de datos personales en América Latina está en evolución. Mientras que algunos países han avanzado más que otros, la tendencia general es hacia la modernización de las leyes de protección de datos para alinearlas con estándares internacionales como el RGPD. Esto representa un paso importante para la protección de la privacidad y los derechos de los individuos en la región.

De manera especial, se analizaron tres países Argentina, Brasil y Chile; por lo importante de sus legislaciones en la materia; para el caso de Brasil se revisaron las principales características y funciones de la Autoridad Nacional de Protección de Datos Personales de Brasil, la Dirección Nacional de Protección de Datos Personales de Argentina y la Agencia de Protección de Datos Personales de Chile, que como ya se ha analizado en líneas anteriores, son organismos especializados en la protección de datos personales e independientes de otro derecho como es el acceso a la información pública y de la política pública de transparencia.

En Brasil, el marco normativo sobre protección de datos y privacidad se encuentra en la Constitución Federal, ahí se consagra la inviolabilidad de la intimidad y la vida privada, la correspondencia y los datos telegráficos, y las comunicaciones telefónicas; por ello se crean bajo este contexto diversas normativas como:

1. La Ley 9.507 de 1997 que regula el derecho de acceso a la información en poder del Estado;
2. El Código de Defensa del Consumidor, que garantiza a las personas no solo poder acceder a sus datos personales contenidos en registros y archivos, sino también a un debido tratamiento de esta información; en la Ley Positiva de Registro.
3. Ley 12.414 de 2011, que resguarda la formación y consulta de bases de datos con información e historial crediticio de personas naturales o jurídicas; en la Ley de Acceso a la Información

4. Ley 12.527 de 2011, que define el concepto de información personal como aquella relacionada con una persona identificada o identificable; y en el Marco de Derechos Civiles en Internet
5. Ley 12.965 de 2014, que no obstante delimitar responsabilidades en el entorno web, no logró garantizar la privacidad y protección de datos de manera integral, completa y estructurada.

La Ley 13.709 merece un pronunciamiento especial, se refiere al tratamiento de cualquier tipo de registro personal o base de datos, física o electrónica, que tenga cualquier entidad pública o privada, y cómo debe ser tratada esta información, en cuanto a su recolección, producción, recepción, clasificación, uso, acceso, reproducción, transmisión, distribución, procesamiento, archivo, almacenamiento, eliminación, evaluación o control, modificación, comunicación, transferencia, difusión o extracción.

Esta ley se aprobó en agosto de 2018, cuyo objetivo, además de resguardar los datos de las personas, es proteger el flujo de datos existentes entre los países miembros y las transferencias que se desarrollen con destinos fuera de sus fronteras.

La Ley General de Protección de Datos Personales, por su parte, regula cómo serán tratados los datos personales en el país y en el exterior, pero solo si esta información a que sido extraída o el titular se encuentra en Brasil.

La ley de protección de datos brasileña, en armonización con las directrices mundiales, se apoya en los siguientes principios: “a) respeto a la privacidad y autodeterminación informativa; b) libertad de expresión, información, comunicación y opinión; c) inviolabilidad de la intimidad, el honor y la imagen; d) desarrollo económico, tecnológico e innovación; e) libre iniciativa, libre competencia y protección al consumidor; y f) protección a los derechos humanos, el libre desarrollo

de la personalidad, la dignidad y el ejercicio de la ciudadanía por parte de las personas naturales.” (Ley 13.709), artículos 55 a 59.

Un aspecto importante a considerar en esta ley es el veto que se hizo de los artículos que crearon tanto la Autoridad Nacional como el Consejo Nacional de Protección de Datos (artículos 55 a 59 de la Ley 13.709), siendo la ley sancionada sin el establecimiento de un organismo regulador y supervisor de las determinaciones contenidas en sus disposiciones.

Además, la ley establece los derechos de los titulares, los criterios para el uso y tratamiento de los datos personales, los agentes que podrán utilizarlos, las sanciones por el incumplimiento de sus disposiciones y, previa aprobación de la Ley 13.853 de 2019, la creación de la Autoridad Nacional de Protección de Datos.

La ANPD es un organismo independiente, con autonomía técnica y decisional en el ejercicio de sus funciones.
Ahora bien, la Dirección Nacional de Protección de Datos Personales de Argentina (DNPDP), misma que creada en 2017 mediante el Decreto 746/2017 y tiene como objetivo principal la protección de los datos personales en Argentina.

Dentro de sus funciones incluyen la promoción y difusión de normas y políticas de protección de datos, el control y fiscalización del cumplimiento de la Ley de Protección de Datos Personales, la recepción y tramitación de denuncias y la imposición de sanciones en caso de incumplimiento.

Es de reconocer que al igual que la (ANDP) La (DNPDP) es un organismo descentralizado que depende del Ministerio de Justicia y Derechos Humanos.

Por último, analizaremos a la Agencia de Protección de Datos Personales de Chile (APDP):

Esta Agencia creada en 2017 a través de la Ley de Protección de Datos Personales, tiene como objetivo principal proteger los derechos de las personas en relación al tratamiento de sus datos personales en Chile. Sus funciones incluyen la promoción de la protección de datos personales, la fiscalización y control del cumplimiento de la ley, la recepción y tramitación de denuncias, la realización de investigaciones y la imposición de sanciones en caso de incumplimiento; la APDP es un servicio público descentralizado.

De lo anterior, se observa que las autoridades de protección de datos personales de Brasil, Argentina y Chile comparten el objetivo común de garantizar la protección de los datos personales de los individuos. Sin embargo, difieren en cuanto a su independencia o dependencia, así como en las funciones específicas que desempeñan. Cada una de estas autoridades desempeña un papel crucial en la supervisión y aplicación de las leyes de protección de datos en sus respectivos países.

3.2 El escenario Constitucional

Por lo respecta a este capítulo denominado “Marco Jurídico de la Protección de Datos Personales”, encontramos que en el Estado Mexicano el derecho a la protección de datos personales se deriva como límite del derecho de acceso a la información pública y al flujo transfronterizo de datos personales entre naciones o instituciones.

Para ello, es imperante traer a colación el artículo 1° de la Constitución Política de los Estados Unidos Mexicanos, el cual refiere que, en México, todas las personas sin distinción alguna gozarán de los derechos en ella reconocidos, así como en los tratados internaciones en los que México forma parte, en este sentido es que analizaremos el artículo 16° de la Constitución Política de los Estados Unidos Mexicanos.

En México, el derecho a la protección de los datos personales tuvo su naturaleza como límite del derecho de acceso a la información pública, por lo que su camino normativo se refleja en éste si bien su reconocimiento constitucional se dio 30 años después del propio acceso a la información pública, sin embargo y como se ha visualizado a lo largo de este trabajo de investigación, se puede apreciar que a través de tiempo se han ido modificando y creando nuevos ordenamientos jurídicos que regulan la salvaguarda de los datos personales.

El derecho a la protección de datos personales surgió el 6° de diciembre de 1977, mediante la primera reforma al artículo 6° de la Constitución Política de los Estados Unidos Mexicanos, y sienta su base constitucional en la adición al texto de ese articulado, el 20 de julio de 2007[9], de un segundo párrafo con siete fracciones que, en concreto, sobresalen los numerales II y III, las cuales refieren lo siguiente:

- “La información referente a la vida privada y a los datos personales debe protegerse en los términos y con las excepciones fijados en las leyes.
- Toda persona, sin necesidad de acreditar interés alguno o justificar su uso, puede acceder a sus datos personales o a solicitar su rectificación.” artículo 6 de la Constitución Política del os Estados Unidos Mexicanos.

Para el año de 2009, las reformas a los artículos 16° y 73° de la Constitución Política de los Estados Unidos Mexicanos, reconocieron el pleno derecho a la protección de datos personales como un derecho fundamental, autónomo e independiente del derecho de acceso a la información pública y de la propia transparencia, dando como resultado que las reformas dotaran de facultades y atribuciones al Congreso de la Unión (Enríquez O. A., 2023) para emitir las leyes secundarias y reglamentos, lineamientos en materia de protección de datos personales.

[9] Cámara de Diputados del H. Congreso de la Unión, artículo 6 de la Constitución Política de los Estados Unidos Mexicanos.

Dichas reformas dieron origen a los que actualmente se aprecia en el artículo 16 de la Constitución Política de los Estado Unidos Mexicanos, el cual refiere:

> “Toda persona tiene derecho a la protección de datos personales, al acceso, rectificación, cancelación de estos, así como a manifestar su oposición en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por las razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros” OBJ

De lo transcrito, se advierte que la protección de datos personales y el ejercicio de los derechos ARCO, es un derecho fundamental que el Estado debe salvaguardar, de ahí que se emanaron legislaciones y órganos garantes en cada entidad federativa, para salvaguardar dicho derecho.

Es preciso señalar según (RICCI, 2023) que, desde sus primeras conceptualizaciones, el derecho a la privacidad se definió como el derecho a no ser molestado. En tal sentido, se observan dos componentes centrales: el derecho a aislarse de todos y el derecho a controlar la información de uno mismo, en cuya esfera se inscribe la protección de los datos personales. Siguiendo al mismo autor, el fundamento constitucional del derecho a la privacidad se asienta en el primer párrafo del artículo 16°, enfocado a establecer el respeto a la vida privada personal y familiar; por su parte el párrafo segundo del mismo ordenamiento refiere el ejercicio de los derechos ARCO, los cuales, si bien no aluden al derecho a la privacidad, son el instrumento para su salvaguarda.

En este sentido y para el año 2014, el artículo 6° Constitucional sufrió una nueva reforma el 7 de febrero de 2014, mediante el cual se adicionó la fracción VIII, misma que establece el reconocimiento de un organismo autónomo, especializado,

imparcial y colegiado[10] como responsable de garantizar el debido cumplimiento y ejercicio de los derechos de acceso a la información pública y protección de datos personales.

Una vez que se logra la consolidación del instituto garante a nivel nacional en materia de transparencia y protección de datos personales en 2014, se obliga a las entidades federativas a la creación de organismos autónomos, especializados, imparciales y colegiados, responsables para garantizar los derechos de protección a los datos personales y el ejercicio de los derechos ARCO, en sus constituciones locales, y del mismo modo, señala la obligación de crear una ley general de la materia, destinada a fijar las bases, principios generales y procedimientos para hacer valer el acceso a la información pública, la protección de los datos personales y el ejercicio de los derechos ARCO, con la cual se armonizaron las normas estatales.

En este orden de ideas y con la necesidad de regular de manera eficaz y eficiente la protección de datos personales a nivel nacional, se crea el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, el cual tiene como objetivo “la organización de los esfuerzos de cooperación, colaboración, promoción, difusión y articulación permanente en materia de transparencia, acceso a la información y protección de datos personales, de conformidad con lo señalado en la Ley General de Transparencia y Acceso a la Información Pública y demás normatividad aplicable” (Transparencia, 2023).

3.3 Legislación Federal.

En México, actualmente se cuenta con dos leyes regulatorias en materia de protección de datos personales, una para el ámbito privado y otra en posesión de

[10] Artículo 7 fracción VIII de la Constitución Política de los Estados Unidos Mexicanos

sujetos obligados por ejemplo: (las entidades estatales y municipales, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos), siempre y cuando ejerzan recurso públicos, de lo contrario se estaría violentando el derecho a la vida privada, ya que es información que únicamente le concierne al titular de esos datos considerados como confidenciales, en términos de la Ley de Transparencia y Acceso a la Información Pública del Estado de México.

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

En este orden de ideas, la Ley de Protección de Datos Personales en Posesión de Particulares (LFPDPPP) vio la luz para el año dos mil diez, la cual tiene por objeto la “protección de datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas” (Unión C. d., 2023).

En dicho ordenamiento legal se contemplan las obligaciones, principios y deberes que cada encargado debe cumplir, entre ellos, lo siguientes, independientemente y para el caso de no cumplir con estos principios y deberes, se podría ser acreedor a infracciones y sanciones administrativas y delitos del tratamiento indebido de datos personales civiles o penales.

Derechos ARCO: Los individuos tienen derecho a Acceder, Rectificar, Cancelar y Oponerse (derechos ARCO) al tratamiento de sus datos personales.

Aviso de Privacidad: Obligación de los responsables de recabar datos personales de informar a los titulares sobre el uso y manejo de sus datos a través de un aviso de privacidad.

Transferencias de Datos: La ley regula las transferencias nacionales e internacionales de datos personales, asegurando que se cumplan con los requisitos legales y se respeten los derechos de los titulares.

Medidas de Seguridad: Establece que los responsables deben contar medidas de seguridad de carácter administrativo, físicas y técnicas, para garantizar la salvaguarda ante posibles daños, incidentes, alteración vulneraciones destrucción o el mal uso, acceso o tratamiento no autorizado de datos personales.

Es menester señalar que esta Ley surgió, en una parte por la necesidad de armonizar la regulación de este derecho en todo el país, así como estandarizar los principios, derechos y procedimientos para ejercer los derechos ARCO, dando como resultado que en todas instituciones privadas tengan un marco igualitario para su tratamiento; y otra razón que dio paso a la creación de esta ley fue que el estado mexicano es un sujeto de derecho internacional y debe contar con una regulación para este derecho fundamental para con otras entidades de carácter privado internacionales.

No obstante de contar con una Ley de protección de datos personales en posesión de los particulares que ponía a México como una nación competitiva y que abría las puertas para formar parte de la Unión Europea por contar con instrumentos regulatorios de carácter internacional, el 21 de diciembre del año de 2011, se publicó el Reglamento de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, el cual tenía como objeto reglamentar las disposiciones de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Unión C. d., 2024).

3.3.1.1 Reglamento de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados.

Este reglamento, detalla y amplía las disposiciones de la LFPDPPP. Proporciona directrices más específicas sobre la implementación de la ley, incluyendo los

procedimientos para el ejercicio de los derechos ARCO, la elaboración del aviso de privacidad, las transferencias de datos y las medidas de seguridad.

A continuación, se presentan los puntos más destacados del reglamento:

1. Definiciones y Principios Generales

Definiciones: El reglamento amplía las definiciones de términos clave como "responsable", "encargado", "titular", "consentimiento", entre otros, para asegurar una interpretación clara y consistente.

Principios: Reitera y detalla los principios de protección de datos (licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad).

2. Aviso de Privacidad

Contenido del Aviso: Especifica los elementos que deben incluirse en el aviso de privacidad, como el nombre y domicilio del responsable, las finalidades primarias y secundarias para el tratamiento, los mecanismos que el responsable ofrece a los titulares de los datos personales para limitar el uso o divulgación de sus datos, los medios para el ejercicio de los derechos ARCO, y en su caso especificar si existen o no trasferencias de datos personales.

Formatos del Aviso: Permite que el aviso de privacidad se presente en formatos diversos (escrito, electrónico, verbal, entre otros) y proporciona directrices para su elaboración según el medio de obtención de los datos personales.

3. Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)

Procedimiento para Ejercer Derechos ARCO: Detalla el proceso que deben seguir los titulares para ejercer sus derechos, incluyendo los plazos y las formas en que el responsable debe responder.

