Compilado sobre transparencia,
privacidad y la era digital
del INFO CDMX

EL DERECHO DE PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

Olivia Andrea Mendoza Enríquez

AUTORA

01

U N A M

FACULTAD DE DERECHO

Olivia Andrea Mendoza Enríquez

Profesora Investigadora Titular de Tiempo Completo de la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas (CIDE). Miembro del Sistema Nacional de Investigadores, Nivel I de la Secretaría de Ciencia, Humanidades, Tecnología e Innovación (SECIHTI). Ha sido reconocida dentro de las 15 abogadas más influyentes de México por su labor profesional por la revista *Foro Jurídico* edición 2024.

El derecho de protección de datos personales en México

OLIVIA ANDREA MENDOZA ENRÍQUEZ

U N A M
FACULTAD DE DERECHO

info
Compilado sobre transparencia, privacidad y la era digital del INFO CDMX

Título
El derecho de protección de datos personales en México

© ***Autora***
Olivia Andrea Mendoza Enríquez

Compilado sobre Transparencia, Privacidad y la Era Digital del INFO CDMX

Editora
Patricia Daniela Lucio Espino

ISBN: 978-607-642-223-6

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE DERECHO
Ciudad Universitaria
Coyoacán, 04510
Ciudad de México
www.derecho.unam.mx

La presente obra ha sido dictaminada y aprobada para su publicación, de acuerdo con el sistema de revisión por pares doble ciego, por el Comité Editorial del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México 2025.

Diseño de interiores y portada UNAM, 2025.

Comité Editorial del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México 2025

Mtra. Laura Lizette Enríquez Rodríguez
Comisionada Presidenta del INFO CDMX

Dr. Julio César Bonilla Gutiérrez
Comisionado Ciudadano del INFO CDMX

Dra. Sonia Venegas Álvarez
Especialista externa

Dra. Patricia Daniela Lucio Espino
Especialista externa

Mtro. Juan Gómez Pérez
Especialista externo

Coordinadora del Comité
Lcda. Nora Angelica Damian Santiago
Directora de Vinculación y Proyección Estratégica del INFO CDMX

Secretaria Técnica del Comité
Lcda. Georgina Mena López
Directora de Comunicación Social del INFO CDMX

info
Compilado sobre transparencia, privacidad y la era digital del INFO CDMX

Pleno del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México

Laura Lizette Enríquez Rodríguez
Comisionada Presidenta
del INFO CDMX

Julio César Bonilla Gutiérrez
Comisionado Ciudadano
del INFO CDMX

María del Carmen Nava Polina
Comisionada Ciudadana
del INFO CDMX

Compilado sobre transparencia,
privacidad y la era digital
del INFO CDMX

Universidad Nacional Autónoma de México

Leonardo Lomelí Vanegas
Rector

Patricia Dolores Dávila Aranda
Secretaria General

Facultad de Derecho

Sonia Venegas Álvarez
Directora

Sarah Mis Palma León
Secretaria General

U N A M
FACULTAD DE DERECHO

Coordinación Editorial de la Facultad de Derecho

Patricia Daniela Lucio Espino
Coordinadora Editorial y Editora

Alan David Barraza Guerrero
Ana María Ramírez Sánchez
Coeditores y Validación de Contenidos

María Concepción Cárdenas Ostria
Cinthya Gutiérrez Ruiz
Corrección de Estilo

Michelle Sánchez Cabello
Ricardo Pérez Rodríguez
Diseño Editorial

Jonathan Salvador Bastida Ávila
Protección a la Propiedad Intelectual

Jennifer Valeria Galicia Bastida
Asistente Administrativo

Mariana Areli Santos Osnaya
Mariana Basilio Añorve
Miguel Hernández Morales
Alicia Monserrat Velázquez Arias
Ximena Guadalupe Viccon Hernández
Servicio social y prácticas profesionales

FACULTAD DE DERECHO-UNAM
COORDINACIÓN
EDITORIAL
- LEX -

Índice

Capítulo III

Desafíos del derecho de protección de datos personales desde una óptica de los derechos humanos

Prólogo

Mtra. Laura Lizette Enríquez Rodríguez[1]

Vivimos una época sin precedentes en la historia de la humanidad, marcada por una aceleración tecnológica vertiginosa. Las capacidades de recopilación, análisis, almacenamiento y transferencia de datos se han multiplicado exponencialmente, transformando no sólo a la economía, sino también las relaciones sociales, políticas, culturales y, en última instancia, nuestra concepción de la dignidad humana.

Tan sólo en 2024, se estima que el número de usuarios de internet en el mundo alcanzó los 5.5 mil millones, lo que representa el 68% de la población global (ITU, 2024). Esta expansión digital no sólo ha democratizado el acceso a la información y al conocimiento, sino que también ha intensificado la recolección masiva de datos personales a través de plataformas, dispositivos y servicios conectados. Cada clic, búsqueda, ubicación o preferencia queda registrada y potencialmente perfilada, comercializada o incluso manipulada.

Este contexto de hiperconectividad, se suma al desarrollo de nuevas tecnologías, como la inteligencia artificial, que no sólo ha redefinido la forma en que interactuamos en nuestro día a día, sino que también ha planteado preguntas profundas sobre autonomía, consentimiento y control sobre nuestros propios datos.

En ese sentido, la privacidad, otrora concebida como un refugio estático, se ha transformado en un derecho dinámico que exige nuevas herramientas jurídicas. El derecho a la protección de datos personales se erige como una respuesta imprescindible a los desafíos de la sociedad digital contemporánea, con el objetivo de garantizar que el desarrollo tecnológico sirva al bienestar humano y no comprometa derechos fundamentales.

Esta realidad ha hecho ineludible la necesidad de contar con un marco normativo sólido que garantice los derechos fundamentales de las personas. Modelos cada vez más sofisticados son capaces de procesar enormes volúmenes de datos personales en tiempo real, anticipar comportamientos, generar perfiles detallados y tomar decisiones automatizadas que impactan directamente la vida de las personas.

[1] Comisionada Presidenta del INFO CDMX.

Durante las últimas décadas, este derecho ha transitado de ser una extensión de la privacidad a consolidarse como un derecho autónomo, transversal y progresivo, reconocido en instrumentos internacionales y consagrado en las constituciones de numerosos países, incluido México.

Su fortalecimiento ha sido impulsado por una creciente conciencia social, por el acelerado avance tecnológico que permite un tratamiento masivo de información, y, especialmente, por los múltiples casos vinculados al uso indebido o explotación de datos sensibles, que han evidenciado la necesidad de proteger la autodeterminación informativa de las personas.

Así, el tratamiento de datos personales ha dejado de ser una cuestión meramente técnica o administrativa para convertirse en uno de los principales temas de debate ético, jurídico y político de nuestro tiempo.

Actualmente, más de 150 países cuentan con legislación específica en materia de protección de datos personales (UNCTAD, 2025), cada uno con distintos enfoques y niveles de exigencia. Mientras algunos adoptan modelos comprehensivos, como el Reglamento General de Protección de Datos de la Unión Europea, otros han optado por enfoques sectoriales o fragmentados, como en el caso de los Estados Unidos.

Estos marcos legales han evolucionado con la incorporación de principios como la privacidad desde el diseño, la rendición de cuentas, el consentimiento informado, la minimización de datos y el derecho a la portabilidad, evidenciando el carácter técnico y evolutivo de este derecho.

En el caso mexicano, el derecho a la protección de datos personales comenzó a consolidarse normativamente con la reforma constitucional de 2009, seguida de la promulgación de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010) y, posteriormente, con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017).

Estos hitos fueron clave para establecer principios rectores, derechos ARCO y obligaciones para entes públicos y privados. Hoy, este derecho se encuentra en un momento de transformación derivado de la reforma constitucional de 2024 en materia de simplificación orgánica, así como de las leyes secundarias en materia de acceso a la información pública y protección de datos personales, que han supuesto un rediseño institucional para su garantía.

Anteriormente, la protección de datos personales en México se concentraba en un modelo unificado bajo una autoridad garante nacional, que supervisaba tanto al sector público federal como al privado. Con el nuevo modelo derivado de esta reforma constitucional y las leyes en la materia, esta responsabilidad se descentraliza, pasando a una autoridad para el sector privado y a 16 autoridades a nivel federal para el sector público.

En este contexto de cambio, resulta especialmente oportuno analizar y estudiar la evolución del derecho a la protección de datos personales en México. Por ello, desde el Comité Editorial del Instituto de Transparencia, Acceso a la Información Pública,

Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO CDMX), hemos impulsado diversos proyectos que buscan contribuir a la comprensión crítica de los cambios que configuran este derecho.

La obra que el lector tiene en sus manos constituye precisamente un esfuerzo por ofrecer una visión integral sobre el derecho de protección de datos personales, un campo relativamente reciente en el panorama jurídico, pero de enorme trascendencia en la vida pública y privada. A lo largo de los capítulos de esta obra, Olivia Andrea Mendoza Enríquez, una de las mayores autoridades académicas en materia de protección de datos personales en México, presenta un análisis que combina rigor técnico con una mirada práctica a los principales desafíos que enfrenta este derecho en el contexto actual.

En primer término, se revisa su relación con el derecho a la privacidad, distinguiendo conceptos y reflexionando sobre las aportaciones que la protección de datos ofrece para garantizar la vida privada de las personas. Posteriormente, se explora la evolución del marco jurídico mexicano, los principios rectores que lo sostienen, así como nuevas figuras y tensiones que se desprenden de su ejercicio frente a intereses como la seguridad nacional o la salud pública.

La obra también ofrece un panorama internacional al examinar los compromisos que México ha adquirido en la materia, y recupera criterios relevantes tanto de la Corte Interamericana de Derechos Humanos como de la Suprema Corte de Justicia de la Nación. Con ello, se delínean no sólo los avances, sino también los retos que impone la era digital, en especial la salvaguarda de los derechos humanos en el ciberespacio.

Finalmente, el libro adquiere un carácter especialmente oportuno al situarse en un momento de transición institucional: la reconfiguración del sistema de transparencia y protección de datos personales en México. Este contexto lo convierte en un referente obligado para comprender no sólo la evolución normativa y doctrinal del derecho de protección de datos personales, sino también las interrogantes que hoy se abren para su futuro.

Se trata de una obra novedosa y de actualidad que contribuye a la consolidación de la cultura de la privacidad en nuestro país, acercando a los operadores jurídicos, académicos y a la sociedad en general, los elementos necesarios para comprender, reflexionar y debatir sobre uno de los derechos más relevantes de nuestra era digital.

Este esfuerzo editorial fortalece la formación especializada y propicia una reflexión colectiva e informada en torno a derechos fundamentales que, lejos de perder vigencia, adquieren cada vez mayor relevancia frente al avance de tecnologías emergentes.

Es importante subrayar que el futuro de la protección de datos personales en México no puede comprenderse únicamente como un debate jurídico o técnico, exige la construcción de una hoja de ruta clara que articule instituciones sólidas, regulación moderna y una sociedad crítica capaz de exigir sus derechos.

Esta agenda debe tener presente, en primer lugar, el fortalecimiento de las instituciones y del marco normativo. Ante el rediseño orgánico del sistema de transparencia y privacidad, el país enfrenta el reto de garantizar que la nueva estructura institucional cuente con capacidades técnicas suficientes para cumplir con sus atribuciones.

El segundo gran tema que esta agenda no puede perder de vista está relacionado con las tecnologías y los derechos emergentes. México no puede permanecer ajeno a los desafíos que plantean la inteligencia artificial, el reconocimiento facial, los datos biométricos o las neurotecnologías. Estos desarrollos exigen reglas precisas que limiten los riesgos de vigilancia masiva y discriminación, al tiempo que reconozcan nuevos derechos, como el derecho al olvido, a la desconexión digital, a la explicación frente a decisiones automatizadas y a la autodeterminación algorítmica. Se trata de buscar en todo momento una regulación que proteja derechos sin inhibir la innovación.

Finalmente, cualquier agenda en la materia debe concebirse desde la perspectiva de una sociedad digital con enfoque de derechos humanos. Ello implica apostar por la alfabetización digital y la cultura de la privacidad como herramientas de empoderamiento ciudadano, en particular para niñas, niños, adolescentes y personas en situación de vulnerabilidad. Supone también incorporar un enfoque interseccional que atienda las desigualdades estructurales que inciden en la protección efectiva de los datos personales, así como fortalecer la cooperación internacional para asegurar estándares globales y reglas claras en la transferencia transfronteriza de información.

En suma, hablar de datos personales en México es hablar del presente y del futuro de la democracia. La solidez institucional, la regulación de las tecnologías emergentes y la construcción de una sociedad digital con enfoque de derechos humanos no son aspiraciones abstractas, sino condiciones mínimas para garantizar la autodeterminación informativa en el siglo XXI. Esta obra se inserta en ese horizonte, no sólo como una aportación académica, sino como una invitación a reflexionar colectivamente sobre el rumbo que debe tomar nuestro país para proteger uno de los derechos más decisivos de nuestro tiempo.

La defensa de la privacidad y de la autodeterminación informativa constituye uno de los mayores retos de esta era digital. No basta con marcos normativos sólidos, se requiere voluntad política, instituciones fuertes, ciudadanía crítica y un debate constante que acompañe la innovación tecnológica.

Este libro no sólo busca abrir un espacio de comprensión y debate, sino también sembrar la convicción de que la protección de los datos personales es una tarea compartida. En el marco del décimo noveno aniversario del INFO CDMX, asumimos la responsabilidad de seguir impulsando una agenda que, frente a los retos tecnológicos, sociales y políticos de nuestro tiempo, sitúe siempre a las personas y a sus derechos humanos como el eje rector de toda política pública y decisión institucional.

Introducción

El derecho de protección de datos personales es relativamente nuevo y ha sido reconocido tanto en instrumentos internacionales como en diversas legislaciones del mundo. Su importancia radica en que establece las reglas para el tratamiento de datos personales, necesarias, sobre todo, a partir del vertiginoso desarrollo tecnológico que hace recabar y procesar grandes cúmulos de información, en tiempo real, para diversos fines.

No obstante, si bien el derecho de protección de datos personales se ha incorporado de forma reciente en algunas constituciones, es una figura que encuentra su antecedente más importante en la Declaración Universal de Derechos Humanos de 1948, especialmente en el artículo 12 de dicho instrumento. En este sentido, se debe precisar que el citado artículo reconoce la no injerencia en la vida privada de las personas, lo cual dio pauta a un desarrollo normativo que vio nacer derechos generales, como la privacidad y la intimidad, y a derechos habilitadores de éstos, como el derecho a la protección de datos personales.

Es decir, el reconocimiento del derecho a la no injerencia en la vida privada de las personas y el deber de garantía por parte del Estado ha permitido desarrollar nuevas figuras jurídicas, que se desprenden del derecho a la privacidad y se han reconocido bajo denominaciones, como las del derecho de protección de datos personales.

Para el caso de la Constitución Política de los Estados Unidos Mexicanos, el artículo 16 de dicho instrumento fue modificado en 2009 para reconocer como un derecho fundamental y humano el de la protección de los datos personales en posesión de los sectores público y privado.

Es así como en el capítulo I se analiza el derecho de protección de datos personales a la luz de los textos y tratados internacionales y de su reconocimiento en el marco constitucional mexicano, teniendo un primer acercamiento para estudiar la diferencia entre el derecho a la privacidad y el de protección de datos personales, desde diversos conceptos involucrados en ambos derechos.

En estas líneas también se reflexiona sobre la aportación que hace el derecho de protección de datos personales como elemento necesario para garantizar el derecho a la privacidad, repasando algunos antecedentes doctrinarios de ambos derechos.

En el capítulo II se aborda la recepción del derecho de protección de datos personales en México, los principios que lo rigen, el reconocimiento e incorporación de nuevas figuras, como el derecho de portabilidad y el derecho al olvido y algunos temas

complejos, como los límites que existen entre conceptos como la seguridad nacional, la seguridad pública, la salud pública y el derecho de protección de datos personales; es decir, los límites, tensiones y restricciones de este derecho, necesarios para garantizar la subsistencia del Estado Constitucional de Derecho. Por otro lado, se analiza la trascendencia del derecho de protección de datos personales para la consolidación del Estado democrático.

En el capítulo III se estudian las implicaciones jurídicas de la suscripción y ratificación por parte de México de algunos instrumentos internacionales con disposiciones en materia de protección de datos personales. Asimismo, se estudian algunas posturas de la Corte Interamericana de Derechos Humanos en torno al derecho a la privacidad y los pronunciamientos de la Suprema Corte de Justicia en materia de protección de datos personales.

También se señalan algunos desafíos en lo que respecta al derecho de protección de datos personales, como el derecho de reparación en materia de derechos humanos, diferenciando aquellos que tienen que ver con la salvaguarda de este derecho en el ciberespacio y las dificultades que esto conlleva.

Finalmente, en el capítulo IV de esta obra, se examinan las implicaciones que la nueva reconfiguración del derecho de protección de datos personales en México entraña: la desaparición del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, las nuevas facultades de la Secretaría Anticorrupción y Buen Gobierno tanto en materia de transparencia y acceso a la información como de protección de datos personales –el tema que nos ocupa–.

Esta obra se escribe en un momento de transición para el derecho de protección de datos personales en México y tiene como objetivo dar cuenta de la construcción del derecho de protección de datos personales en el país, de los aspectos generales y puntos finos de este derecho y, en general, de acercar a los operadores jurídicos los aspectos que rigen el derecho de protección de datos personales en México, así como generar reflexiones en torno a sus desafíos, especialmente en el ciberespacio.

Capítulo I
Aspectos generales del derecho a la privacidad y del derecho de protección de datos personales

Cuando hablamos del derecho de protección de datos personales es inevitable asociarlo con otros derechos como el de la privacidad; sin embargo, ambos derechos no son sinónimos y encuentran no sólo diferencias conceptuales, sino de aplicación y garantía por parte de los Estados. Es por esta razón que resulta pertinente analizar el derecho a la privacidad, con la finalidad de entender cómo a partir de éste se desarrollan nuevos derechos como el de la protección de datos personales, que otorga un poder de control de la información de carácter personal a sus titulares y establece las reglas para el tratamiento de dichos datos.

En las siguientes líneas se examina el tratamiento que se le ha dado al derecho de protección de datos personales en los textos y tratados internacionales de los que México forma parte, para así considerar conceptos en torno al derecho a la privacidad y el derecho de protección de datos personales que permitan establecer diferencias entre ambos. De igual manera, se reflexiona sobre el papel que juega el derecho de protección de datos personales para garantizar el derecho a la privacidad. Asimismo, se estudia la importancia del derecho de protección de datos personales como elemento necesario para garantizar la privacidad.

I.1. El derecho de protección de datos personales en los textos y tratados internacionales

Cuando se habla del derecho de protección de datos personales es usual pensar que estamos frente a un derecho nuevo que nace a partir de la economía digital, del uso de internet y del vertiginoso desarrollo de las Tecnologías de la Información y Comunicación (TIC).

No obstante, si bien es un derecho de reciente reconocimiento en la Constitución Política de los Estados Unidos Mexicanos (CPEUM), tiene antecedentes importantes en los años cuarenta del siglo pasado, en la época de posguerra en Europa. Pensemos en una Alemania nazi que trató los datos de miles de judíos a través de un censo realizado por el Estado y con la ayuda de las tarjetas perforadas de la empresa IMB, con el objetivo de identificar a dicha población y planear su exterminio de forma más efectiva (Véliz, 2025).

A partir de atrocidades como éstas, se volvió evidente la necesidad de establecer límites del Estado frente a la vida privada de las personas, y ejemplo y consecuencia de ello se manifiesta en el artículo 12 de la Declaración Universal de Derechos Humanos (DUDH).

Antes de analizar este artículo, es pertinente dar un contexto sobre la necesidad histórica de reconocer en instrumentos internacionales un concepto tan importante como el de *dignidad humana*, que hasta el día de hoy es sustento de los instrumentos jurídicos en materia de derechos humanos. Es decir, a partir de las atrocidades cometidas durante la Segunda Guerra Mundial, países ganadores y vencidos encontraron esencial reconocer derechos mínimos a las personas, en una invocación inédita a la dignidad humana (estos derechos mínimos se plasman en la DUDH de 1948). Es así que la manifestación del límite del Estado, respecto de la vida privada de las personas, está plasmado en el ya mencionado artículo 12 de la DUDH, el cual señala lo siguiente:

> 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. (DUDH, 1948).

Como se puede advertir, este artículo no reconoce de forma expresa el derecho de protección de datos personales, pero sí es un antecedente importante para la evolución normativa manifestada a través de nuevos derechos –como el que ocupa a este documento–.

Aunado a la DUDH, existen otros instrumentos internacionales en materia de derechos humanos que reconocen límites del Estado frente a la vida privada de las personas, como el artículo 11 de la Convención Americana de Derechos Humanos de 1969 (Pacto de San José),[1] el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966,[2] el artículo 8 del Convenio Europeo de Derechos Humanos de 1950,[3] así como la Carta de los Derechos Fundamentales de la Unión Europea de 2000.[4]

---

1 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.

2 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.

3 Artículo 8. Derecho al respeto a la vida privada y familiar: "1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".

4 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

Por otro lado, también existen textos y tratados internacionales en diversas materias que contienen disposiciones sobre el derecho de protección de datos personales, tales como las Directrices relativas a la Protección de la Intimidad y de la Circulación Transfronteriza de datos Personales de la Organización para la Cooperación y Desarrollo Económicos (1980); el Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (1981); el Protocolo Adicional del Convenio Número 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y relativo a Transferencias de Datos (2001 y Convenio 108 Plus, 2018); la Resolución 45/95 de la Organización de las Naciones Unidas relativas a las Directrices para la Regulación de los Archivos de Datos Personales Informatizados (1990); la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos (1995); el Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico (1999); los Estándares Internacionales sobre Protección de Datos Personales y Privacidad, mejor conocida como Resolución Madrid (2009) y el Reglamento de Protección de Datos Personales de la Unión Europea,[5] entre otros.

El derecho de protección de datos personales tiene dos vertientes: la perspectiva desde los derechos humanos y la perspectiva comercial y/o económica. Esto explica incluso los dos grandes modelos de regulación en esta materia en el mundo: por un lado, el modelo europeo o de derecho continental, que privilegia la garantía de los derechos humanos y reconoce la dignidad humana como el límite para el desarrollo tecnológico; y, por otro, el modelo de regulación en materia de protección de datos personales anglosajón o del *common law*, que privilegia la eficacia y eficiencia, dejando al propio mercado la autoregulación en materia de protección de datos personales.

En este sentido, existen diversos foros y organismos internacionales en los cuales México participa y de los que ha contraído obligaciones y compromisos encaminados a garantizar un marco legislativo adecuado de protección de datos personales y, a la vez, impedir la creación de barreras que obstaculicen la libre circulación de la información de carácter personal en un mundo globalizado.

---

previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente".

[5] El Reglamento General de Protección de Datos Personales fue aprobado por el Parlamento Europeo el 14 de abril de 2016, con el fin de dar respuesta a la necesidad de proteger la información de las personas en el ciberespacio. El objetivo de este instrumento es devolver a las personas que se encuentren en la Unión Europea el control de sus datos personales y garantizar elevados estándares de protección, adaptados al entorno digital; asimismo, determina nuevas normas mínimas sobre el uso de datos para fines judiciales y policiales. Este documento sustituye a la normativa comunitaria de protección de datos personales, particularmente, la Directiva 95/46/CE del Consejo de Europa, ya que, cuando ésta fue aprobada, el uso de internet no estaba extendido como ahora. Este instrumento resulta paradigmático, debido a que eleva la protección de la información de las personas y se emite en concordancia con la Sentencia de Puerto Seguro de 2015.

Entre los diversos foros internacionales que en materia de protección de datos personales explican las acciones tomadas por el gobierno mexicano destacan los siguientes: la Organización para la Cooperación y el Desarrollo Económicos (OCDE), la Organización de las Naciones Unidas (ONU), el Foro de Cooperación Económica Asia-Pacífico (APEC), el Tratado de Libre Comercio con la Unión Europea, la Alianza para la Seguridad y la Prosperidad de América del Norte (ASPAN), la Red Iberoamericana de Protección de Datos (RIPD), el Comité Trilateral para el Flujo Transfronterizo de Información, y el Convenio sobre la Ciberdelincuencia, también denominado de Budapest, mismo que el Senado mexicano finalmente no ratificó.

En virtud de lo anterior, es posible afirmar que, si bien el primer antecedente del derecho a la privacidad y, por ende, del derecho de protección de datos personales surge con el reconocimiento del derecho de no injerencia en la vida privada de las personas, ha sido en los últimos años en los que de forma exponencial se han desarrollado textos e instrumentos internacionales que dictan disposiciones en materia de protección de datos personales con las dos visiones señaladas previamente: la de los derechos humanos y la de eficacia y eficiencia del mercado.

I.2. Análisis conceptual del derecho a la privacidad

Para hacer un análisis de los conceptos relacionados con el derecho a la privacidad, es necesario repasar brevemente los antecedentes doctrinarios de este derecho.

El primer reconocimiento doctrinal del derecho a la intimidad lo encontramos en 1873, cuando Thomas McIntyre Cooley, en su obra *The elements of torts*, definió la *privacidad* como "*the right to be let alone*"; no obstante, será algunos años después cuando Samuel Warren y Louis Brandeis, en su artículo "The right to privacy", publicado en 1890 en la *Harvard Law Review*, elaboraron los lineamientos teóricos de la configuración jurídica de un nuevo derecho: el derecho a la privacidad (Ríos Vega, 2020).

En el artículo de Warren y Brandeis, se manifestaba el necesario reconocimiento del derecho a no ser molestados (*right to be alone*); posteriormente, Alan Westin amplió este concepto e incluyó, dentro del derecho a la privacidad, el derecho de todo individuo para determinar cómo, cuándo y hasta qué punto su información personal es comunicada a los demás –materializado en la actualidad a través del derecho de protección de datos personales– (Westin, 1968).

A partir de este texto, el concepto de *privacidad* se define casi de la misma manera y se mantiene el elemento constante de que la privacidad se describe como un derecho a ser dejado en paz y un derecho de cada individuo para determinar, en circunstancias normales, cuáles son sus pensamientos, los sentimientos y las emociones comunicadas a otros (Holvast, 2009).

A pesar de que el concepto de privacidad se configura en un inicio –desde la perspectiva doctrinaria– en países pertenecientes al *common law*, ha existido un desarrollo normativo y de mayor protección –reconocimiento del derecho de protección de datos personales como un derecho fundamental– en los países pertenecientes a la familia romana germánica (como el caso de España y México), lo que da la pauta a la construcción del derecho a la protección de datos personales.

Cuando se habla del *derecho a la privacidad*, normalmente se asocia a derechos como el de la protección de datos personales y el del honor, así como a conceptos como la inviolabilidad del domicilio o el secreto de las comunicaciones; empero, resulta evidente que existen diferencias entre todos estos elementos, ya que, si bien estos ayudan a preservar la privacidad, entendemos que la vida privada es un concepto mucho más amplio que el propio derecho de protección de datos personales.

Es importante decir que la privacidad no es un concepto terminado y dependerá del contexto y de las circunstancias de los casos particulares su acotación; esto es, lo que en un país puede considerarse como del ámbito privado, en otro pertenece al público. Vemos, por ejemplo, la manera en la que las personas normalizan, cada vez más, compartir imágenes en redes sociales, las cuales antes hubieran formado parte del ámbito privado: las rutinas diarias de ejercicio, los platillos de comida, el desarrollo de las infancias, etcétera.

El derecho a la privacidad no es ajeno a los fenómenos sociales, económicos o políticos, por lo que se adapta a esta evolución, considerando las variables de la economía digital, la hiperconexión y la inmediatez de internet. De forma general, la "privacidad" se puede entender como el "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión" (RAE, 2025, acepción 2).

El derecho a la privacidad no es fácil de definir, ya que hasta el momento no se tiene una idea clara de sus alcances, sobre todo porque la tecnología replantea nuevas necesidades de protección a través de este derecho. Veamos algunas posturas de los tribunales relativas al concepto en análisis.

El Tribunal Europeo de Derechos Humanos (TEDH) considera la privacidad como "un concepto amplio no susceptible de una definición exhaustiva" (Piñar Mañas, 2010, p. 16). De igual forma, la Sentencia del Tribunal Constitucional Español 292/2000 de 30 de noviembre señala que el derecho fundamental a la intimidad no aporta por sí solo una protección suficiente frente a las amplias posibilidades que la informática ofrece, dado que una persona puede ignorar no sólo que los datos se han recogido en un fichero, sino también que se han trasladado a otro y su finalidad. Esta sentencia define y delimita el derecho a la protección de datos de carácter personal previsto en el artículo 18.4 de la Constitución española como un derecho fundamental autónomo y distinto de los derechos al honor y a la intimidad personal, reconocido y amparado en el artículo 18.1 del propio texto constitucional (Gutiérrez Zarza, 2012). Para el caso de México, la Suprema Corte de Justicia de la Nación (SCJN) ha establecido lo siguiente:

> Las afirmaciones contenidas en las resoluciones nacionales e internacionales [relacionadas a la privacidad o vida privada] son útiles en la medida en que no se tomen de manera descontextualizada, emerjan de un análisis cuidadoso de los diferentes escenarios jurídicos en los 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. (Tesis: 1a. CCXIV/2009, diciembre de 2009).

Dicho lo anterior, resulta pertinente también establecer que los términos *privacidad* y *derecho a la privacidad* no necesariamente se refieren a lo mismo:

> [La] privacidad es un elemento consustancial a la dignidad humana y [por ende debe ser] protegido por el Derecho […] el derecho a la privacidad [es] aquel que todo individuo tiene a separar aspectos de su vida privada del escrutinio público. (García Ricci, 2013, p. 1045).

Es así como podemos afirmar que 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; en este segundo componente –como se ha dicho–, se manifiesta el derecho de protección de datos personales.

Por otro lado, vincular el concepto de privacidad a elementos tan relevantes, como la dignidad humana, no es cosa menor, ya que esto ha permitido establecer obligaciones a los Estados para su efectiva garantía a partir de la teoría de los derechos humanos y de la articulación, en este caso, desde el Sistema Interamericano de Derechos Humanos (SIDH), del cual forma parte nuestro país. A partir del derecho a la privacidad, convergen algunos conceptos relacionados a éste, entre los que destacan:

a) *Vida privada*: Esfera de la vida que se decide dejar en el ámbito de lo privado o de lo íntimo y que no puede ser invadida por persona o entidad alguna, salvo excepciones previstas en la norma suprema. En otras palabras, aquello que se decide dejar fuera del conocimiento de lo público.

> La protección constitucional de la vida privada [implica poder] conducir parte de [la] vida [de las personas], de la mirada y las injerencias de los demás, y guarda conexiones [de varios tipos] con pretensiones [más concretas que los textos constitucionales actuales reconocen a veces como derechos conexos:] el derecho de poder tomar libremente ciertas decisiones relativas al propio plan de vida, el derecho a ver protegidas ciertas manifestaciones de integridad física y moral, el derecho al honor o reputación, el derecho a no ser presentado bajo una falsa apariencia, el derecho a impedir la divulgación de ciertos hechos o la publicación no autorizada de cierto tipo de fotografías, la protección contra el

> espionaje, la protección contra el uso abusivo de las comunicaciones privadas, o la protección contra la divulgación de informaciones comunicadas o recibidas confidencialmente por un particular. (García Ricci, 2013, p. 1065).

Es decir, la garantía de la vida privada contiene diversos derechos necesarios para su existencia.

b) *Intimidad*: Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia. Existe un debate en torno a si debemos considerar que intimidad y privacidad son conceptos que se pueden utilizar como sinónimos. Algunos tribunales han determinado que sí, y otros doctrinarios, como Garzón Valdés, han estimado que ambos conceptos refieren a situaciones distintas (Garzón Valdés, 2008).

La SCJN hace una diferencia entre vida privada e intimidad en el Amparo Directo en Revisión 402/2007, en el que establece que "la intimidad se constituye con los extremos más personales de la vida y del entorno familiar, cuyo conocimiento está restringido a los integrantes de la unidad familiar" (p. 23). Con las reservas y posturas de los tribunales respecto del debate, podemos decir que la intimidad es un elemento manifestado dentro del ámbito privado, cuya afectación requeriría un nivel más alto de protección jurídica.

c) *Autodeterminación informativa*: El derecho a la autodeterminación informativa fue reconocido en el sistema jurídico anglosajón bajo el vocablo *privacy* o *right to privacy*. No obstante, para el derecho romano germánico esta acepción llega cuando el Tribunal Constitucional Alemán, en la sentencia de 15 de diciembre de 1983 sobre el Censo, completó los derechos constitucionales de la personalidad, sobre la base del derecho a la dignidad humana y al libre desarrollo de la personalidad, lo cual garantizó la continuidad de las libertades básicas reconocidas anteriormente, a través de la formulación de un nuevo derecho, denominado *autodeterminación informativa* (Heredero Higueras, 1983). Esta sentencia reconoce que el derecho de la personalidad abarca la facultad del individuo (derivada de la autodeterminación), de decidir por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida, protegiéndole contra la recogida, el almacenamiento, la utilización y la transmisión ilimitada de los datos concernientes a la persona. De la Cuadra (1991), afirma que "el Constitucional alemán anuló parte del censo de 1983, similar al español de 1991". Al efecto, este derecho reconoce la facultad de las personas para decidir sobre el tratamiento de sus datos personales y así garantizar derechos conexos, como el derecho a la no discriminación o al libre desarrollo de la personalidad (Huber, 2009).

d) *Derecho de protección de datos personales*: Derecho que le confiere a las personas control sobre su información personal. Se manifiesta a través de los denominados derechos de acceso, rectificación, cancelación y oposición (derechos ARCO), frente al tratamiento de datos personales. Se entiende como el poder del titular del dato personal para decidir quién, cuándo, cómo y hasta qué punto utilizan su información personal. Al respecto, para el caso de nuestro país, "el derecho a la protección de datos

personales [tiene un] reconocimiento constitucional, desarrollado en el marco de los postulados de la doctrina europea y los esquemas de autorregulación y sectorización del sistema anglosajón" (Mendoza Enríquez, 2018b, p. 273).

e) *Inviolabilidad de las comunicaciones*: Con la denominación *secreto de las comunicaciones* u otras como *inviolabilidad de la correspondencia* se ha constituido "una de las dimensiones o garantías clásicas de los derechos fundamentales que protegen la vida privada de la persona, aunque es ya, en definitiva, un derecho fundamental autónomo" (Díaz Revorio, 2006, p. 125). Para el caso de México, el Código Nacional de Procedimientos Penales (CNPP) proporciona una definición de intervención de comunicaciones privadas, al prever en el párrafo segundo del artículo 291 lo siguiente:

> Artículo 291. […] La intervención de comunicaciones privadas, abarca todo un sistema de comunicación, o programas que sean fruto de la evolución tecnológica, que permitan el intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos, que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, las cuales se pueden presentar en tiempo real o con posterioridad al momento en que se produce el proceso comunicativo. (CNPP, 2024).

El derecho reconocido constitucionalmente en México de la inviolabilidad de las comunicaciones dispone que las comunicaciones privadas son inviolables y que únicamente la autoridad judicial federal, a petición del Ministerio Público Federal o su homólogo en las entidades federativas, puede solicitar la intervención de comunicaciones privadas. En su momento, existió un debate interesante entorno a facultades reservadas para las mismas autoridades antes citadas, respecto de solicitudes de geolocalización en tiempo real. Este derecho protege a la persona frente a intromisiones no sólo de terceros particulares, sino del Estado, siempre que no se encuentre en alguna de las excepciones de ley (Mendoza Enríquez, 2016).

De igual forma, para el caso de México, en 2025 se modificó el régimen normativo en materia de telecomunicaciones, las leyes en materia de protección de datos personales y acceso a la información, la autoridad garante en dicha materia y la asignación de nuevas facultades a la Guardia Nacional, lo cual implicó un impacto significativo, especialmente a las excepciones de la inviolabilidad del domicilio, al reconocer nuevas facultades, por ejemplo, a la Guardia Nacional para restringir dicho derecho.

Finalmente, también es importante considerar que el derecho a la privacidad tiene, cada vez más, nuevas formas de manifestarse; por ejemplo, el derecho a la privacidad mental, cuyo contenido esencial busca proteger los pensamientos humanos de cualquier intromisión a través de nuevas tecnologías como las neurociencias. La manera en que este derecho se ha insertado en algunas normas de la región de América Latina, como es el caso específico de Chile, es a través de los llamados neuroderechos; no obstante, la tropicalización de esta figura dependerá de la manera en la que normativamente se organice un Estado: el derecho a la privacidad mental

puede reconocerse desde los neuroderechos, pero también desde normas en materia de protección de datos personales (aunque no sería lo más óptimo porque no todos los pensamientos se consideran datos personales); sin dejar de soslayar las normas de inteligencia artificial que tendrían un abordaje desde la técnica o en normas generales de derechos humanos que de forma transversal identifiquen derechos humanos que posiblemente puedan verse afectados por el desarrollo de las neurociencias y, en general, de la tecnología, como el derecho a la no discriminación.

I.3. Configuración del derecho a la privacidad en México

El derecho a la privacidad no es un derecho reconocido expresamente por la Constitución, no obstante, a partir de criterios jurisprudenciales se ha establecido su interpretación y límites para la garantía de dicho derecho.

En este sentido, la SCJN al resolver el Amparo en Revisión 134/2008[6] determinó que el fundamento del derecho a la privacidad en México se encuentra en el primer párrafo del artículo 16 constitucional, al establecer la garantía de seguridad jurídica de todo gobernado a no ser molestado en la privacidad de su persona, de su intimidad familiar o de sus posesiones, sino mediante mandamiento escrito. La privacidad no se acota al espacio físico del domicilio (lugar donde normalmente se manifiesta la intimidad), incluye también aquellas intromisiones o molestias que por cualquier medio puedan realizarse en el ámbito de la vida privada.[7]

Existen algunos otros reconocimientos constitucionales implícitos en relación con la salvaguarda del derecho a la privacidad, entre los que se encuentran los siguientes:

a) Información confidencial en términos del derecho de acceso a la información: La fracción segunda del artículo 6 de la CPEUM, establece límites en el ejercicio del derecho de acceso a la información, lo cual hace necesario que las

[6] Este juicio de amparo (SCJN, Amparo en Revisión 134/2008) dio origen a la Tesis: 2a. LXIII/2008, Derecho a la privacidad o intimidad. Está protegido por el artículo 16, primer párrafo de la Constitución Política de los Estados Unidos Mexicanos.