Medios y Plazos: Establece que el responsable debe contar con los medios para atender las solicitudes de los titulares y cumplir con los plazos establecidos para responder dichas solicitudes.

4. Medidas de Seguridad

Medidas Administrativas, Físicas y Técnicas: Define las medidas de seguridad que los responsables deben implementar para proteger los datos personales ante la vulneración o incidente de datos personales (daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado)

Evaluación de Riesgos: Estipula la necesidad de realizar evaluaciones periódicas de los riesgos y vulnerabilidades a los que están expuestos los datos personales y de ajustar las medidas de seguridad conforme a los resultados de estas evaluaciones.

5. Transferencias de Datos.

Condiciones para Transferencias: Especifica las condiciones bajo las cuales se pueden realizar transferencias de datos personales, tanto nacionales como internacionales, asegurando que se obtenga el consentimiento del titular y que el destinatario cumpla con los principios y obligaciones de la LFPDPPP.

Cláusulas Contractuales: Requiere que las transferencias internacionales de datos personales se formalicen mediante cláusulas contractuales que aseguren un nivel adecuado de protección.

6. Encargados del Tratamiento.

Relación Responsable-Encargado: Define las obligaciones del encargado en relación con el tratamiento de datos personales, incluyendo la implementación de medidas de seguridad y el manejo adecuado de los datos conforme a las instrucciones del responsable.

Contratos y Convenios: Establece que la relación entre el responsable y el encargado debe formalizarse mediante un contrato o convenio que especifique las obligaciones del encargado y las medidas de seguridad a adoptar.

7. Procedimientos y Sanciones.

Inspección y Vigilancia: Detalla los procedimientos para las inspecciones y auditorías que el INAI puede realizar para verificar el cumplimiento de la LFPDPPP y su reglamento.

Sanciones: Define las sanciones administrativas aplicables a los responsables que incumplan con las disposiciones de la ley y el reglamento, incluyendo multas y otras medidas correctivas.

8. Disposiciones Finales.

Adaptación y Actualización: Incluye disposiciones sobre la actualización y mejora continúa de las políticas y procedimientos relacionados con la protección de datos personales, adaptándose a los cambios tecnológicos y normativos.

En resumen, el RLFPDPPP proporciona un marco detallado para la aplicación práctica de la LFPDPPP, asegurando que los responsables del tratamiento de datos personales implementen medidas adecuadas para proteger los datos de los titulares y cumplan con las obligaciones legales en México.

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

Así, tenemos que en el año 2016 se creó la ley regulatoria de los artículos 6 base a y 16° párrafo segundo de la Constitución Política de los Estados Unidos Mexicanos, tal fue el caso de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual está compuesta por once títulos y tiene por objeto que:

> "Artículo 1. La presente Ley es de orden público y de observancia general en toda la República, reglamentaria de los artículos 6o., Base A y 16, segundo párrafo, de la Constitución Política de los Estados Unidos Mexicanos, en materia de protección de datos personales en posesión de sujetos obligados…" [11]

Este ordenamiento legal nos rige actualmente y establece los derechos, principios, deberes y obligaciones que cada responsable debe cumplir para salvaguardar el derecho a la protección de datos personales.

Asimismo, en dicho ordenamiento en su numeral artículo refiere a cuáles son los sujetos obligados que deben garantizar la protección de los datos personales, así como las personas físicas que utilicen, manejen y dispongan recursos públicos.

En este orden de ideas, se abordarán los aspectos fundamentales de esta Ley, sus implicaciones y los desafíos que enfrenta su implementación.

1. Contexto y Objetivo de la Ley

[11] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.- véase en https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

La LGPDPPSO fue creada para regular el tratamiento de datos personales por parte de los sujetos obligados, que incluyen a los poderes Ejecutivo, Legislativo y Judicial, así como a organismos autónomos y cualquier otra entidad pública en los tres niveles de gobierno (federal, estatal y municipal). Su objetivo principal es garantizar el derecho a la privacidad y la protección de datos personales de los individuos, promoviendo la transparencia y la rendición de cuentas en el sector público.

2. Principios de Protección de Datos

La ley establece una serie de principios que deben guiar el tratamiento de datos personales por parte de los sujetos obligados:

Licitud, Consentimiento, Información: Los datos deben ser tratados de manera lícita y con el consentimiento del titular, quien debe ser informado sobre el uso que se dará a sus datos.

Calidad y Finalidad: Los datos personales deben ser exactos, completos y actualizados, y solo deben ser utilizados para las finalidades para las cuales fueron recabados.

Lealtad y Proporcionalidad: El tratamiento debe ser leal y proporcional, evitando la obtención y uso excesivo de datos personales.

Responsabilidad: Los sujetos obligados deben asegurar el cumplimiento de la ley y adoptar las medidas necesarias para proteger los datos personales.

3. Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición)

La LGPDPPSO garantiza a los titulares de datos personales el ejercicio de los derechos ARCO:

- Acceso: Derecho a conocer los datos personales que poseen los sujetos obligados.
- Rectificación: Derecho a solicitar la corrección de datos personales incorrectos o incompletos.
- Cancelación: Derecho a solicitar la eliminación de los datos personales cuando ya no sean necesarios para las finalidades por las que fueron recabados.
- Oposición: Derecho a oponerse al tratamiento de sus datos personales por motivos legítimos.

4. Medidas de Seguridad

La ley obliga a los sujetos obligados a implementar medidas de seguridad administrativas, técnicas y físicas para proteger los datos personales contra el acceso no autorizado, pérdida, daño, modificación y destrucción. Estas medidas deben ser proporcionales al riesgo asociado con el tratamiento de los datos personales.

5. Transferencia de Datos

La LGPDPPSO regula las transferencias de datos personales entre sujetos obligados y a terceros, estableciendo que estas deben realizarse bajo condiciones que aseguren la protección de los datos personales y el respeto a los derechos de los titulares.

6. Aviso de Privacidad

Los sujetos obligados deben proporcionar un aviso de privacidad que informe a los titulares sobre la existencia y características del tratamiento de sus datos personales. Este aviso debe incluir información como la identidad del responsable del

tratamiento, las finalidades del mismo, los derechos ARCO y los procedimientos para ejercerlos.

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

El INAI es el organismo encargado de supervisar y garantizar el cumplimiento de la LGPDPPSO. Sus funciones incluyen la recepción y resolución de quejas y denuncias, la realización de verificaciones y auditorías, y la imposición de sanciones en caso de incumplimiento.

8. Sanciones y Responsabilidades

La ley establece un régimen de sanciones para los sujetos obligados que no cumplan con las disposiciones de la LGPDPPSO. Las sanciones pueden incluir desde amonestaciones hasta multas y otras medidas correctivas, dependiendo de la gravedad de la infracción.

En síntesis, la LGPDPPSO establece un marco legal integral para la protección de datos personales en posesión de sujetos obligados en México, garantizando el derecho a la privacidad de los individuos y promoviendo la transparencia y la responsabilidad en el sector público. No obstante, su efectividad depende de la correcta implementación y cumplimiento por parte de todas las entidades públicas, así como de la adaptación continua a los cambios tecnológicos y sociales.

Una vez que se emitió la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y de conformidad con los artículos 89, fracciones XVII, XIX, XXVII y XXVIII, 157 y quinto transitorio de la Ley General de Protección de Datos Personales, el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, este cuenta con atribuciones para emitir

disposiciones generales para el desarrollo del procedimiento de verificación (Instituto Nacional de Transaprencia, 2023), dando paso a los Lineamientos Generales de Protección de Datos Personales para el sector Público.

Estos lineamientos tienen por objeto desarrollar las disposiciones previstas en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en el ámbito federal, asimismo establecen cuáles son los principios, deberes y obligaciones que debe acatar cada sujeto obligado, en caso de incumplimiento se contemplan medidas de apremio por incumplimiento y vulneración a datos personales, tanto a ley como a los lineamientos.

Ahora bien y como ya se mencionó en líneas anteriores, el veintiséis de enero de dos mil diecisiete cuando se promulgo la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, específicamente en su artículo transitorio segundo, otorgo un plazo de seis meses para que todas la entidades federativas, se ajustarán a las nuevas disposiciones en materia de protección de datos personales, en este orden de ideas el Estado de México, no se quedó atrás y fue uno de los primeros estados en dar cumplimiento a este artículo segundo transitorio de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, situación en la que abundaremos en el próximo capítulo.

3.4 La regulación en el Estado de México

Es trascendental señalar que el Estado de México, contaba desde agosto del año 2012, con una Ley en la materia, la cual llevaba por nombre “Ley de Protección de Datos Personales del Estado de México”, sin embargo, y como consecuencia de la publicación de la Ley General y específicamente del artículo segundo transitorio, la legislatura del Estado de México, presentó la iniciativa con proyecto de decreto que abroga la Ley de Protección de Datos Personales en el Estado de México, para dar paso a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios (LEGISLATURA, 2023).

Ahora bien en primer término se hablará de la Constitución Política del Estado Libre y Soberano del Estado de México, en la cual en su artículo 5 establece que todas las personas gozarán de los derechos humanos reconocidos en la Constitución Política de los Estados Unidos Mexicanos, en los tratados internacionales en los que el Estado mexicano sea parte, especialmente, dicho ordenamiento legal se refiere al derecho de transparencia, acceso a la información pública y la protección de datos personales, dando paso a la creación del órgano garante encargado de la salvaguardad de estos derechos.

> *"*En el Estado de México todas las personas gozarán de los derechos humanos reconocidos en la Constitución Política de los Estados Unidos Mexicanos, en los tratados internacionales en los que el Estado mexicano sea parte, en esta Constitución y en las leyes que de ésta emanen, por lo que gozarán de las garantías para su protección, las cuales no podrán restringirse ni suspenderse salvo en los casos y bajo las condiciones que la Constitución Política de los Estados Unidos Mexicanos establece. En el Estado de México la Naturaleza o biodiversidad, especies endémicas y nativas son sujetos de derecho, los cuales son otorgados, protegidos y promovidos por la constitución y las leyes del Estado.
>
> …
>
> Para garantizar el ejercicio del derecho de transparencia, acceso a la información pública y protección de datos personales, los poderes públicos y los organismos autónomos, transparentarán sus acciones, en términos de las disposiciones aplicables, la información será oportuna, clara, veraz y de fácil acceso.
>
> …
>
> > II. La información referente a la intimidad de la vida privada y la imagen de las personas será protegida a través de un marco jurídico rígido de tratamiento y manejo de datos personales, con las excepciones que establezca la ley reglamentaria.

…

> VIII. El Estado contará con un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía técnica y de gestión, con capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de transparencia, acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley.[12] (Artículo 5°)

En este sentido y una vez que se creó el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios y la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y municipios, estos mecanismos regulan este derecho bajo los principios y bases de salvaguardar la intimidad de las personas, específicamente a la vida privada y a su imagen.

Es así como, para el 30 de mayo de 2017, se publica la nueva ley de la materia, la cual lleva por nombre “Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios”, esta nueva ley local establece las bases, principios y procedimientos que cada sujeto obligado debe tomar en cuenta para garantizar el derecho a la protección de datos personales, en armonización con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, por lo que en obviedad a que ya se mencionó el objetivo de esa Ley y sus principios y deberes que cada sujeto obligado debe garantizar para na adecuada protección al derecho fundamental de la protección de datos personales, ya no es necesario retomarlos, sino únicamente tenerlo presente y no perderlo de vista.

[12] Constitución Política del Estado Libre y Soberano de México.- véase en https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/ley/vig/leyvig001.pdf

> “Artículo 1. La presente Ley es de orden público, interés social y observancia obligatoria en el Estado de México y sus Municipios. Es reglamentaria de las disposiciones en materia de protección de datos personales previstos en la Constitución Política del Estado Libre y Soberano de México.
>
> Tiene por objeto establecer las bases, principios y procedimientos para tutelar y garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de los sujetos obligados.” [13]

En este orden de ideas y para que el Estado de México siga a la vanguardia en el marco jurídico que tutela el derecho a la protección de datos personales, el 30 de mayo del año dos mil veintitrés se publicó en el Periódico Oficial “Gaceta de Gobierno” del Estado Libre y Soberano de México, el acuerdo mediante el cual, se expiden los “LINEAMIENTOS PARA IMPLEMENTAR LOS PROCEDIMIENTOS DE INVESTIGACIÓN Y VERIFICACIÓN, ASÍ COMO LA PRÁCTICA DE AUDITORÍAS VOLUNTARIAS A LOS RESPONSABLES DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DEL ESTADO DE MÉXICO Y MUNICIPIOS”, los cuales tiene por objeto:

> “**Objeto.**
>
> **PRIMERO.** Los presentes Lineamientos son de observancia obligatoria para los responsables en materia de protección de datos personales del Estado de México, así como para el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado d México y Municipios.
>
> Tienen por objeto regular la implementación de los procedimientos de investigación y verificación, así como la práctica de las auditorías voluntarias realizadas por la Dirección General de Protección de Datos Personales del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, previstos en el Título

[13] Constitución Política del Estado Libre y Soberano de México, véase en: https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/ley/vig/leyvig244.pdf

Décimo Segundo Procedimientos para verificar el Cumplimiento de la Ley, en su Capítulo Único de las Facultades de Verificación, de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios.” [14]

Como ya se refirió en líneas anteriores la protección de datos personales cuenta con amplia normatividad que rige la materia en sus dos vertientes tanto en posesión de los particulares, como en posesión de sujetos obligados, ello, en atención a lo marcado en la Constitución Política de los Estatutos Unidos Mexicanos, la cual reconoce el derecho a la protección de datos personales y el ejercicio de los derechos ARCO, con ello, se demuestra que México al formar parte del Convenio 108 y de la Organización así también se demuestra que México al formar parte del Convenio 108 y a las directrices que marza Organización para la Cooperación y el Desarrollo Económico en materia de protección de datos personales, el Estado mexicano reconocerá y salvaguardará este derecho sin distinción alguna.

Luego entonces, es de hacer notar que los seres humanos en todo momento y a través de su vida, proporciona datos personales para la prestación de un servicio o compra de bienes, por ello, es vital que este regulado para saber con exactitud cuál será el tratamiento que se les brinde a estos datos personales e informar de manera clara objetiva y cierta finalidad para la cual serán recabados los datos personales; en este sentido en ocasiones se tiene que hacer un análisis a las diferentes ordenamientos legales que se relacionada con la materia, por ejemplo en el caso concreto de este trabajo, se analizó desde la Declaración de los Derecho Humanos, hasta el Convenio 108, ordenamientos internacionales, que México ha tratado de igualar los altos estándares de protección, en un primer momento porque México forma parte de estos grupos y le exigen normatividad actualizada para el flujo

[14] Lineamientos para Implementar los Procedimientos de Investigación y Verificación, así como la práctica de Auditorías Voluntarias a los Responsables de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios., véase en:
https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/gct/2022/mayo/may301/may301d.pdf

transfronterizo de datos y poder tener una economía estable y en un segundo momento para proteger y salvaguardar los derechos de los connacionales.