[7] Primer párrafo del artículo 16 constitucional: "[…] la garantía de seguridad jurídica de todo gobernado a no ser molestado en su persona, familia, papeles o posesiones, sino cuando medie mandato de autoridad competente debidamente fundado y motivado, de lo que deriva la inviolabilidad del domicilio, cuya finalidad primordial es el respeto a un ámbito de la vida privada personal y familiar que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, con la limitante que la Constitución Política de los Estados Unidos Mexicanos establece para las autoridades. En un sentido amplio, la referida garantía puede extenderse a una protección que va más allá del aseguramiento del domicilio como espacio físico en que se desenvuelve normalmente la privacidad o la intimidad, de lo cual deriva el reconocimiento en el artículo 16, primer párrafo, constitucional, de un derecho a la intimidad o vida privada de los gobernados que abarca las intromisiones o molestias que por cualquier medio puedan realizarse en ese ámbito reservado de la vida" (Tesis: 2a. LXIII/2008, mayo de 2008).

autoridades federales, estatales y municipales protejan, cuando concedan el ejercicio del derecho de acceso a la información pública, lo referente a la vida privada y datos personales de las personas, en los términos y con las excepciones que fijen las leyes.

b) Límites de la libertad de imprenta: El artículo 7o. constitucional determina como límite a la libertad de imprenta el respeto a la vida privada de las personas.

c) La inviolabilidad de las comunicaciones: El artículo 16 constitucional mandata que las comunicaciones privadas son inviolables, y que únicamente la autoridad judicial federal, a petición del Ministerio Público Federal o de su homólogo en las entidades federativas, podrá solicitar la intervención de las comunicaciones privadas. Existe la posibilidad de realizar intervenciones de comunicaciones privadas en cualquier materia, siempre y cuando la comunicación grabada sea aportada por alguna de las partes que participen en ella. También se establece la obligación de instaurar juzgados de control que den trámite a las solicitudes de intervención de comunicaciones, y llevar a cabo un registro de todas las comunicaciones sostenidas por jueces y autoridades de investigación para estos fines.

d) El derecho a la protección de datos personales: El mismo artículo 16 constitucional garantiza este derecho y –como vimos líneas arriba– se trata de un articulador natural del derecho a la privacidad. En 2009, se reformó el artículo 16 mencionado, a fin de reconocer el derecho a la protección de datos personales y las acciones inherentes al ejercicio de este derecho bajo los denominados derechos ARCO.

e) Resguardo de identidad y datos personales de víctimas: Otra disposición constitucional que abona a la garantía del derecho a la privacidad, es la establecida en el artículo 20, apartado C, fracción V de la CPEUM, que reconoce el derecho que tienen las víctimas del delito, a que sea resguardada su identidad y sus datos personales en los casos relacionados con menores de edad, delitos de violación, secuestro, delincuencia organizada, o bien, cuando a juicio del juzgador sea necesario para la protección de la víctima.

A manera de resumen, podemos decir que, si bien el derecho a la privacidad no se encuentra expresamente reconocido en el texto constitucional, sí se puede lograr su efectiva salvaguarda, a través de derechos "habilitadores"–como los mencionados en líneas previas–.

I.4. Definición del derecho de protección de datos personales y su reconocimiento como elemento necesario para la salvaguarda del derecho a la privacidad

Una vez que se ha analizado el derecho a la privacidad y que es posible identificar sus diferencias respecto del derecho de protección de datos personales, resulta necesario hacer una breve explicación de cómo este último derecho permite la salvaguarda de la privacidad para las personas.

En relación con lo anterior, podríamos explicar en un ejemplo sencillo que el derecho a la privacidad es una pizza, y que el derecho a la protección de datos personales, el derecho al honor, el secreto de las comunicaciones y la inviolabilidad del domicilio, son rebanadas de esa pizza; es decir, sin dichas rebanadas, el derecho a la privacidad no podría garantizarse, pero una rebanada en lo individual no garantiza por sí misma, la vida privada de las personas.

Cuando hablamos del derecho de protección de datos personales, nos referimos al segundo componente del derecho a la privacidad, esto es, el derecho de controlar la información de carácter personal, considerando que Westin (1968) amplió este concepto e incluyó, dentro del derecho a la privacidad, el derecho de todo individuo para determinar cómo, cuándo y hasta qué punto su información personal es comunicada a los demás. Es así que sin el derecho de protección de datos personales resultaría complejo garantizar la vida privada.

Dicho lo anterior, abordemos algunos aspectos generales del derecho de protección de datos empezando por algunas definiciones y sus principios.

Los *datos personales* refieren a la información del individuo que permite identificarlo por medio de su descripción, origen, lugar de residencia, trayectoria académica, laboral y otros. A medida que la tecnología avanza, aparecen nuevos tipos de datos personales, por ejemplo, los datos biométricos que a través de características físicas y/o corporales hacen posible identificar a una persona.

En este sentido, los datos personales también describen aspectos más sensibles sobre el individuo, como su forma de pensar, el estado de salud, las características físicas, la ideología, la vida sexual, entre otros; este tipo de datos se denominan *datos personales sensibles*. Así pues, "los datos de [un individuo] son personales y [éste] tiene el derecho a la reserva y confidencialidad o a la cobertura mayor de la libertad de intimidad" (Gozaíni, 2011, p. 59). Para Oscar R. Puccinelli, no todos los datos de carácter personal cuentan con la misma rigidez de tutela, y refiere la distinción que Gils Carbó hace respecto de la gradación de su protección:

> a) Los datos que son de libre circulación, como los de identificación: nombre, apellido, documento de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio.
>
> b) Los de circulación restringida a un sector o actividad determinada que son susceptibles de tratamiento en tanto se presente una causa de justificación legítima y con las limitaciones que resulten de esa especialidad.
>
> c) Los de recolección prohibida porque afectan la intimidad personal o familiar, que son los denominados datos sensibles. (Puccinelli, 2004).

Diversos instrumentos han proporcionado una definición de datos personales, entre los que destacan:

> [El] Convenio 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de sus datos de carácter personal, [así como] las directrices de la Organización para la Cooperación y el Desarrollo Económico sobre la protección de la privacidad y flujos transfronterizos de datos personales (2008), y la Directiva 95/46/CE del Parlamento Europeo y del Consejo de Europa, los cuales definen como datos personales: "Toda la información sobre una persona física identificada o identificable". (Gómez-Robledo y Ornelas, 2006, p. 17).

Para el caso de México, el artículo 2o., fracciones V y VI de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) define los datos personales de la siguiente forma:

> Datos personales: [como] Cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.
>
> [El mismo instrumento normativo, define los] datos personales sensibles: [como] aquellos datos personales que afecten a la esfera más íntima de la persona titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para ésta. De manera enunciativa, más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual. (LFPDPPP, 2025).

Ampliando el concepro: "En este sentido, se consideran datos sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, y preferencia sexual" (Mendoza Enríquez, 2018b, pp. 275-276). Respecto a lo anterior, Javier Nájera (2008) hace una aproximación a la protección de datos personales, desde una perspectiva axiológica, entre los que destacan:

a) El origen étnico o racial: Aquellos datos que competen a la especie humana como tal y su clasificación (p. 107).

b) Las características físicas, morales y emocionales: "Las peculiaridades, particularidades o rasgos del aspecto físico, del ámbito moral o emocional de cualquier persona física serán considerados datos personales" (p. 111).

c) La vida afectiva y familiar:

> [Los datos personales] que se originan del carácter social del ser humano, es decir, de la interrelación e interacción entre dos o más personas. Estos datos representan la materialidad de los diversos vínculos que las personas van creando, fomentando o diseñando, como son lazos familiares y sentimentales, o aquellos basados en el respeto, amistad o amor. (p. 113).

d) El domicilio: Datos referentes al "espacio físico, en donde una persona habita o realiza una actividad productiva por un tiempo determinado, o en su caso donde se confina" (p. 113).

e) El número telefónico: Datos cuya característica principal "en cuanto a su naturaleza, […] axiológicamente no representan la materialidad de la intimidad, es decir, el uso, manejo o tratamiento de esta clase de dato [no implica] un reflejo, expresión o agresión al ámbito íntimo de una persona" (p. 117).

f) El patrimonio: Aquellos datos relacionados a los "bienes de carácter económico, es decir, bienes con un contenido meramente pecuniario, y bienes que representan un valor de afección o moral" (p. 119).

g) La ideología: Aquellos datos personales que abarcan lo siguiente:

> […] lo concerniente a la ideología, entendida como el conjunto de ideas, creencias y valores compartidos por un grupo de personas, relativos a un determinado campo del conocimiento; sustentada, guiada y gobernada por un objetivo y una finalidad predeterminados. Actualmente, la ideología se traduce en una idea compartida por un grupo de seres humanos sobre una realidad que sirve como sustento o justificación de actos personales o colectivos. (p. 122).

h) Las opiniones políticas: El dato personal "resultado de un proceso integrado por un juicio de valor y un objeto de valoración que se traduce en un determinado conocimiento, conteniendo una afirmación o negación del objeto de conocimiento con un cierto grado de incertidumbre" (p. 123).

i) Las creencias y las convicciones religiosas o filosóficas: Los datos que refieren a "las creencias y convicciones [estos dos conceptos no son iguales, ya que] para que exista una creencia, debe existir un cierto grado de convicción" (p. 124).

j) El estado de salud físico o mental: Los datos relacionados al "estado completo de bienestar físico, síquico y social de los individuos" (p. 124).

k) Las preferencias sexuales: Los datos de "elementos condicionantes de carácter físico, biológico, emocional, cultural o social que provocan un grado de identificación y distinción prohibido dentro de un grupo o comunidad" (pp. 125-126).

En síntesis, "son muchas las características y seguimientos específicos de los distintos tipos de datos personales, los cuales […] tienen una importancia y significado", de acuerdo con la utilización de la información que constituyen (Gamboa Montejano, 2009, p. 13).

Capítulo II
Configuración del derecho de protección de datos personales en México desde una perspectiva constitucional

Como se ha analizado líneas arriba, el derecho de protección de datos personales encuentra su base más importante en el reconocimiento del derecho a la no injerencia en la vida privada de las personas, contenido en el artículo 12 de la DUDH de 1948.

A partir de ese momento y derivado del impacto del desarrollo tecnológico en la vida privada de las personas, derechos como el de la protección de datos personales se han internacionalizado con una doble vertiente: su reconocimiento como elemento esencial para el mercado (por ejemplo, pensando en la transferencia internacional de datos que requiere el comercio digital), y su reconocimiento como garantía de un derecho humano. Es así que en esta internacionalización del derecho de protección de datos personales, encontramos instrumentos jurídicos de índole económico que contienen reglas para el tratamiento de la información de carácter personal, como las Reglas de Privacidad del Foro Económico Asia-Pacífico (APEC, 2005) y, a su vez, encontramos instrumentos en materia de derechos humanos, como el propio Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, mejor conocido como Convenio 108, del Consejo de Europa (1981).[8]

A partir de la internacionalización de este derecho, también algunos Estados han encontrado necesario su incorporación y, por ende, su reconocimiento en los instrumentos normativos de la más alta jerarquía (en el caso concreto de México, lo señala el artículo 16 de la Carta Magna).

En las siguientes líneas, se analizará el desarrollo del derecho de protección de datos personales en México desde una perspectiva principalmente de derecho constitucional.

[8] Este fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos y su objetivo es "garantizar […] a cualquier persona física […] el respeto de 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" (Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, 1981).

II.1. Recepción del derecho de protección de datos personales

En el caso particular de México, la legislación en materia de protección de datos personales ha surgido y evolucionado rápidamente durante los últimos años. En este sentido, la Ley Federal de Acceso a la Información Pública Gubernamental de 2002 marcó la primera pauta en el ámbito nacional, para incluir disposiciones relativas a la protección de los datos personales en posesión del sector público.

No obstante lo anterior, la protección de datos personales no tenía un reconocimiento expreso como derecho y, por lo tanto, carecía de principios de interpretación, considerándola, en un principio, sólo como una limitante para el ejercicio del derecho de acceso a la información pública.

Posteriormente, en 2009 las reformas constitucionales de los artículos 16 y 73 otorgaron reconocimiento pleno a la protección de datos personales como un derecho fundamental y autónomo y dotaron de facultades al Congreso de la Unión para legislar en esta materia, respectivamente.

En 2010, se publicó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), siendo la primera ley en regular la protección de datos para el sector privado –sería abrogada por su homóloga en 2025–. Se determinó que sería una ley de índole federal para permitir que las empresas fueran competitivas y que el cumplimiento normativo del derecho de protección de datos personales no fuera un obstáculo, dejando una sola ley de aplicación a las empresas que cumplieran dos condiciones: prestar servicios en México y/o estar establecidos en México.[9]

En 2017, se publicó la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGPDPPSO), normativa que dicta las reglas para los datos en manos de sujetos obligados del sector público.

Esta ley fue relevante, porque le permitió a México alcanzar el nivel óptimo normativo para ser aceptado en el Convenio 108 del Consejo de Europa, ya que existía una disparidad entre las normas en materia de protección de datos personales del sector privado y la inextistencia de regulación para los datos personales en manos del sector público, lo que impedía su admisión a este instrumento internacional.

[9] Estas dos condiciones se completaron a través del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP, 21 de diciembre de 2011), siendo esto relevante porque resolvía, al menos desde la parte normativa, el problema jurisdiccional que implicaba la falta de cumpimiento de las normas nacionales en materia de datos personales por parte de las plataformas tecnológicas que invocaban el argumento de que sólo prestaban servicios en México y que tenían su sede corporativa en otros países y, por ende, respondían sólo a las normas de esos países. No obstante, este fenómeno sigue siendo un desafío, hasta en tanto no se refuerce el alcance de las resoluciones de la autoridad nacional en materia de protección de datos personales y/o se enlace el cumplimiento de dichas resoluciones a aspectos comerciales entre Estados-Nación o, incluso, se vincule a procesos de integración económica de la región de América Latina.

Finalmente, en esta cronología normativa, 2025 constituyó un año de reestructura para el derecho de protección de datos personales, ya que el 20 de marzo de ese año se publicaron dos nuevas leyes que derogaron el marco normativo en materia de datos personales del sector público y privado vigente hasta ese momento en el país. Ambas leyes conservaron los nombres originales –LFPDPPP y LGPDPPSO–, pero incluyeron cambios significativos, como la desaparición del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), órgano constitucionalmente autónomo que hasta ese momento ostentaba facultades en materia de protección de datos personales, así como la nueva asignación de facultades en la materia a la Secretaría de Anticorrupción y Buen Gobierno y la simplificación normativa en el tema.

Hagamos un breve análisis del contenido de estas cuatro normas enunciadas, precisando que la LFPDPPP y la LGPDPPSO de 20 de marzo de 2025 son las plenamente vigentes en México.

a) Ley LFPDPPP de 5 de julio de 2010

Este ordenamiento fue la primera ley específica en materia de protección de datos personales, la cual tuvo por objeto determinar las reglas para el tratamiento de datos 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; asimismo, este ordenamiento refleja los principios de interpretación del derecho de protección de datos personales a nivel internacional.

En lo que respecta a los sujetos regulados por esta ley, son todas aquellas personas físicas o morales con carácter privado que lleven a cabo el tratamiento de datos personales, exceptuando a las sociedades de información crediticia[10] y a las personas que traten datos para su uso personal.

[10] La Ley de Instituciones de Crédito (LIC) dicta las disposiciones que rigen los datos financieros. Este tipo de datos, a pesar de ser datos personales, se encuentran expectuados de la LFPDPPP, en términos del artículo 1o. fracción I del citado ordenamiento. No obstante, dicha excepción ha sido recurrentemente cuestionada, especialmente a partir del Amparo en Revisión 179/2021 del ministro Alberto Pérez Dayán, en el que se "[…] resolvió que es inconstitucional esta excepción sobre las sociedades de información crediticia, como Buró de Crédito, pues no existen 'razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros' que las exceptúen del cumplimiento". Estas condiciones, que no se actualizan en el caso de los datos financieros y que se analizan en el amparo en comento, son las únicas reconocidas por la Carta Magna como circunstancias constitucionales y excepcionales que permiten restringir el derecho humano a la protección de datos personales. En este amparo también se reconoce que al no "[…] cumplirse esas excepciones, como obliga el artículo 16 de la CPEUM y la fracción I del artículo 2o. de la [anterior] ley de datos personales, se genera 'una violación a los principios de legalidad y seguridad jurídica del quejoso, al no encontrar ninguna justificación o supuesto legal válido que permita excluir a las 'instituciones de crédito' o incluso que impida al INAI conocer del procedimiento de *habeas data* para el efectivo ejercicio de los derechos ARCO de los usuarios del servicio de banca y crédito" (Soto Galindo, 2023).

Cabe resaltar que, en términos de esta normativa, los responsables de los datos deben dar a conocer a quienes son titulares de ellos la información que se recaba y los fines para los cuales serán utilizados sus datos, a través del aviso de privacidad.

De igual manera, la LFPDPPP estipula obligaciones para los particulares que lleven a cabo tratamiento de datos personales, respecto de la seguridad administrativa, técnica y física que permita proteger los datos contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado. En caso de existir alguna vulneración de seguridad, éstas deberán ser informadas de forma inmediata por el responsable al titular, a fin de que este último pueda emprender acciones que ayuden a la defensa de sus derechos. La ley, como se constata en los artículos 19 y 20, considera mecanismos que, frente al desarrollo de las nuevas tecnologías de la información y de las vulnerabilidades implícitas en ellas, permitan tomar medidas operativas, tanto al responsable como al titular de los datos.

Cabe señalar también lo estipulado por la LFPDPPP respecto de las transferencias nacionales e internacionales de datos, las cuales aumentan con el uso del cómputo en la nube, la inteligencia artificial, los algoritmos y el big data en el sector público y privado, pues recordemos que, en la mayoría de los casos, los centros de datos se encuentran fuera del país. Estas transferencias, de acuerdo con la LFPDPPP, sólo podrán realizarse en tanto el titular otorgue su consentimiento y, tratándose del responsable, éste deberá comunicar al receptor el aviso de privacidad e informar las finalidades a las que el titular sujetó su tratamiento. En relación con lo anterior, en todo tratamiento de datos existe una expectativa razonable de privacidad, por lo que se presume que, tratándose de una transferencia de datos internacional, el titular de los datos confía en que su información será tratada conforme al aviso de privacidad, pues el nuevo responsable deberá asumir las mismas obligaciones que corresponden al responsable transferente.

El régimen de transferencias nacionales, por su parte, sigue un camino similar al régimen de transferencias internacional. Se exige que el receptor trate los datos conforme al aviso de privacidad, el cual deberá ser previamente comunicado por el transferente.

En lo referente a infracciones, la LFPDPPP contempla en su Capítulo X "De las Infracciones y Sanciones" un listado de acciones que, de realizarse u omitirse, serán motivo de la imposición de una sanción.

Lo anterior volvió a cobrar relevancia a partir del acceso ilegítimo a la base de datos del Buró de Crédito en diciembre de 2022, por lo que los titulares de datos se cuestionaron por qué la autoridad garante del derecho de protección de datos personales en México, el INAI, no iniciaba un procedimiento de protección y/o verificación, como lo mandata la ley para afectaciones a los datos personales en general.

Las penas para quienes estén en los supuestos señalados consisten en una multa de 100 a 320,000 días de salario mínimo vigente en la Ciudad de México,[11] existiendo la posibilidad de que la pena se duplique si las infracciones son cometidas en el tratamiento de datos sensibles (IFAI, 2013).

b) LGPDPPSO de 26 de enero de 2017

Este ordenamiento fue publicado el 26 de enero de 2017 y fue de vital importancia para la protección de la información tratada por el sector público, ya que por primera vez se tuvo una legislación acorde con las características de la administración pública. Dicha legislación es consecuencia de los requisitos para ser aprobada la solicitud de admisión de México en el Convenio 108 del Consejo de Europa.

Tiene como particularidades que su ámbito de aplicación, al ser general, es a los tres niveles de gobierno y contempla un catálogo de sujetos obligados, dentro de los cuales se encuentra cualquier autoridad, entidad, órgano u organismo de los poderes ejecutivo, legislativo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como las empresas del Estado Mexicano.

Esta ley tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales en posesión de sujetos obligados, y persigue, entre otros objetivos, los siguientes: fijar las bases mínimas y condiciones homogéneas que regirán el tratamiento de los datos personales y el ejercicio de los derechos ARCO, mediante procedimientos sencillos y expeditos; garantizar la observancia de los principios de protección de datos personales; proteger los datos personales en posesión de cualquier autoridad, entidad, órgano u organismo de los poderes ejecutivo, legislativo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de la Federación, las entidades federativas y los municipios, con la finalidad de regular su debido tratamiento; garantizar que toda persona pueda ejercer el derecho a la protección de los datos personales; y, finalmente, determinar los mecanismos para garantizar el cumplimiento y la efectiva aplicación de las medidas de apremio que correspondan para aquellas conductas que contravengan las disposiciones previstas en este ordenamiento, así como regular los medios de impugnación.