CAPÍTULO CUARTO
EFICACIA DE LAS ACCIONES GUBERNAMENTALES EN LA PROTECCIÓN DE DATOS PERSONALES

4.1. Alcances de las acciones gubernamentales

En el presente apartado tiene como objetivo analizar el rumbo de la protección de datos personales en nuestro país bajo la óptica de las reformas propuestas por el ejecutivo federal, las cuales impactan directamente en la permanencia del Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI), organismo constitucional, hasta la fecha, autónomo, por ello de partirá una breve reseña acerca de ese instituto.

El INAI como se conoce actualmente, obtuvo su autonomía constitucional plena en el año 2014, con esta reforma se diseñó e implemento la política de transparencia, la garantía plena del derecho de acceso a la información y de protección de datos personales, de la promoción de estos derechos, así como de la resolución de recursos de inconformidad, la atracción de los recursos de revisión en los estados y la coordinación del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT).

Dentro de las facultades otorgadas al INAI está la de verificar de oficio el cumplimiento de obligaciones de transparencia por parte de los sujetos obligados federales; y, permite a los particulares que presenten denuncias ante el Instituto por incumplimiento o falta de actualización de las obligaciones de transparencia; regula las atribuciones otorgadas al INAI para imponer medidas de apremio a los responsables de los sujetos obligados, para asegurar el cumplimiento de sus resoluciones, así como para imponer sanciones a infractores que no cuenten con el carácter de servidores públicos, ni sean partidos políticos; y norma los vínculos entre el Instituto y la sociedad mexicana, estableciendo las bases para la integración y operación del Consejo Consultivo del Instituto.

El aviso de privacidad, es el marco de actuación a través del cual se establecen las bases, principios y procedimientos para salvaguardar el derecho a la protección de datos personales de toda persona que obre en los registros de los sujetos obligados ya se del ámbito Federal, Estatal o Municipal, en términos de la Ley General de Transparencia, Acceso a la Información Pública.

Dichos avances legislativos propiciaron el desarrollo de una serie de instrumentos jurídicos que permiten reforzar el marco regulatorio de este derecho, al tiempo que se emiten e implementan herramientas y mecanismos que facilitan a las dependencias y entidades gubernamentales, así como a las personas físicas o morales que tratan datos personales, el cumplimiento de sus obligaciones en la materia.

Además, el Instituto cuenta con el Programa Institucional 2017-2020 y, dentro del Sistema Nacional de Transparencia, con dos programas nacionales, el Programa Nacional de Acceso a la Información (PROTAI) y el Programa Nacional de Protección de Datos Personales (PRONADATOS), que contribuyen al cumplimiento de los objetivos institucionales y a la correcta salvaguarda de los derechos de acceso a la información y protección de datos personales.

Ello es muestra del compromiso del Ejecutivo para que a través de sus Órganos Garantes creados mediante las reformas constituciones del año 2009, como se mencionó en el marco normativo ha encaminado sus esfuerzos primero para reconocer la protección de datos personales como un derecho fundamental, pleno y autónomo e independiente del acceso a la información pública.

En las reformas constitucionales de 2009, el Congreso de la Unión tenía facultades y atribuciones para emitir las leyes secundarias y reglamentos, lineamientos de protección de datos personales, garantizar la protección de los datos personales en posesión de las dependencias y entidades de la Administración Pública Federal (Enríquez, 2023); en este sentido desde mi perspectiva, México empieza a

considerar el derecho a la protección de datos personales, a la privacidad, a la intimidad, a la dignidad y honor con los alcances que marcaban los estándares internacionales.

En ese nuevo orden jurídico se asientan los parámetros y demás disposiciones que deben implementarse a nivel nacional y estatal, de manera que garanticen a las dependencias y órganos garantes de cada entidad realizar las acciones necesarias y gestiones que permitan los avances significativos, mejoren la calidad y se garantice una adecuada protección de datos personales en posesión de dependencias gubernamentales, así como el sector privado.

Estas acciones, que órganos garantes y sujetos obligados han implementado durante 20 años de reconocimiento constitucional, buscan resultados en protección de datos personales y una adecuada salvaguarda ante posibles vulneraciones.

En este sentido una acción gubernamental, se traduce en una intervención de los órganos e instituciones estatales, en materia de protección de datos personales, para reconocer, difundir, capacitar fortalecer la cultura de la protección de datos personales. No es óbice mencionar que independientemente de las acciones gubernamentales que se generen para la debida protección de datos personales, no se debe dejar de lado a la participación ciudadana que es el elemento social con la capacidad para proteger en un primer momento su dignidad, honor, intimidad, y protección de datos personales.

Cada uno es responsable de cuidar y proteger los datos personales, es decir, de aquellos que compartimos sin medida, ni precaución, sin tener la certeza de a quien se están compartiendo.

La sociedad debe ayudar a la encomienda que tiene el Estado en la salvaguarda de un derecho humano como el derecho a la protección de datos personales, aunque el Estado implemente acciones.

En este orden de ideas, podemos decir que el funcionamiento del Estado incide en los ciudadanos, por tanto, en un estado democrático se necesita que la sociedad conozca sus derechos para que con ello pueda ejercerlos de manera razonable y objetiva sabiendo que en caso de vulneraciones el Estado cuenta con mecanismo para restituir esos derechos.

Aunque la sociedad y el Gobierno dependen entre sí, es el Estado quien garantiza la salvaguarda de los derechos, debe tener claro que ese acto se llama acción gubernamental. Las acciones gubernamentales son las que emprende el estado para salvaguardar un derecho o atender una necesidad social, que a veces no son los resultados esperados para todos, porque siempre existen contratiempos que no permiten la aplicabilidad total de las políticas públicas o las acciones gubernamentales.

Un claro ejemplo en materia de protección de datos lo encontramos en escritos académicos, entrevistas, conferencias o reuniones dónde se encuentran presentes especialistas de todo el mundo en la materia, verbigracia la GLOBAL PRIVACITY ASSEMBLY; en este espacio se establecen algunas políticas que no siempre resultan aplicables para todos los países que participan, en consecuencia, los resultados no son los mismos para todos y puede parecer que esas acciones no son funcionales.

Ante este escenario se advierte que las acciones del Gobierno son fundamentales para el desarrollo de una nación, pero que no siempre es conveniente replicar los modelos de países con los que los niveles de comparación o puntos de coincidencia son bajos, por qué entonces los resultados no serán los esperados; en el caso de los datos personales en México se replicó un modelo europeo que se intenta implementar pero se ve una situación muy forzada, primero porque no se tiene las capacidades técnicas y económicas que tiene un país de esos y segundo porque a

mi parecer tampoco se cuenta con una conciencia plena del cuidado de nuestra información; ante este escenario resulta poco viable cada acción desarrollada.

4.2 Deficiencias en la Protección de Datos Personales

Una vez lo anterior, es momento de observar que las acciones emprendidas no siempre resultan como se esperaba, es momento de analizar cuáles, desde mi perspectiva jurídica, han sido las deficiencias al momento de reconocer el derecho a la protección de datos personales.

La primera situación que se trae a discusión es la relacionada con los datos personales como insumo del crimen organizado, en México es normal que la sociedad sea víctima de alguna extorsión telefónica o bancaria, todo esto lo hemos vivido en alguna parte de nuestras vidas, en donde supuestamente te realizan ofertas tratando de engañar a las personas usuarias de tarjetas de débito o de crédito, para acceder a sus cuentas bancarias o utilizar las tarjeta de manera desproporcionada y te dejan en estado de indefensión.

El crimen organizado está lleno de bases de datos que se compran ya sea en el mercado negro o bien por medio de la contratación de personal especializado que interviene a través de virus maliciosos en el software ya sea de los sujetos obligados o de los particulares y obtiene nombre completo, números telefónicos, domicilio y en ocasiones hasta el número de tu tarjeta de crédito o débito.

Es difícil saber con certeza de dónde ocurre esta vulneración a datos personales, ya que dicha vulneración puede ser ocasionada por la falta de regulación de la vida privada o bien, por la falta de ética que tienen las personas en la recopilación y/o tratamiento de datos personales; en México es probable apropiarse una base de datos, esto a comparación de algunos países de norte américa o de Europa, en dónde los sistemas de seguridad son más complejos.

Otro ejemplo, es la pandemia ocasionada por el COVID 2019, la enfermedad que ataco al mundo entero y que puso de manifiesto el estado de vulnerabilidad que

tiene el mundo, y no solo eso, sino que vino a cambiar la perspectiva de propios y extraños, a raíz de esta obtención de datos personales, por parte de empresas e instituciones públicas fue algo cotidiano, ya sea para conservar la salud o bien para allegarse de bienes que permitirán sobrevivir ante este situación compleja e incierta.

Según el mercado empezó a ver en los datos personales una moneda de cambio bastante rentable y fácil, los encargados de recoger datos personales y no solo del nombre sino de otros datos considerados sensibles. Sin embargo, no había un nivel de protección adecuado, en el mejor de los casos, había aviso de privacidad de manera visible en el establecimiento o en los formatos para llenado por los solicitantes de pruebas COVID, pero ¿Esta medida de seguridad realmente era eficiente para saber cuál era el tratamiento que se le otorgaba a estas dependencias o solo era para cumplir con la Ley? Nadie sabe cuál fue el destino de los datos personales obtenidos para las pruebas COVID, que en su momento fue una medida eficaz para contener los contagios, pero nada se supo del tratamiento que recibieron esos datos.

La Secretaría de Salud deja en la incógnita cual fue el tratamiento que le dio a los datos personales, pues no se sabe en realidad que fue lo que paso con todos los datos que recolectaba al momento de llegar el formato para obtener la vacuna, si bien se dio en un momento alarmante no hubo medidas compensatorias, para dar certeza a los titulares de los datos de tratamiento que se le estaba dando a su información.

Los retos de la protección de datos personales, supera las propuestas tradicionales de la política pública. Esto debido a la complejidad de los contextos institucionales débiles que están inmerso en lo general en la corrupción, ilegalidad y en la poca ética de los que recopilan y tratan datos personales, ello sin dejar de lado que la misma sociedad en un momento de preocupación como el COVID-19, privilegiara su estado de salud a saber cuál es el destino o tratamiento de sus datos personales.

En este orden de ideas también podemos encontrar la falta o nula cultura de la protección de datos personales, pues carece de información y herramientas institucionales para hacer frente a abusos y hacer valer su derecho a la privacidad.

En efecto, también hay una desactualización magna en comparación con las normas de otros países de la región. Para subrayar, tenemos los casos de Uruguay y Argentina, únicos Estados de América Latina que han sido declarados países con un adecuado nivel de protección de datos, según lo expresado en la Directiva 95/46 del Parlamento Europeo y del Consejo, agregando que “Uruguay incluso cuenta con un organismo dedicado exclusivamente a la tutela de este tipo de información (Unidad Reguladora y de Control de Datos Personales”(URCDP).

También hay deficiencias en la protección de datos personales desde la aprobación de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, ya que la ley solo se aboca al tratamiento de estos, quitando el derecho como titular a controlar tus propios datos personales. En cambio, para cualquier persona natural es complejo restringir el tratamiento de su información personal que se encuentra en los medios de comunicación social (o redes sociales).

El problema identificado, es la definición que la Ley otorga a la fuente. En efecto, la norma define como fuentes accesibles al público “los registros o recopilaciones de datos personales públicos o privados, de acceso no restringido o reservado a los solicitantes”. Lo anterior, en palabras simples, determina que salvo que el titular de los datos permita su divulgación, o a menos que la ley prohíba expresamente su divulgación, cualquiera puede dar tratamiento a la información que se encuentra en estas “fuentes accesibles al público”.

Por tanto, y aplicando las definiciones y excepciones de la normativa las redes sociales, y en general la información contenida en internet, es considerada una información accesible al público. En este sentido, nos encontramos ante una excepción tan amplia que termina transformando la falta de protección en la regla

general, generando como consecuencia la proliferación de sitios web que exponen nuestros datos o de empresas que los utilizan para entregar inteligencia de negocio a campañas políticas.

La autoridad encargada de controlar el tratamiento de los datos personales no es suficiente para abastecer todas las necesidades; ante esta realidad, son los propios titulares de la información quienes deben velar por el resguardo de estos, debiendo acudir a la presentación de sus denuncias ante los órganos garantes correspondientes, dependiendo de la naturaleza de la entidad involucrada, sujeto obligado o sujeto regulado.

Aunado a la anterior la propuesta de reforma presentada por el ejecutivo federal en febrero del año 2024, sugiere que el órgano garante es oneroso, con una estructura burocrática gruesa que lo único que ha buscado es solapar la corrupción; sin embargo desde la perspectiva ciudadana el personal que labora en los órganos encargados de la transparencia y la protección de datos no es suficiente para dar atención a una población que sin importar edad, generó condición económica o social, nacionalidad; proporciona datos personales para todas las actividades cotidianas desde las más básicas hasta las más complejas que dentro de un flujo normal se puedan presentar.

4.3 Prospectiva de la protección de datos personales.

Definitivamente la protección de datos personales enfrenta un gran desafío con la reforma constitucional en la que el ejecutivo pretende desaparecer los órganos autónomos, la incertidumbre que esto genera sobre la autoridad que ahora será responsable de restituir el derecho a la protección de datos personales que puede ser vulnerado en cualquier momento, desde mi perspectiva representa un gran atraso a lo que se había avanzado en la materia, me parece que ante este escenario los datos personales están más vulnerables.

No pasa desapercibido que hoy en día los datos personales son una moneda de cambio y que es equiparable a ciertos activos que son tangibles que pueden ser vendidos para la obtención de recursos económicos o bien para usarlos en contra de uno mismo y cometer delitos.

Bajo estas líneas argumentativas, no se debe soslayar que un dato personal por sí solo no puede generar información importante, sino, como ya se refirió en líneas anteriores y específicamente en la teoría de los mosaicos, se debe asociar con otros datos que sean de utilidad para hacer identificable a una persona, dando como resultado que toda la información quede vulnerable y permita lucrar a través de la comercialización licita o ilícita.

En la protección de sus datos personales se encuentra una oportunidad para generar confianza entre los diversos elementos que intervienen en las operaciones comerciales, para así consolidar los modelos de negocio.

Ahora, si bien es cierto que el impulso de la regulación en materia de protección de datos personales para empresas establecidas en México atiende a la garantía de un derecho humano, también encuentra su origen en aspectos económicos a nivel internacional y acaso más en alcanzar estándares de niveles adecuados para la protección de la información que ha sido una condicionante para que el país se pueda declarar seguro en el intercambio comercial.

Luego entonces, se tiene que a pesar de contar con un marco jurídico en materia de protección de datos personales en posesión de particulares en México, este sistema recoge estándares internacionales y proporciona garantías para la efectiva tutela de este derecho, sin embargo, el cumplimiento de las disposiciones enfrenta grandes desafíos.

Un ejemplo de lo que se refiere en este apartado es la ingenuidad de los alcances legales del tratamiento de la información, la falta de valores, por ejemplo, la ética

para el tratamiento de datos personales, el poco tacto respecto a las consecuencias del mal uso de la información y el desconocimiento de los mecanismos legales para exigir la protección de este derecho fundamental.

En este cariz, podemos confirmar que en la actualidad la economía digital la información de carácter personal, como ya se mencionó anteriormente, se ha convertido en petróleo negro que ha adquirido un valor, lo que conlleva a que distintos modelos de negocio tengan su sustento en la misma ya sea de forma reglamentaria o de manera clandestina.

La prospectiva de este derecho, es un tema de gran relevancia en la era digital en la que vivimos. A medida que la tecnología avanza y se recopila cada vez más información personal, por lo cual es necesario establecer un marco legal sólido que salvaguarde la privacidad y garantice la seguridad de los datos de carácter personal.

El derecho a la protección de datos personales se refiere al derecho fundamental de las personas a controlar la información que se recopila sobre ellas, así como el uso y la divulgación de dicha información. Este derecho busca proteger la privacidad y la dignidad de las personas en un mundo cada vez más interconectado.

En un contexto prospectivo, es importante considerar los desafíos y las oportunidades que el avance tecnológico plantea para la protección de datos. Por un lado, la recopilación masiva de datos y el uso de técnicas de inteligencia artificial pueden ser beneficiosos para el desarrollo de servicios personalizados y la toma de decisiones automatizadas. Sin embargo, también plantean riesgos en cuanto a la seguridad y el uso indebido de la información personal.

Por tanto, es fundamental que existan leyes y regulaciones claras que protejan los derechos de las personas en relación con sus datos personales. Estas leyes deben establecer principios básicos, como el consentimiento informado, la finalidad

específica de la recopilación de datos, la minimización de la información recopilada y la seguridad de los datos.

Además, es necesario que los organismos encargados de hacer cumplir estas leyes tengan los recursos y la capacidad para garantizar su implementación efectiva. Esto implica no solo la capacidad de sancionar a aquellos que violen las normas de protección de datos, sino también de educar a la población sobre sus derechos y las mejores prácticas para proteger su información personal.

Bajo este panorama, el Doctor Nelson Remolina (Mendoza, 2018) ha analizado la longitud que ha adquirió la protección de datos personales a partir del uso de las Tecnologías de la Información y la comunicación afirmando que en hoy en día existen cuantiosos y remunerados modelos de negocios establecidos a partir de la información de las personas en ámbitos digitales, de modo que las empresas están interesadas en incidir en las legislaciones locales.

En concordancia con lo antes planteado, existen técnicas como el ***big data,*** el cual permite que las empresas basen sus decisiones en el análisis de la información, por ejemplo, el perfil de consumo mensual de sus clientes, para así elevar sus ganancias y ampliar su campo de competitividad económica.

Finalmente, para el caso de México y en términos económicos, la publicación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados buscan consonancia para reunir estándares no solo nacionales, sino estar en aptitud de competir con estándares Internacionales como el Convenio 108, actualmente reformado, ello, en atención a los avances socio-tecnológicos, ya que como se ha visto dentro de la presente investigación la evolución tecnológica y los cambios sociales se han creado nuevos cambios de exploración.

En este orden de ideas, es imperante recalcar que este derecho (a la protección de datos personales) es el derecho a la no injerencia en la vida privada de las personas, derecho humano reconocido desde la Declaración Universal de los Derechos Humanos de 1948. Sin embargo, en el caso de México, el reconocimiento expreso del régimen de protección de datos personales en posesión de las empresas se hizo hasta 2010, lo que genera un desfase entre la normatividad Europea, pues ellos tienen ventaja al ya conocer y garantizar este derecho muchos años antes que en México.

Los principios rectores del derecho de protección de datos personales ayudan a su interpretación, sobre todo frente a colisión de derechos humanos como el de acceso a la información.

Bajo ese contexto, la ley de protección de datos personales en posesión del Estado de México y Municipios reconoció que se deberá atender al principio del interés superior del menor como eje transversal en la garantía de los datos personales de niñas, niños y adolescentes.

En conclusión, a 20 años de su reconocimiento constitucional, los datos personales siguen siendo un tema relevante y desafiante. A medida que avanzamos hacia el futuro, es importante encontrar soluciones que protejan la privacidad de las personas sin obstaculizar la innovación y el avance tecnológico. La regulación, la ética y la conciencia pública desempeñarán un papel crucial en la forma en que se abordan los retos y se desarrolla la perspectiva futura de los datos personales.

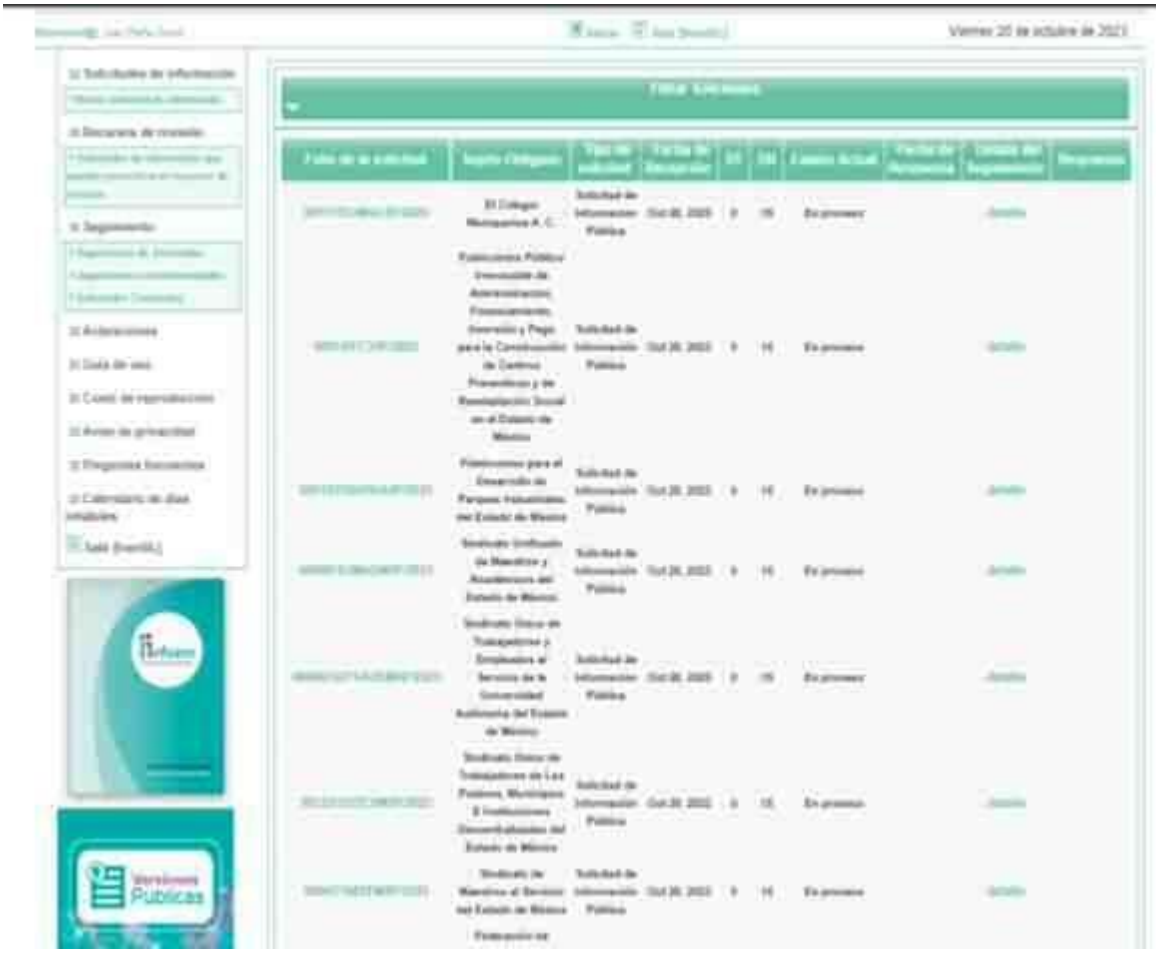
4.4 Resultados del análisis cualitativo

Analizados los puntos de vulnerabilidad de la sociedad, es necesario revisar qué hacen las instituciones para salvaguardar el derecho de protección de datos personales pública, por ello para elaborar una propuesta más robusta, se realizó un cuestionario diseñado como parte del proceso de recopilación de información.

El cuestionario se encuentra integrado por un apartado de datos sobre el encuestado, así como por 23 preguntas sobre las medidas y procedimientos que ese sujeto obligado ha implementado al amparo de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, las cuales están agrupadas en tres bloques: Bloque 1: Reconocimiento, Bloque 2: Medidas de Seguridad y 3: Acciones preventiva.

Mismas que fueron enviadas a través del Sistema de Acceso a la Información Mexiquense (SAIMEX), a 54 sujetos obligados, entre el Poder Legislativo, Poder Ejecutivo, Poder Judicial, Organismos Autónomos, Fideicomisos y Partidos Políticos; tal como se puede apreciar en la siguiente imagen:

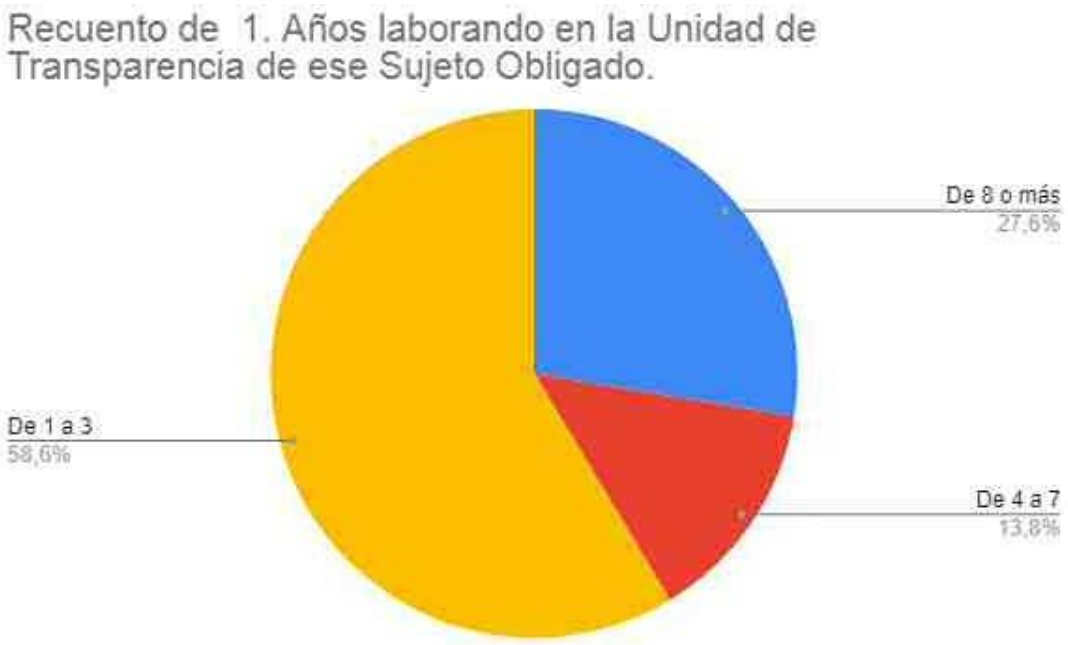
Imagen 1: Solicitudes presentadas a 54 sujetos obligados a través del SAIMEX



Fuente: Imagen obtenida de la cuenta personal del SAIMEX:
https://saimex.org.mx/saimex/ciudadano/login.page

Derivado de las 54 solicitudes de acceso a la información pública referidas en líneas anteriores, se obtuvieron los siguientes resultados cuantitativos y cualitativos; es necesario señalar que únicamente contestaron de manera favorable 28, en el resto de las respuestas los sujetos obligados manifestaron incompetencia para atenderlas o bien se justificaron señalando que era un derecho de petición y que no estaban obligados a procesar la información conforme a mi interés, fundando su dicho en el artículo 12 de la LTAIPEMYM; lo que en términos prácticos de esta investigación se traduce en un obstáculo para el investigador, sin embargo, de los cuestionarios atendidos se arrojan los siguientes resultados:

Grafica 1. Antigüedad en la Unidad de Transparencia.



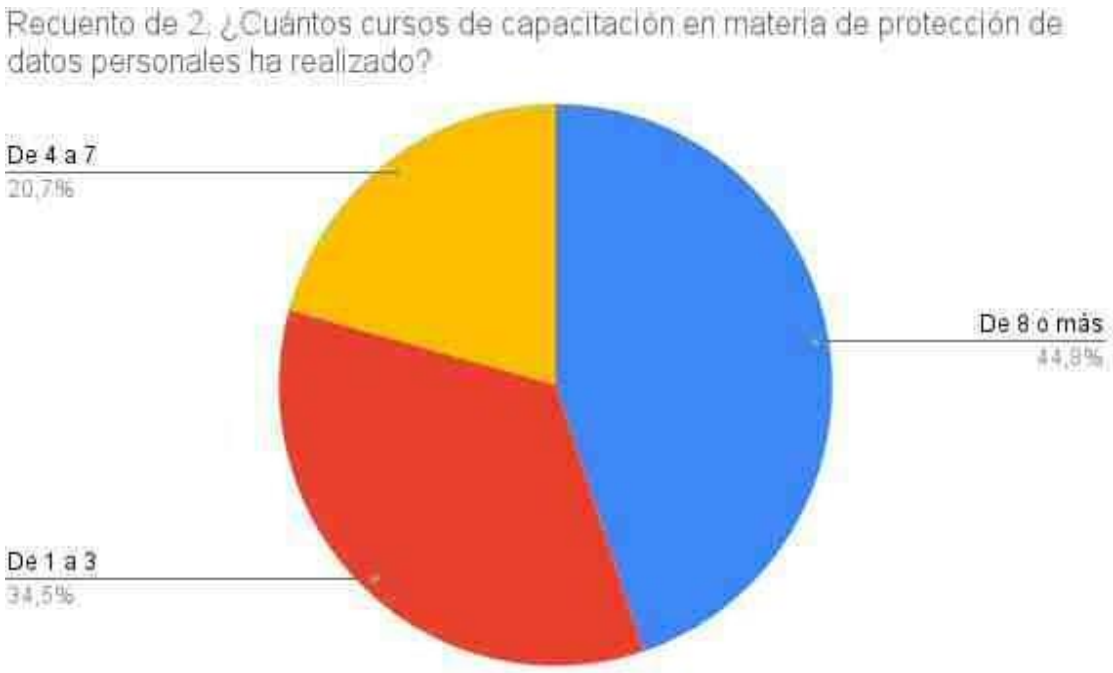
Fuente: Elaboración propia a partir de los resultados de los cuestionarios hechos a los sujetos obligados.

En el primer apartado del cuestionario se solicitó a los sujetos señalarán el tiempo que llevan ocupando la titularidad de la unidad de transparencia, con el objetivo de tener un panorama claro de la situación; para la cual la pregunta fue: ¿Cuántos años tiene laborando en la unidad de transparencia?