Los elementos más relevantes de esta ley refieren al reconocimiento pleno de la totalidad de derechos ARCO (acceso, rectificación, cancelación y oposición, respecto al tratamiento de datos personales). También, por primera vez, se habla del concepto

[11] Uno de los casos paradigmáticos en la materia por haber sido de los primeros a la luz de la entonces reciente LFPDPPP de 2010 y por su relevancia en términos del monto de sanción impuesto (9 millones 848 mil 140 pesos), lo constituye las multas por parte del entonces Instituto Federal de Acceso a la Información Pública y Protección de Datos con las que sanciona a la entidad financiera BANAMEX por el no cumplimiento de las disposiciones en materia de protección de datos personales (IFAI, 2013).

portabilidad de los datos referido a que en el caso de que se traten datos personales por vía electrónica, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.

Por otro lado, se hace una diferencia entre los conceptos de *responsable* y *encargado*, a fin de definir las facultades y responsabilidades respecto al tratamiento de datos personales, y la necesidad de formalizar esta relación mediante contrato o cualquier otro instrumento jurídico que decida el responsable, de conformidad con la normativa que le resulte aplicable y que permita acreditar su existencia, alcance y contenido.

Existen disposiciones relativas a las transferencias de datos personales, reconociendo que pueden ser nacionales o internacionales y manifestando que se encuentran sujetas al consentimiento del titular de los datos personales.

En relación con las acciones preventivas, como parte de las buenas prácticas, el responsable podrá desarrollar o adoptar, en lo individual o en acuerdo con otros responsables, encargados u organizaciones, esquemas de mejores prácticas que permitan elevar el nivel de protección de los datos personales, armonizar el tratamiento de datos personales en un sector específico, facilitar el ejercicio de los derechos ARCO por parte de los titulares, facilitar las transferencias de datos personales, complementar las disposiciones previstas en la normatividad que resulte aplicable en materia de protección de datos personales y demostrar, ante el órgano garante de la protección de datos personales (INAI), el cumplimiento de la normatividad que resulte aplicable en materia de protección de datos personales.

A manera de conclusión de esta norma analizada, resulta relevante decir que hasta hace unos años México no contaba con un marco legal en la materia, adecuado y armonizado con los estándares internacionales –al menos desde la óptica del modelo de regulación europeo, por el que más se ha inclinado el legislativo–, de ahí que aspirar a un nivel de protección mayor, que privilegie la dignidad humana por encima de los valores del mercado, a través de nuevas formas de interpretar los derechos humanos, permitía la posibilidad de un mayor nivel de protección, en el que la persona era el centro y, no así, la corporación o el desarrollo tecnológico.

Esta legislación dotó de un nuevo mecanismo para ejercer el derecho de protección de datos personales en el sector público, ya que hasta ese momento los datos en manos del Estado se regían por las normas en materia de transparencia y bajo la perspectiva de ser sólo un límite para el derecho de acceso a la información.

c) LFPDPPP de 20 de marzo de 2025

Este ordenamiento de reciente publicación da pauta a una transición de la configuración del derecho de protección de datos personales en México. En primer lugar, derivado del Decreto en materia de simplicación orgánica de 20 de diciembre de

2024 (Decreto, 2024), el INAI desaparece y se decreta que las facultades que este órgano constitucionalmente autónomo tenía en materia de transparencia, acceso a la información y protección de datos personales pasan a la Secretaría Anticorrupción y Buen Gobierno (SABG).

Esta Secretaría, en términos del Decreto publicado en el *Diario Oficial de la Federación* el 21 de marzo de 2025, atenderá los asuntos referentes a datos personales del sector privado a través de la Dirección General de Datos Personales en el Sector Privado, la cual se auxiliará en el ejercicio de sus atribuciones por las direcciones de Protección de Derechos del Sector Privado, así como de Atención a Denuncias y Verificación del Sector Privado y de Procedimientos Administrativos y Sanciones del Sector Privado.

Este ordenamiento exceptúa de nueva cuenta a las sociedades de información crediticia de la aplicación de dicha ley, al igual que los tratamientos de datos que se hagan para uso personal.

Este ordenamiento incluye la Ley Federal de Procedimiento Administrativo (LFPA) como norma supletoria de las disposiciones no previstas por la ley, y reconoce los mismos principios que rigen el derecho de protección de datos personales previstos en la LFPDPPP de 2010. Asimismo, no incluye disposiciones específicas sobre el tratamiento de datos personales de niños, niñas y adolescentes sobre el derecho de portabilidad (la ley anterior tampoco lo hace, pues la portabilidad sólo se reconocía en la ley de datos en manos del sector público), la privacidad por diseño y por defecto, y los estudios de impacto en la privacidad.

Esta ley elimina las referencias que la ley de 2010 hacía a la Secretaría de Economía. El artículo 2o., fracciones V y XVIII de esta normativa define *datos personales* como "cualquier información concerniente a una persona identificada o identificable" y *titular* como la "persona a quien corresponden los datos personales". A este respecto, se elimina el concepto de *persona física* previsto en la definición de titular de la ley de 2010, abriendo la posibilidad de un nuevo reconocimiento del derecho de protección de datos personales para personas morales.

Las leyes mexicanas no han reconocido previamente que el derecho de protección de datos personales sea aplicable a empresas y/o personas morales, y no existe un consenso sobre la viabilidad en términos del alcance jurídico que tomaría esta figura. Cabe mencionar que existen otras figuras legales que pueden tener alcances parecidos y que son plenamente aplicables a las empresas, como la responsabilidad civil por la divulgación de datos que afecten a una empresa, siempre que se sujeten a las reglas, por ejemplo, el derecho a la libertad de expresión. Este supuesto nos remite a la ponderación casuística de la que se habla en este texto.

También existen cambios sobre el consentimiento, ya que en el artículo 9o. se excluye el consentimiento del titular cuando el tratamiento de sus datos personales esté previsto en una disposición jurídica, y no en una norma con rango de ley como anteriormente expresaba la ley de 2010. En el mismo tenor, se incluye la posibilidad de

no requerir el consentimiento para el tratamiento de datos cuando dichos datos sean necesarios para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable (la ley anterior sólo reconocía esta excepción respecto del cumplimiento de obligaciones derivadas de una relación jurídica).

Finalmente, en el rubro del consentimiento, la fracción VII del mismo artículo 9o. mandata que el consentimiento no será obligatorio cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente, lo cual amplía los supuestos de excepción a los que originalmente estaban previstos en la ley de 2010; es decir, se abre el catálogo de supuestos en los que una autoridad puede solicitar datos personales de un responsable, sin necesidad del consentimiento por parte del titular.

La nueva ley, en términos del artículo 11, también prevé que, si el responsable pretende tratar los datos para una finalidad distinta a las establecidas en el aviso de privacidad, se requerirá obtener nuevamente el consentimiento del titular (en la ley anterior si los datos personales se pretendían tratar para una finalidad compatible o análoga a las finalidades informadas y previstas en el aviso de privacidad, no era necesario recabar nuevamente el consentimiento).

Otro de los cambios importantes de la nueva ley de 2025 es que, en contra de las resoluciones de la Secretaría Anticorrupción y Buen Gobierno, en términos del artículo 51, procede el juicio de amparo, el cual se tramitará ante Juzgados de Distrito y Tribunales Colegiados de Circuito especializados en materia de acceso a la información pública y protección de datos personales (la ley anterior establecía que en contra de las resoluciones del INAI procedía el juicio de nulidad promovido ante el Tribunal Federal de Justicia Fiscal y Administrativa).

d) LGPDPPSO de 20 de marzo de 2025

Este ordenamiento sustituye la ley general de la misma denominación publicada en 2017, y completa el paquete normativo de transición descrito previamente. Esta ley tiene por objeto reglamentar los artículos 6o., Base A y 16, segundo párrafo de la Constitución Política de los Estados Unidos Mexicanos. El primer cambio tiene que ver con las entidades reconocidas como *sujetos obligados*, en términos del artículo 3o. fracción XXVII de la ley, ya que expresa que son cualquier autoridad, entidad, órgano u organismo de los poderes ejecutivo, legislativo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, en el ámbito federal, estatal y municipal o de las demarcaciones territoriales de la Ciudad de México, es decir, incluye de manera expresa a la CDMX. Esto si bien clarifica el ámbito de aplicación de la norma, no es indispensable, ya que la naturaleza general de la norma permite establecer un piso mínimo para los tres poderes del Estado a nivel federal, estatal y municipal.

Sobre el tema de los sindicatos, estos no estaban previstos en la LGPDPPSO de 2017, ya que son ámbito de aplicación de la ley de datos para el sector privado. Pese a la controversia que existe sobre este tema, los sindicatos tienen también que cumplir

con la LFPDPPP y los principios que de ella emanan, por lo que también se garantiza este derecho para trabajadores y agremiados. Es decir, no existe un detrimento para las personas respecto de sus datos personales, ya que, si bien dichos tratamientos están previstos en la ley de datos del sector público, atendiendo a su propia naturaleza, el ámbito de aplicación de la ley de datos en manos de particulares ampara este tipo de tratamientos.

En cuanto a la defensa de derechos, la reforma elimina el recurso de inconformidad y deja el juicio de amparo como la vía para impugnar las decisiones de la autoridad competente. Se mantiene el recurso de revisión en materia de seguridad nacional previsto en la ley de 2017.

II.2. Principios del derecho de protección de datos personales

El derecho de protección de datos personales está reconocido en México como un derecho humano en el segundo párrafo del artículo 16 constitucional. A partir de este reconocimiento, se han desarrollado normas secundarias que dan vida al derecho de protección de datos personales, a través de reglas específicas, autoridades, principios y procedimientos para la salvaguarda de este derecho. Es específicamente en la legislación secundaria, tanto para el sector público como para el privado, en la que se reconocen principios de interpretación que ayudan al operador jurídico y/o al responsable en materia de protección de datos personales, a entender y aplicar las disposiciones generales en la materia.

De acuerdo con Alexy (1993), los principios son mandatos de optimización, es decir, son normas que ordenan que algo sea realizado en la medida de las posibilidades jurídicas y reales existentes. Dichos principios están caracterizados por el hecho de que pueden ser cumplidos en diferente grado, ya que su cumplimiento no sólo depende de las posibilidades reales, sino de las jurídicas. Esto, a su vez, está determinado por reglas y, sobre todo, por principios que juegan en sentido contrario, por lo que es necesaria su ponderación.

Es así que los principios resultan de mucha utilidad al momento de determinar los límites del derecho de protección de datos personales, respecto de otros, como el derecho de acceso a la información o frente a situaciones como el interés público, la seguridad nacional o la salud pública –abordados algunos apartados más adelante–. Derivado de lo anterior, resulta necesario hacer un breve repaso de los principios del derecho de protección de datos personales reconocidos a nivel internacional, en el marco de la Unión Europea y de México.

A nivel internacional, "la Resolución 45/95 de la Asamblea General de la ONU [prevé una] lista básica de principios en materia de protección de datos personales con un ámbito de aplicación mundial, entre otros, los de licitud, exactitud, finalidad, acceso y no discriminación" (Ornelas y López, 2010, p. 63).

En el ámbito europeo, los principios más importantes respecto a la configuración del derecho de la protección de datos personales son los siguientes: consentimiento, información, finalidad, calidad de los datos, con especial referencia a la proporcionalidad y seguridad; sin embargo, la Carta Europea de Derechos reconoce otro de los principios que ya es inherente a la protección de datos: el principio de control independiente (Ornelas y López, 2010).

En el caso de México, la legislación reconoce una serie de principios y deberes, entre los que encontramos: a) principios: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad; y b) deberes: confidencialidad y seguridad, los cuales explicaremos, en términos generales, en los siguientes párrafos (IFAI, 2016).

a) *Principio de la licitud*: La licitud mandata tanto a responsables como a encargados de datos personales, que el tratamiento de la información de carácter personal tenga que hacerse de forma lícita y legítima o leal, con apego a la normativa aplicable y conforme lo acordado entre el responsable del tratamiento y el titular de los datos personales, bajo los términos establecidos, de manera que se cumpla con la expectativa razonable de privacidad.

Para el caso de la protección de datos personales en México, especialmente en el sector público, no puede realizarse tratamiento de datos personales que signifique violaciones a derechos humanos, ya que dicho tratamiento se considerará inconstitucional.

b) *Principio de consentimiento*: Todo tratamiento de datos personales requiere el consentimiento por parte de su titular, salvo excepciones previstas en las normas. El consentimiento se obtiene normalmente a través del aviso de privacidad y puede ser expreso o tácito, según el tipo de datos que se someten al tratamiento.

c) *Principio de información*: A través de este principio, el responsable del tratamiento de los datos personales informa al titular sobre la información recabada y el objetivo de su tratamiento; asimismo, el responsable deberá proporcionar al titular de los datos la información para ejercer los derechos ARCO garantizados por la Constitución.

d) *Principio de calidad*: Este principio mandata que los datos que sean tratados deben ser correctos, exactos, completos y actualizados respecto del fin para el que fueron recabados. Este principio también obliga al responsable del tratamiento de datos personales a dotar de procedimientos que permitan la actualización y corrección de estos, mediante el denominado derecho de rectificación.

e) *Principio de finalidad*: Este principio está vinculado directamente con los principios de información, consentimiento, proporcionalidad y calidad. Su objetivo es garantizar que los datos personales sean tratados exclusivamente para los fines para los que fueron autorizados por el titular del dato a través del aviso de privacidad o, en términos, por ejemplo, del principio de proporcionalidad, pensando en tratamientos de datos que haga el Estado y que no requieran de consentimiento por parte de su titular. Este

principio también garantiza que los datos personales sean tratados únicamente para los fines para los que fueron recabados y establece límites frente a tratamientos que pudieran derivar en posibles vulneraciones de otros derechos humanos.

f) *Principio de lealtad*: Este principio está asociado con el de licitud y tiene que ver con el deber del responsable de tratar los datos personales de manera lícita y leal, lo que implica actuar en apego al marco jurídico aplicable, es decir, con pleno cumplimiento y respeto de la buena fe de la información que es sometida al tratamiento.

g) *Principio de proporcionalidad*: Este principio implica que los datos personales que son sometidos al tratamiento son los estrictamente necesarios para lograr el fin del tratamiento, amparado por el consentimiento del titular del dato.

h) *Principio de responsabilidad*: Este principio implica que los responsables de los datos personales adoptarán e implementarán todas las medidas necesarias para el cumplimiento de los principios antes expuestos.

II.3. La portabilidad y el derecho al olvido dentro del derecho de protección de datos personales

Existen dos figuras relativamente nuevas que se han insertado dentro del derecho de protección de datos personales y que han cobrado especial importancia, sobre todo a partir del desarrollo tecnológico. Se trata del llamado *derecho a la portabilidad* y del *derecho al olvido*.

a) *Derecho de portabilidad*: Una vez que se analizaron los aspectos constitucionales y de legislación secundaria del derecho de protección de datos personales, se puede advertir una figura muy particular asociada a los derechos ARCO reconocidos en la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (2025), la denominada *portabilidad*. A este respecto, es el artículo 51 de dicho ordenamiento el que reconoce este concepto y el cual a la letra señala lo siguiente:

> Artículo 51. Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el titular tendrá derecho a obtener del responsable una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos.
>
> Cuando el titular haya facilitado los datos personales y el tratamiento se base, en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales.

Sobre el particular: "La portabilidad, conceptualmente, constituye una respuesta técnica a la necesidad humana de 'llevar consigo' ciertos bienes que son de utilidad y es un concepto clave en la evolución […] de las TIC" (Puccinelli, 2018, p. 157).

El primer elemento para definir en torno al concepto de la portabilidad, es si se trata de un derecho que completaría el catálogo de los denominados derechos ARCO o, en su caso, si es una forma de manifestación del derecho de acceso; es decir, si se trata más bien de un formato de acceso a los datos personales, cuyo ejercicio ya se reconoce de forma tradicional en las normas en materia de datos personales.

A pesar de los debates doctrinarios respecto de lo planteado, se puede considerar que la portabilidad no es otra cosa más que la materialización del derecho de acceso a datos, sólo que a través de un formato portable que permite al titular del dato acceder y llevar consigo o trasladar a un nuevo responsable los datos personales en el formato en el que originalmente se hayan resguardado.

El ejemplo más evidente de la utilidad de la portabilidad en materia de datos personales, lo constituye el expediente clínico electrónico, el cual permite que la información de salud de una persona vaya de una plataforma interoperable a otra, con la sola solicitud expresa del titular del dato y esto, a su vez, permitiría no sólo eficientar el servicio de salud, sino garantizar otros derechos humanos, como el derecho de acceso a la salud o el de acceso a la justicia, pensando en casos de probables negligencias médicas.

A pesar de la notoria utilidad de la portabilidad en materia de datos personales, no es una figura reconocida como un derecho de los titulares de datos personales en manos de las corporaciones, por lo que hoy día existe en México una evidente disparidad del nivel de protección y goce del derecho humano de protección de datos personales, dando un trato diferenciado entre aquellos datos en manos de responsables del sector privado respecto de aquellos datos personales en posesión de responsables del sector público.

No obstante lo anterior, y a pesar de que no existe un reconocimiento expreso de la portabilidad de datos en el sector privado, las consecuencias de la reforma constitucional de derechos humanos de 2011 y la inserción del principio pro persona como herramienta indispensable de interpretación para los operadores jurídicos del Estado, no sólo permitiría sino obligaría al Estado a otorgar el mismo nivel de prerrogativas, no limitadas a un reconocimiento expreso en las normas secundarias.

Aquí resulta pertinente decir que el *principio pro persona* es "un principio de interpretación para que todas las autoridades del país lleven a cabo la protección más amplia de los derechos humanos de todos los habitantes del territorio nacional" (Cossío Díaz, 2012, p. 50).

No se puede obviar que la portabilidad no está reconocida de forma expresa en la Constitución, pero sí lo está en la ley de datos aplicable al sector público, por lo que el mismo principio pro persona permitiría invocar la aplicación de los beneficios de dicha norma.

Aunado a lo anterior, es importante resaltar que, tanto en 2017 como en 2025, el legislador en México hace un trabajo extraordinario al momento de desarrollar la LGPDPPSO, incorporando y manteniendo una figura de avanzada que el propio modelo europeo de regulación en la materia no ha alcanzado, pese a los notables avances a favor de este derecho previstos en el Reglamento Europeo de Protección de Datos Personales.

Asimismo, recordando una de las características de los derechos humanos, como lo es la progresividad, se entendería que el legislador nacional podría ir más allá en favor del derecho de portabilidad del dato –reconocer la figura de forma expresa en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares– y no en sentido contrario, eliminando la obligación del Estado para garantizar la portabilidad en el sector público. Sin embargo, debe precisarse que, más allá de la armonización legislativa –como se ha señalado–, el principio pro persona permite invocar este beneficio tanto para los datos en manos del sector público como para el privado.

b) *Derecho al olvido*: Cuando hablamos de derecho al olvido, debemos recordar que esta figura tiene su origen en la Sentencia T-414 de 16 de junio de 1992 dictada por la Corte Constitucional de la República de Colombia, así como su incorporación en legislaciones nacionales, como el caso del "artículo 10 de la Ley 787 de 2012 de la República de Nicaragua y el artículo 11 del Decreto 37.554 de 2012 de la República de Costa Rica" (Remolina Angarita, 2017, pp. 199, 211 y 212).

Por otro lado, el derecho al olvido a través del derecho de desindexación tiene su origen en la Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de 13 de mayo de 2014, Asunto C-131/12, consecuencia de la negativa de Google frente a la solicitud formulada por Mario Costeja González, ya que el buscador había indexado dos anuncios del periódico *La Vanguardia*, que originalmente fueron publicados en una versión impresa, relativos a una subasta de inmuebles relacionada con él y con un embargo derivado de deudas a la Seguridad Social. El señor Costeja corroboró que al introducir su nombre y apellidos en Google aparecía un enlace a las páginas del periódico que incluían dichos anuncios, y solicitó la retirada de la información considerando que carecían de relevancia. Frente a la negativa del buscador, el señor Costeja pidió la intervención de la Agencia Española de Protección de Datos, que recurrió a la Audiencia Nacional que, a su vez, envió el caso al Tribunal Europeo. La sentencia obligó al buscador a desindexar la información por considerar que los hechos estaban obsoletos al haber ocurrido hace varios años y estando al corriente el señor Costeja de pagos (Caso C-131/12, 13 de mayo de 2014). Por su parte, el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, a través del derecho de supresión también reconoce la figura del derecho al olvido.

Por otro lado, encontramos el primer pronunciamiento sobre derecho al olvido del Tribunal Constitucional Español (TCE), mediante la Sentencia 58/2018 de 4 de junio del mismo año, en el cual se declaró que se habían vulnerado los derechos de los

recurrentes al honor, a la intimidad y a la protección de datos por el uso de las tecnologías de internet, dado que sus nombres y apellidos aparecían en los buscadores de hemerotecas digitales. El Tribunal consideró vulnerado su derecho al olvido, recogido en el artículo 17 del RGPD (Sentencia 58/2018), y expresó lo siguiente:

> […] la prohibición de indexar los datos personales, en concreto los nombres y los apellidos de las personas recurrentes, para su uso por el motor de búsqueda interno de "El País" [ya que la información debe ser limitada], idónea, necesaria y proporcional, a fin de evitar una difusión de la noticia lesiva de los derechos invocados. (TCE, Sentencia 58/2018, 2018).

El primer antecedente del derecho al olvido en México (interpretado como un derecho de desindexación), se encuentra en la postura del INAI respecto a una solicitud de protección de derechos –particularmente el de cancelación–, formulada por un empresario mexicano, quien primero solicitó a Google la eliminación de varios resultados de búsqueda relacionados con su nombre –argumentando que la información afectaba su esfera más íntima y también sus relaciones financieras actuales, ya que uno de esos enlaces direccionaba al reportaje periodístico "Fraude en Estrella Blanca alcanza a Vamos México", publicado en 2007 por la revista *Fortuna*–. En esta nota, el empresario es mencionado como uno de los implicados en presuntos actos de corrupción. En este sentido, la legislación mexicana en materia de datos personales en el sector privado establece que, en caso de que la solicitud de derecho de cancelación no sea atendida por el particular (Google), el titular del dato podrá acudir a través de la denominada solicitud de protección de derechos ante el órgano garante, a fin de iniciar una investigación y, de ser el caso, iniciar un procedimiento sancionatorio contra el particular. En este caso planteado, el INAI sancionó a Google por no atender la solicitud de cancelación del dato, sin contar que la fuente original –la revista *Fortuna*– se ampararía, ya que no fue escuchada dentro del procedimiento [y argumentando una afectación del derecho de libertad de expresión de concederse la cancelación].

Hoy día en el país se discute cuáles son los límites del derecho al olvido frente a derechos como la libertad de expresión, el derecho de acceso a la información o el derecho a la verdad, porque no resulta lo mismo solicitar eliminar información que es de interés de la colectividad y que refiere a un servidor público, que la solicitud de borrar información que atenta contra la dignidad humana, siendo posiblemente relacionada a una persona que no es figura pública, que no tiene cierto grado de exposición o a información concerniente a niños, niñas y adolescentes. En este mismo sentido, surge el debate de los límites de la libertad de expresión y el grado de exposición de personas públicas, en los cuales no existe cabida a preguntarnos si los datos de niños, niñas y adolescentes deberían ser borrados o no, atendiendo al mandato del principio del interés superior del menor. (Mendoza Enríquez, 2018a, pp. 348-349).

Aunado a lo anterior, el derecho al olvido funciona como un habilitador y muchas veces se asocia a otro tipo de derechos, como el derecho de acceso a la justicia, por lo que deberá estudiarse de forma casuística las particularidades de cada situación. En el mismo sentido, el derecho al olvido y, en general, el derecho de protección de datos personales, no pueden ser ajenos a temas como la perspectiva de género, desde la cual se han desarrollado avances normativos en México, como la denominada Ley Olimpia.[12]

Por otro lado, otro asunto relevante sobre derecho al olvido en México es el Caso Ulricht Richter vs. Google, Inc., ya que, el 13 de junio de 2022, la Sala Octava de lo Civil de la Ciudad de México (segunda instancia) condenó a dicha empresa al pago de aproximadamente 250 millones de dólares (5 mil millones de pesos mexicanos) como daño moral (Soto Galindo, 2025). Esta sanción atiende a que el buscador toleró la existencia de un blog en el que se difamaba al demandante y a su esposa (Soto Galindo, 2022).

Finalmente, es importante destacar que aunque muchas veces se utilicen como sinónimos conceptos como desindexación, derecho al olvido y cancelación de datos personales, cada uno tiene sus particularidades: el primero, vincula a la liga, en sentido hipotético, une la información contenida en una fuente original de información digital con los resultados que arroja un buscador en línea; el segundo refiere a una esfera más amplia de protección, que de garantizarse implicaría la eliminación de información tanto en las fuentes originales como en aquellas que la hubieren replicado y no únicamente la eliminación de la "liga" entre una fuente de información y un resultado de un buscador como Google; y la tercera se centra únicamente en cancelar datos que estén en manos de un responsable, aunque eso no signifique que se eliminen por completo, especialmente considerando la inmediatez y la ubicuidad de internet.

Como se puede advertir, son bastante complicadas las tensiones entre el derecho al olvido y otros derechos, como la libertad de expresión, pensamiento e incluso acceso a la información, por lo que serán los precedentes judiciales los que indiquen la construcción, configuración y alcances del denominado derecho al olvido, incluso clarificando el concepto mismo, para diferenciar la extensión de los términos antes referidos (la cancelación, el olvido, la supresión o la desindexación en los motores de búsqueda de la información de carácter personal).

[12] La Ley Olimpia es un conjunto de reformas a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal Federal, que busca reconocer la violencia digital y sancionar los delitos que violen la intimidad sexual de las personas a través de medios digitales, también conocida como ciberviolencia.

II.4. Límites, tensiones y restricciones constitucionales del derecho de protección de datos personales: seguridad nacional, salud pública, orden público

Al igual que los demás derechos humanos, el derecho de protección de datos personales no es un derecho absoluto y su ejercicio sólo puede estar limitado por aquellas restricciones prescritas en la ley que resulten razonables en una sociedad democrática, por ejemplo, seguridad nacional, seguridad pública, preservación de la salud, prevención del delito y la protección de los derechos y libertades de los demás.

El artículo 16 constitucional reconoce que todas las personas tienen derecho a la protección de datos personales, al acceso, rectificación, cancelación y oposición frente al tratamiento de dicha información, salvo que se esté en alguno de los supuestos de excepción por razones de seguridad nacional, orden público, seguridad y salud pública o para proteger derechos de terceros.

> Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento […].
>
> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de estos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los *supuestos de excepción* a los principios que rijan el tratamiento de datos, *por razones de seguridad nacional*, *disposiciones de orden público*, *seguridad y salud públicas o para proteger los derechos de terceros* […] (CPEUM, 2025). [énfasis añadido].

Estos supuestos de excepción representan enormes desafíos para los operadores jurídicos, ya que la determinación final tiende a ser casuística considerando diferentes variables, por lo que a continuación desglosaremos cada supuesto con ejemplos de la vida diaria:

1) *Seguridad nacional*: La no obligación del responsable del dato para garantizar el ejercicio de derechos ARCO frente a situaciones que ponen en riesgo la seguridad nacional. Es importante advertir que, en situaciones excepcionales, el responsable será una entidad privada. Por ejemplo, una aerolínea comercial, cuyos datos sometidos a tratamiento estén vinculados con un asunto de seguridad nacional y que compartirá con el Estado, previo requerimiento fundado y motivado por parte de la autoridad competente. En este caso hipotético, una solicitud de acceso por parte del pasajero, respecto de los datos personales que la aerolínea haya compartido con autoridades, será negado y si esa misma solicitud se redirecciona a alguna instancia estatal, pasará lo mismo, ya que

de demostrarse que esa información tiene un vínculo directo con temas de seguridad nacional y que el tratamiento de datos que haga el Estado es proporcional y razonable, se acreditará la restricción constitucional del ejercicio de un derecho humano.

2) *Disposiciones de orden público*: Aquellas restricciones sobre el ejercicio de derechos ARCO, que permitan la prevalencia del orden público, es decir, el normal funcionamiento de las instituciones, recordando que las restricciones a los derechos humanos, en específico al de protección de datos personales, siempre tendrán que ser proporcionales en el marco de un Estado democrático.

3) *Seguridad pública*: La restricción respecto del ejercicio de derechos ARCO que pudiera afectar las instancias y actividades de seguridad pública. Por ejemplo, pensemos en una solicitud de cancelación del dato personal correspondiente a la imagen de una persona que participó en una manifestación, y de la cual la policía local demuestre que debe conservarla en términos de sus funciones para salvaguardar la seguridad, siempre que dicho tratamiento demuestre ser proporcional, lícito, razonable y cumpla con los plazos de conservación señalados por la ley (normalmente leyes en materia de archivos y memoria histórica).

4) *Salud pública*: La restricción del ejercicio de derechos ARCO que pudiera afectar la salud pública en el país. Por ejemplo, una solicitud de cancelación del dato de una persona diagnosticada como positiva a covid-19, ya que, para el caso de México, la Secretaría de Salud tiene facultades conferidas por ley, para llevar a cabo un registro de enfermedades epidemiológicas que representen un riesgo sanitario. Esto no significa que en cualquier momento el Estado pueda divulgar datos de los pacientes positivos, ya que prevalecerán no sólo los principios en materia de protección de datos personales, sino las obligaciones del responsable, en términos de la confidencialidad de la información y las medidas de seguridad para el resguardo de ésta.

5) *Proteger derechos de terceros*: La restricción del ejercicio de derechos ARCO cuando de concederse pudieran dañar los derechos de un tercero. Por ejemplo, que el Área de Recursos Humanos de una empresa sea notificada por una instancia judicial, respecto de la obligación de retener una parte del sueldo de un trabajador para cubrir una pensión alimenticia a favor de un menor, y que al enterarse el trabajador solicitara la cancelación del dato que permitiera llevar a cabo dicha retención y traslado del monto económico. Esto es, de otorgarse la cancelación del dato, se obstaculizaría el cumplimiento de una obligación en términos del derecho civil e incluso podrían verse afectados otros derechos, como los de la infancia, por lo que la restricción resulta legítima al estar prevista en la Constitución y acorde con el Estado Constitucional de Derecho.

Como se puede ver de las líneas previas, el régimen de restricciones sólo aplica al ejercicio de derechos ARCO y no así, por ejemplo, a los principios que deben regir el tratamiento de estos. Pensemos en las instancias de seguridad nacional de Estados Unidos de Norteamérica, en relación con el principio de proporcionalidad y finalidad reconocido en el marco jurídico mexicano y comunitario europeo.

Si bien los supuestos previstos en el artículo 16 constitucional limitan en casos muy específicos el ejercicio de derechos ARCO, no así la obligación del responsable de garantizar la aplicación de los principios durante todo el tratamiento, incluidos los de proporcionalidad y finalidad. Esto no es nada menor, ya que es la clave para considerar que muchas de las transferencias internacionales de datos que hace el Estado Mexicano al país del norte, en el marco de colaboración del flujo migratorio de personas, pudieran considerarse inconstitucionales en términos de los compromisos internacionales que México ha adoptado a través de la adhesión al Convenio 108 del Consejo de Europa y en términos de la propia legislación nacional.

Como se advierte, también, las situaciones de excepción –como su nombre lo dice– tratan de situaciones extraordinarias, que de no acreditarse el supuesto exacto previsto en la Constitución simplemente no podrán invocarse para restringir el ejercicio del derecho humano a la protección de datos personales.

No obstante hemos hablado de supuestos de excepción al ejercicio de los derechos ARCO, reconocidos en el artículo 16 constitucional, también resulta necesario hablar de las tensiones naturales del derecho de protección de datos personales con otros derechos, como el de acceso a la información, la libertad de pensamiento y la libertad de expresión.

Para los operadores del derecho de protección de datos personales en el sector público, resulta muy complejo determinar los límites de este derecho, sobre todo en relación con el ejercicio del derecho de acceso a la información, ya que, en la práctica, existen solicitudes formuladas al Estado, cuya respuesta puede incluir datos personales protegidos por el derecho que nos atañe en este trabajo.

Aunado a lo anterior, la particularidad del derecho de acceso a la información en México, que a lo largo de su desarrollo se ha constituido más como un derecho de aplicación casuística con variables diversas que ante similares situaciones pueden existir distintos límites. Esto trae consigo innumerables desafíos y, tratando de simplificar directrices generales que rigen el derecho de protección de datos personales contra el derecho de acceso a la información, podemos decir lo siguiente.

Una de las causales de reserva de la información en términos del derecho de acceso a la información previstas en la ley es aquella información que tenga carácter de confidencial. Si bien los datos personales constituyen una de las categorías de la información confidencial prevista en la Ley General de Transparencia y Acceso a la Información Pública (LGTAIP), no todos los datos personales son confidenciales, ya que, por ejemplo, existen datos de servidores públicos que cumplen con todas las características de identificar o hacer identificable a la persona que, pese a ello, serán

públicos en las páginas web institucionales o son sujetos a ser entregados mediante solicitudes de acceso a la información (entre ellos, nombre, correo electrónico institucional, remuneración mensual recibida, número de celular asignado como servidor público y pagado con recursos públicos o la dirección de la oficina de despacho).

En este sentido, no existen reglas generales, sino criterios establecidos por la autoridad garante del derecho de acceso a la información y protección de datos personales en México –a nivel nacional el INAI y a nivel estatal los órganos garantes de las entidades federativas–, los cuales pueden ser orientadores en situaciones similares, por lo que las tensiones entre ambos derechos tienen diversas formas de resolverse, aun ante situaciones aparentemente similares.

Por otro lado, el ya mencionado derecho al olvido también genera tensiones entre el derecho de protección de datos personales y derechos como la libertad de pensamiento, expresión y el propio derecho de acceso a la información.

Finalmente, los precedentes judiciales y la responsabilidad de las instancias administrativas deben ponderar de forma correcta derechos como la protección de datos personales, a la luz del interés público y la libertad de expresión, ya que, de no hacerlo, podrían transgredirse otros derechos humanos e incluso propiciar afectaciones graves a la democracia moderna.

II.5. Relevancia del derecho de protección de datos personales y su relación con el fortalecimiento del Estado democrático

El derecho humano de protección de datos personales normalmente se asocia exclusivamente con el derecho a la privacidad, sin embargo, la realidad y la vida cotidiana han puesto en relieve su eje transversal con otros derechos tan importantes como los político-electorales y, por ende, su evidente relación con la democracia en los Estados.

Aunado a esto, se ha demostrado que el derecho de protección de datos personales resulta un elemento de partida imprescindible para el fortalecimiento de la vida democrática de los Estados y la consolidación del Estado Constitucional de Derecho.

Ejemplos como los de Cambridge Analytical[13] permitieron replantear la importancia del derecho de protección de datos personales, y cómo a partir de su vulneración y del uso poco ético de la información de carácter personal por parte de las corporaciones se podía incidir en los resultados de las elecciones, especialmente de Estados Unidos de Norteamérica.

[13] Cambridge Analytica fue una compañía privada que, a través de la minería y análisis de datos, ofreció servicios de comunicación estratégica para campañas electorales, los cuales influyeron en varias elecciones de Estados democráticos, como las de Estados Unidos de Norteamérica. A partir de la colaboración de empresas como Facebook mediante la transferencia de datos personales a terceros para realizar dicha minería de datos, se replantearon los alcances de las políticas de privacidad de las redes sociales, dando un peso significativo a la necesidad de incoporar la ética corporativa en el uso de la información de carácter personal.

Es decir, el derecho de protección de datos personales no sólo se debe entender como un derecho fundamental de reconocimiento constitucional, sino como un elemento necesario y detonador para la vida democrática de los Estados. Es así como la democracia constitucional conforma "el marco institucional, político y cultural por antonomasia para lograr la vigencia de los derechos humanos" (Cerdas, 1994, p. 301), "pues la realización efectiva de estos últimos conforma la esencia de lo que persiguen los regímenes democráticos. Ello explica la relación de interdependencia de la democracia frente a la privacidad y la protección de datos personales […]" (Maqueo y Barzizza, 2020, p. 29).

De esta forma, el reconocimiento y salvaguarda del derecho a la privacidad, garantizado a través del derecho de protección de datos personales, no sólo manifiesta una serie de libertades para las personas, sino que establece un límite frente a injerencias en la vida privada de los ciudadanos, y ese límite en primer término es señalado para el Estado. Por otro lado, podemos afirmar:

> […] el autoritarismo como una forma de gobierno incompatible con un sentido moderno de democracia, se caracteriza por la ausencia de privacidad, e incluso, de protección de datos personales […] [en el que] la centralización del poder en una sola persona o varias (pero no en la mayoría), facilita el establecimiento de medidas de control y persecución. (Maqueo y Barzizza, 2020, p. 30).

En palabras de Westin, bajo una exigencia de absoluta lealtad al régimen, los Estados totalitarios "niegan la privacidad, destruyen las relaciones confidenciales tradicionales, introducen sistemas extendidos de vigilancia y de informantes, y recopilan expedientes completos de millones de ciudadanos" (Westin, 1968, p. 1069).

Incluso las medidas de control y persecución establecidas en algunas dictaduras de Latinoamérica permitirían justificar la necesidad, por ejemplo, del anonimato como figura garantizada en el ejercicio del derecho de acceso a la información o algunas vinculadas con la garantía de la libertad de pensamiento y de expresión, como los mecanismos de responsabilidad ulterior en el ejercicio del derecho de la libertad de expresión, relacionado con labores periodísticas.

Por otro lado, no puede obviarse que, si bien la tecnología permite nuevos mecanismos de participación ciudadana que fortalecen la democracia, también otorga posibilidades de ser utilizada como atentado directo contra la democracia. Es así como temas aparentemente sin una relación con el derecho de protección de datos personales están siendo hoy discutidos en México, y cuyo componente esencial radica precisamente en el tratamiento que se haga de la información que identifique o haga identificable a una persona, por ejemplo, el voto electrónico o, en su caso, el voto a través de internet.

Ejemplos específicos que tienen que ver con el derecho de protección de datos personales y que hoy representan un desafío para la democracia moderna en México, los encontramos en el uso de *bots*, creación y difusión de información falsa, programas estatales de vigilancia masiva, *big data* y uso de información en campañas políticas y su influencia en la intención del voto.

Dicho lo anterior, podemos concluir que el derecho de protección de datos personales y todos aquellos mecanismos que en su conjunto garanticen el derecho a la privacidad permiten fortalecer la democracia moderna y desmotivan un Estado concentrador de información que pueda ser utilizada como mecanismo de control social o electoral.

Asimismo, se advierte la necesidad de que el derecho constitucional se ocupe de proteger la privacidad y, por ende la democracia, ya que, de no hacerlo, serán otros los que escriban las reglas del juego (desarrolladores de código o software y en general las corporaciones), bajo una visión de eficiencia de mercado y no en términos de los valores intrínsecos a la privacidad y a la dignidad humana y, por tanto, a la protección de datos como un derecho humano necesario en una sociedad democrática (Boehme-Neßler, 2016).

Capítulo III
Desafíos del derecho de protección de datos personales desde una óptica de los derechos humanos

El desarrollo del derecho de protección de datos personales en los últimos años ha sido evidente, sobre todo a partir del vertiginoso progreso tecnológico. Esto ha sido posible gracias a los instrumentos normativos que reconocen la dignidad de las personas y reflejan en los principios, obligaciones y deberes para el tratamiento de datos, los alcances que dieron origen a la Declaración Universal de Derechos Humanos.

Ejemplos paradigmáticos como el Convenio 108 del Consejo de Europa y su protocolo modernizado (Convenio 108 Plus, 18 de mayo de 2018), así como el Reglamento Europeo de Protección de Datos Personales (RGPD, 14 de abril de 2016) envían un mensaje claro al poder económico y político de las corporaciones como Meta y X, obligando a las empresas a incorporar políticas de privacidad acordes con las normas aprobadas en los territorios en los que prestan su servicio y dando pauta a conceptos necesarios, como la ética en el uso de la información.