El 58.6 por ciento de los titulares tienen en el cargo de uno a tres años, el 13. 8 % de cuatro a siete años y el 27.6 por ciento de ocho o más años, ante esta circunstancia se infiere que más de la mitad de los titulares está en desventaja, ya que el conocimiento y la experiencia se adquieren a través del tiempo, y se perfecciona con la capacitación constante y el estudio permanente, aunando al número de situaciones sobre el tratamiento, salvaguarda y la protección de los datos personales a las que se enfrentan dentro de cada sujeto obligado, esto es, en poco tiempo no se puede conocer una materia que conlleva un grado de importancia al

tratarse de un derecho fundamental, por eso considero que a medida que se tiene un mayor grado de experiencia se cuenta con elementos sólidos para salvaguardar un derecho y en su caso defenderlo de cualquier posible vulneración.

Grafica 2. Cursos de Capacitación.



Fuente: Elaboración propia a partir de los resultados de los cuestionarios hechos a los sujetos obligados.

El 44.8% de los encuestados señaló que tomó más cursos de capacitación, en la que se interesaba conocer el nivel de capacitación a través de los cursos tomados, el 20.7% señaló que participó de entre 4 y 7 cursos y el 34.7% está en el nivel de 1 a 3 cursos, ante esto preocupa la poca capacitación en este tema, sin olvidar que está ante la obligación de proteger la intimidad de las personas.

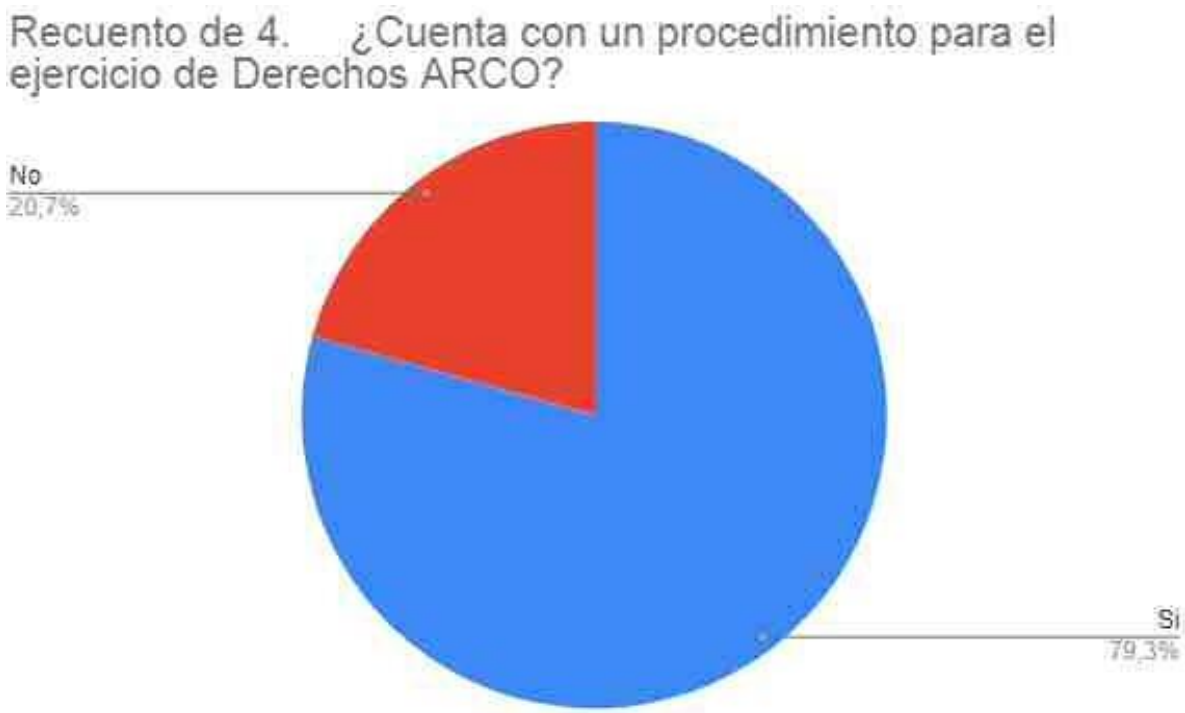
Grafica 3. El titular de la Unidad está certificado.

Fuente: Elaboración propia a partir de los resultados de los cuestionarios hechos a los sujetos obligados.

Para fortalecer el apartado de capacitación, se les preguntó a los titulares de las unidades de transparencia que si contaban con la certificación en protección de datos que la ley señala, pero el asombro fue tal al observar que el 79.3% no cuenta con dicha certificación, por lo que se concluye un incumplimiento por parte de los titulares de las unidades de transparencia a lo establecido en la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios, específicamente en su artículo 92, que refiere que, para ser oficial de Protección de Datos Personales, se debe contar con una certificación en dicha materia, lo que garantizará la debida protección y salvaguarda de este derecho; con ello se arriba al siguiente posicionamiento, qué es lo que hace el Órgano Garante de la entidad ante esa situación, toda vez que es el responsable de que los sujetos obligados cumplan con lo que marca la Ley, y más aún cuando él es el generador de esas Certificaciones, por tanto es su deber y su compromiso que los titulares estén certificados en esas materias.

Con lo anterior de infiere que el camino de la actualización y capacitación en protección de datos personales por parte del Infoem y de los titulares avanza de manera muy pausada, me atrevería a decir que muy lento, con las gráficas se refleja la poca preparación, quizá por falta de interés o conocimiento de los cursos, talleres o foros de capacitación en los cuales pueden participar los integrantes de la unidades de transparencia y no solo los titulares; situación que en términos prácticos conlleva un menor riesgo a la exposición de datos personales; aunado a ello no se puede dejar de ver que es un derecho humano que evoluciona vertiginosamente, en la medida que la tecnología avanza, por lo que es indiscutible su capacitación constante, debido a las nuevas necesidades de la sociedad, por ejemplo, la inteligencia artificial, el flujo transfronterizo de datos personales, y las transferencias entre sujetos obligados y entidades particulares.

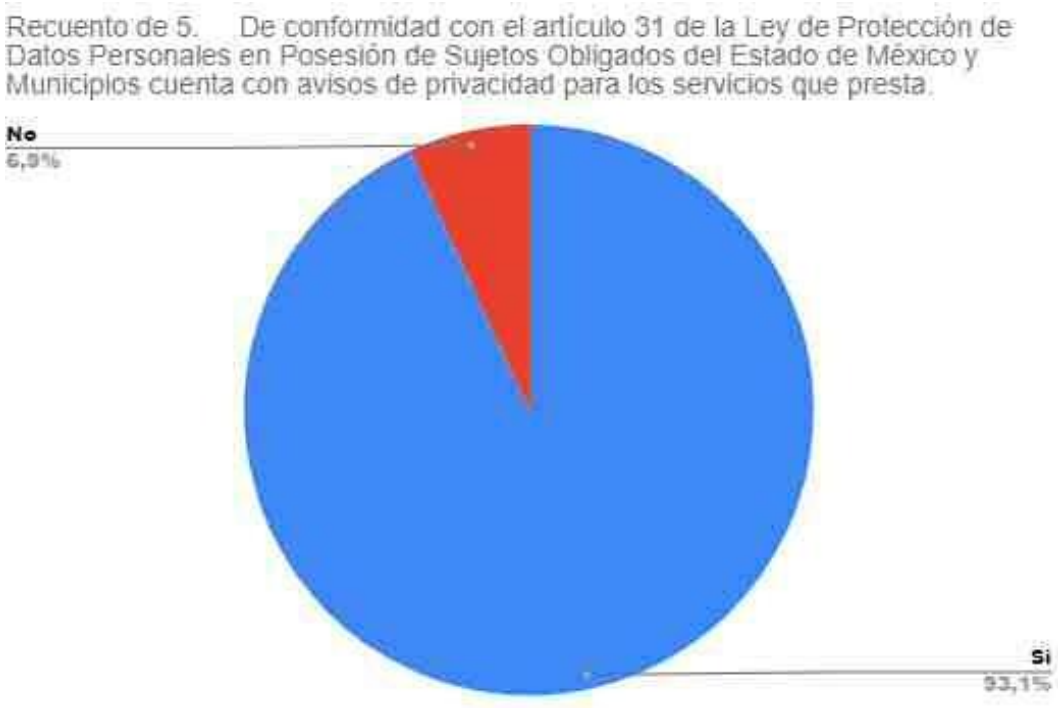
Grafica 4. Procedimiento para el ejercicio de Derechos ARCO.



Fuente: Elaboración propia a partir de los resultados de los cuestionarios hechos a los sujetos obligados.

Cuando la ley expresa que todo sujeto obligado debe garantizar el derecho a la protección de datos personales y al ejercicio de derechos ARCO, solo el 79.3 % tiene un procedimiento para garantizar dicho derecho fundamental, frente al 20.7 % que aún no tiene un procedimiento establecido, entonces sí la ley es clara, por qué no todos los sujetos obligados cumplen, quizá porque los particulares desconocemos este derecho y no sabemos cómo ejercerlo o hacer frente ante una posible vulneración de datos personales.

Grafica 5. Aviso de Privacidad.

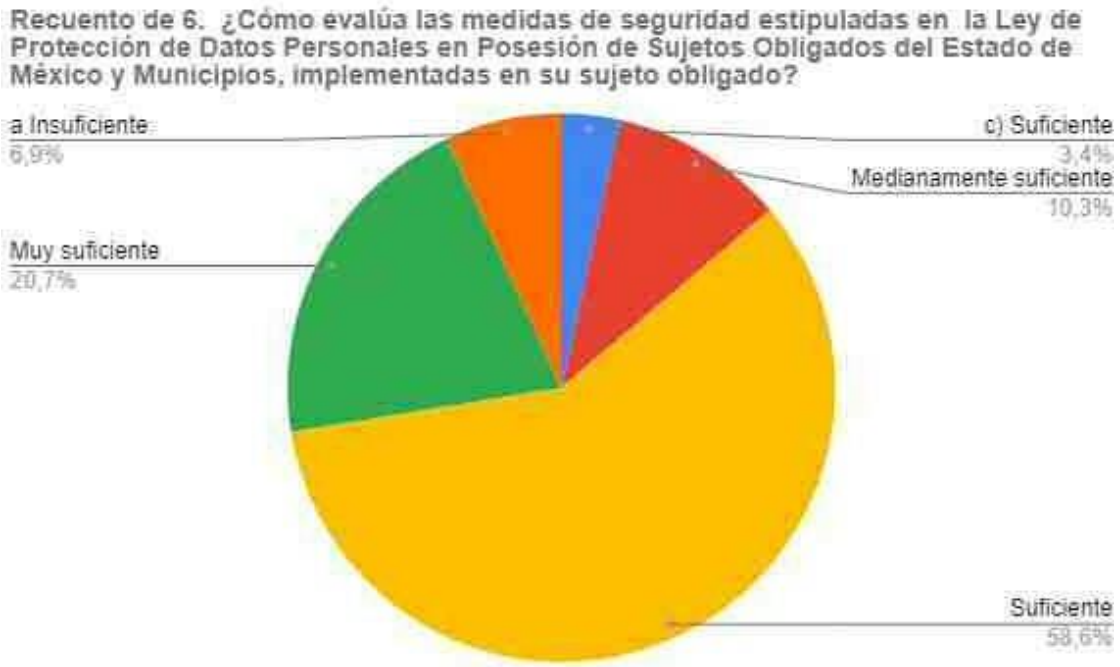


Fuente: Elaboración propia a partir de los resultados de los cuestionarios hechos a los sujetos obligados.

Siguiendo con el análisis a los resultados cualitativos y cuantitativos obtenidos se advierte que, de los 28 sujetos obligados del Estado de México, el 93.1 % cumple con lo obligación plasmada en el artículo 31 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados, el Aviso de Privacidad, el número es significativo sin embargo, no es la totalidad, y eso si es una preocupación

mayúscula, pues el aviso de privacidad es un instrumento que da cuenta de los datos personales que los sujetos obligados van a recabar, finalidad de su uso y el tratamiento de los mismos, al no contar con ese instrumento, el particular no tiene la certeza de un tratamiento adecuado y conforme a lo establecido en la normatividad.

Grafica 6. Medidas de seguridad.

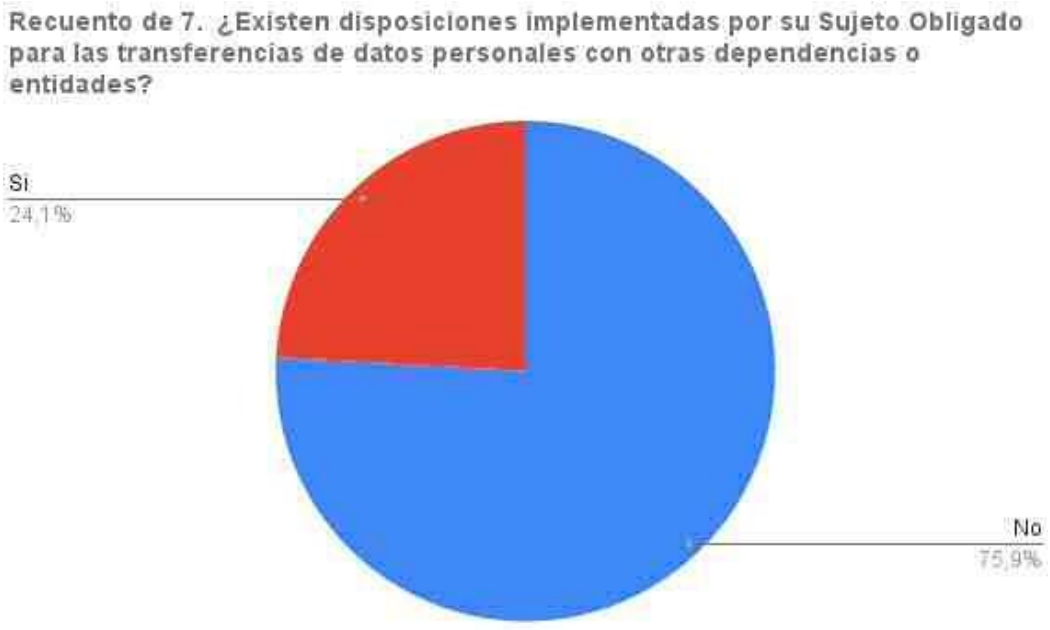


Fuente: Elaboración propia a partir de los resultados de los cuestionarios hechos a los sujetos obligados.

Siguiendo con este apartado, se preguntó a los sujetos obligados como evaluaban las medidas de seguridad que la ley estipula, se observa que los titulares de las unidades de transparencia consideran que las medidas de seguridad estipuladas en la Ley de Protección de Datos Personales son insuficientes para garantizar la adecuada protección de datos personales y el debido ejercicio de este derecho, lo que demuestra que, independientemente de lo que refiere la Ley, la percepción de

las unidades de transparencia es distinta, incrédula ante el escenario legal que resulta incongruente con lo que se vive y con lo que la sociedad enfrenta día con día, el uso indiscriminado de las redes sociales frente a la falta de conciencia e importancia de los datos personales.

Grafica 7. Disposiciones implementadas para las transferencias.