A pesar de que México se ha decantado por reconocer la máxima protección para los titulares de datos personales, en consonancia con las normas de derecho comunitario de la Unión Europea, existen importantes desafíos que hoy plantean una posible regresión del nivel de protección otorgado por el Estado Mexicano, lo cual resulta contrario a las características propias de los derechos humanos, como la progresividad de estos.

En las siguientes líneas, se analizará la adhesión de México al Convenio 108 del Consejo de Europa, así como el desafío de tener un nivel adecuado de protección, pensando en el protocolo de modernización de dicho convenio y las implicaciones de la ratificación por parte de México del Tratado de Libre Comercio entre este país, Estados Unidos de Norteamérica y Canadá.

Por otro lado, se identificarán desafíos en cuanto a los pocos precedentes sobre el derecho de protección de datos personales por parte de la Corte Interamericana de Derechos Humanos (Corte IDH), analizando los pronunciamientos que sí ha hecho sobre el derecho a la privacidad, y que podrían servir como eje transversal para el desarrollo específico del derecho que interesa a este trabajo.

Asimismo, se estudiará, de forma general, algunos de los precedentes que ha establecido la Suprema Corte de Justicia de la Nación (SCJN) sobre el derecho de protección de datos personales, para finalmente hablar de los desafíos de la efectiva salvaguarda de este derecho, incluido el entorno digital.

Finalmente, en este apartado se examinará lo referente al derecho a la protección de datos personales en la era digital, que pone de relieve desafíos derivados de la ubicuidad del ciberespacio, las multiplicidades de jurisdicciones y la falta de escrutinio de los derechos humanos por parte de los Estados-Nación.

III.1. Adhesión de México al Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

En 2018, México fue aceptado y se incorporó al Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal –un instrumento paradigmático en materia de protección de datos personales en el ámbito europeo y de países terceros (no miembros de la Unión Europea) que sean admitidos a formar parte de éste–, lo cual establece las bases para una máxima protección de la información de las personas, en un reconocimiento jurídico, histórico y político de la dignidad humana frente al desarrollo tecnológico.

También se debe resaltar que, si bien la adhesión de México al Convenio 108 establece un antecedente inédito para fijar el rumbo hacia donde debe evolucionar normativamente este derecho en el marco legal doméstico –atendiendo, primero, a la progresividad de los derechos humanos y, segundo, al principio pro persona y la interpretación conforme, reconocidos en la Constitución, a partir de la reforma de derechos humanos de 2011–, están pendientes los trabajos de análisis y revisión de la adhesión al Convenio 108 en su versión modernizada (Convenio 108 Plus), que reconoce y mitiga el impacto de la tecnología en la vida privada de las personas.

En este sentido, México no sólo ha detenido la estrategia de adhesión al Convenio 108 Plus, sino que ha tenido importantes retrocesos al aceptar disposiciones de menor protección para el tratamiento de datos personales, como las previstas en el Capítulo 19 del Comercio Digital del Tratado de Libre Comercio entre Estados Unidos de Norteamérica, Canadá y México (T-MEC).

Este fenómeno tiene su explicación en la forma en la que el valor económico de los datos prevalece sobre el reconocimiento del derecho de protección de datos personales del modelo europeo, que considera la dignidad humana como el eje rector para el desarrollo tecnológico, de ciencia y de innovación, y hace un enérgico llamado a las corporaciones a insertar aspectos éticos que sirvan como límites frente a tratamientos que atenten en contra de la dignidad de las personas.

También, este fenómeno se explica por condiciones geopolíticas y de economía regional y global, que obligan a los Estados-Nación a privilegiar la colaboración a través de compartir información (incluídos datos personales), pese a que no se garantice el mismo nivel óptimo para su tratamiento. Un ejemplo claro de esto son los datos que México comparte con Estados Unidos de Norteamérica en materia migratoria, en el

que preceptos como la seguridad nacional y la colaboración internacional buscan justificar tratamientos ilícitos en términos de las vulneraciones a otros derechos humanos que surgen a partir de dichos tratamientos.

Es decir, en su momento, México decidió sobre el modelo de regulación por el que optaría, siendo el modelo europeo de protección de datos personales[14] el que consideró el más idóneo. Dicho modelo también incluye algunas directrices, por lo que, en el marco del Estado Constitucional y Democrático de Derecho, se debe guardar congruencia a este reconocimiento y protección de la dignidad de las personas, sobre aquellos intereses comerciales o económicos que podrían estar contenidos en otros instrumentos internacionales, posteriores a la adhesión de México al referido Convenio 108.

Para una mejor explicación del tema, en el caso de la Unión Europea, fue la Comisión Europea la que aprobó las disposiciones para los flujos de datos transfronterizos, derivadas del cierre de la consulta sobre la orientación del artículo 49 del Reglamento Europeo de Protección de Datos Personales. Estas disposiciones se aprueban como horizontales para los flujos de datos transfronterizos y la protección de datos personales en los acuerdos comerciales, ya que los datos personales son un derecho fundamental y no pueden ser objeto de negociación en los acuerdos comerciales de la Unión Europea.

Esto es, la Comisión Europea está tratando de romper las barreras al flujo de datos entre empresas, en futuros acuerdos comerciales, como parte de su impulso hacia una economía más digital, al tiempo que salvaguarda los principios fundamentales del derecho de protección de datos personales.

Las disposiciones están diseñadas para insertarse en futuros acuerdos comerciales y garantizar que los principios subyacentes al Reglamento Europeo de Protección de Datos Personales no se vean socavados. Lo interesante de esta propuesta para suscribir acuerdos internacionales es que las cláusulas relativas a datos personales incluidas en un tratado comercial serán excluidas de cualquier tribunal de inversión establecido por el acuerdo para arbitrar y resolver disputas, lo que significa que las disposiciones estarán sujetas a la jurisdicción del más alto tribunal de la Unión Europea (O'Donoghue y McCluskye, 2018).

Derivado de lo anterior, el T-MEC, si bien reconoce el margen de apreciación para que un Estado regule a través de sus normas domésticas el derecho de protección de datos personales, establece las normas del Foro de Cooperación Económica Asia-Pacífico (APEC) como un punto de encuentro para realizar transferencias internacionales de datos, lo cual no está redactado en términos de lo resuelto por la Comisión Europea, específicamente en el tema de la resolución de controversias, ya

[14] Si bien la LFPDPPP de 2010 incorpora características del modelo regulatrio de datos personales del *common law*, como la autoregulación, la mayor parte de normas, precedentes judiciales e interpretaciones del órgano garante facultado, han sido en el sentido de privilegiar la perspectiva del modelo regulatorio de datos europeo, considerando una interpretación amplia a favor del titular del dato.

que no sería el alto tribunal europeo el que resuelva una posible controversia sobre datos personales de ciudadanos o residentes de alguno de los países miembro de la Unión Europea que estén en manos de un responsable en México y que sean transferidos a Estados Unidos o Canadá, sino probablemente los árbitros señalados dentro de los mecanismos alternativos que reconoce el Foro, lo cual propiciaría que, si no se cumplen las disposiciones de datos que ya se tienen en México, su revisión no recaería sobre una instancia europea (cuando las transferencias involucren datos de personas nacidas o que vivan en alguno de los países miembros de la Unión Europea), sino en la instancia señalada por el propio APEC. Esto sería algo menor si México no fuera parte del Convenio 108 del Consejo de Europa.

Asimismo, es importante resaltar que el que un Estado-Nación sea considerado como un país seguro por Europa (país tercero fuera de Europa que brinda garantías para un debido tratamiento de datos que reciba por transferencia) permite impulsar lazos comerciales entre países miembro de ese espacio comunitario y el país seguro. Y, por otra parte, subrayar que la Unión Europea considera a Estados Unidos de Norteamérica como un país seguro para recibir transferencias internacionales de datos, siempre que se encuentre actualizado el escudo de privacidad, por lo que sería una guía para determinar la forma en la que deberíamos transferir datos personales al país del norte, siempre que se tenga un acuerdo tipo escudo o puerto seguro, que dote de certeza sobre el tipo de tratamiento proporcional y razonable que haga un país receptor y que no derive en vulneraciones a la dignidad humana, como sucedió con los datos personales de migrantes al ser compartidos por instancias mexicanas a autoridades migratorias de Estados Unidos.[15]

Sólo para tener mejor contexto sobre el tema, es fundamental decir que, en 2015, el Tribunal de Justicia de la Unión Europea (TJUE) declaró la invalidez del acuerdo sobre la transferencia internacional de datos personales, pues entendía que la legislación estadounidense no brindaba las garantías suficientes para proteger aquella información que provenía del espacio europeo. Tras un nuevo acuerdo, en julio del 2020, el mismo tribunal declaró la invalidez del *privacy shield* como herramienta jurídica válida para garantizar el derecho de protección de los datos de los ciudadanos europeos en supuestos de transferencia internacional. El 10 de julio de 2023, entró en vigor el Marco de Privacidad de Datos (MPD) UE-EEUU que permitió que las empresas estadounidenses registradas con la certificación escudo de privacidad pudieran acogerse a éste de inmediato.

[15] El 16 de julio de 2020, el TJUE ha hecho pública una sentencia en la que anula la Decisión 2016/1250 de la Comisión que declaraba el nivel adecuado de protección del esquema del Escudo de Privacidad (*Privacy Shield*) para las transferencias internacionales de datos a EEUU. Esta decisión sustituía, a su vez, a Puerto Seguro, que también fue declarado inválido por el TJUE en octubre de 2015. La sentencia, cuyas implicaciones marcan un nuevo punto de inflexión sobre la forma en la que se realizan las transferencias internacionales de datos a EEUU, establece, al mismo tiempo, la validez de las cláusulas contractuales estándar adoptadas por la Comisión Europea para realizar transferencias internacionales de datos entre un responsable establecido en la UE y un encargado del tratamiento fuera de la UE (AEPD, 2021).

III.2. Implicaciones de la suscripción del Tratado de Libre Comercio entre México, Canadá y Estados Unidos a la luz del principio de progresividad del derecho humano a la protección de datos personales

Como se ha podido advertir, la adhesión de México al Convenio 108 del Consejo de Europa fue un paso significativo para pensar en el máximo nivel de protección de los datos, al optarse por un modelo regulatorio de amplia protección a las personas. No obstante, en los últimos años se han identificado preocupaciones en torno a la aceptación por parte de México de cláusulas contenidas en un instrumento primordialmente económico, como el Tratado comercial entre México, Estados Unidos de Norteamérica y Canadá (T-MEC), que están por debajo del nivel de protección que el país se comprometió a otorgar en 2018, a través del citado Convenio 108 (Gobierno de México, 2023). Desde la perspectiva de los derechos humanos, el derecho de protección de datos personales, al ser un derecho humano, tendría que ser progresivo.

Sobre el Capítulo 19 de Comercio Digital del T-MEC, el artículo 19.8 aborda lo relativo a la *protección de la información personal* y hace un reconocimiento de "los beneficios económicos y sociales de la protección de la información personal de los usuarios del comercio digital y la contribución" (T-MEC, 2019, art. 19.8.1.) que dicha protección aporta para generar confianza en el consumidor. En principio, este artículo otorga un margen de apreciación para que cada Estado adopte o mantenga:

> […] un marco legal que disponga la protección de la información personal de los usuarios de comercio digital [e incluso señala que cada Estado, podrá] tomar en consideración los principios y directrices de los organismos internacionales pertinentes, tales como el Marco de Privacidad de APEC y la Recomendación del Consejo de la OCDE relativa a las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales […]. (T-MEC, 2019, p. 1193).

Los Estados también reconocen la importancia de asegurar el cumplimiento de las medidas para proteger la información personal y asegurar que las restricciones a los flujos transfronterizos de información personal sean necesarias y proporcionales a los riesgos presentados.[16] Lo que llama la atención de este capítulo es el numeral 6 que indica:

> 6. Reconociendo que las Partes podrán tomar diferentes enfoques legales para proteger la información personal, cada Parte debería fomentar el desarrollo de mecanismos para promover la compatibilidad entre estos diferentes regímenes. Las Partes procurarán intercambiar información sobre los mecanismos

[16] Se recomienda revisar las restricciones señaladas por la Unión Europea a Estados Unidos de Norteamérica y antecedentes como el *Safeharbor*.

> aplicados en sus jurisdicciones y explorarán maneras de extender estos u otros acuerdos adecuados para promover la compatibilidad entre estos. Las Partes reconocen que el sistema de Reglas de Privacidad Transfronterizas de APEC es un mecanismo válido para facilitar las transferencias transfronterizas de información mientras se protege la información personal. (T-MEC, 2019, p. 1194).

> Es decir, el artículo 19.8 en el capítulo del USMCA sobre Comercio Digital (Capítulo 19) requiere que los tres países desarrollen "mecanismos para promover la compatibilidad" entre sus diferentes regímenes legales de protección de la información personal, reconociendo las partes que el sistema de Reglas de Privacidad Transfronteriza de APEC (CBPR) es un mecanismo válido para facilitar las transferencias de información transfronterizas mientras se protege la información personal. Además de reconocer los CBPR, este lenguaje apoya firmemente el reconocimiento del concepto más amplio de herramientas de responsabilidad, como los códigos de conducta de privacidad y las certificaciones en los EEUU Ley de Privacidad. Los CBPR de APEC son una certificación de privacidad desarrollada por las 21 economías miembros del foro de APEC. Los requisitos específicos del programa de esta certificación implementan los nueve Principios de Privacidad de APEC establecidos en el Marco de Privacidad de APEC. (CIPL, 2020, pp. 1-2. La traducción es nuestra).

La reflexión sigue siendo la misma ¿los CBPR (reglas de privacidad transfronteriza) de APEC son suficientes para garantizar un nivel adecuado de protección de la información de carácter personal en términos de los compromisos adquiridos del Convenio 108 del Consejo de Europa del cual México forma parte? En este sentido, la Comisión Europea ya se ha pronunciado sobre elementos que se deben advertir al momento de negociar tratados internacionales en materia comercial, dejando asentado que los aspectos económicos no pueden estar por encima de la dignidad humana.

Para aterrizar la idea, es importante señalar que las Reglas de Privacidad Trasfronteriza de APEC, se han desarrollado en el marco de un foro primordialmente económico y que la Unión Europea hoy día no las reconoce aún como un instrumento con un nivel adecuado de protección. Es decir –y como ya se ha dicho–, frente a los compromisos que México asumió a través del Convenio 108 del Consejo de Europa, las transferencias internacionales de datos personales entre México, Estados Unidos de Norteamérica y Canadá tendrían que darse en el marco de un acuerdo de puerto seguro, que permitiera a las autoridades garantes, en el ámbito nacional del derecho de protección de datos personales, asegurarse que el tratamiento de datos se haga en términos de los principios de los deberes y responsabilidades que fija el propio Convenio 108.

III.3. Algunas aproximaciones de la Corte Interamericana de Derechos Humanos en torno al derecho de protección de datos personales

Si bien la Corte Interamericana de Derechos Humanos[17] (Corte IDH) no se ha pronunciado de forma específica sobre el derecho de protección de datos personales, sí ha reconocido que el derecho a la privacidad tiene como objeto lo siguiente:

1) Proteger la vida privada y domicilio de injerencias arbitrarias o abusivas, es decir, el derecho de quedar exento de las invasiones por parte de particulares o de las autoridades estatales.
2) Controlar la información de carácter personal, incluso después de haberla proporcionado a un particular o entidad del Estado.

Por la misma razón, reconoce que los aspectos de la vida sexual de las personas están protegidos dentro del derecho a la privacidad. En las siguientes líneas analizaremos algunos elementos que la Corte IDH ha incorporado al derecho a la privacidad,

a) Caso de las Masacres de Ituango vs. Colombia: "[El] domicilio y la vida privada se encuentran intrínsecamente ligados, ya que el domicilio se convierte en un espacio en el cual se puede desarrollar libremente la vida privada" (Corte IDH, 2006, párr. 194), por lo que el domicilio se encuentra dentro del ámbito de protección del derecho a la privacidad.
b) Caso Fontevecchia y D'Amico vs. Argentina: Aunado al reconocimiento del domicilio como elemento de la vida privada, determina que el ámbito de la privacidad "comprende, entre otras dimensiones, tomar decisiones libremente relacionadas con diversas áreas de la propia vida, tener un espacio de tranquilidad personal, mantener reservados ciertos aspectos de la vida privada y controlar la difusión de información personal hacia el público" (Corte IDH, 2011, párr. 48). En este caso, la Corte IDH reconoce expresamente el derecho de controlar la información de carácter personal, lo cual se traduce en el derecho a la protección de datos personales.
c) Caso Fernández Ortega y Otros vs. México (2010, párr. 129) y Caso Rosendo Cantú y Otra vs. México (2010, párr. 119): La Corte IDH incorpora la vida sexual dentro del concepto de vida privada, al señalar que se trata de:

[17] La reforma constitucional de 2011 en materia de derechos humanos, en México, obliga que las autoridades en cualquier ámbito respeten los instrumentos jurídicos internacionales y la jurisprudencia de tribunales especializados en la protección de derechos humanos, como la Corte Interamericana de Derechos Humanos.

> […] un término amplio no susceptible de definiciones exhaustivas, pero que comprende, entre otros ámbitos protegidos, la vida sexual y el derecho de establecer y desarrollar relaciones con otros seres humanos. [En estos casos, la Corte IDH establece que ante la violación sexual que sufrieron las víctimas, se vulneraron] valores y aspectos esenciales de su vida privada [y] supuso una intromisión en su vida sexual y anuló su derecho a tomar libremente decisiones respecto de con quien tener relaciones sexuales, perdiendo de forma completa el control sobre sus decisiones más personales e íntimas y sobre las funciones corporales básicas. (Corte IDH, 2010, párr. 119).

d) Caso Tristán Donoso vs. Panamá, la Corte IDH reconoció:

> […] aunque las conversaciones telefónicas no se encuentren expresamente previstas en el artículo 11 de la Convención Americana sobre Derechos Humanos, se trata de una forma de comunicación que, al igual que la correspondencia, se encuentra incluida dentro del ámbito de protección de la vida privada. (Corte IDH, 2009, párr. 55).

En este mismo caso, la Corte IDH identifica dos elementos primordiales vinculados con el derecho a la privacidad: la honra y la reputación, al señalar que el primero "se relaciona con la estima y valía propia, mientras que la reputación se refiere a la opinión que otros tienen de una persona" (Corte IDH, 2009, párr. 57).

A manera de conclusión, podemos decir que la Corte IDH reconoce como elementos inherentes al derecho a la privacidad, el derecho a la vida privada, la inviolabilidad del domicilio, de las conversaciones telefónicas y de cualquier comunicación, así como el derecho a la honra y la reputación.

III.4. Pronunciamientos de la Suprema Corte de Justicia de la Nación sobre el derecho de protección de datos personales

Las primeras tesis aisladas y jurisprudencias emitidas por el Poder Judicial Federal en materia de protección de datos personales se dieron a partir de 2006, entre las cuales destacan las siguientes:

> Amparo en Revisión 51/2019 / 7 de noviembre de 2019 / Unanimidad de votos / Ponente: Jerónimo José Martínez Martínez / Secretario: José Irving Cruz Bibiano / Reconocimiento de paternidad. *La orden de girar oficio para conocer los bienes e ingresos del demandado en el juicio relativo vulnera su derecho a la protección de datos personales*, si no se ha demostrado la filiación entre las partes para tener derecho a recibir alimentos (inaplicabilidad del artículo 563 del Código Procesal Civil del Estado de Guerrero). (Tesis: XXI.3o.C.T.11 C, febrero de 2020). [énfasis añadido].

Amparo en Revisión 51/2019: Los datos financieros y patrimoniales constituyen datos personales considerados como sensibles y, por ende, tienen especial nivel de protección y hasta en tanto no se determine la paternidad del demandado en el juicio, la instancia judicial no podrá requerir conocer de esa información a las entidades que la resguarden y, por tanto, no se integrará al expediente de consulta.