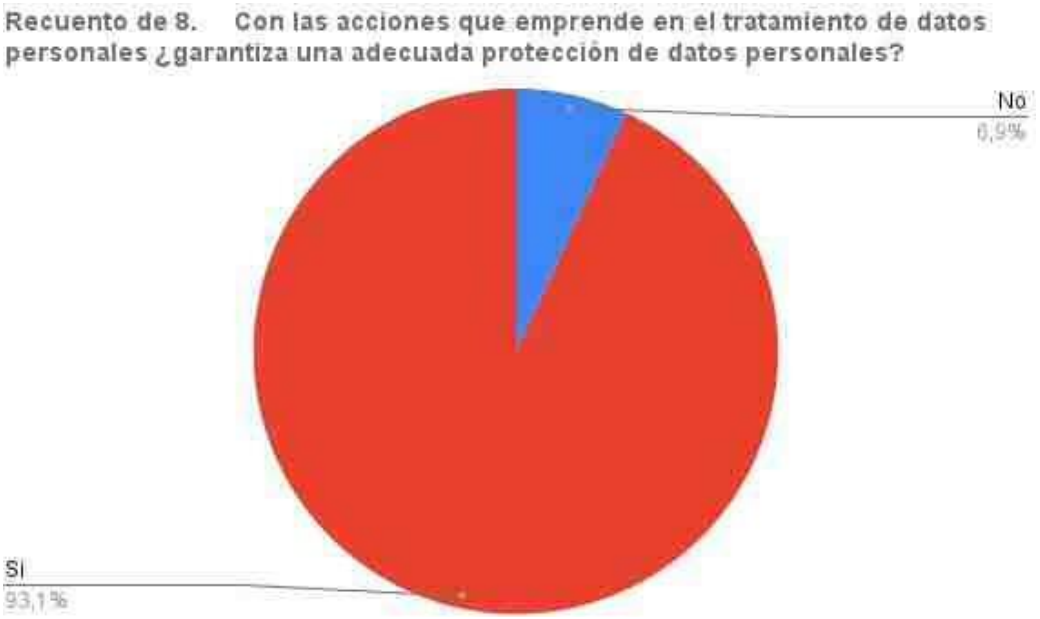


Fuente: Elaboración propia a partir de los resultados de los cuestionarios hechos a los sujetos obligados.

Con el resultado de la gráfica anterior, queda de manifiesto que a México le falta un gran camino para ser parte del Convenio 108 Plus; para adherirse a ese Convenio, México debe garantizar el flujo transfronterizo seguro de datos personales, situación que se torna difícil, si consideramos que ni entre las unidades administrativas de un mismo sujeto obligado se tiene control de las transferencias de datos personales, esa situación confirma que ni en el Estado de México se puede garantizar el flujo de datos personales entre sujetos obligados y entidades privadas, luego entonces, si no se garantiza la protección de datos personales a una menor escala (pero no

menos importante) como es que se quiere adherir a un flujo transfronterizo, cuando aún no ha quedado claro a que se refiere con un proceso de transferencia o remisión de información, considerada como confidencial.

Grafica 8. Acciones en el tratamiento de datos personales.

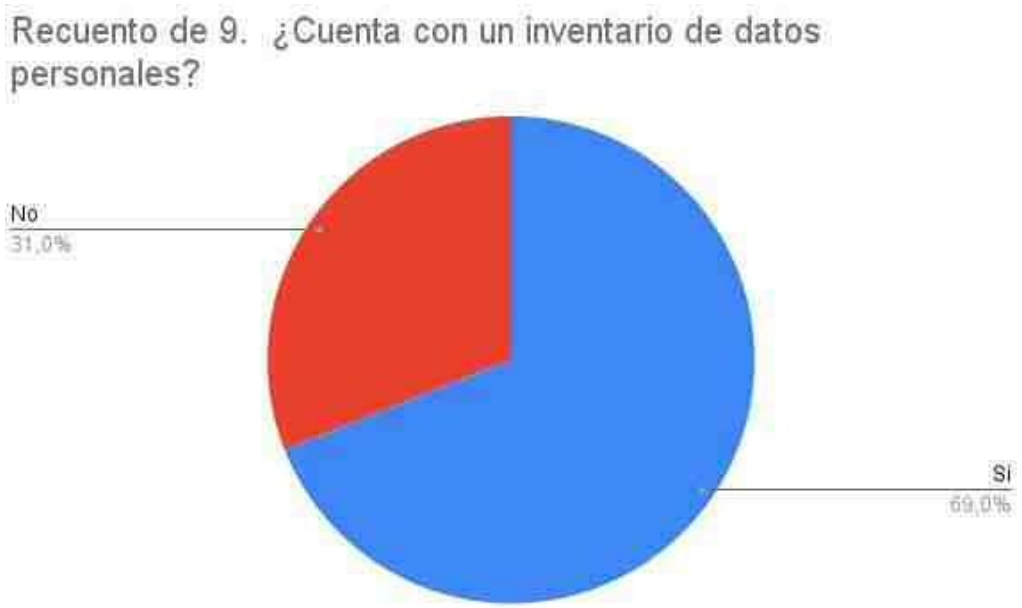


Fuente: Elaboración propia a partir de los resultados de los cuestionarios hechos a los sujetos obligados.

Se puede demostrar que el 93.1 % de los sujetos obligados consideran que con las acciones implementadas al interior de su dependencia garantiza la protección de datos personales, pero el 6.9 % considera que aún las acciones que realiza o no, son insuficientes para garantizar el derecho a la protección de datos personales; por lo que, existe una veda de oportunidad por parte del Órgano Garante a fin de homogenizar los criterios y realizar una guía que contenga las medidas de seguridad necesarias para la salvaguarda de la protección de datos personales en todos los sujetos obligados y que sus esfuerzos, no solo se dirijan al derecho de acceso a la

información pública, sino que se debe concientizar de los riesgos ocasionados por la inadecuada protección a datos personales.

Grafica 9. Inventario de Datos Personales



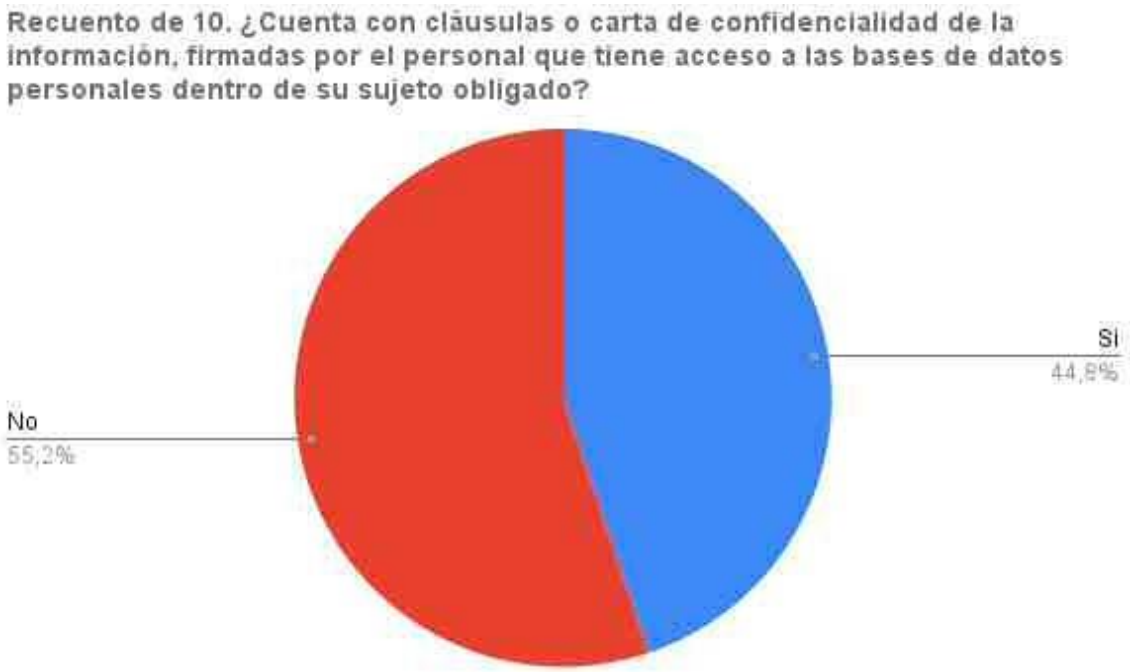
Fuente: Elaboración propia a partir de los resultados de los cuestionarios hechos a los sujetos obligados.

Según la Ley de Protección de Datos Personales, cada sujeto obligado debe contar con un inventario de datos personales, pero la misma ley no lo refiere; solo menciona que es una obligación de cada dependencia, para después elaborar y registrar un sistema de bases de datos personales, pero en ningún momento es claro, pues no existe un concepto claro de qué es un inventario de datos personales, situación que puede dejar vulnerable a los sujetos obligados que comprenden el 31% restante.

Asimismo, se puede advertir que el titular puede no tener interés sobre el tema y no se ha dado a la tarea de realizar una investigación o estudio relacionado con el tema de inventario de datos personales.

Documentos que son preponderantes para una debida protección de datos personales, luego entonces, si no se cuenta con un inventario mucho menos se va a contar con un registro ante el Infoem y tampoco el documento de seguridad el cual contiene las medidas de seguridad que cada sujeto obligado debe tener para la vulneración o incidente de datos personales.

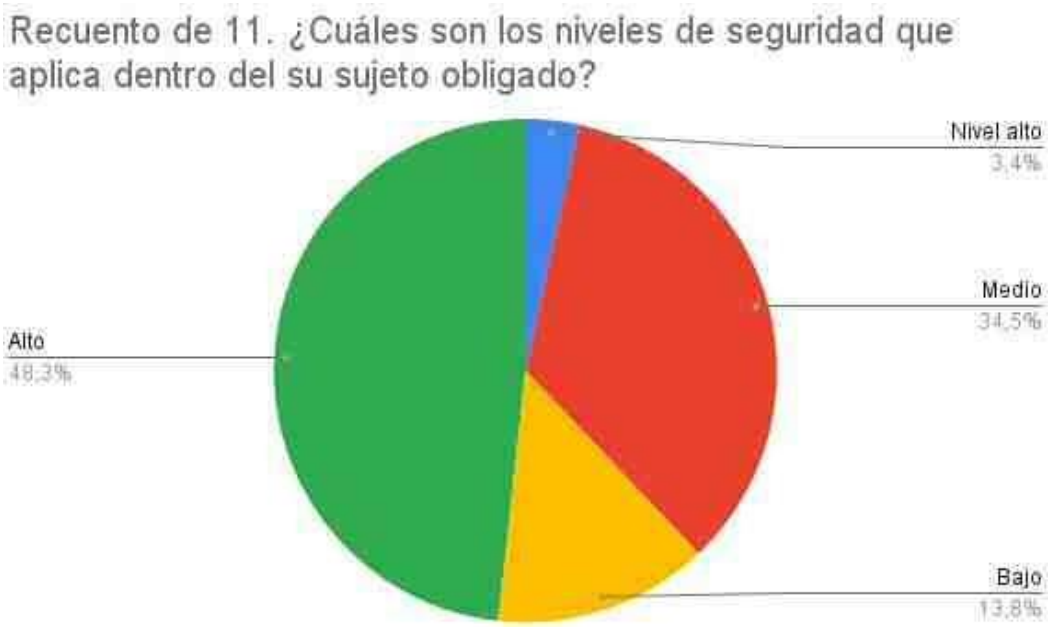
Grafica 10. Cláusulas o carta de confidencialidad



Fuente: Elaboración propia a partir de los resultados de los cuestionarios hechos a los sujetos obligados.

Aunque las cláusulas o carta de confidencialidad se usan para formalizar la transferencia, también es cierto que, es una media preventiva que cada sujeto obligado debería contar con este instrumento en su interior, ello debido a que este documento limitará el uso y divulgación de la información considerada confidencial, al saber que pueden acreedores a una sanción por no usar adecuadamente la información que maneje o de la que tengan conocimiento, y que es una manera preventiva de un incidente o vulneración de datos personales.

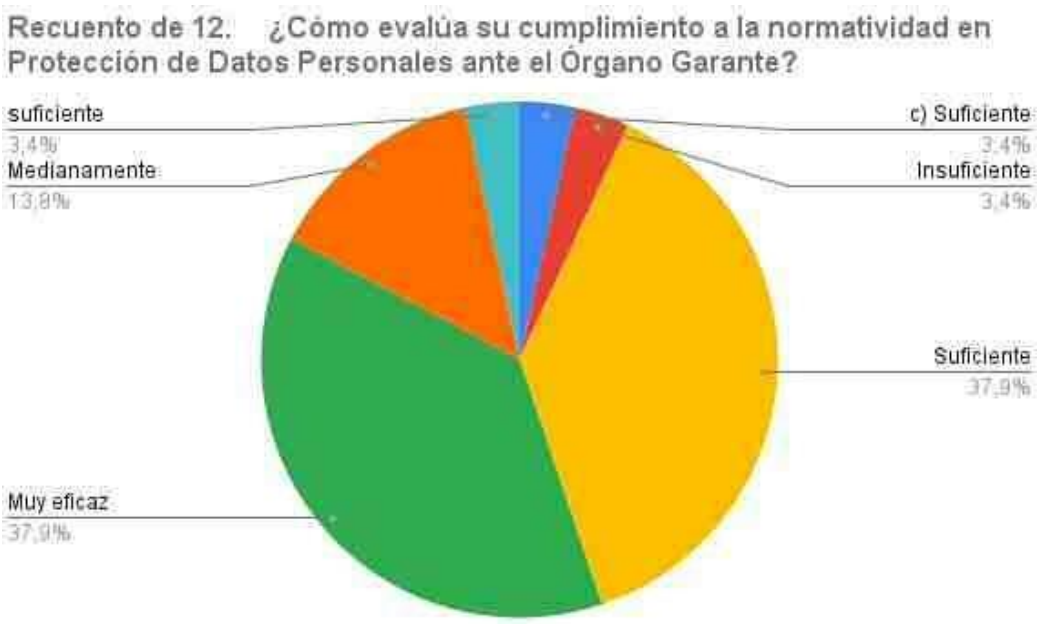
Grafica 11. Niveles de seguridad.



Fuente: Elaboración propia a partir de los resultados de los cuestionarios hechos a los sujetos obligados.

Del análisis a la presente gráfica, se advierte que supuestamente los sujetos obligados tienen un alto nivel de seguridad para la protección de datos personales, sin embargo y como ya se ha visto en las gráficas anteriores, muchos sujetos obligados no cuentan con los conocimientos básicos del derecho a la protección de datos personales, aunado a ello, también, del análisis a las anteriores gráficas se advierte que algunos sujetos obligados no tiene a disposición del titular de los datos personales los avisos de privacidad contemplados en la Ley General, Ley Federal y Leyes locales de las entidades Federativas que rigen la materia. Lo que podría generar que los resultados a esta gráfica sean subjetivos, pues con base en preguntas anteriores en algo incongruente.