Hoy la legislación aplicable a la materia prevé sanciones en caso de que el responsable entregue información a un tercero sin que medie una orden judicial. En caso de que exista una orden judicial de solicitud de datos personales a un tercero con carácter de responsable, que no responda a los principios que rigen el tratamiento de datos personales, la sanción se impondrá en términos de la LGPDPPSO.

> Amparo en Revisión 661/2014 / Fundación para la Justicia y el Estado Democrático de Derecho A.C. / 4 de abril de 2019 / Mayoría de diez votos de los ministros Alfredo Gutiérrez Ortiz Mena, Juan Luis González Alcántara Carrancá, Yasmín Esquivel Mossa, José Fernando Franco González Salas, Luis María Aguilar Morales, Jorge Mario Pardo Rebolledo, Norma Lucía Piña Hernández, Eduardo Medina Mora I., Javier Laynez Potisek y Alberto Pérez Dayán, respecto del estudio de los agravios correspondientes; votó en contra del sentido, pero a favor de las consideraciones contenidas en esta tesis: Arturo Zaldívar Lelo de Larrea / Ponente: Norma Lucía Piña Hernández / Secretario: Eduardo Aranda Martínez / Derecho a la información. *La relación con sus límites constitucionales no debe plantearse en términos absolutos*. (Tesis: P. II/2019, enero de 2020). [énfasis añadido].

Amparo en Revisión 661/2014: Ningún derecho humano es absoluto. La clasificación de la información como reservada tiene relación con el interés público previsto en el artículo 6o. constitucional. La información confidencial tiene como objetivo proteger la vida privada de las personas. No se pueden plantear límites de un derecho humano (acceso a la información y protección de datos personales) en términos absolutos, se tendrá que lograr un balance en términos de un Estado democrático y de los precedentes que de forma casuística se hayan establecido.

> Amparo Directo 535/2018 / Pablo Agustín Meouchi Saade / 25 de abril de 2019 / Unanimidad de votos / Ponente: Jorge Arturo Camero Ocampo / Secretario: Ángel García Cotonieto / Protección de datos personales. *El deber del Estado de salvaguardar el derecho humano relativo debe potencializarse ante las nuevas herramientas tecnológicas, debido a los riesgos que éstas representan por sus características*. (Tesis: I.10.A.6 CS, septiembre de 2019). [énfasis añadido].

Amparo Directo 535/2018: El Estado tiene el deber de salvaguarda frente al derecho de los gobernados a decidir qué aspectos de su vida deben o no ser conocidos o reservados por el resto de los individuos que integran la sociedad. Esto conlleva la obligación de dejarlos exentos e inmunes a invasiones agresivas o arbitrarias por parte de terceros o de la autoridad, y debe potencializarse ante las nuevas herramientas tecnológicas.

Las tecnologías de la información y comunicación permiten recabar, almacenar y transmitir datos personales en tiempo real reduciendo barreras de tiempo y espacio, por lo que es obligación del Estado dotar de mecanismos de salvaguarda del derecho de protección de datos personales frente a los nuevos desafíos que impone el desarrollo tecnológico al ámbito de la privacidad de las personas.

Son diversos los tópicos de los que el Poder Judicial Federal se ha pronunciado en relación con el derecho de protección de datos personales, y los precedentes que establece son de suma importancia para el operador jurídico, recordando que tradicionalmente desde la recepción de este derecho a nuestro país –si bien su reconocimiento, límites y restricciones están previstos en la Carta Magna–, su ponderación y aplicación normalmente es casuística, a través de las resoluciones que hacía el INAI, como segunda instancia garante de este derecho (en los casos en los que se pronunciaba mediante recurso de revisión).

Actualmente, la autoridad facultada para velar por el derecho de protección de datos personales en México es la Secretaría Anticorrupción y Buen Gobierno (SABG) y la normativa correspondiente es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) de 2025. Se elimina el recurso de revisión previsto en la LGPDPPSO de 2017 para habilitar el juicio de amparo como segunda instancia revisora.

Se debe tener en cuenta que las solicitudes de derechos ARCO se hacen valer frente al responsable del tratamiento de datos personales y frente a la negativa de atenderlas o su atención fuera de lo establecido por la norma antes procedía el recurso de revisión ante el INAI tratándose de datos personales en resguardo del sector público, y de la solicitud del procedimiento de protección de derechos, tratándose de datos personales en manos del sector privado.

III.5. Desafíos y retos del derecho de protección de datos personales

Como hemos visto, el artículo 12 de la Declaración Universal de Derechos Humanos, que reconoce límites del Estado respecto a la no injerencia en la vida privada de las personas, ha sido un antecedente importante para el desarrollo del derecho a la privacidad y del derecho a la protección de datos personales.

No obstante, y pese al reconocimiento constitucional y avance normativo en México del derecho de protección de datos personales, aún hacen falta mecanismos que en la práctica hagan efectiva la obligatoriedad de aplicación de los principios que rigen este derecho durante todas las fases del tratamiento de la información de carácter personal.

En este sentido, las normas nacionales en materia de protección de datos personales responden a un modelo híbrido de protección que retoma aspectos del sistema anglosajón, como la autorregulación y la regulación a través de normas sectoriales y, a la vez, compromete el nivel de protección más alto en términos del modelo europeo.

Pese a ello y a la ratificación por parte de México de tratados internacionales y documentos de *soft law* en la materia, existen tareas pendientes a resolver, tales como:

1) La efectiva garantía del derecho a la portabilidad, considerando, desde una perspectiva técnica, que las plataformas hoy día, al menos para el sector público, carecen de interoperabilidad, lo cual dificulta, más allá de lo jurídico, la garantía de este derecho. Situación nada diferente para los datos personales que son tratados por responsables en el sector privado.
2) La expectativa depositada en el principio de información y consentimiento como una fórmula aparentemente efectiva para el empoderamiento del titular del dato, aun cuando la mayoría de personas sólo firman los avisos de privacidad para acceder a un servicio pese a que los responsables muchas veces condicionan la prestación de dicho servicio a la autorización expresa para el tratamiento de datos con diversos fines. Es decir, se ha planteado la idea de que el consentimiento legitima y hace lícito el tratamiento de datos personales, pero esto no necesariamente garantiza un tratamiento ético de la información.

   Otro punto a considerar es que los avisos de privacidad son redactados en un lenguaje nada sencillo, lo cual dificulta que el titular de un dato personal entienda los alcances del tratamiento que se pretende hacer a su información.
3) Las políticas de privacidad como cláusulas de adhesión no acordes a la dimensión que constitucionalmente cobra el derecho de protección de datos personales en México, por ejemplo, en el caso de los términos y condiciones de servicios como las redes sociales.
4) Una autoridad garante del derecho de protección de datos personales cuyo poder se diluye cuando se enfrenta a las corporaciones globales que operan en el ciberespacio. Es decir, pese a que las normas secundarias reconocen la jurisdicción y competencia de esta autoridad, las plataformas de servicios digitales simplemente desconocen esta atribución y, al no estar condicionado el reconocimiento de la autoridad nacional a actos de comercio o a la prestación del servicio en el país, simplemente existen dos espacios de manifestación del derecho de protección de datos personales: el físico o tradicional, con todas las prerrogativas de la ley; y el digital, en el que la ubicuidad da pauta a que los titulares de datos sólo cuenten con las prerrogativas que las corporaciones quieran otorgar a través de sus políticas de privacidad. Todo ello propicia una evidente reducción del Estado-Nación que no garantiza el principio de escru-

tinio en materia de derechos humanos y que cede la expectativa de garantía a empresas que tienen otros intereses, acordes con su propia naturaleza.

5) En relación con los puntos tres y cuatro, la extraterritorialidad de las normas que pretenden hacer valer empresas de servicios digitales constituidas en Estados Unidos de Norteamérica, como Patriot Act que, entre otras cosas, obligaba a las empresas a atender sólo las normas de ese país y no las de países terceros en donde presten sus servicios, contraviniendo evidentemente las bases del derecho internacional público y la soberanía de los Estados. Para el caso de México, incluso el Reglamento de la LFPDPPP señalaba que el marco jurídico en la materia sería obligatorio, siempre que se cumplieran dos condiciones: ser empresas establecidas en México o ser empresas que presten algún servicio en el país.

   Es decir, cuando hablamos de tecnología, a pesar de que México cuenta con un marco legal en materia de protección de datos personales robusto que retoma los más altos estándares de protección de la persona, en la lógica del derecho europeo y de la tradición heredada de la familia romano germánica, todos estos esfuerzos se ven reducidos frente a sistemas de inteligencia artificial, redes sociales, *big data* o algoritmos, ya que al examinar las políticas de privacidad de las redes sociales más utilizadas en el mundo, como Facebook o X (antes Twitter), podríamos advertir la falta de armonización de dichas políticas con las normas nacionales en materia de protección de datos personales.[18]

6) Otro de los desafíos pendientes es dimensionar la relevancia del derecho de protección de datos personales para el fortalecimiento del Estado democrático, y visibilizar que su salvaguarda permite el ejercicio de otros derechos como la participación política y la construcción de la democracia moderna.

7) Un nuevo fenómeno que se materializa en el derecho de protección de datos personales en ámbitos digitales, tiene que ver con que ahora son nuevos actores en los que se ha depositado la responsabilidad de la salvaguarda de derechos humanos, ya que no es el Estado directamente el que garantiza, por ejemplo, el ejercicio de derechos ARCO en una red social, sino las corporaciones. Esto hace evidente la necesidad de un verdadero y efectivo modelo *multistakeholder* pensando en la gobernanza de los datos y del ciberespacio y en mecanismos de control para que particulares doten de medios digitales efectivos para el ejercicio de derechos humanos, como la protección de datos personales en internet.

[18] Por ejemplo, el ejercicio efectivo de derechos de cancelación sobre datos personales no es otorgado por esas plataformas y la cancelación de una imagen que constituye un dato personal en el caso de Facebook, se materializaría únicamente si se acredita que la fotografía viola las normas de convivencia establecidas por dicha corporación.

8) A nivel regional, también es necesario el pronunciamiento de la Corte Interamericana de Derechos Humanos, específicamente sobre el derecho de protección de datos personales, ya que, si bien lo ha hecho sobre el derecho a la privacidad y esto ha permitido establecer los primeros precedentes de dicha instancia en la materia, no se cuenta con criterios específicos sobre el derecho que atañe a este trabajo.

9) Otro elemento es que, al reconocerse el derecho de protección de datos personales como un derecho humano en México, se tendría que garantizar la reparación del daño en caso de afectaciones a dicho derecho; en otras palabras, las multas que durante años impuso el INAI y se cobraron a través de la Tesorería de la Federación no tienen un retorno para la persona afectada titular del dato.

   Casos como el de Olimpia Corral no tienen una vía de reparación del daño por lo que deriva de su afectación al derecho de protección de datos personales. Si bien existen otros canales jurídicos, como la responsabilidad civil o el daño al honor, no existen mecanismos específicos atendiendo a la naturaleza de derecho humano que México ha reconocido a la protección de datos personales.

   Así, la interacción simultánea de dos modelos de regulación en materia de protección de datos personales que imperan a nivel global. No todos los países asumen las mismas medidas de protección de datos personales, lo cual complica la transferencia internacional de datos, no sólo derivada de actos comerciales, sino de colaboración internacional entre autoridades y esto obliga a impulsar la efectividad de los Acuerdos de Puerto Seguro, en concordancia con la ratificación de México del Convenio 108 del Consejo de Europa.

En definitiva, los acontecimientos que hemos visto durante los últimos meses ponen en evidencia que los datos personales no únicamente son el petróleo de la economía digital, sino que despiertan un profundo interés en actores políticos y económicos, por lo que prácticamente quien tenga el dato ostentará el poder. Esto hace necesario abrir el espacio de reflexión sobre el papel que deben jugar los Estados-Nación para garantizar los derechos a la privacidad y datos en el ciberespacio.

Por último, es relevante considerar los llamados que hizo el Papa Francisco en diversos foros económicos a que se regulara el uso de la IA (inteligencia artificial) y a que los Estados asumieran el liderazgo, a fin no sólo de garantizar los derechos de las personas, sino la subsistencia de la humanidad misma.

III.6. El derecho de protección de datos personales en la era digital

El desarrollo tecnológico ha permitido un avance considerable de tecnologías como la inteligencia artificial, cómputo en la nube, algoritmos, internet de las cosas, *big data* y una carrera por el desarrollo de los ordenadores cuánticos.

Un elemento común de estas tecnologías es que necesitan información para funcionar y que mucha de esta información se recaba a través del ciberespacio. Por este motivo, los datos personales han adquirido un valor alto tanto para empresas como para los propios Estados.

Como se dijo líneas arriba, quien tiene el dato ostenta el poder, por lo que, en un mundo hiperconectado, las personas funcionan como sensores humanos a través de sus dispositivos móviles conectados en tiempo real a aplicaciones móviles y a internet en general.

En este mundo postmoderno, vivimos en una aldea global hiperconectada, en la que todas las personas en mayor o menor medida terminan siendo usuarios tecnológicos, por una parte, y sensores humanos,por otra, que están generando de forma permanente información y datos respecto de sus interacciones con otros usuarios, con las empresas y, en general, respecto de sus actividades tanto digitales como físicas.

Estos datos están sujetos a un régimen legal en términos del país del que se trate. Algunos modelos han logrado con éxito la extrapolación de sus normas jurídicas casi a nivel global, como el Reglamento General de Protección de Datos y, por otro lado, están las normas locales en materia de privacidad y datos personales que aún enfrentan problemas para sobreponer su obligatoriedad a las plataformas digitales (reducción del Estado-Nación).

En consonancia con lo anterior, en el ciberespacio se encuentran actores, algunos casi omnipresentes (como las corporaciones de servicios tecnológicos y/o plataformas digitales) y otros actores que apenas se asoman a este espacio ubicuo de fronteras difusas y complejo, que desafía los conceptos jurídicos tradicionales relacionados a la jurisdicción y competencia con fronteras difusas o inexistentes, como el caso de los Estados-Nación.

En consecuencia, se deposita la expectativa de salvaguarda del derecho humano de protección de datos personales en el ciberespacio en manos de las corporaciones tecnológicas, pero éstas tienen máximas para su modelo de negocio, como la eficiencia, la eficacia y la escalabilidad por encima de la perspectiva de los derechos humanos del derecho público.

De la experiencia del rumbo que han tomado las plataformas durante los últimos años, se advierte que dichas máximas, que tienden a sobreponerse a los derechos humanos e incluso a espacios ambiguos que aún no estén tan clarificados desde los

derechos del consumidor, serán espacios idóneos de expansión para sus modelos de negocio. Derivado de lo anterior, es necesario un rol más activo por parte de los Estados-Nación, que permita garantizar el escrutinio de los derechos humanos en internet.

Por otro lado, la nueva dimensión que cobra el derecho a la privacidad a la luz del desarrollo tecnológico o incluso la manera en la que las personas ceden espacios que antes eran privados a la exposición en redes sociales, hacen posible que los usuarios sean más tolerantes a invasiones a su privacidad por parte de prestadores de servicios digitales.

A nivel internacional, organismos como la Organización de las Naciones Unidas (ONU) no han sido ajenos al fenómeno de la privacidad y la protección de datos personales en la era digital, por lo que han desarrollado documentos de *soft law*, dentro de los que destaca la Resolución 68/167 de la Organización de las Naciones Unidas sobre privacidad (18 de diciembre de 2013), que aborda el derecho a la privacidad en la era digital, enfatizando que los derechos que se tienen en el mundo físico, también deben salvaguardarse en el mundo virtual.

A pesar de que los Estados-Nación se han esforzado por establecer mecanismos internacionales de colaboración para la efectiva garantía de derechos humanos en el ciberespacio, existe una disparidad considerable no sólo respecto de los instrumentos internacionales de los que los Estados-Nación forman parte, sino de la manera interna en la que cada uno ha regulado tanto el derecho a la privacidad como la protección de datos personales.

De estos esfuerzos, se desprende que, salvo el Reglamento General de Protección de Datos Personales de la Unión Europea, no existen procesos normativos y de derecho internacional cercanos a la estandarización de compromisos que permitan hacer que el ciberespacio sea un lugar seguro para el ejercicio de derechos humanos. Esfuerzos como el Convenio de Budapest no han sido suficientes para establecer compromisos en materia de combate a la ciberdelincuencia por parte de todos los Estados-Nación.

Otro de los problemas tiene que ver con las diferencias entre los modelos regulatorios en materia de protección de datos personales –como se ha explicado en líneas previas–. Existen dos modelos predominantes en el mundo: el modelo de derecho continental y el modelo anglosajón. Las principales diferencias entre ambos son las siguientes:

MODELO ANGLOSAJÓN O DEL *COMMON LAW*	MODELO EUROPEO O DE DERECHO CONTINENTAL
Regula disposiciones de protección de datos personales en leyes secundarias.	Reconoce el derecho de protección de datos personales como un derecho humano.
Incorpora una perspectiva de mercado y deposita en la autorregulación los límites para las empresas.	Incorpora una perspectiva de derechos humanos y reconoce que la dignidad humana será el límite para el tratamiento de datos personales.
Normalmente carece de una autoridad específica en materia de protección de datos personales.	Habilita un ente supervisor del derecho de protección de datos personales.

Existen otros puntos clave para entender el derecho de protección de datos personales en la era digital, que se pueden resumir en: la ubicuidad de internet y los problemas que esto genera en el tema de responsabilidad civil y jurisdicción y competencia de las autoridades nacionales; la simultaneidad e inmediatez de fenómenos que permiten que la información viaje en tiempo real por muchos sitios y eso permita la pérdida de control sobre la misma; las múltiples familias jurídicas interactuando e intentando ser compatibles cuando de origen tienen diferencias significativas; el poder de la *lex mercatoria* y la débil perspectiva de los derechos humanos en servicios digitales; las cláusulas de adhesión incompatibles con los marcos nacionales en materia de protección de datos personales; países que fungen como periféricos y se limitan a consumir tecnología (al no participar del desarrollo, no tienen poder real para establecer reglas acordes con los marcos normativos), etc.

Podemos nombrar como ejemplos algunos problemas complejos y actos simbólicos de resistencia que se dan en distintas latitudes. Analicemos el debate que abre el Caso Ulricht Richter (2015) sobre la libertad de expresión en internet y la responsabilidad de las plataformas digitales como intermediarios que no sólo contienen información, sino que ayudan a su transmisión y, con esto, contribuyen a posibles afectaciones a derechos de terceros. No pueden obviarse dos fenómenos interesantes:

1) La manera en que las corporaciones tecnológicas han habilitado figuras deliberativas respecto de derechos humanos, como la libertad de expresión, el acceso a la información y la protección de datos personales, a través de los llamados Consejos de Expertos Asesores o Juntas Supervisoras. Es decir, estamos frente a un grupo de expertos que deliberan y resuelven sobre el ejercicio de derechos humanos, a pesar de no ser representantes oficiales de algún Estado-Nación, por ende, cualquier resolución que de ahí emane podría ser fácilmente cuestionada en los tribunales tradicionales nacionales. Este fenómeno permite entender una de las complejidades de la efectiva garantía del derecho de protección de datos personales en el ciberespacio: estamos frente a la necesidad

de garantizar derechos humanos, pero los Estados-Nación pretenden que esa necesidad sea prioritaria para las empresas tecnológicas, incluso por encima de las máximas de mercado: eficiencia y eficacia.

2) La frecuencia con la que Tribunales y Cortes Supremas en el mundo tienen que resolver sobre las consecuencias que se materializan en el mundo físico respecto de contenidos que se alojan en plataformas digitales en el ciberespacio. Por ejemplo, las consecuencias legales de la divulgación a través de Google Maps de fotografías no anonimizadas de personas que estaban en espacios públicos y privados al momento de capturarse la fotografía, los suicidios de infantes a partir de contenidos de Instagram o el acceso a información que ha permitido que ciertos ataques terroristas hayan sido más letales y precisos.

   En este sentido, asuntos como el Caso González vs. Google (2023) han puesto sobre la mesa no sólo la discusión de la responsabilidad, en algunos casos civil, de algoritmos y plataformas digitales, sino la manera en la que la *lex mercatoria* logra posicionarse por encima de derechos humanos, como la vida o el acceso a la justicia.

   El resultado de la Corte Suprema de Estados Unidos de Norteamérica sobre el asunto del señor González explica también el poder corporativo y económico acumulado por las empresas tecnológicas y lo que hubiera implicado para el modelo creciente de negocio que la Corte reconociera una determinada responsabilidad corporativa.

Así mismo, derivado del uso de la inteligencia artificial, se advierte la necesidad de reconocer al menos dos figuras jurídicas que den respuesta a los posibles riesgos asociados al uso de inteligencia artificial para la toma de decisiones: el derecho a no ser sometido a decisiones automatizadas y el derecho de reconsideración o revisión frente a una decisión automatizada que afecte derechos humanos de las personas. Ambas figuras no existen en la ley nacional.

Finalmente, se advierte la necesidad de analizar figuras como el reconocimiento normativo del derecho a la privacidad para garantizar los últimos espacios privados de las personas, a la luz del desarrollo tecnológico. En este sentido, se ha abierto un debate sobre la naturaleza de este derecho y si debe acogerse a una norma en materia de derechos humanos, de no discriminación específicamente o de datos personales. Esto dependerá del legislador en cada país, el foco debe estar en reconocer y garantizar este derecho de manera general para que la sombrilla de protección alcance a todas las personas en la mayoría de los supuestos que vaya planteando el desarrollo tecnológico.

A manera de conclusión, si bien se debe desbloquear el valor de los datos en la era digital para su uso y explotación, se deben buscar garantías de seguridad para que las personas no sean discriminadas y tengan pleno ejercicio de sus derechos humanos.

La ecuación no debe plantearse como derechos humanos vs. tecnología, sino desarrollo tecnológico y derechos humanos en un ecosistema que permita la innovación, pero no a costa de la vulneración de los derechos de los usuarios.

Referencias

Agencia Española de Protección de Datos (AEPD). (9 de junio de 2021). *El Tribunal de Justicia de la Unión Europea declara inválido el Escudo de Privacidad para la realización de transferencias internacionales de datos a EEUU.* https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/transferencias-internacionales/comunicado-privacy-shield

Alexy, R. (1993). *Teoría de los derechos fundamentales.* Centro de Estudios Constitucionales. https://www.iecm.mx/www/sites/DDHH/publicaciones/01.pdf

Asia-Pacific Economic Cooperation Secretariat (APEC). (2005). Privacy Framework. https://www.apec.org/publications/2005/12/apec-privacy-framework

Boehme-Neßler, V. (august, 2016). Privacy: a matter of democracy. Why democracy needs privacy and data protection. *International Data Privacy Law*, 6(3), 222-229. https://doi.org/10.1093/idpl/ipw007

Carta de los Derechos Fundamentales de la Unión Europea. (7 de diciembre de 2000). https://www.europarl.europa.eu/charter/pdf/text_es.pdf

Centre for Information Policy Leadrship (CIPL). (17de enero de 2020). White Papper. What Does the USMCA Mean for a Federal Privacy Law? https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_-_what_does_the_usmca_mean_for_a_federal_privacy_law__01.17.2020___2_.pdf

Cerdas, R. (1994). Democracia y derechos humanos. En Instituto Interamericano de Derechos Humanos (IIDH). *Estudios básicos de derechos humanos I* (pp. 295-311). Prometeo. https://es.scribd.com/document/466828568/ESTUDIOS-BASICOS-DE-DERECHOS-HUMANOS-TOMO-I-pdf#page=295

Código Nacional de Procedimientos Penales (CNPP). (última reforma: 16 de diciembre de 2024). https://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP.pdf

Constitución Política de los Estados Unidos Mexicanos (CPEUM). (5 de febrero de 1917). https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Convención Americana de Derechos Humanos (Pacto de San José). (22 de noviembre de 1969). https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

Convenio Europeo de Derechos Humanos. (4 de noviembre de 1950). https://www.echr.coe.int/documents/d/echr/convention_spa

Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108). (28 de enero de 1981). Consejo de Europa (CE). https://rm.coe.int/16806c1abd

Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108 Plus). (18 de mayo d 2018). Consejo de Europa (CE). https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1

Corte Interamericana de Derechos Humanos (Corte IDH). (1 de julio de 2006). Caso de las Masacres de Ituango vs. Colombia. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia Serie C No. 148. https://www.corteidh.or.cr/docs/casos/articulos/seriec_148_esp.pdf

Corte IDH. (27 de enero de 2009). Caso Tristán Donoso vs. Panamá. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia Serie C No. 193. https://www.corteidh.or.cr/docs/casos/articulos/seriec_193_esp.pdf

Corte IDH. (30 de agosto de 2010). Caso Fernández Ortega y Otros vs. México. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia Serie C No. 215. https://www.ordenjuridico.gob.mx/JurInt/STCIDHM2.pdf

Corte IDH. (31 de agosto de 2010). Caso Rosendo Cantú y Otra vs. México. Excepción Preliminar, Fondo, Reparaciones y Costas. Sentencia Serie C 216. http://www.ordenjuridico.gob.mx/JurInt/STCIDHM5.pdf

Corte IDH. (29 de noviembre de 2011). Caso Fontevecchia y D'Amico vs. Argentina. Fondo, Reparaciones y Costas. Sentencia Serie C 238. https://www.corteidh.or.cr/docs/casos/articulos/seriec_238_esp.pdf

Cossío Díaz, J.R. (enero-junio de 2012). Primeras implicaciones del Caso Radilla. *Cuestiones Constitucionales*, (26), 31-63. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-91932012000100002&lng=es&tlng=es

Declaración Universal de los Derechos Humanos (DUDH). Resolución 217 A (III). (10 de diciembre de 1948). https://www.un.org/es/about-us/universal-declaration-of-human-rights

Decreto por el que se Reforman, Adicionan y Derogan diversas Disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en Materia de Simplificación Orgánica (20 de diciembre de 2024). https://www.dof.gob.mx/nota_detalle.php?codigo=5745905&fecha=20/12/2024#gsc.tab=0

De la Cuadra, B. (01 de marzo de 1991). El Constitucional alemán anuló parte del censo de 1983, similar al español de 1991. *El País.* https://elpais.com/diario/1991/03/02/espana/667868420_850215.html?event_log=go

Díaz Revorio, F.J. (2006). El derecho fundamental al secreto de las comunicaciones: una visión desde la jurisprudencia europea y su influencia en el Tribunal Constitucional Español. *Derechos Humanos México. Revista del Centro Nacional de Derechos Humanos*, 1(2), 125-145. https://revistas-colaboracion.juridicas.unam.mx/index.php/derechos-humanos-cndh/article/view/5526/4873

Gamboa Montejano, C. (2009). *Datos personales: Estudio teórico conceptual de su regulación actual y de las iniciativas presentadas para la creación de una ley en la materia (Primera Parte)*. Cámara de Diputados, Centro de Documentación, Información y Análisis. https://www.diputados.gob.mx/sedia/sia/spi/SPI-ISS-24-09.pdf

García Ricci, D. (2013). Artículo 16 constitucional. Derecho a la privacidad. En E. Ferrer Mac-Gregor Pisot, J.L. Caballero Ochoa y Ch. Steiner (Coords.), *Derechos humanos en la Constitución. Comentarios de jurisprudencia constitucional e interamericana I* (pp. 1043-1079). Suprema Corte de Justicia de la Nación (SCJN); UNAM, Instituto de Investigaciones Jurídicas; Fundación Konrad Adenauer. https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/42.pdf

Garzón Valdés, E. (2008). *Lo íntimo, lo privado y lo público*. Instituto Federal de Acceso a la Información Pública (IFAI). https://www.uaq.mx/contraloriasocial/diplomado/biliografia-modulo3/IFAI%20-%20cuadernillo%206.pdf

Gobierno de México. (27 de octubre de 2023). Textos finales del Tratado entre México, Estados Unidos y Canadá (T-MEC). https://www.gob.mx/t-mec/acciones-y-programas/textos-finales-del-tratado-entre-mexico-estados-unidos-y-canada-t-mec-202730?state=published

Gómez-Robledo, A. y Ornelas Núñez, L. (2006). *Protección de datos personales en México: el caso del Poder Ejecutivo Federal*. UNAM, Instituto de Investigaciones Jurídicas. https://repositorio.unam.mx/contenidos/5019858

González vs. Google LLC, (2023), 598 U.S. https://supreme.justia.com/cases/federal/us/598/21-1333/

Gozaíni, O.A. (2011). *Derecho procesal constitucional. Hábeas Data protección de datos personales*. (2a. ed.). Rubinzal-Culzoni Editores. https://gozaini.com/wp-content/uploads/2023/10/habeas_data-1.pdf

Gutiérrez Zarza, A. (Coord.) (2012). *Nuevas tecnologías, protección de datos personales y proceso penal: manual para jueces y fiscales europeos, especial referencia al ordenamiento jurídico español*. La Ley.

Heredero Higueras, M. (1983). La sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del Censo de Población de 1983. *Documentación Administrativa*, (198), 139-158. https://revistasonline.inap.es/index.php/DA/article/view/4687/4741

Holvast, J. (2009). History of Privacy. En V. Matyáš, S. Fischer-Hübner, D. Cvrček y P. Švenda (Eds.). *The future of identity in the information society*. (pp.13-42). Springer. https://doi.org/10.1007/978-3-642-03315-5_2

Huber, R. (Ed.). (2009). *Jurisprudencia del Tribunal Constitucional Federal Alemán. Extractos de las sentencias más relevantes compiladas por Jürger Schwabe*. Konrad Adenauer Stiftung. https://www.ajp.org.py/archivos/materiales/20160714081221.pdf

Instituto Federal de Acceso a la Información Pública (IFAI). (6 de septiembre de 2013). Impone el IFAI cuatro mil multas a tarjetas Banamex por incumplir la Ley Federal de Protección de Datos Personales. Comunicado. https://inicio.inai.org.mx/Comunicados/Comunicado%20IFAI-082-13.pdf

IFAI. (29 de agosto de 2016). INAI y UVM inauguran el Aula Iberoamericana en materia de Protección de Datos. Comunicado. https://inicio.inai.org.mx/Comunicados/Comunicado%20INAI-239-16.pdf

International Telecommunication Union (ITU). (2024). *Statistics*, *Individual using the Internet*. https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

Ley Federal de Procedimiento Administrativo (LFPA). (última reforma: 18 de mayo de 2018). https://www.diputados.gob.mx/LeyesBiblio/pdf/112_180518.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) (vigente). (publicada: 20 de marzo de 2025). https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) (abrogada) (publicada: 5 de julio de 2010). https://www.gob.mx/cms/uploads/attachment/file/123648/Ley_Federal_de_Protecci_n_de_Datos_Personales_en_Posesi_n_de_los.pdf

Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGPDPPSO) (vigente). (publicada: 20 de marzo de 2025). https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) (abrogada) (publicada: 26 de enero de 2017). https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017#gsc.tab=0

Ley General de Transparencia y Acceso a la Información Pública (LGTAIP). (publicada: 20 de marzo de 2025). https://www.diputados.gob.mx/LeyesBiblio/pdf/LGTAIP.pdf

Maqueo Ramírez, M.S. y Barzizza Vignau, A. (2020). *Democracia*, *privacidad y protección de datos personales*. Instituto Nacional Electoral (INE). https://www.ine.mx/wp-content/uploads/2021/02/CDCD-41.pdf

Mendoza Enríquez, O.A. (2016). El secreto de las comunicaciones en el ámbito de internet. En M. Recio Gayo (Coord.). *La Constitución en la sociedad y economía digitales*. (pp.131-167). Suprema Corte de Justicia de la Nación, Centro de Estudios Constitucionales. https://www.sitios.scjn.gob.mx/cec/sites/default/files/publication/documents/2022-10/00_La%20constitucion%20en%20la%20sociedad%20y%20economia%20digitales%20%28entero%29.pdf

Mendoza Enríquez, O.A. (2018a). Derecho al olvido de niños, niñas y adolescentes en la era digital: una visión desde México. En C. Cobo, S. Cortesi, L. Brossi, S.

Doccetti, A. Lombana, N. Remolina, R. Winocur y A. Zucchetti (Eds.). *Jóvenes, transformación digital y formas de inclusión en América Latina* (pp. 345-353). Penguin Random House Grupo Editorial; Fundación Ceibal.

Mendoza Enríquez, O.A. (2018b). Marco jurídico de la protección de datos personales en las empresas de servicios establecidas en México: desafíos y cumplimiento. *Revista IUS*, 12(41), 267-291. https://doi.org/10.35487/rius.v12i41.2018.355

Mendoza Enríquez, O.A. (2022). El derecho de protección de datos personales en los sistemas de inteligencia artificial. *Revista IUS*, 15(48), 179-207. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1870-21472021000200179#B3

Nájera Montiel, J. (enero-junio de 2008). El aspecto axiológico de los datos personales en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. *Revista de Derecho Comparado de la Información*, (11), 97-129. https://revistas-colaboracion.juridicas.unam.mx/index.php/decoin/article/view/33148/30112

O'Donoghue, C. y McCluskye, C. (4 de abril de 2018). *European Commission approves provisions for cross-border data flows while consultation on GDPR Article 49 guidance closes*. https://www.technologylawdispatch.com/2018/04/privacy-data-protection/european-commission-approves-provisions-for-cross-border-data-flows-while-consultation-on-gdpr-article-49-guidance-closes/

Organización de las Naciones Unidas (ONU). (18 de diciembre de 2013). A/RES/68/167. Derecho a la privacidad en la era digital. https://docs.un.org/es/A/RES/68/167

Ornelas Núñez, L. y López Ayllón, S. (2010). La recepción del derecho a la protección de datos personales en México: breve descripción de su origen y estatus legislativo. En Instituto Federal de Acceso a la Información Pública (IFAI) (Ed.). *Protección de datos personales. Compendio de lecturas y legislación*. (pp. 56-75). Tiro Corto Editores. http://ru.juridicas.unam.mx/xmlui/handle/123456789/41833

Pacto Internacional de Derechos Civiles y Políticos (PIDCP). (16 de diciembre de 1966). https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Piñar Mañas, J.L. (2010). ¿Existe privacidad? En Instituto Federal de Acceso a la Información Pública (IFAI) (Ed.). *Protección de datos personales. Compendio de lecturas y legislación*. (pp. 15-55). Tiro Corto Editores. https://itaipue.org.mx/documentos/2020/dp04-CompendioProteccIondeDatos8.pdf

Puccinelli, O.R. (2004). *Protección de datos de carácter personal*. Astrea.

Puccinelli, O.R. (2018). De la portabilidad de los datos. En M.S. Maqueo (Coord.), *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, Comentada*. (pp. 157-183). Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. https://tachiapas.gob.mx/wp-content/uploads/2021/09/LEY_PROTECC_DATOS_COMENT.pdf

Real Academia Española (RAE). (20 de junio de 2025). *Diccionario de la lengua española*. (23a. ed.). https://dle.rae.es

Reglamento General de Protección de Datos (RGPD). (14 de abril de 2016). https://gdpr-info.eu/

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP). (21 de diciembre de 2011). https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf

Remolina Angarita, N. (2017). ¿Derecho al olvido en el ciberespacio? Principios internacionales y reflexiones sobre las regulaciones latinoamericanas. En A. Del Campo (Comp.), *Hacia una internet libre de censura II. Perspectivas en América Latina*. (pp. 199-226). Universidad de Palermo, Facultad de Derecho; Centro de Estudios en Libertad de Expresión y Acceso a la Información. https://www.palermo.edu/cele/pdf/investigaciones/Hacia_una_internet_libre_de_censura_II.pdf

Ríos Vega, L.E. (2020). Presentación de casos líderes en materia de privacidad y protección de datos personales. En I. Spingo y L.E. Ríos Vega (Dirs.), *Estudios de casos líderes europeos. Vol. XII Cuestiones actuales del derecho a la vida privada y la protección de datos personales en el Tribunal Europeo de Derechos Humanos* (pp. XXV-XXVII). Tirant lo Blanch; Cedecomp.

Soto Galindo, J. (16 de junio de 2022). Tribunal de México condena a Google a pagar 5,000 millones de pesos por daño moral. *El Economista*. https://www.eleconomista.com.mx/tecnologia/Tribunal-de-Mexico-condena-a-Google-a-pagar-5000-millones-de-pesos-por-dano-moral-20220616-0055.html

Soto Galindo, J. (13 de septiembre de 2023). Buró de Crédito debe cumplir con la ley de datos personales, propone MC en Diputados. *El Economista*. https://www.eleconomista.com.mx/sectorfinanciero/Diputado-de-MC-propone-reforma-que-obliga-al-Buro-de-Credito-a-cumplir-con-la-ley-de-datos-personales-20230913-0036.html

Soto Galindo, J. (27 de mayo de 2025). El juicio millonario que puede cambiar internet en México. *El Economista*. https://economicon.mx/blog/el-juicio-millonario-que-puede-cambiar-internet-en-mexico/

Suprema Corte de Justicia de la Nación (SCJN). (23 de mayo de 2007). Amparo Directo en Revisión 402/2007. https://www2.scjn.gob.mx/juridica/engroses/1/2007/10/2_89948_0_firmado.pdf

SCJN. (30 de abril de 2008). Amparo en Revisión 134/2008. https://www2.scjn.gob.mx/juridica/engroses/2/2008/2/2_97847_0_firmado.pdf

Tesis: 2a. LXIII/2008. (mayo de 2008). *Semanario Judicial de la Federación y su Gaceta*, Reg. 169700. Tomo XXVII, p. 229. https://sjf2.scjn.gob.mx/detalle/tesis/169700

Tesis: 1a. CCXIV/2009. (diciembre de 2009). *Semanario Judicial de la Federación y su Gaceta*, Reg. 165823. Tomo XXX, p. 277. https://www.catalogoderechoshumanos.com/165823-2/

Tesis: I.10.A.6 CS (10a.). (septiembre de 2019). *Gaceta del Semanario Judicial de la Federación*, Reg. 2020564. Libro 70, Tomo III, p. 2200. https://sjf2.scjn.gob.mx/detalle/tesis/2020564

Tesis: P. II/2019 (10a.). (enero de 2020). *Gaceta del Semanario Judicial de la Federación*, Reg. 2021411. Libro 74, Tomo I, p. 561. https://www.catalogoderechoshumanos.com/2021411-2/

Tesis: XXI.3o.C.T.11 C (10a.). (febrero de 2020). *Gaceta del Semanario Judicial de la Federación*, Reg. 2021622. Libro 75, Tomo III, p. 2399. https://sjf2.scjn.gob.mx/detalle/tesis/2021622

Tratado entre los Estados Unidos Mexicanos, los Estados Unidos de América y Canadá (T-MEC), Tomo II. (10 de diciembre de 2019). Artículo 19. Comercio Digital. https://www.gob.mx/cms/uploads/attachment/file/708696/T.MEC_TOMO_II_CAP_TULO_14_AL_34_y_Acuerdos_Paralelos.pdf

Tribunal Constitucional de España (TCE). (4 de junio de 2018). Sentencia 58/2018. https://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/25683

Tribunal de Justicia de la Unión Europea (TJUE). (13 de mayo de 2014). Caso C-131/12. AEPD, Mario Costeja González vs. Google Spain, S.L., Google Inc. Sentencia. https://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=ES

United Nations Trade & Development (UNCTAD). (2 de julio de 2025). *Data Protection and Privacy Legislation Worldwide.* https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Véliz, C. (11 de septiembre de 2021). Protejamos nuestros datos. No olvidemos cómo los usaban los nazis. *El País.* https://elpais.com/ideas/2021-09-12/protejamos-nuestros-datos-no-olvidemos-como-los-usaban-los-nazis.html

Westin, A.F. (1968). Privacy and freedom. *Washington and Lee Law Review*, 166(25), 1064-1075. https://core.ac.uk/download/pdf/289230796.pdf


info


9 786076 422236