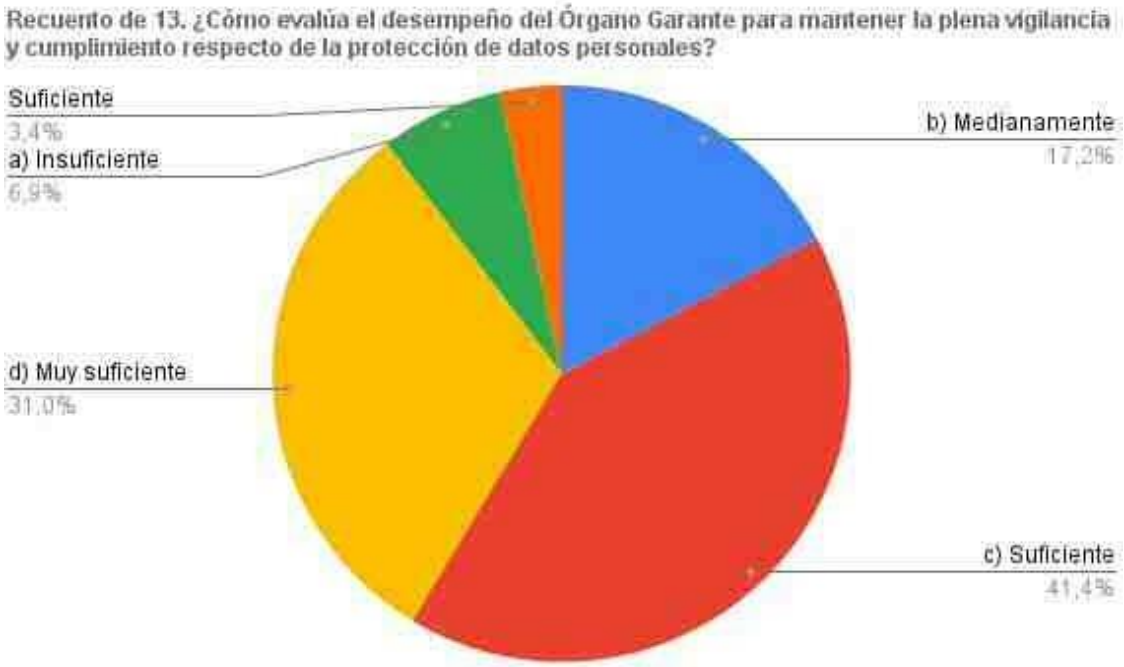
Grafica 12. Normatividad en Protección de Datos Personales.



Fuente: Elaboración propia a partir de los resultados de los cuestionarios hechos a los sujetos obligados.

De la gráfica que antecede, se puede observar que algunos sujetos obligados tienen la percepción de que la normatividad no se cumple al 100%, por ende, en los sujetos obligados a donde no se aplica la norma pueden ser candidatos a una posible vulneración o incidente, lo que provocaría una afectación a la esfera más íntima de la persona. Aquí es necesario manifestar que aún y con la aplicación de la norma se puede proteger y garantizar dicho derecho, sin embargo, la ley está prevista para actuar de manera preventiva y no correctiva, que en lo personal ese punto es lo que hace falta en la Ley de Protección de Datos Personales, que sea coercible, ya que sería una manera en la que se puede obligar a los servidores públicos a proteger y salvaguardar los datos personales.

Grafica 13. Normatividad en Protección de Datos Personales.



Fuente: Elaboración propia a partir de los resultados de los cuestionarios hechos a los sujetos obligados.

En esta grafica se puede demostrar que el Instituto de Transparencia, Acceso a la Información Pública y Protección Datos Personales, tiene áreas de oportunidad donde puede mejorar, a través de mayores capacitaciones, elaboración de documentos base que sirvan de guía para que los sujetos obligados puedan seguir y así elaborar los documentos necesarios que marca la ley, desde el debido requisitado del formato de cédula de bases de datos personales, registro en el nuevo sistema redatosem, (que dicho sea de paso ni el propio personal de ese Órgano Garante sabe cómo funciona), hasta terminar con el documento de seguridad contemplando los análisis de brecha y de riesgos.

En este orden de ideas, el Instituto debe sancionar a los sujetos obligados que incumplan esta ley, ya que el derecho a la protección de datos personales es fundamental, que, si es transgredido, no solo se pierden datos personales, sino la esfera más íntima de las personas afectando con ello, la honra, la reputación y pudiendo rechazarse de la sociedad.

Bajo este contexto, y para ir finalizando es notable traer a colación la pregunta de investigación, la cual consistió en saber ¿si son eficaces las acciones gubernamentales para el reconocimiento, ejercicio, salvaguarda y restitución del Derecho a la Protección de Datos Personales desde su institucionalización Constitucional? De la cual se ha demostrado que, aunque es cierto que existen mecanismos, políticas públicas y herramientas para proteger y ejercer datos personales, también se comprobó que aún este derecho está en construcción, ya que se debe incrementar y fortalecer la cultura de la protección de datos personales, capacitar a los titulares de las unidades de transparencia para analizar la brecha y elaborar un análisis de riesgos y su plan de contingencia ante un incidente o ante una vulneración, fortalecer los mecanismos para transferir datos personales transfronterizos o nacionales.

Asimismo y del análisis realizado a lo largo de esta investigación, se advirtió que el derecho a la protección de datos personales es un derecho ya consolidado en países de la Unión Europea, sin embargo, en América Latina aún está en proceso de implementación; no es óbice manifestar que se han realizado esfuerzos considerables para dar operatividad a lo señalado por la legislación en la materia, pero aún se está en vías de desarrollo; en México, se creó una Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual ha sido considerada por los expertos como una ley innovadora, vanguardista; acorde a los instrumentos internacionales, es decir, que cuenta con los instrumentos necesarios para garantizar el derecho a la protección de datos personales, empero, en la práctica tanto al Órgano Garante como los sujetos obligados les está costando

trabajo poner en marcha los deberes, principios y obligaciones para ejercer los derechos ARCOP y salvaguardar el derecho a la protección de datos personales.

De igual guisa, en los estados americanos se han desarrollado e implementado algunas estrategias que abordan de mejor manera desde mi perspectiva, el tema de los datos personales; probablemente las recientes publicaciones de la leyes en la materia que atiende en mayor medida a lo señalado por los tratados y convenios internacionales para mayor protección al tránsito transfronterizo de datos personales; muestra de ello son las actividades realizadas por los países como Argentina y Chile que tienen propuestas más robustas y con mayores elementos.

Con estos elementos y en atención a la Agenda 2023 aprobada por las Naciones Unidas, que incluye 17 Objetivos de Desarrollo Sostenible y que supone una oportunidad para gobiernos, sociedades, organizaciones e instituciones de emprender un nuevo camino para construir un mundo mejor y más justo; especialmente al objetivo número 16.10, que tiene como finalidad garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales; es que me permito formular una propuesta de mejora a la legislación sobre protección de datos personales.

La presente propuesta también está alineada a los trabajos de la ODCE por sus siglas en inglés, también contemplan dentro de sus directrices la protección de la privacidad y flujos transfronterizos de datos personales entre los estados miembros, comprometiéndose a reforzar la confianza en los flujos transfronterizos de datos personales y que son fundamentales para la economía tanto tradicional como la digital. Estas Directrices sobre privacidad son un punto de referencia común para proteger los datos personales y pretenden facilitar los flujos de datos transfronterizos, mientras defienden los valores democráticos, el Estado de Derecho, la protección de la privacidad y otros derechos y libertades.

Aunado a lo anterior, la propuesta se centra en la necesidad de acercar a nuestra nación a los estándares internacionales de los que México quiere adherirse, por ejemplo el convenio 108+, lo que permitirá que nuestro sistema normativo se asimile respecto de aquellos que ya lo consagran, por ejemplo la Agencia Española de Datos Personales o la nueva creación de Agencia de Protección de Datos Personales en Chile o la Dirección Nacional de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos en Argentina.

Con este orden de ideas, sería esencial dotar de mayor autoridad al Órgano Garante para sancionar a quienes incumplan la ley que rige la materia, o en su defecto se podría configurar como delito, porque ponen en riesgo la integridad física del titular de los datos personales, la honra y la reputación, pero acaso más a los integrantes de su ciclo social, pudiendo afectar a un mayor número de personas y, por consecuencia, a la sociedad que nos rodea.

Por último y una vez analizados los datos obtenidos del trabajo de gabinete, así como del análisis al avance al cuestionario que se envió a través del Sistema de Acceso a la Información Pública, el cual permitió recolectar más información de las áreas encargadas de la protección de datos personales, se advierte algunas deficiencias considerables en el quehacer institucional que pueden y deben ser solventadas desde la concepción legislativa.

CONCLUSIONES

Primera: La Unión Europea ha sido un factor para que los países latinoamericanos salvaguarden el derecho a la protección de datos personales apegados a altos estándares de regulación.

Segunda: El derecho a la protección de datos personales es un derecho fundamental consagrado en diversos ordenamientos jurídicos nacionales e internacionales.

Tercera: En México existe un marco normativo amplio en materia de protección de datos personales, sin embargo, aún se identifican desafíos para la salvaguarda de este derecho.

Cuarta: El avance tecnológico incide invariablemente en usuarios mal informados que sobre exponen sus datos personales; por lo que es imprescindible fortalecer la cultura de la protección de datos personales y ejercicio de los derechos ARCO de manera general en toda la sociedad.

Quinta: El tratamiento de los datos personales debe estar concebido para servir a la humanidad, y que, si bien es cierto, todo derecho no es absoluto, se debe interpretar funcionalmente y conservar su equilibrio al igual que otros derechos fundamentales, como el derecho a la vida, la educación y la igualdad.

Sexta: El INAI, el INFOEM y todos los órganos garantes de las Entidades Federativas son instituciones que buscan la correcta salvaguarda del derecho a la protección de datos personales, sin embargo, las reformas constitucionales atentan contra su autonomía, lo que pone en riesgo la seguridad de los datos personales.

Séptima: La falta de conocimiento del derecho a la protección de datos personales, puede provocar la violación de derechos fundamentales como la dignidad, la intimidad, no solamente de las personas que exponen o sobrexponen datos personales, sino acaso más del núcleo familiar, y que ponen en peligro la vida de los titulares de los datos personales y de la gente que los rodea.

Octava: Por lo que es imperante, avanzar en la promoción, fortalecer la protección de datos personales, que contribuirá al bienestar de las personas y al desarrollo de la sociedad en su conjunto.

ANÁLISIS CRÍTICO

Del resultado a la presente investigación se pudo advertir que tanto el Órgano Garante como los sujetos obligados carecen de la infraestructura, no solo física, sino material, humana y económica para garantizar la adecuada protección de datos personales, ya que aún hay desconocimiento del derecho fundamental a la Protección a la los Datos Personales, a ello se le agrega el avance tecnológico por lo cual se debe restructurar el andamiaje jurídico y aprovechando la reforma constitucional se considere contar con elementos que doten a los titulares de los datos personales de certeza jurídica, que se incorpore el ejercicio el derecho al olvido, el internet de las cosas, la privacidad en la era digital, y el big data y análisis de datos, modificar el acrónimo ARCO para que se adhiera el derecho a la portabilidad y quedar de la siguiente manera: ARCOP.

La desaparición del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) por parte del ejecutivo federal es una medida que ha generado preocupación y críticas por parte de diversos sectores de la sociedad. El INAI es una institución autónoma que tiene como objetivo garantizar el acceso a la información pública y promover la transparencia en el gobierno.

La propuesta de reforma para el INAI debe ser cuidadosamente analizada, considerando los posibles impactos en la rendición de cuentas y la protección de los datos personales de los ciudadanos. Es importante que cualquier reforma se realice de manera transparente y participativa, involucrando a la sociedad civil y a expertos en la materia.

Por lo que, es necesario analizar críticamente la desaparición del INAI, proponer reformas que fortalezcan su funcionamiento y combatir de manera contundente los actos de corrupción, el mal uso de recursos públicos y los nombramientos basados en lazos de amistad. La transparencia y la rendición de cuentas son fundamentales para fortalecer la democracia y construir un país más justo y equitativo.

Entonces se tiene que, si el INAI desaparece, podrían surgir varios riesgos en el manejo de los datos personales, entre ellos,

Falta de regulación y supervisión: Sin la presencia del INAI, podría haber una falta de regulación clara y consistente en el manejo de los datos personales. Además, la ausencia de supervisión y control podría aumentar el riesgo de mal uso o abuso de los datos por parte de las instituciones públicas y privadas.

Violación de la privacidad: El manejo inadecuado de los datos personales podría resultar en violaciones a la privacidad de los individuos. Sin la supervisión del INAI, las instituciones podrían no implementar medidas adecuadas de seguridad y protección de datos, lo que aumentaría el riesgo de filtraciones o accesos no autorizados a la información personal.

Uso indebido de los datos: Sin una autoridad reguladora y supervisora, las instituciones podrían utilizar los datos personales para fines no autorizados o sin el consentimiento de los individuos. Esto podría incluir el uso de los datos para actividades de mercadotecnia no deseadas, la venta de datos a terceros sin consentimiento o el uso de los datos para discriminar a ciertos grupos de personas.

Pérdida de control sobre los datos: La desaparición del INAI podría resultar en una pérdida de control sobre los datos personales de los individuos. Sin una institución que defienda y proteja los derechos de los ciudadanos en relación con sus datos, podría ser más difícil para los individuos ejercer su derecho de acceso, rectificación, cancelación y oposición (derechos ARCO) sobre sus datos personales.

Menor transparencia: El INAI promueve la transparencia en el manejo de los datos personales por parte de las instituciones públicas. Sin esta institución, podría haber menos incentivos para que las instituciones divulguen información sobre el

tratamiento de los datos personales, lo que dificultaría el monitoreo y la rendición de cuentas en el manejo de los datos.

En resumen, la desaparición del INAI podría resultar en una falta de regulación y supervisión efectivas, lo que aumentaría el riesgo de violaciones a la privacidad, uso indebido de los datos y pérdida de control sobre los mismos. Además, la falta de transparencia en el manejo de los datos personales podría dificultar el ejercicio de los derechos de los individuos y la rendición de cuentas por parte de las instituciones.

La presidenta puede proponer reformas constitucionales que afecten a los órganos autónomos, como el INAI (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) u otros organismos similares.

Las reformas constitucionales son cambios en la Constitución de un país y requieren un proceso legislativo específico para ser aprobadas. En el caso de México, la iniciativa de reforma constitucional puede ser presentada por el presidente, los legisladores o por un porcentaje determinado de ciudadanos.

Si la presidenta propone reformas constitucionales que afecten a los órganos autónomos, es importante, considerar el impacto que esto podría tener en la autonomía e independencia de estos organismos. La autonomía de los órganos autónomos es fundamental para su correcto funcionamiento y para garantizar que puedan cumplir con sus atribuciones de manera imparcial y sin interferencias políticas.

Es necesario evaluar cada propuesta de reforma constitucional en detalle para determinar cómo podría afectar a los órganos autónomos y si se garantiza su independencia y autonomía. Además, es importante promover un debate amplio y participativo sobre estas reformas, considerando las opiniones de expertos, de la sociedad civil y de los propios organismos autónomos.

MARCO PROPOSITIVO

Una vez analizado cada uno de los puntos de interés en esta investigación es oportuno recordar la pregunta de investigación ¿son eficaces las acciones gubernamentales para el reconocimiento, ejercicio, salvaguarda y restitución del Derecho a la Protección de Datos Personales desde su institucionalización Constitucional? Ante el escenario actual, refiriéndome al cambio del ejecutivo federal y la tan anunciada reforma constitucional, en el que se pretende desaparecer al órgano garante de estos derechos, para algunos actores políticos la reforma tiene el propósito de rediseñar el rumbo de la burocracia en la materia por considerar muy costoso el mantener un instituto como el INAI, sin embargo, el discurso de la administración saliente y la actual es el mismo.

El mandato presidencial se ha caracterizado por soberbio, autoritario e impositivo con una clara tendencia a quitar todo aquello que es contrario a sus ideales o intereses, muestra de ello el INE y el INAI, que han servido de contrapeso al poder ejecutivo, situación que no le gustó y que derivó en estas iniciativas, pero no hay que perder de vista lo fundamental, la garantía de dos derechos fundamentales, el acceso a la información pública y el de protección de datos personales.

Los cambios son buenos, siempre y cuando sirvan para mejorar, para hacer algo benéfico; por lo que en aras de contribuir al fortalecimiento del derecho a la protección de datos personales y ante la eminente desaparición del INAI, considero viable realizar los siguientes ajustes:

A través de esta investigación, se advirtió que el derecho a la protección de datos personales es un derecho ya consolidado en países de la Unión Europea, sin embargo, en América Latina aún está en proceso de implementación; no es óbice manifestar que se han realizado esfuerzos considerables para dar operatividad a lo señalado por la legislación en la materia, pero aún se está en operación ; en México, se creó una Ley General de Protección de Datos Personales en Posesión de Sujetos

Obligados, la cual ha sido considerada por los expertos como una ley innovadora, vanguardista; acorde a los instrumentos internacionales, es decir, que cuenta con los instrumentos necesarios para garantizar el derecho a la protección de datos personales, empero, en la práctica tanto al Órgano Garante como los sujetos obligados les está costando trabajo poner en marcha los deberes, principios y obligaciones para ejercer los derechos ARCOP y salvaguardar el derecho a la protección de datos personales.

De igual guisa, en los estados americanos se han desarrollado e implementado algunas estrategias que abordan de mejor manera desde mi perspectiva, el tema de los datos personales; probablemente las recientes publicaciones de la leyes en la materia que atiende en mayor medida a lo señalado por los tratados y convenios internacionales para mayor protección al tránsito transfronterizo de datos personales; muestra de ello son las actividades realizadas por los países como Argentina y Chile que tienen propuestas más robustas y con mayores elementos.

Con estos elementos y en atención a la Agenda 2023 aprobada por las Naciones Unidas, que incluye 17 Objetivos de Desarrollo Sostenible y que supone una oportunidad para gobiernos, sociedades, organizaciones e instituciones de emprender un nuevo camino para construir un mundo mejor y más justo; especialmente al objetivo número 16.10, que tiene como finalidad garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales; es que me permito formular una propuesta de mejora a la legislación sobre protección de datos personales e informar con claridad cuál es la finalidad de la obtención de datos personales, y la aplicación de manera correcta al principio de proporcionalidad, el cual consiste en informar a los titulares de los datos personales cuál será el tratamiento de los datos personales y qué únicamente serán utilizados para ese fin.

La presente propuesta también está alineada a los trabajos de la OCDE por sus siglas en inglés, también contemplan dentro de sus directrices la protección de la

privacidad y flujos transfronterizos de datos personales entre los estados miembros, comprometiéndose a reforzar la confianza en los flujos transfronterizos de datos personales y que son fundamentales para la economía tanto tradicional como la digital. Estas Directrices sobre privacidad son un punto de referencia común para proteger los datos personales y pretenden facilitar los flujos de datos transfronterizos, mientras defienden los valores democráticos, el Estado de Derecho, la protección de la privacidad y otros derechos y libertades.

Aunado a lo anterior, la propuesta se centra en la necesidad de acercar a nuestra nación a los estándares internacionales de los que México quiere adherirse, por ejemplo, el convenio 108 plus, lo que permitirá que nuestro sistema normativo se asimile respecto de aquellos que ya lo consagran, por ejemplo, la Agencia Española de Datos Personales y poder informar con mayor detenimiento, cuál es el tratamiento claro y concreto a los datos personales atendiendo el principio de proporcionalidad.

Por tal motivo se considera necesaria la creación de una **institución abocada únicamente a la protección de datos personales, en posesión de particulares y de sujetos obligados, que marque las directrices sobre las cuales se rija la protección de datos ceñidas a los estándares internacionales, a los Objetivos del Desarrollo Sostenible, y a la normativa local.**

El objetivo de esta instancia será velar por la protección de los datos personales, el tratamiento de los mismos. Esto implica garantizar que los datos personales sean utilizados de manera segura, confidencial y respetando las normas y regulaciones establecidas en materia de protección de datos.

El organismo estaría encargado de desarrollar políticas y regulaciones eficientes en el ámbito de la protección de datos personales, con el fin de establecer estándares de seguridad y privacidad para las entidades públicas y privadas que manejan información personal.

Dentro de sus responsabilidades se encuentra las siguientes:

- Brindar asesoramiento y orientación a las personas sobre sus derechos y deberes en relación a la protección de sus datos personales.
- Informar a los ciudadanos sobre cómo ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad (ARCOP)
- Educar sobre las mejores prácticas para proteger la privacidad en el entorno digital.
- Recibir y gestionar denuncias y reclamos relacionados con el tratamiento de datos personales
- Investigar posibles violaciones a la normativa y aplicar las sanciones correspondientes en caso de incumplimiento.

La estructura orgánica propuesta:

- Dirección: Encargada de la planeación estratégica y supervisión general del organismo.
- Secretaría Ejecutiva: Responsable de la coordinación y gestión administrativa del organismo.
- Área de Asesoría Jurídica: Brinda asesoramiento legal en materia de protección de datos y realiza análisis y evaluación de casos.
- Área de Normatividad y Regulación: Encargada de desarrollar y actualizar las normativas y regulaciones en materia de protección de datos.
- Área de Capacitación y Divulgación: Realiza actividades de capacitación y sensibilización sobre la protección de datos dirigidas a distintos públicos.
- Área de Investigación y Análisis: Realiza estudios e investigaciones sobre temas relacionados con la protección de datos y análisis de casos.
- Área de Atención a Denuncias: Recibe, evalúa y gestiona las denuncias y reclamaciones relacionadas con el tratamiento de datos personales.

- Área de Tecnologías de la Información: Encargada de la seguridad y gestión de la infraestructura tecnológica del organismo.

Ante la inminente desaparición del INAI crear un instituto con características básicas como las referidas, resulta viable y funcional, considerando que el grado de importancia y los retos que enfrentan los datos personales cada día son más interesantes, con la evolución descontrolada de la inteligencia artificial, y el desarrollo de tecnologías sofisticadas, los responsables del tratamiento de los datos personales parece que van a pie cuando la tecnología avanza a la velocidad de la luz.

Por ello es importante que desde la academia y mediante la participación de la comunidad universitaria se gesten ideas que puedan fortalecer la administración de los recursos legales y contribuyan al fortalecimiento las garantías y los derechos fundamentales.

Bibliografía

Sánchez Pérez, G., & Rojas González, I. (2018). Leyes de Protección de datos personales en el mundo y la protección de datos biométricos – PARTE I. *Seguridad*.

Bolivia, C. I. (20 de 06 de 2024). *Cumbre Iberoamericana Santa Cruz de la Sierra Bolivia* . Obtenido de Cumbre Iberoamericana Santa Cruz de la Sierra Bolivia : https://www.segib.org/wp-content/uploads/DeclaraciondeSantaCruz.pdf

Colombia, C. d. (24 de Marzo de 2023). *Secretaría General del Senado* . Obtenido de http://www.secretariasenado.gov.co/constitucion-politica

Comisión Interamericana de Derechos Humanos . (11 de 10 de 2023). Obtenido de Comisión Interamericana de Derechos Humanos : https://www.oas.org/es/cidh/mandato/basicos/declaracion.asp

Constituyente, A. N. (24 de Marzo de 2023). *Asamblea Nacional Constituyente*. Obtenido de https://www.asambleanacional.gob.ec/sites/default/files/documents/old/constitucion_de_bolsillo.pdf

Contituyente, C. G. (24 de Marzo de 2023). *Ministerio de Justicia y Derechos Humanos* . Obtenido de https://www.argentina.gob.ar/sites/default/files/constitucion-argentina_lectura-facil_0.pdf

Convención Americana sobre Derechos Humanos. (11 de 10 de 2023). Obtenido de https://www.cidh.oas.org/basicos/spanish/basicos2.htm

Enríquez, L. (24 de Marzo de 2023). *Universidad Andiana Simón Bolívar* . Obtenido de https://www.uasb.edu.ec/ciberderechos/

Enríquez, O. A. (2023). Marco Jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. *Revista IUS del Instituto de Ciencias Jurídicas de Púebla A.C.*, 272-274.

Ernesto, A. C. (2009). El derecho a la Información y la protección de datos personales en el contexto general y su construcción teórica y jurídica. *Revista del Instituto de Ciencias Jurídicas de Puebla A.C.* , 5-10.

García González, A. (2007). La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado. *Boletín Mexicano de Derecho Comparado*, 13-20.

Guzman Camacho, J. J. (21 de 06 de 2024). *Blibliotec Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM* . Obtenido de https://revistas.juridicas.unam.mx/index.php/derecho-informacion/article/view/18070/18338

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2006). *Metodología de la investigación* (Cuarta ed.). Distrito Federal: Mc Graw Hill.

Humanos, C. A. (26 de 04 de 2023). *Convención Americana sobre Derechos Humanos*. Obtenido de https://www.corteidh.or.cr/tablas/17229a.pdf

INAI. (s.f.). Obtenido de INAI: https://home.inai.org.mx/?page_id=1626

INAI. (11 de 10 de 2023). *Diccionario de Protección de Datos Perosnales "CONCEPTOS FUNDAMENTALES"*. Obtenido de https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf

Instituto de Acceso a la Información Pública y Protección de Datos Personales del Distrito Federal, I. (2011). *Texto de apoyo a la formación de servidores públicos en el conocimiento de las leyes de trasnaprencia y protección de datos personales.* Ciudad de México: Editorial Gráfico y/o Omar Aguilar Sánchez.

Instituto Nacional de Transaprencia, A. a. (18 de ABRIL de 2023). *ACUERDO MEDIANTE EL CUAL SE APRUEBAN, LOS LINEAMIENTOS GENERALES dDE PROTECCIÓN DE DATOS PERSONALES PARA EL SECTOR PÚBLICO*. Obtenido de https://www.cenace.gob.mx/Docs/Transparencia/Normatividad/12.%20Lineamientos%20Generales%20de%20Protecci%C3%B3n%20de%20Datos%20Personales%20para%20el%20Sector%20P%C3%BAblico.pdf

La declaración Universal de los Derechos Humanos. (11 de 10 de 2023). Obtenido de La declaración Universal de los Derechos Humanos: https://www.un.org/es/about-us/universal-declaration-of-human-rights

Legislatura, Q. N. (25 de 04 de 2023). *Periódico Oficial del Gobierno del Estado de México*. Obtenido de https://www.infoem.org.mx/doc/normatividad/L_Ley_de_Proteccion_de_Datos_Personales_en_Posesion_de_Sujetos_Obligados_del_Estado_de_Mexico_y_Municipios.pdf

Ley de Protección de Datos Personales en Posesión de Sujetos Obligados del Estado de México y Municipios. (11 de 10 de 2023). Obtenido de https://legislacion.edomex.gob.mx/sites/legislacion.edomex.gob.mx/files/files/pdf/ley/vig/leyvig244.pdf

Lorenzetti, L. R. (24 de 06 de 2024). *LA ESFERA INTIMA DE LA PERSONA Y LA ACTIVIDAD MEDICAL*. Obtenido de LA ESFERA INTIMA DE LA PERSONA Y LA ACTIVIDAD MEDICAL: http://www.notivida.com.ar/Articulos/Aborto/La%20esfera%20intima%20de%20la%20persona%20y%20la%20actividad%20medical.html#:~:text=La%20esfera%20%C3%ADntima%20(3)%20es,su%20comportamiento%20sobre%20los%20dem%C3%A1s.

Nacional, O. J. (24 de Marzo de 2023). *Orden Jurídico Nacional* . Obtenido de http://www.ordenjuridico.gob.mx/constitucion.php#gsc.tab=0

Pacto Internacional de Derechos Civiles y Políticos. (11 de 10 de 2023). Obtenido de Pacto Internacional de Derechos Civiles y Políticos: https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Personales, A. E. (21 de 06 de 2024). *aepd agencia española protección de datos personales* . Obtenido de https://www.aepd.es/preguntas-frecuentes/1-tus-derechos/FAQ-0113-que-es-el-derecho-a-la-portabilidad-de-los-datos#:~:text=Es%20el%20derecho%20del%20afectado,que%20se%20los%20hubiera%20facilitado.

Piña Libien, H. R. (21 de 06 de 2024). *Diálogos Jurídicos entre España y México*. Obtenido de http://ri.uaemex.mx/bitstream/handle/20.500.11799/110864/Dialogos_juridicos_8.pdf?sequence=1&isAllowed=y

Pública, I. F. (Julio de 2008). Obtenido de https://iaipoaxaca.org.mx/biblioteca_virtual/datos_personales/5.pdf

Reglamento (UE) 2016/ 679 del Parlamento. (27 de 04 de 2016). Obtenido de Reglamento (UE) 2016/ 679 del Parlamento: https://www.boe.es/doue/2016/119/L00001-00088.pdf

República, C. d. (24 de Marzo de 2023). *Congreso de la República* . Obtenido de https://www.congreso.gob.pe/Docs/constitucion/constitucion/index.html

Ricard, M. M. (2007). El derecho fundamental a la protección de datos personales: perpectivas. *Revista de Internet, Derecho y Política*, 2-8.

Ricci, D. G. (2023). Artículo 16 Constitucional Derecho a la Privacidad. En D. G. Ricci. Mexico : Instituto de Investigaciones Jurídicas de la UNAM .

Ricci, D. G. (2023). *Artículo 16 Constitucional.* México: Instituto de Investigaciones Jurídicas, Suprema Corte de Justicia de la Nación, Fundación Kond Adenauer.

Rogelio, L. S. (2012). El efecto horizontal del derecho a la protección de datos personales en México. *Cuestiones Constitucionales*, 5-11.

Transparencia, S. N. (18 de 04 de 2023). *Sistema Nacional de Transparencia*. Obtenido de https://snt.org.mx/?page_id=431

Unidas, O. d. (26 de 04 de 2023). *ccpr_SP.pdf*. Obtenido de https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/ccpr_SP.pdf

Unidas, O. d. (26 de 04 de 2023). *UDHR_booklet_SP_web.pdf*. Obtenido de https://www.un.org/es/documents/udhr/UDHR_booklet_SP_web.pdf

Unión, C. d. (24 de 04 de 2023). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* . Obtenido de https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Unión, C. D. (20 de 06 de 2024). *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*. Obtenido de Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Unión, C. d. (21 de 06 de 2024). *Reglamento de la Ley Federal de Protección de Datos Personales en*. Obtenido de https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf