

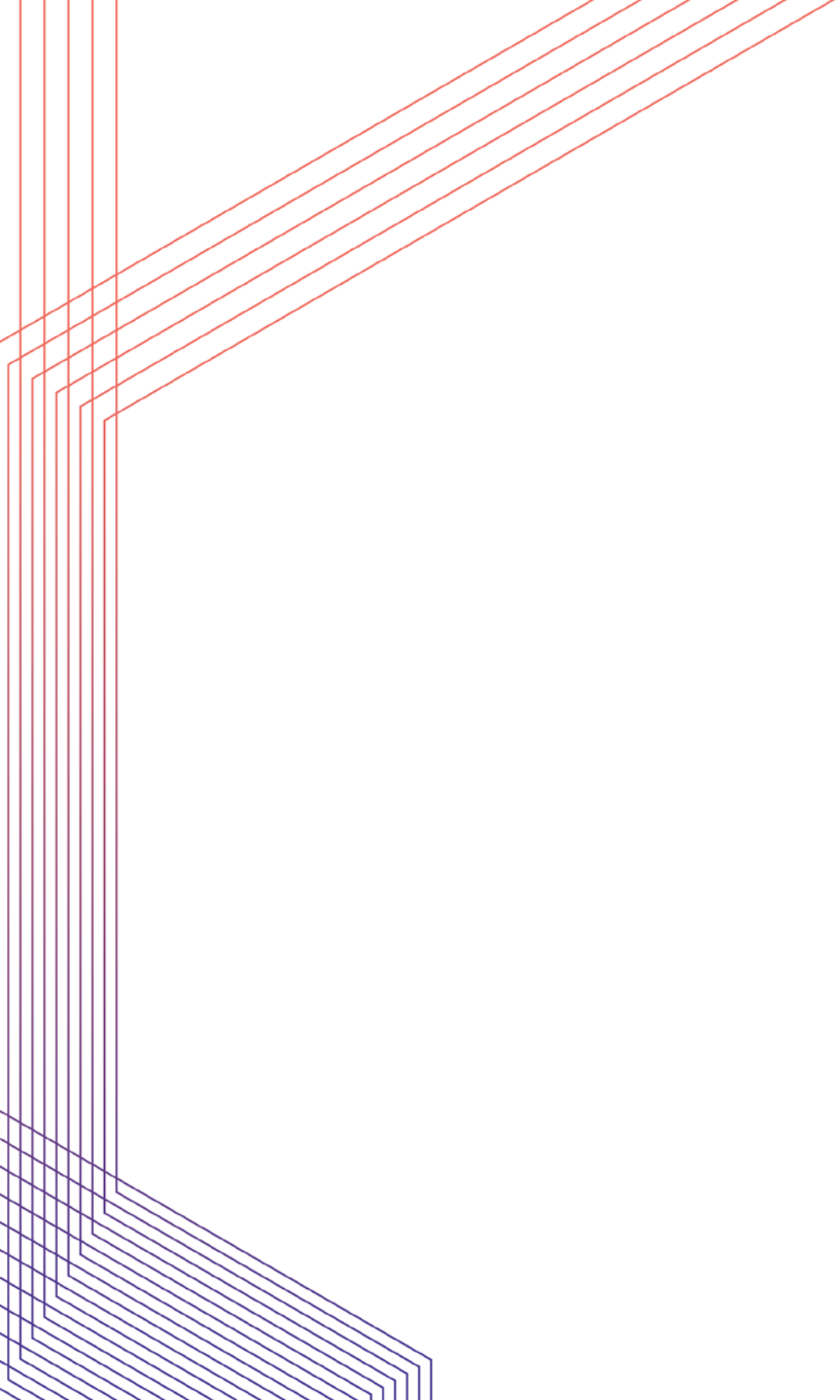
De la Ley al Principio

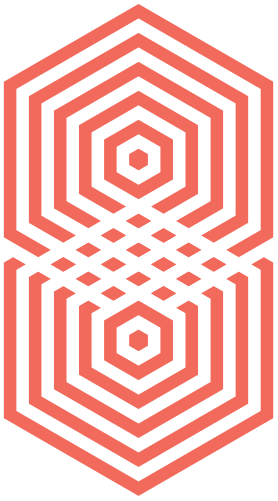
Desempaque normativo y principios para la protección de datos en México

Francia Pietrasanta

R3D
Red en Defensa
de los Derechos Digitales

Brot
für die Welt





De la Ley al Principio

Desempaque normativo y principios para la protección de datos en México



R3D
Red en Defensa
de los Derechos Digitales

Brot
für die Welt

De la Ley al Principio

Desempaque normativo y principios para la protección de datos en México

R3D: Red en Defensa de los Derechos Digitales
Escrito por: Francia Pietrasanta
Editado por: José Flores
Portada e interiores: Gibrán Aquino

Diciembre de 2025

Licencia de Creative Commons Reconocimiento-NoComercial-CompartirIgual4.0 Internacional

Índice

Introducción 05

Derecho a la privacidad y protección de datos como derecho humano 06

México 06

Sistema Interamericano de Derechos Humanos 08

Reformas legislativas y autoridades: ¿Qué tan protegidos están nuestros datos? 12

Reforma constitucional sobre simplificación orgánica 12

Ley Orgánica de la Administración Pública Federal 14

Reglamento Interior SABG 14

Reforma judicial 16

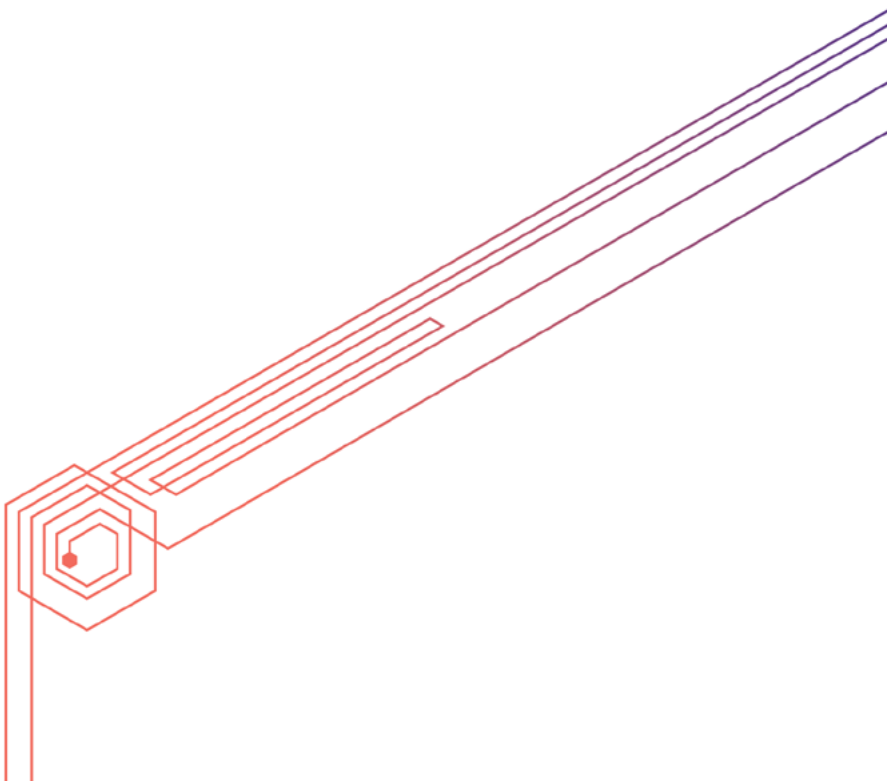
Nuevas leyes en materia de protección de datos personales 18

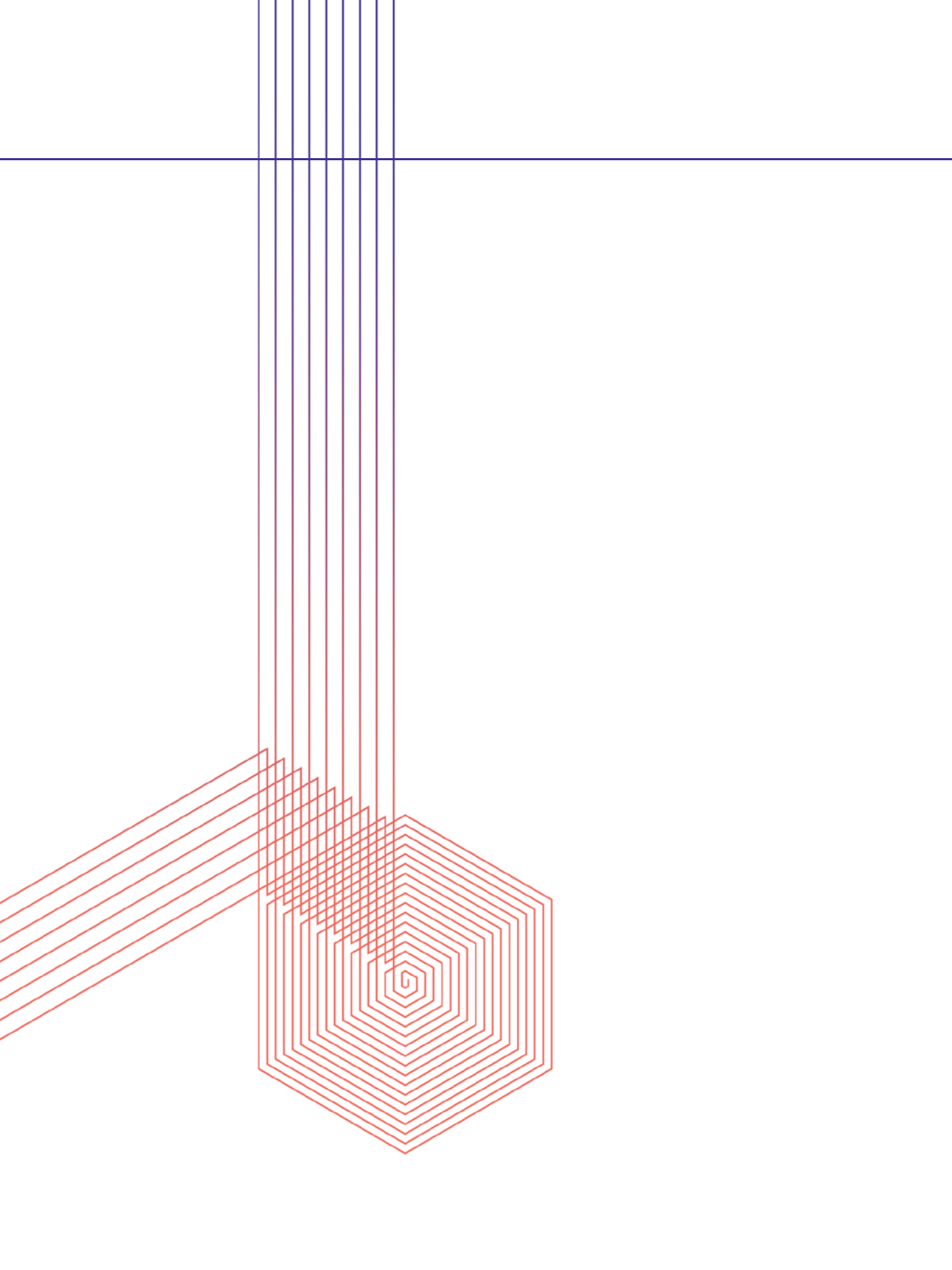
Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados 18

Ley Federal de Protección de Datos Personales en Posesión de Particulares 25

Paquete de leyes que amplían facultades de vigilancia 31

Diagnóstico y principios 36





Introducción

En los últimos años, el gobierno mexicano ha impulsado la digitalización y el uso de tecnologías emergentes para atender áreas prioritarias como la seguridad pública, la seguridad nacional y la prestación de servicios públicos. Estas tecnologías, desarrolladas principalmente por la iniciativa privada, se han convertido en herramientas esenciales para el Estado, el cual funge como uno de sus principales clientes.

En este contexto, los datos personales constituyen el combustible de dichas tecnologías, y las personas, sus generadoras. Este fenómeno se agrava cuando las leyes obligan a las empresas a diseñar sus servicios con capacidades de injerencia en la vida privada, creando un entorno que favorece la vigilancia masiva y debilita los derechos fundamentales.

El desarrollo tecnológico ha permitido tanto a las entidades públicas como a las privadas recabar, analizar y difundir información personal en volúmenes sin precedentes. Al mismo tiempo, los servicios digitales, el e-commerce, la investigación médica, las telecomunicaciones, los sistemas de transporte y las transacciones financieras han incrementado la cantidad de datos generados por cada persona de forma exponencial. Este escenario demanda a los Estados el emprendimiento de acciones para garantizar una protección efectiva frente a los riesgos inherentes del entorno digital.

Las políticas públicas recientes han apostado por la digitalización para resolver problemas de interés público. De manera paradójica, los esfuerzos legislativos suelen centrarse en la expansión tecnológica antes que en la protección de derechos al incentivar el recabo masivo de datos personales sin el establecimiento claro de principios fundamentales.

Los esfuerzos del sector público están encaminados a digitalizar, pero no a asegurar una protección efectiva de los datos personales en un mundo digitalizado. Esta tendencia ha desplazado enfoques orientados a prevenir abusos en el procesamiento masivo de datos y ha promovido una falsa dicotomía entre innovación y los derechos humanos, como si el avance tecnológico implicara inevitablemente renunciar a nuestras libertades.

Este informe tiene como propósito analizar el derecho a la privacidad y el derecho a la protección de datos personales en México y a nivel interamericano a través de dos casos emblemáticos: PANAUT y CAJAR vs. Colombia. De igual forma, desempaca las reformas legislativas recientes en México que, aunque no lleven explícitamente la etiqueta de “en materia de datos personales”, desafían nuestra privacidad. A partir de ello, propone principios y recomendaciones que permitan construir un marco que respete los derechos humanos y responda a las exigencias en el entorno digital.

Derecho a la privacidad y protección de datos personales como derecho humano

México

La Constitución Política de los Estados Unidos Mexicanos reconoce el derecho a la privacidad y a la protección de datos personales en los artículos 6, A, fracción II y 16. Como se desarrollará más adelante, el artículo 6 fue reformado de manera trascendental en diciembre de 2024 al eliminar los órganos garantes de protección de datos en México. Pese a ello, estos derechos mantienen su reconocimiento en el sistema jurídico mexicano.

La Suprema Corte de Justicia de la Nación (SCJN) ha reconocido el derecho a la privacidad desde dos ámbitos: 1) el interno, que implica que la persona **pueda modular a través de su comportamiento aquello que comparte**, y que dicha decisión forme parte del ejercicio del derecho a la privacidad. 2) el externo, **que comprende que este derecho pueda ser limitado al armonizarse con otros derechos**, lo cual implica que su aplicación concreta pueda variar.[1]

Dentro del derecho a la privacidad, se encuentra el derecho a la intimidad, la cual comprende los extremos más personales y del entorno familiar de una persona. Es un núcleo esencial que debe tener una protección reforzada, ya que su ejercicio efectivo permite la protección de bienes individuales. Una de las manifestaciones de este derecho son los datos personales sensibles.

Para la SCJN, la autodeterminación informativa comprende el control de la información personal y el uso que se le dé. Este derecho refiere a la facultad de cada persona para decidir libremente sobre el uso y destino de sus datos personales, incluyendo el derecho a acceder, rectificar, cancelar y oponerse legítimamente a su tratamiento.[2] Protege a la persona frente a: a) la **recopilación y conservación** de su información privada y datos personales (incluyendo la información relativa a la intimidad y datos sensibles), y b) el **uso** que se le dé a esta información, lo cual incluye el **acceso** por parte de terceros, particulares o el Estado.

1. Pleno de la Suprema Corte de Justicia de la Nación. Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021. Sentencia de 26 de abril de 2022. Párrafo, 161es.
2. Suprema Corte de Justicia de la Nación. Acción de inconstitucionalidad 101/2017 y su acumulada.

La autodeterminación informativa incluye la protección de datos personales dentro de esta tríada de derechos: privacidad, intimidad y protección de datos personales.

Uno de los asuntos más emblemáticos en esta materia es la Acción de Inconstitucionalidad 82/2021 promovida contra las reformas que buscaban crear un Padrón Nacional de Usuarios de Telefonía Móvil (AI 82/202), donde la SCJN declaró la invalidez de esta medida.

El PANAUT implicaba el tratamiento masivo de datos personales, incluyendo biométricos y otros datos personales, por parte del Estado y de compañías de telefonía a fin de crear una base de datos para asociar todas las líneas telefónicas del país con datos personales. Esta información podía ser compartida con autoridades.

La SCJN consideró que en este tipo de medidas el consentimiento de la persona para entregar sus datos personales no era un elemento relevante. Esto se debía a que no era optativo otorgarlos, sino que se establecía como una condición obligatoria para acceder o mantener el servicio de telefonía móvil. Además, la persona titular no tenía intervención en el tratamiento que se le daría a la misma, o los terceros que podrían acceder a ella, lo que tenía un impacto en la autodeterminación informativa.

En segundo lugar, consideró que el PANAUT podía generar una afectación intensa a la privacidad, la intimidad y la protección de datos personales. Para la Corte, el catálogo de información recaba que incluía nombre, nacionalidad, CURP, domicilio y datos biométricos, permitía extraer conclusiones muy precisas sobre la vida privada de las personas. Esta información sería recabada por los concesionarios de telecomunicaciones y entregada directamente al Estado para ser operada y administrada por el mismo. Por ello, es indispensable establecer salvaguardas que eviten el abuso de los datos personales en este tipo de medidas.

Adicionalmente, la obligación de entregar los datos a este Padrón involucraba a todas las personas físicas o morales que tuvieran una línea de telefonía móvil. En un país que tenía 98 líneas por cada 100 habitantes, estas medidas no establecieron una temporalidad alguna para conservar los datos, lo cual denotaba la falta de controles mínimos.[3]

El derecho a la privacidad constituye un derecho llave para el ejercicio de otros, como la dignidad humana, la libertad de expresión, la igualdad y la no discriminación y la libertad de asociación.

Dado el incremento de prácticas de vigilancia en medios digitales, la Corte delimita que toda limitación a los derechos a la privacidad debe estar prevista en una ley. Dicha ley debe ser lo suficientemente accesible, clara y precisa para que una persona pueda leerla y saber quién está autorizado a realizar actividades de vigilancia de datos y en

3. Pleno de la Suprema Corte de Justicia de la Nacion. Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021. Sentencia de 26 de abril de 2022. Párrafos 180-192.

qué circunstancias. Además, la limitación debe ser necesaria para alcanzar un objetivo legítimo, así como proporcional, y ser la opción menos invasiva disponible.

La SCJN estimó mediante una prueba de proporcionalidad (donde evaluó el objetivo legítimo, la necesidad, la idoneidad y la proporcionalidad) que el PANAUT perseguía el fin legítimo de combatir la criminalidad y que era una medida que contribuía en cierta medida a dicho fin. Sin embargo, consideró que existen otras medidas menos restrictivas para el derecho a la privacidad, como aquellas que controlen el acceso, requieran autorización judicial y limiten el tiempo que los datos serán conservados. También, que recaben datos de menor sensibilidad que los biométricos o eviten el registro generalizado de datos personales. Por ello, no resulta una medida proporcional.

Además, dado el fuerte impacto que el PANAUT generaría en los derechos humanos a la privacidad y protección de los datos personales, y dado que también se afectan los datos sensibles de los usuarios de telefonía móvil, este Padrón requería de una evaluación de impacto en la protección de datos personales, contemplada en la ley de protección de datos aplicable a sujetos obligados.

Esta sentencia es de relevancia para la protección de datos personales porque reconoce que las bases de datos personales (incluidos datos sensibles) pueden ser utilizadas para la vigilancia masiva y acceder a detalles específicos de las personas. También reconoce que no existe un consentimiento real cuando la persona está obligada a entregarlo y registrar los datos para acceder a un servicio. Aplica la prueba de proporcionalidad para determinar la invalidez del PANAUT y reconoce la importancia de la evaluación de impacto en la protección de datos personales, antes de que las iniciativas legislativas que estipulen estas medidas sean aprobadas.

Sistema Interamericano de Derechos Humanos

El artículo 11.2 de la Convención Americana de Derechos Humanos (CADH) reconoce el derecho a la privacidad al proteger a las personas de interferencias abusivas o arbitrarias por parte del Estado.[4] Al mismo tiempo, el artículo 11.3 estipula que los Estados deben brindar protección contra aquellas injerencias[5], por lo que no basta con que los Estados se abstengan de ejercer acciones arbitrarias para la privacidad, sino que deben garantizar el derecho a la vida privada mediante medidas que lo protejan tanto de autoridades públicas como de otros actores.

La Corte Interamericana de Derechos Humanos (CIDH) reconoce que este derecho no es absoluto y que puede ser limitado cuando las restricciones no sean abusivas o

4. 11.2. 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.

5. 11.3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

arbitrarias. Por ello, estas limitaciones deben estar previstas en ley, perseguir un fin legítimo y cumplir con los requisitos de idoneidad, necesidad y proporcionalidad.

En el caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia (caso CAJAR). Durante la década de 1990, las Fuerzas Armadas, la Policía Nacional y el Departamento Administrativo de Seguridad (en adelante "DAS") recopilaron información de distintos miembros del CAJAR, a partir de lo cual elaboraron registros relacionados con dichas personas y sus familias.

Estos registros implicaron seguimiento, vigilancia, interceptaciones de comunicaciones de teléfonos institucionales, celulares, correos electrónicos, comunicaciones vía fax y correspondencia, requerimientos de información a entidades privadas para obtener sus datos personales, así como tomas de fotografías de sus residencias, oficinas de trabajo y círculos familiares.

Estas actividades fueron descritas por el Estado colombiano como "actividades de inteligencia". No obstante, la CIDH determinó que implicaban una injerencia en el derecho a la vida privada, pues Colombia obtuvo y utilizó información y datos personales de este grupo de personas abogadas defensoras de derechos humanos para perseguirlas de manera sistemática.

La Corte consideró que las medidas adoptadas en este ámbito deben estar expresamente previstas en ley, la cual debe contener controles o límites en el ejercicio de estas actividades. Además, estas medidas deben cumplir con la prueba de proporcionalidad (perseguir un fin legítimo y cumplir con los requisitos de idoneidad, necesidad y proporcionalidad). Para la CIDH, los propósitos que perseguían las actividades de inteligencia no representaban fines legítimos necesarios en una sociedad democrática, sino que constaban de intereses con trasfondo político. En suma, destacó que las acciones desplegadas, al haber sido realizadas sin control judicial, eran incompatibles con la CADH.

Para este tribunal, la recopilación de datos personales por facultades de servicios de inteligencia (que generalmente son ejercidas con la falta de consentimiento del titular), debe basarse en leyes que incluyan lo siguiente:

> *a) los motivos que habilitan la existencia de archivos con datos personales por parte de los organismos de inteligencia; tales motivos, acordes con los fines propios de las actividades de inteligencia, habrán de limitar el actuar de las autoridades en esta materia; b) las clases y tipos de datos de carácter personal que las autoridades están facultadas para conservar en sus archivos, y c) los parámetros aplicables para la utilización, conservación, verificación, rectificación, eliminación o revelación de tales datos [...].*[6]

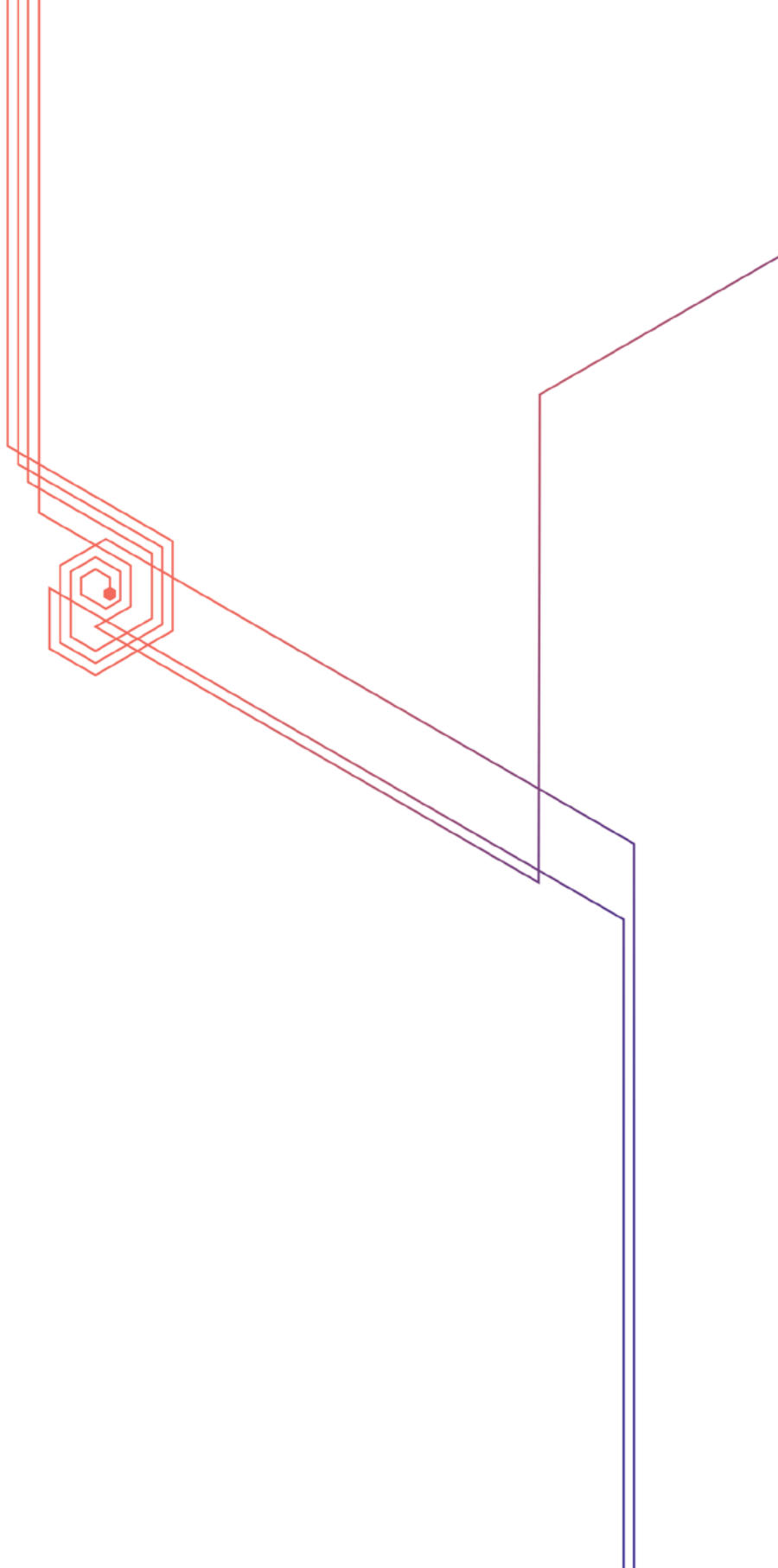
6. Corte IDH, Caso *Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" vs. Colombia, (Excepciones Preliminares)*, Sentencia de 18 de octubre de 2023, Fondo, Reparaciones y Costas, párr. 577.

Las medidas de reparación que Colombia debe implementar incluyen adecuar sus leyes y manuales de inteligencia al marco interamericano de derechos humanos, capacitar a los organismos de inteligencia acerca de estándares de derechos humanos, establecer limitaciones y controles en actividades de inteligencia y tratamiento de datos personales, así como aprobar la normativa necesaria para garantizar el derecho a la autodeterminación informativa con mecanismos y procedimientos específicos.

La relevancia de este asunto radica en que la CIDH reconoce el derecho a la autodeterminación informativa como un derecho autónomo y exigible. Delimita que dicho derecho se materializa cuando la persona ejerce control sobre la información que se encuentra en manos de autoridades públicas.

Por ello, establece el derecho de las personas del colectivo CAJAR a acceder a los archivos de inteligencia, así como la posibilidad de rectificar, cancelar o eliminar los datos que consten en los archivos de los organismos que tengan en sus manos dicha información. Reconoce cómo las razones de seguridad nacional o el hecho de que la información se encuentre en archivos de organismos de inteligencia pueden ser utilizados para mantener y aumentar la opacidad.

Finalmente, enfatiza que el derecho a la protección de datos personales implica que se recopilen, almacenen, traten y divulguen tales datos mediante consentimiento libre e informado de la persona titular, o que exista una facultad expresa para ello. Sin embargo, en todos los casos debe existir una finalidad legítima para el tratamiento de datos, estar previstas en ley con controles y límites y cumplir con la prueba de proporcionalidad, conforme a la CADH.



Reformas legislativas y autoridades: ¿Qué tan protegidos están nuestros datos?

En años recientes, el marco normativo de datos personales ha cambiado de manera significativa. Reformas constitucionales, como la de simplificación orgánica y la reforma judicial han establecido nuevos paradigmas en este ámbito. En suma, la expedición de nuevas leyes sobre datos personales y reformas a otras normas generales también representan cambios importantes para esta materia, como se desarrolla a continuación.

Reforma constitucional sobre simplificación orgánica

La reforma en materia de simplificación orgánica fue la primera que generó un cambio trascendental en la situación de protección de datos personales en México. Esta reforma eliminó a nivel constitucional siete órganos autónomos[7], entre ellos el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), encargado de la función de transparencia y protección de datos a nivel federal.

Desde el inicio de su sexenio, el entonces presidente Andrés Manuel López Obrador cuestionó en diversas ocasiones en sus conferencias mañaneras el funcionamiento efectivo de algunos de estos órganos. Además, argumentó que era necesario reducir gastos presupuestales a nivel federal, por lo que era necesario recortarlo mediante la eliminación de estos órganos autónomonos.[8]

Respecto al INAI, dichas posturas generaron un amplio debate público, pues diversos sectores señalaban que las verdaderas razones se relacionaban con las tensiones entre el INAI y el Ejecutivo. Esto se debía a que este Instituto, en ejercicio de sus atribuciones como órgano garante de la transparencia, había ordenado la publicación de información que el gobierno mantenía clasificada, como los contratos de Pegasus o el

7. Además del INAI, la reforma suprimió la Comisión Federal de Competencia Económica (COFECE), el Consejo Nacional de Evaluación de la Política de Desarrollo Social (CONEVAL), Instituto Federal de Telecomunicaciones (IFT), la Comisión Nacional para la Mejora Continua de la Educación (MEJOREDU), la Comisión Reguladora de Energía (CRE) y la Comisión Nacional de Hidrocarburos (CNH).

8. Animal Político. (31 de diciembre de 2023). *AMLO vs. organismos autónomos; cinco años de amenazas sobre desaparecer al INAI.* https://animalpolitico.com/politica/amlo-organismos-autonomos-desaparecer-inai

Tren Maya.[9] Por ello, parte de la opinión pública interpretó la reforma no solo como una medida de austeridad, sino también como una respuesta a dichas tensiones.

El 5 de febrero de 2024 AMLO presentó la iniciativa para eliminar órganos autónomos. Una vez con el apoyo de la mayoría calificada consolidada en septiembre de 2024, necesaria para avanzar esta reforma constitucional, la reforma siguió su tramitación en el Poder Legislativo y fue publicada en el Diario Oficial de la Federación el 20 de diciembre de 2024 durante el gobierno de Claudia Sheinbaum.[10]

El primer informe de gobierno de Claudia Sheinbaum afirma que con la eliminación del INAI se tendrá un costo 52% menor, lo cual representa ahorros por más de 500 millones de pesos anuales para el erario federal.[11] No obstante, dicho informe no presenta detalles sobre la metodología utilizada para calcular ese porcentaje.

La discusión pública respecto a la extinción del INAI en su carácter de órgano garante de transparencia fue la modificación que incentivó la discusión pública, lo cual dejó en segundo plano las implicaciones que su eliminación tendría para la protección de datos personales.

La reforma de simplificación orgánica trasciende en la protección de datos de la siguiente manera:

- Sujetos obligados con facultades para atender cuestiones de datos personales en el ámbito público.[12]
- Bases, principios generales y procedimientos del ejercicio de estos derechos serán determinados en las leyes en la materia.[13]
- Autoridades de control interno y vigilancia u homólogos en el ámbito federal y local de los sujetos obligados tienen competencia para conocer de los procedimientos de revisión contra los actos que emitan dichos sujetos obligados.[14]
- Ley Orgánica de la Administración Pública Federal determina la competencia para conocer los procedimientos relacionados con la protección de datos en manos de particulares.[15]

9. R3D: Red en Defensa de los Derechos Digitales. (23 de julio de 2024). *Juez ordena a la SEDENA cumplir resolución del INAI que le obliga a entregar contratos de Pegasus*.https://r3d.mx/2024/07/23/juez-ordena-a-la-sedena-cumplir-resolucion-del-inai-que-le-obliga-a-entregar-contratos-de-pegasus/; y López, A.(23 de octubre de 2023). *INAI ordena a Procuraduría Agraria entregar información de afectaciones a tierras por Tren Maya en Yucatán.* El Universal. https://www.eluniversal.com.mx/nacion/inai-ordena-a-procuraduria-agraria-entregar-informacion-de-afectaciones-a-tierras-por-tren-maya-en-yucatan/
10. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5745905&fecha=20/12/2024#gsc.tab=0
11. Gobierno de México. (2025). Primer Informe de Gobierno 2024 - 2025. pg. 26. https://www.informegobierno.gob.mx/usercontent/68b4162a4d926-1IG-INFORME-INTEGRADO-FINAL_26_08_2025
12. Constitución Política de los Estados Unidos Mexicanos. [C.M.] art. 6 A fracción II.
13. *Ibidem*, art. 6 A fracción VIII.
14. *Idem*.
15. *Ibidem*, art. 6 A fracción II.

- Eliminación de todos los párrafos referentes a un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con plena autonomía.
- Régimen transitorio que ordena a las entidades federativas a armonizar su marco jurídico sobre transparencia y protección de datos con esta reforma.[16]

Ley Orgánica de la Administración Pública Federal

La reforma de simplificación orgánica y el artículo 90 de la CPEUM ordenaron a la Ley Orgánica determinar la competencia para conocer de los procedimientos relativos a la protección, verificación e imposición de sanciones sobre protección de datos.

El 1 de noviembre de 2024, la presidenta presentó la iniciativa para reformar dicha ley, la cual fue aprobada por el Congreso de la Unión y promulgada en el DOF el 28 de noviembre de 2024. Por un lado, esta reforma implicó cambios como la creación de las secretarías de las Mujeres y de Ciencia, Humanidades, Tecnología e Innovación. Por otro, contiene los siguientes para el ámbito de datos personales:

- Sustituye la Secretaría de la Función Pública (SFP) por la Secretaría de Anticorrupción y Buen Gobierno (SABG).[17]
- La SABG absorbe la función de datos personales y transparencia.[18]
- Crea la Agencia de Transformación Digital y Telecomunicaciones (ATDT).[19] La cual tiene facultades que incluyen:[20]
  - » Formular políticas para la identidad digital y establecer el mecanismo único de autenticación digital con CURP.
  - » Integrar el Servicio Nacional de Identificación Personal.
  - » Gestionar bases de datos que permitan interoperar los sistemas nacionales y de la Administración Pública Federal con el Registro Nacional de Población, en coordinación con la Secretaría de Gobernación.
  - » Promover soluciones tecnológicas para la digitalización de trámites y servicios.

Reglamento Interior SABG

El 21 de marzo de 2025 la presidenta publicó en el DOF el Reglamento Interior de la Secretaría Anticorrupción y Buen Gobierno vigente.[21] De esta forma, estructura las áreas administrativas dentro de la SABG con facultades para la protección de datos

16. *Ibidem*, art. Cuarto Transitorio.

17. Ley Orgánica de la Administración Pública Federal. [L.O.A.P.F.] art. 26 fracción XIII.

18. *Ibidem*, art. 37 fracción XIV y XV.

19. *Ibidem*, art. 26 fracción XXII.

20. *Ibidem*, art. 42 ter fracción II.

21. Disponible en: https://dof.gob.mx/nota_detalle.php?codigo=5752650&fecha=21/03/2025#gsc.tab=0

personales, la cual se prometía desde la reforma constitucional sobre simplificación orgánica. La organización es la siguiente:

- Unidad de Protección de Datos Personales:[22]
  - » Emitir políticas, parámetros, estrategias, criterios de interpretación, recomendaciones, disposiciones, normas, entre otros en materia de protección y de seguridad de datos personales.
  - » Autorizar medidas compensatorias.
  - » Ordenar, por sí o por medio de las unidades administrativas a su cargo, el inicio de los procedimientos de verificación.
  - » Esta Unidad se auxilia por las direcciones de Normativa y Prevención, de Datos Personales en el Sector Público y de Datos Personales en el Sector Privado.

- Dirección de Normativa y Prevención:[23]
  - » Atender consultas, proponer interpretaciones, elaborar e instrumentar políticas, coadyuvar en la administración de sistemas y registros.
  - » Evaluar medidas compensatorias y realizar auditorías en materia de protección de datos personales.
  - » Dictaminar las solicitudes de evaluación de impacto a la protección de datos personales que se presenten y, en su caso, emitir recomendaciones.
  - » Se auxilia de las direcciones de Normatividad de Datos Personales, de Esquemas como los de Prevención de los Sectores Público y Privado, de Certificación de los Sectores Público y Privado, y de Seguridad de Datos Personales de los Sectores Público y Privado. Sin embargo, no se desarrolla sobre estas direcciones y esquemas.

- Dirección de Protección de Datos en el Sector Público:[24]
  - » Sustanciar y resolver recursos de revisión, realizar investigaciones previas, iniciar y resolver procedimientos de verificación, celebrar audiencias de conciliación, aplicar medidas de apremio y realizar diligencias necesarias (audiencias, requerimientos, pruebas).
  - » Denunciar actos u omisiones violatorios de la LGPDPPSO. Diseñar y aplicar indicadores y criterios para evaluar el desempeño de los responsables en materia de protección de datos personales en el sector público.
  - » Se auxilia por las direcciones de Atención a Denuncias, Investigación, Verificación y Evaluación del Sector Público, y de Recursos de Revisión.

22. Reglamento Interior de la Secretaría Anticorrupción y Buen Gobierno. [S.A.B.G.]. (31 de diciembre de 2024). Diario Oficial de la Federación [D.O.F.], (México). art. 30 B.

23. Reglamento Interior de la Secretaría Anticorrupción y Buen Gobierno. [S.A.B.G.]. (31 de diciembre de 2024). Diario Oficial de la Federación [D.O.F.], (México). art. 30 C.

24. Reglamento Interior de la Secretaría Anticorrupción y Buen Gobierno. [S.A.B.G.]. (31 de diciembre de 2024). Diario Oficial de la Federación [D.O.F.], (México). art. 30 D.

- Dirección de Protección de Datos en el Sector Privado:[25]
  - » Sustanciar y resolver procedimientos de protección de derechos, conciliaciones, verificación e imposición de sanciones. Realizar diligencias necesarias (audiencias, requerimientos y desahogo de pruebas).
  - » Dar vista y denunciar actos u omisiones violatorias de la LFPDPPP.
  - » Se auxilia por las direcciones de Protección de Derechos del Sector Privado, de Atención a Denuncias y Verificación del Sector Privado, y de Procedimientos Administrativos y Sanciones del Sector Privado.

- Dirección General de Transparencia:[26]
  - » Recibir y turnar solicitudes.
  - » Dirigir las acciones de atención a los recursos de revisión interpuestos ante la autoridad competente para conocer de los mismos, respecto de las solicitudes de información y protección de datos personales;
  - » Promover buenas prácticas internas sobre protección de datos.

Reforma judicial

La reforma judicial surgió de una iniciativa impulsada durante la administración anterior. Algunos afirman que el anhelo del expresidente AMLO proviene de tensiones con el Poder Judicial que datan de la jefatura de gobierno de AMLO en el Distrito Federal.[27] Otros indican que surgió a partir de resoluciones del Poder Judicial que eran contrarias a su administración.[28]

El 5 de febrero de 2024 fue presentada esta reforma por el expresidente. Posteriormente, el 15 de septiembre de 2024, a inicios del gobierno de Claudia Sheinbaum y tras su aprobación en el Legislativo que contaba con una mayoría calificada, la presidenta promulgó la reforma judicial.[29] Las principales implicaciones de la reforma que influyen en la protección de datos personales son las siguientes:

25. *Ibidem*, art. 30 F.

26. *Ibidem*, art. 68 D.

27. Lastiri, D. (13 de octubre de 2024.) *López Obrador vs. el Poder Judicial, una pugna de 30 años*. Proceso. https://www.proceso.com.mx/reportajes/2024/10/13/lopez-obrador-vs-el-poder-judicial-una-pugna-de-30-anos-338375.html

28. Hernández, M. (24 de septiembre de 2024.) *Reforma judicial de AMLO es una venganza: ministro González Alcántara; "quiere jueces dóciles y obedientes"*. El Universal. https://www.eluniversal.com.mx/nacion/reforma-judicial-de-amlo-es-una-venganza-ministro-gonzalez-alcantara-quiere-jueces-dociles-y-obedientes/

29. Constitución Política de los Estados Unidos Mexicanos. [C.M.], Reformada, Diario Oficial de la Federación [D.O.F.], 15 de septiembre de 2024, (México). https://www.dof.gob.mx/nota_detalle.php?codigo=5738985&fecha=15/09/2024#gsc.tab=0

- Elección del poder judicial por voto popular, lo que conlleva la renovación de las personas encargadas de resolver los asuntos en la materia.[30]
- Eliminación de las salas especializadas de la SCJN.
- Reducción del número de ministros de 11 a 9.
- Limitación de los efectos de las suspensiones y los amparos contra normas generales.
- Reducción del número de votos para aprobar las decisiones tomadas por el Pleno de 8 a 6, las cuales configuran precedentes obligatorios para todas las autoridades jurisdiccionales.

En otras materias, la reforma definió criterios de elegibilidad que incluían al menos ocho puntos o su equivalente, y nueve puntos o su equivalente en las materias relacionadas con el cargo al que se postula dentro de la licenciatura, especialidad, maestría o doctorado. Adicionalmente, en el caso de aspirantes a magistraturas, se requirió un mínimo de tres años de experiencia en un área afín.

Sin embargo, al momento de la entrada en vigor de la reforma y de la elección judicial del 1 de junio de 2025, aún no se habían instituido jueces especializados en la materia. En consecuencia, la reforma no establece requisitos mínimos para la elección de jueces en los ámbitos de transparencia y protección de datos personales.

Así como en otros rubros, los amparos contra normas generales y suspensiones en materia de protección de datos concedidos a las organizaciones de la sociedad civil,[31] o a personas físicas no cuentan con la posibilidad de tener efectos generales en beneficio de la población, pues estos serían aplicables solamente a quien los promovió. Si bien por regla general las sentencias ya estaban limitadas por el principio de relatividad, la reforma elimina por completo la posibilidad de que sus efectos se extiendan y puedan beneficiar a terceros.

Los asuntos resueltos en materia de privacidad y protección de datos que anteriormente hubiesen sido resueltos por las Salas serían abordados en Pleno, lo cual podría causar rezago y congestionamiento de asuntos. Incluso, dicha situación podría causar problemas de especialización y profundidad de las discusiones.

30. En la elección de jueces y magistrados del 1 de junio de 2025, aún no se había determinado qué jueces y tribunales serían competentes en materia de protección de datos personales, conforme a lo dispuesto en el régimen transitorio de las nuevas leyes sobre la materia. El desarrollo de este punto se aborda en el apartado siguiente.

31. R3D: Red en Defensa de los Derechos Digitales. (2 de septiembre de 2025). *R3D presenta demandas de amparo contra el paquete legislativo que amplía las facultades de vigilancia.* https://r3d.mx/2025/09/02/r3d-presenta-demandas-de-amparo-contra-el-paquete-legislativo-que-amplia-las-facultades-de-vigilancia/

Nuevas leyes en materia de protección de datos personales

El 20 de febrero de 2025, la presidenta Sheinbaum presentó en el Senado las iniciativas que expiden las nuevas leyes en materia de transparencia y datos personales. Estas reformas formalizaron a nivel operativo la extinción del INAI y tienen implicaciones sustantivas para estos ámbitos en México. Tras ser discutidas y aprobadas en el Legislativo, fueron promulgadas en el DOF el 20 de marzo de 2025.[32]

Aunque las nuevas leyes de protección de datos retomaron cuestiones sustantivas de las anteriores, hay cambios que las distinguen. A continuación, se muestran los de mayor trascendencia.

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

Definiciones

Como punto relevante, esta ley introduce la definición de autoridades garantes que se encuentran a cargo de la protección de datos personales de la siguiente manera:

Son autoridades garantes: "El órgano de control y disciplina del Poder Judicial; los órganos internos de control de los órganos constitucionales autónomos; las contralorías internas del Congreso de la Unión; el Instituto Nacional Electoral, por cuanto hace al acceso a la protección de datos personales a cargo de los partidos políticos; y los órganos encargados de la contraloría interna u homólogos de los Poderes Ejecutivo, Legislativo y Judicial, así como de los órganos constitucionales autónomos, de las entidades federativas".[33]

Por otra parte, elimina la definición de terminología asociada con el INAI, como el Consejo Nacional, Instituto, Programa Nacional de Protección de Datos Personales, Sistema Nacional de Transparencia Acceso a la Información y Protección de Datos Personales, entre otros. Consecuentemente, elimina o modifica los artículos que mencionan estos términos.

Mantiene la definición de datos sensibles como: "Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discrimina-

32. Disponible en: https://www.dof.gob.mx/nota_detalle.php?codigo=5752569&fecha=20/03/2025#gsc.tab=0

33. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados [L.G.P.D.P.P.S.O.], Reformada, Diario Oficial de la Federación [D.O.F.], 14 de noviembre de 2025, (México). art. 6 A fracción VIII: "Las leyes en la materia determinarán las bases, principios generales y procedimientos del ejercicio de estos derechos, así como la competencia de las autoridades de control interno y vigilancia u homólogos en el ámbito federal y local para conocer de los procedimientos de revisión contra los actos que emitan los sujetos obligados."

ción 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". De este modo, no proporciona una clasificación concreta de los datos que se consideran sensibles, lo cual posibilita que esta definición quede abierta a interpretaciones.

Por otro lado, mantiene la definición de tratamiento al referirse a este término como: "Cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, comunicación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales".

Si bien algunas posturas consideran que la definición es excesivamente amplia, su alcance resulta razonable ante la variedad de supuestos en los que se efectúa el tratamiento de datos en el sector público y las diferentes excepciones previstas para evitar la obtención del consentimiento que se desarrollarán en este mismo apartado.

Facultades

Tal como lo estableció la reforma sobre simplificación orgánica, la Secretaría Anticorrupción y Buen Gobierno hereda la mayoría de las atribuciones del INAI y se establece como la autoridad rectora en el ámbito de la protección de datos,[34] con la ejecución operativa que establece el Reglamento Interior de la SABG. Por otra parte, las autoridades garantes son las responsables dentro de cada entidad; tanto a nivel federal como a nivel local.

De esta forma, el esquema de autoridades queda de la siguiente manera:

Autoridades garantes a nivel federal

Antes INAI, ahora:

- Una autoridad garante por cada poder de la Unión:
- Poder Ejecutivo: expresamente no se establece en esta ley; sin embargo, sí lo establece la CPEUM.
- Poder Judicial: órgano de control y disciplina.
- Poder Legislativo: contralorías internas.
- Partidos políticos: INE.
- Órgano constitucionales autónomos: contraloría interna u homólogo.

34. *Ibidem*, art. 81.

Autoridades garantes nivel local

Antes 32 organismos locales homólogos al INAI, ahora una autoridad garante de cada:

- Poder Ejecutivo: contraloría interna u homólogo. 32, uno por cada entidad federativa.
- Poder Legislativo: contraloría interna u homólogo. 32, uno por cada entidad federativa.
- Poder Judicial: contraloría interna u homólogo. 32, uno por cada entidad federativa.
- Órganos constitucionales autónomos: contraloría interna u homólogo de cada uno.

Como ya fue mencionado anteriormente, las leyes en la materia determinarán las bases, principios generales y procedimientos del ejercicio de estos derechos, así como la competencia de las autoridades de control interno y vigilancia u homólogos en el ámbito federal y local para conocer de los procedimientos de revisión contra los actos que emitan los sujetos obligados.

Las facultades de la SABG y las autoridades garantes van desde resolver recursos de revisión, emitir criterios sobre buenas prácticas, expedir reglas sobre las Evaluaciones de Impacto en Protección de Datos Personales (EIPDP) y decidir sobre dichas evaluaciones,[35] entre otras cuestiones.

La figura del consentimiento

Define el consentimiento como "la manifestación de la voluntad libre, específica e informada de la persona titular de los datos mediante la cual se efectúa el tratamiento de los mismos". Igualmente, mantiene el consentimiento tácito por regla general. Al mismo tiempo, establece que no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de la persona titular o aplique el artículo 16 sobre las excepciones.

Esta ley determina que el aviso de privacidad simplificado deberá contener:[36]

- La denominación y el domicilio del responsable.
- Las finalidades para las cuales se obtienen los datos personales, distinguiendo aquéllas que requieren el consentimiento de la persona titular.
- Cuando se realicen transferencias de datos personales que requieran consentimiento, se deberá informar: a) Las autoridades, poderes, entidades, órganos y organismos gubernamentales de los tres órdenes de gobierno y las personas físicas o morales a las que se transfieren los datos personales, y

35. La ley anterior contaba con disposiciones administrativas emitidas por el Sistema Nacional para deliberar esta evaluaciones. A la fecha de redacción de este informe, no se han emitido nuevas para el nuevo régimen en materia de protección de datos.

36. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados [L.G.P.D.P.P.S.O.], Reformada, Diario Oficial de la Federación [D.O.F.], 14 de noviembre de 2025, (México). art. 21.

b) Las finalidades de estas transferencias.
- Los mecanismos y medios disponibles para que la persona titular, en su caso, pueda manifestar su negativa para el tratamiento de sus datos personales para finalidades y transferencias de datos personales que requieren su consentimiento.
- Señalar el sitio donde puede consultar el aviso de privacidad integral.

Dado que mantiene los mismos requisitos que la ley anterior, no obliga a que en el aviso de privacidad simplificado se brinde información sobre los datos personales que serán tratados, identificando los que son sensibles. Tampoco obliga a que en este aviso de privacidad simplificado se informe sobre la posibilidad de ejercer derechos ARCO. Mantener las disposiciones en estos términos posibilita la obtención de consentimiento para el tratamiento de datos sensibles en el ámbito público sin tener la información completa disponible.

Esta falta de información completa puede agravarse en el acceso a servicios públicos, donde muchas veces no entregar datos personales implica el impedimento de acceder a dicho servicio. La SCJN en las acciones de inconstitucionalidad 82/2021 y 86/2021 sobre la invalidez del PANAUT dejó claro que cuando la entrega de datos personales es obligatoria, el consentimiento no es un elemento relevante porque la persona no tiene opción de negarse ni de decidir qué sucede con su información.

Excepciones para la obtención del consentimiento
Las excepciones del artículo 16 son las siguientes:

Artículo 16. El responsable no estará obligado a recabar el consentimiento de la persona titular para el tratamiento de sus datos personales en los siguientes casos:

I. Cuando una legislación aplicable así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos en esta Ley, y en ningún caso podrán contravenirla;
II. Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;
III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;
IV. Para el reconocimiento o defensa de derechos de la persona titular ante autoridad competente;
V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre la persona titular y el responsable;
VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;
VII. Cuando los datos personales sean necesarios para efectuar un tratamien-

to para la prevención, diagnóstico o la prestación de asistencia sanitaria;

VIII. Cuando los datos personales figuren en fuentes de acceso público;

IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o

X. Cuando la persona titular de los datos personales sea una persona reportada como desaparecida en los términos de las disposiciones jurídicas en la materia.

La amplitud de estas excepciones puede ser utilizada para permitir abusos en el tratamiento de datos. Sería suficiente con que una ley lo estableciera, o que una autoridad absorba una facultad relacionada con la transferencia de datos o hubiera un mandato. En este sentido, la reforma mantiene disposiciones que pueden facilitar el acceso a datos personales por parte de entidades gubernamentales y terceros sin justificación, consentimiento ni información clara.

Derechos ARCO

Los derechos ARCO son los que posee la persona titular de los datos personales para acceder, rectificar, cancelar u oponerse al tratamiento de sus datos. A continuación, se presentan definiciones de estos derechos:

- **El derecho de acceso** implica solicitar y recibir información sobre nuestros datos personales para conocer las condiciones del tratamiento y finalidad que se les está dando.[37]
- **El derecho de rectificación** involucra la corrección de nuestros datos personales cuando sean inexactos o incompletos.[38]
- **El derecho de cancelación** implica solicitar que los datos personales ya no estén disponibles y dejen de ser tratados.[39]
- **El derecho de oposición**[40] consiste en impedir el tratamiento de nuestros datos personales, especialmente si la información fue recabada sin nuestro consentimiento, nos causa daño, o tiene un tratamiento automatizado que afecta nuestros intereses o derechos.[41]
- **El derecho de portabilidad** es reconocido en esta ley, pero no está com-

37. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados [L.G.P.D.P.P.S.O.], Reformada, Diario Oficial de la Federación [D.O.F.], 14 de noviembre de 2025, (México). art. 38.

38. *Ibidem*, art. 39.

39. *Ibidem*, art. 40.

40. Para que este derecho pueda materializarse, deben darse estas dos causales: **I.** [Cuando] aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia le cause un daño o perjuicio, y **II.** Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales de la misma o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

41. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados [L.G.P.D.P.P.S.O.], Reformada, Diario Oficial de la Federación [D.O.F.], 14 de noviembre de 2025, (México). art. 41.

prendido dentro el rubro de derechos ARCO, aunque a nivel internacional sí ha sido reconocido dentro de este cúmulo de derechos. La portabilidad consiste en el derecho a obtener del responsable una copia de sus datos en un formato electrónico estructurado que le permita seguir utilizándolos. Es una manera de darle control al titular sobre su información. Esta versión de la LGPDPPSO elimina la designación de a quién le corresponde emitir los lineamientos técnicos y procedimentales para materializar la portabilidad de datos.[42] Bajo el sistema anterior, estos fueron emitidos por el extinto Sistema Nacional de Transparencia.[43]

El titular debe presentar la solicitud de derechos ARCO conforme a lo que establece el artículo de la LGPDPPSO. En esencia, los derechos y obligaciones centrales se mantienen en comparación con la ley anterior.

Aunque no se añaden nuevos requisitos para ejercer estos derechos,[44] se mantienen las amplias excepciones para negar el acceso a derechos ARCO de la siguiente manera:

Artículo 49. Las únicas causas en las que el ejercicio de los derechos ARCO no serán procedente son:

I. Cuando la persona titular o su representante no estén debidamente acreditadas para ello;
II. Cuando los datos personales no se encuentren en posesión del responsable;
III. Cuando exista un impedimento legal;
IV. Cuando se lesionen los derechos de un tercero;
V. Cuando se obstaculicen actuaciones judiciales o administrativas;
VI. Cuando exista una resolución de autoridad competente que restrinja el acceso a los datos personales o no permita la rectificación, cancelación u oposición de los mismos;
VII. Cuando la cancelación u oposición haya sido previamente realizada;
VIII. Cuando el responsable no sea competente;
IX. Cuando sean necesarios para proteger intereses jurídicamente tutelados de la persona titular;
X. Cuando sean necesarios para dar cumplimiento a obligaciones legalmente adquiridas por la persona titular;

42. *Ibidem*, art. 57.

43. Resulta cuestionable que el medio de defensa sea el Amparo Indirecto y no el juicio contencioso administrativo ante el Tribunal Federal de Justicia Administrativa (TFJA), puesto que este último tiene, en principio, competencia para revisar los actos emitidos por los órganos de la Administración Pública Federal, dentro de los que se incluye la Secretaría Anticorrupción y Buen Gobierno. https://www.gob.mx/cms/uploads/attachment/file/685004/Ley_General_Protecci_n_Datos_Personales_Sujetos_Obligados.pdf

44. Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados [L.G.P.D.P.P.S.O.], Reformada, Diario Oficial de la Federación [D.O.F.], 14 de noviembre de 2025, (México). art. 46.

XI. Cuando en función de sus atribuciones legales el uso cotidiano, resguardo y manejo sean necesarios y proporcionales para mantener la integridad, estabilidad y permanencia del Estado mexicano, o

XII. Cuando los datos personales sean parte de la información que las entidades sujetas a la regulación y supervisión financiera del sujeto obligado hayan proporcionado a éste, en cumplimiento a requerimientos de dicha información sobre sus operaciones, organización y actividades.

En todos los casos anteriores, el responsable deberá informar a la persona titular el motivo de su determinación,en el plazo de hasta veinte días a los que se refiere el primer párrafo del artículo 45 de la presente Ley, y por el mismo medio en que se llevó a cabo la solicitud, acompañando en su caso, las pruebas que resulten pertinentes.

Estas excepciones pueden limitar demasiado el ejercicio de los derechos ARCO. Las que señalan un impedimento legal, lesión a derechos de un tercero, así como las relacionadas con supervisión financiera o estabilidad del Estado, dejan márgenes interpretativos que pueden aplicarse arbitrariamente.

Medios de impugnación

La reforma conserva el recurso de revisión para combatir las respuestas a las solicitudes ARCO de los sujetos obligados, las cuales debe presentar el titular ante la SABG, Autoridades Garantes o la unidad de transparencia del sujeto obligado que haya respondido a la solicitud ARCO.[45] Por otro lado, elimina el recurso de inconformidad para combatir decisiones de los sujetos obligados a nivel local, por lo que deja el juicio de amparo como la única vía para combatir las decisiones de los mismos.

De esta manera, el juicio de amparo se convierte en el único medio para impugnar las respuestas sobre solicitud de derechos ARCO, sea cual sea el ámbito de competencia del sujeto obligado.[46] Esto reduce significativamente el acceso a mecanismos rápidos y accesibles para la protección de datos.

La creación de nuevos juzgados especializados en transparencia y protección de datos plantea interrogantes en un contexto de restricciones presupuestarias y cambios en el poder judicial. Mientras tanto, con el pretexto de estos cambios los procesos judiciales en trámite quedaron suspendidos por 180 días, lo cual canceló la protección de datos personales durante dicho periodo.[47]

45. *Ibidem*, art. 86.

46. *Ibidem*, art. 107.

47. *Ibidem*, art. transitorio Vigésimo.

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

La nueva normativa de protección de datos en posesión de particulares replica disposiciones de la ley aplicable a sujetos obligados. Dicha ley tiene las implicaciones siguientes:

Definiciones

Detalla algunas definiciones ya existentes. Por ejemplo, en la definición de fuentes de acceso público, agrega que "no se considerará fuente de acceso público cuando la información contenida en la misma sea obtenida o tenga una procedencia ilícita, conforme a las disposiciones establecidas por la presente Ley y demás disposiciones jurídicas aplicables".[48] Esta es una disposición que ya estaba incluida en el Reglamento de la LFPDPPP.

En la definición de base de datos, agrega que es un "conjunto ordenado de datos personales referentes a una persona identificada o identificable condicionados a criterios determinados, con independencia de la forma o modalidad de su creación, tipo de soporte, procesamiento, almacenamiento y organización".[49]

Define con mayor claridad el consentimiento al establecer que es la "manifestación de la voluntad libre, específica e informada de la persona titular de los datos mediante la cual se efectúa el tratamiento de los mismos". Pese a ello, como se desarrollará a continuación, la ley introduce el consentimiento tácito como regla general, lo cual puede debilitar el refuerzo adherido a esta definición.

Sobre los datos personales sensibles, agrega que "de manera enunciativa mas no limitativa"[50] son 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, sin incluir una lista más específica. En tal sentido, hubiera resultado óptimo contemplar los datos biométricos para fines de identificación como datos sensibles, como se prevé, por ejemplo, en el RGPD de la Unión Europea.[51]

Esta ley armoniza la definición de tratamiento con la de la LGPDPPSO y lo define como "cualquier operación o conjunto de operaciones efectuadas mediante procedimientos manuales o automatizados aplicados a los datos personales, relacionadas con la obtención, uso, registro, organización, conservación, elaboración, utilización, co-

48. Ley Federal de Protección de Datos Personales en Posesión de los Particulares [L.F.P.D.P.P.P.], Reformada, Diario Oficial de la Federación [D.O.F.], 14 de noviembre de 2025, (México). art. 2 fracción XX.

49. *Ibidem*, art. 2 fracción II.

50. *Ibidem*, art. 2 fracción IV.

51. Reglamento General de Protección de Datos [R.G.P.D.], Parlamento Europeo y Consejo de la Unión Europea, 27 de abril de 2016. art. 9.1.

municación, difusión, almacenamiento, posesión, acceso, manejo, aprovechamiento, divulgación, transferencia o disposición de datos personales". Así, profundiza en su definición en comparación con la ley anterior.

A la definición de transferencia, le agrega que comprende toda comunicación de datos personales "dentro o fuera del territorio mexicano"[52] realizada a persona distinta de la titular, del responsable o de la persona encargada del tratamiento; precisión que ya estaba estipulada en el reglamento de la anterior LFPDPPP.

La ley de sujetos obligados anterior remitía a este ordenamiento para legislar sobre la protección de datos en manos de sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal. Sin embargo, esa redacción fue eliminada de dicha normativa y no está incluida en ninguna de las disposiciones analizadas de la legislación para particulares.

La figura del consentimiento

La ley establece el consentimiento tácito como válido por regla general,[53] tal como en la LGPDPPSO. El consentimiento tácito tiene lugar cuando la persona no se niega al tratamiento de datos, una vez que se le haya dado a conocer el aviso de privacidad.

La ley reconoce que esta regla general no aplica cuando exista obligación de obtener consentimiento expreso. No obstante, sin una lista fehaciente y clara de los datos que son sensibles y con excepciones amplias -de las que se hablará a continuación- se podría esquivar la obtención de consentimientos expresos y reforzar prácticas que dejen a las personas en una posición de vulnerabilidad en donde el "consentimiento tácito" se instrumentalice para procesar datos personales.

Excepciones para la obtención del consentimiento

Esta ley modifica las excepciones para obtener consentimiento de la manera siguiente (el énfasis añadido corresponde a las excepciones agregadas en la ley actual):

Artículo 9. El responsable no estará obligado a recabar el consentimiento de la persona titular para el tratamiento de los datos personales cuando:

I. **Una disposición jurídica así lo disponga;**
II. Los datos personales figuren en fuentes de acceso público;
III. Los datos personales se sometan a un procedimiento previo de disociación;
IV. **Los datos personales se requieran para ejercer un derecho** o cumplir obligaciones derivadas de una relación jurídica entre la persona titular y el responsable;
V. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

52. Ley Federal de Protección de Datos Personales en Posesión de los Particulares [L.F.P.D.P.P.P.], Reformada, Diario Oficial de la Federación [D.O.F.], 14 de noviembre de 2025, (México). art. 2 fracción XX.

53. *Ibidem*, art. 7.

VI. Los datos personales sean indispensables para efectuar un tratamiento para atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, o la gestión de servicios sanitarios, mientras la persona titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o

VII. **Exista una orden judicial, resolución o mandato fundado y motivado** de autoridad competente.

En este sentido, las excepciones agregadas amplían las razones para omitir la obtención del consentimiento por parte de las personas titulares. Es suficiente con que una disposición jurídica permita el tratamiento de datos para que no exista obligación de obtener el consentimiento de las personas titulares de los datos, sin que se tenga que tratar de una ley. Otras excepciones, como que una empresa argumente que está "ejerciendo un derecho", sin desarrollar al respecto, o un "mandato" sin que este provenga de una resolución formal.

Adicionalmente, la ley actual mantiene las causales para transferir datos nacional e internacionalmente sin el consentimiento de la persona titular de la siguiente manera:

Artículo 36. Las transferencias nacionales o internacionales de datos podrán llevarse a cabo sin el consentimiento de la persona titular cuando se ubiquen en alguno de los supuestos siguientes:

I. La transferencia esté prevista en una Ley o Tratado en los que México sea parte;

II. La transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;

III. La transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;

IV. La transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés de la persona titular, por el responsable y un tercero;

V. La transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;

VI. La transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y VII. La transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y la persona titular.

Derechos ARCO

La ley modifica los requisitos de forma para presentar solicitudes para ejercer estos derechos. Por ejemplo, el titular debe describir "el derecho ARCO que se pretende ejercer, o bien, lo que solicita".[54]

Por otro lado, no obliga al responsable a que informe en el aviso de privacidad simplificado -que es el primero que recibe la persona en muchos contextos- sobre los medios, mecanismos y procedimientos para ejercer derechos ARCO.[55] En términos del principio de información, esto genera un problema pues hay muchas personas que no saben que tienen la posibilidad de disponer de sus datos personales una vez que los han entregado.

En suma, retoma disposiciones de la LGPDPPSO y especifica las causas para que la persona titular pueda ejercer su derecho de oposición. Sin embargo, esto puede incrementar la carga al titular, quien tiene que justificar la procedencia de esta oposición.

Derecho de Acceso

Además de la posibilidad de acceder a los datos personales, la ley considera el derecho a conocer las condiciones y generalidades del tratamiento a través del aviso de privacidad como parte del derecho de acceso.[56] A diferencia de los otros derechos ARCO, no es necesario que la persona haga una descripción clara y precisa de lo que solicita cuando busque ejercer el derecho de acceso.[57]

Derecho de Rectificación

La rectificación o corrección de los datos personales puede ser solicitada no solo cuando sean inexactos o estén incompletos, como estipulaba la ley anterior. También cuando no se encuentren actualizados.[58]

Derecho de Cancelación

La ley contempla que "cuando los datos personales hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas en el aviso de privacidad y que motivaron su tratamiento conforme a las disposiciones legales aplicables, deberán ser suprimidos previo bloqueo, en su caso, y una vez que concluya el plazo de conservación de los mismos."[59]

54. *Ibidem*, art. 28.

55. *Ibidem*, art. 16 fracción II.

56. *Ibidem*, art. 22.

57. *Ibidem*, art. 28 fracción III.

58. *Ibidem*, art. 23.

59. *Ibidem*, art. 10.

De esta forma, establece que los datos podrán ser cancelados después de haber cumplido el bloqueo (en su caso) y el "plazo de conservación". En este sentido, se pierden oportunidades para establecer obligaciones y plazos claros para las entidades privadas en torno a los periodos de conservación antes de suprimir los datos personales.

Derecho de Oposición

Como ya se mencionó, introduce las mismas causas para ejercer el derecho de oposición al tratamiento de datos existentes en la ley de sujetos obligados. Estas causas se concretan cuando:[60]

I. Exista causa legítima y su situación específica así lo requiera, lo cual debe justificar que aun siendo lícito el tratamiento, el mismo debe cesar para evitar que su persistencia le cause un daño o perjuicio, o

II. Sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales de la misma o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento.

No procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación legal impuesta al responsable.

Si bien podría considerarse que existe un avance con esta adición, esto puede representar cargas adicionales para las personas titulares, quienes deberán justificar su derecho de oposición. Además, el último párrafo debilita estas disposiciones al establecer que no procederá el ejercicio del derecho de oposición si el tratamiento es necesario para el cumplimiento de una obligación legal impuesta al responsable, por lo que cualquier mandato legal podría ser aplicado en contravención de este derecho.

Rendición de cuentas

La SABG hereda las facultades del extinto INAI en el derecho a la protección de datos personales. Esta centralización ha sido interpretada como un retroceso, al perder a un organismo autónomo especializado.[61]

60. *Ibidem*, art. 26.

61. R3D: Red en Defensa de los Derechos Digitales. (21 de marzo de 2025). *Las nuevas leyes de transparencia y protección de datos personales: retrocesos y oportunidades perdidas.* https://r3d.mx/2025/03/21/las-nuevas-leyes-de-transparencia-y-proteccion-de-datos-personales-retrocesos-y-oportunidades-perdidas/

La ley genera dudas sobre la rendición de cuentas de la SABG, ya que elimina su obligación de presentar informes al Congreso de la Unión.[62] Esta es una práctica que el INAI realizaba de manera anual, donde proporcionaba datos respecto a su labor.[63] Eliminar esta obligación puede implicar que no exista una supervisión clara sobre sus acciones, lo que puede fomentar la opacidad.

Al igual que la ley anterior, la actual no establece la obligación de realizar Evaluaciones de Impacto en la Protección de Datos Personales (EIPDP) para los particulares. Solo establece, sin mayor desarrollo, la facultad de la SABG de elaborar estudios de impacto sobre la privacidad, sin un desarrollo específico sobre este mecanismo.[64] De esta manera, se pierde la oportunidad de clarificar la existencia de la EIPDP de los particulares con obligaciones y una deliberación del proceso específica.

El creciente tratamiento masivo de datos personales y modelos de negocio basados en estas prácticas hacen necesario que este tipo de evaluaciones sean incorporadas de manera clara. Por ejemplo, al resolver sobre la EIPDP[65] del FAN ID utilizado por la Federación Mexicana de Fútbol, se aplicaron disposiciones diseñadas para sujetos obligados porque no existían regulaciones específicas para el sector privado,[66] lo cual generó controversias e irregularidades.[67]

Medios de impugnación

Los procedimientos de protección de derechos, de verificación y de imposición de sanciones son esencialmente los mismos que en la legislación anterior para particulares, conforme a la estructura de la SABG detallada en el apartado del Reglamento Interior de este informe. Al respecto, es necesario enfatizar que a diferencia del extinto INAI, la SABG no es un cuerpo colegiado y no es un órgano autónomo. Por ello, aunque los procedimientos se mantienen, la estructura y los criterios para resolver tenderán a ser diferentes.

62. Ley Federal de Protección de Datos Personales en Posesión de los Particulares [L.F.P.D.P.P.P.], Reformada, Diario Oficial de la Federación [D.O.F.], 14 de noviembre de 2025, (México). art. 39 fracción VIII: "El Instituto tiene las siguientes atribuciones: (...) VIII. Rendir al Congreso de la Unión un informe anual de sus actividades".
63. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2024). Informe de Labores 2024. https://gaceta.diputados.gob.mx/PDF/66/2025/feb/Inai_2024-20250201.pdf
64. Ley Federal de Protección de Datos Personales en Posesión de los Particulares [L.F.P.D.P.P.P.], Reformada, Diario Oficial de la Federación [D.O.F.], 14 de noviembre de 2025, (México). art. 39 fracción IX.
65. Evaluación de Impacto en la Protección de Datos Personales.
66. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, 17 de agosto de 2022, (México). Comunicado INAI/248/22: INAI emite opinión técnica sobre el documento que presentaron la FMF y la Liga Mx ante uso de sistema Fan ID en estadios. https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-248-22.pdf
67. R3D: Red en Defensa de los Derechos Digitales. (21 de marzo de 2025). *Las nuevas leyes de transparencia y protección de datos personales: retrocesos y oportunidades perdidas.* https://r3d.mx/2025/03/21/las-nuevas-leyes-de-transparencia-y-proteccion-de-datos-personales-retrocesos-y-oportunidades-perdidas/

Los jueces y tribunales especializados en materia de protección de datos resolverán los juicios de amparo en contra de las resoluciones de la SABG, al igual que en la LGPDPPSO.

Es necesario destacar que al momento de la redacción de este informe, no hay un reglamento de la nueva LFPDPPP. Será necesario realizar el análisis pertinente cuando el mismo sea expedido.

Paquete de leyes que amplían facultades de vigilancia

En julio de 2025, el Poder Legislativo aprobó en periodo extraordinario un paquete de leyes que, en su conjunto, establecen medidas de vigilancia masiva sin controles. Con el apoyo de la mayoría necesaria en el Congreso de la Unión, estas leyes fueron promulgadas el 16 de julio de 2025 en el DOF.[68]

Estas leyes implican obligaciones para las empresas, facultades para autoridades en materia de seguridad e inteligencia y la obligación de las personas de entregar sus datos personales incompatibles con los derechos a la privacidad, la libertad de expresión, la presunción de inocencia, la no discriminación y el principio de presunción de inocencia.

Al mismo tiempo, este paquete legislativo afecta al conjunto de obligaciones y deberes del sector privado, en particular de las empresas de telecomunicaciones, las plataformas digitales y otras que tienen información relevante para "asuntos de inteligencia". De esta forma, dicho paquete legislativo crea una carga regulatoria sin los controles y límites necesarios, lo que genera incertidumbre jurídica para las empresas y riesgos para las personas.

Ley en Materia de Telecomunicaciones y Radiodifusión

En mayo de 2025, la Ley de Telecomunicaciones llamó la atención de la discusión pública debido a las disposiciones que figuraban en el primer borrador, que conferían a la Agencia de Transformación Digital amplios poderes para bloquear plataformas digitales (artículo 109 de dicha iniciativa), lo que constituía una violación de la prohibición de la censura previa establecida en el artículo 7 de la CPEUM. Este artículo fue eliminado posteriormente en el borrador final; sin embargo, la versión aprobada mantuvo otras cuestiones problemáticas.

Esta ley mantuvo las obligaciones promulgadas desde 2014 que obligaban a las empresas de telecomunicaciones a conservar durante un máximo de dos años los metadatos de todas las líneas móviles, con posibilidad de acceso a una serie de autoridades sin una definición clara sobre el requisito de la orden judicial (artículos 182 y 183 de la antigua ley). Este capítulo también regula el acceso de diversas autoridades a la geolocalización en tiempo real de los dispositivos móviles de cualquier persona.

68. Disponible en: https://www.dof.gob.mx/index_113.php?year=2025&month=07&day=16#gsc.tab=0

Aunque estas disposiciones están vigentes desde 2014, ha sido ampliamente demostrado que las autoridades han abusado de los supuestos controles y protecciones establecidos para acceder a los metadatos y la información de geolocalización.

Por ejemplo, los fiscales locales y federales eludieron el requisito de la autorización judicial, ya sea solicitándola directamente a las empresas de telecomunicaciones -en muchos casos, por parte de diferentes autoridades que no estaban reconocidas por la ley para hacerlo- o mediante un mecanismo excepcional contenido en el artículo 303 del Código Nacional de Procedimientos Penales, que les permitía obtener acceso inmediato a los metadatos y a la geolocalización en tiempo real antes de obtener una orden judicial. También se documentó que las autoridades utilizaron esta información para acosar, vigilar y acechar a defensores de los derechos humanos, periodistas y adversarios políticos.[69]

Además, el artículo 103 de la Ley de Telecomunicaciones establece que las empresas de telecomunicaciones deben mantener un registro de todas las líneas telefónicas asociadas a la identidad de su propietario, utilizando una identificación biométrica (CURP biométrica). Si alguna persona decide no asociar su identidad a su línea, las empresas estarán obligadas a bloquearla y a dejar de prestar cualquier servicio relacionado con ella.

Las directrices del registro aún deben ser establecidas por el nuevo órgano rector, la Comisión Reguladora de Telecomunicaciones, que sustituirá a la antigua agencia reguladora autónoma, el Instituto Federal de Telecomunicaciones. La ley establece como fecha límite enero de 2026 para que estas directrices se publiquen y se comuniquen a las empresas de telecomunicaciones, y la cancelación de las líneas no registradas debe realizarse antes de mayo de 2026.

De esta forma, se aumenta la carga a las empresas y los riesgos e impactos sobre los derechos humanos se encuentran ahora dispersos en este paquete de leyes.

Ley General de Población y Ley General en Materia de Desaparición Forzada

La Ley General de Población establece una identificación biométrica obligatoria. La ley establece que esta identificación será requerida para acceder a todo servicio público o privado,[70] bajo pena de sanciones económicas.[71]

La Ley en Materia de Desaparición Forzada crea la Plataforma Única de Identidad, que recopilará y consolidará toda la información generada por el uso de la identifica-

69. García, L. F., Gaitán, A., Flores, J., Narváez, S., Trnka, M. (enero de 2025). *El Estado de la Vigilancia.* https://r3d.mx/wp-content/uploads/Edo_Vigilancia_DIGITAL.pdf pp. 49-53.

70. Ley General de Población [L.G.P.], Reformada, Diario Oficial de la Federación [D.O.F.], 16 de julio de 2025, (México). art. 91 BIS y 91 Sexies.

71. *Ibidem*, art. 114 BIS, de 10 000 a 20 000 UMA.

ción biométrica,[72] tal y como se describe en la Ley General de Población. Dado que todas las actividades cotidianas requerirán una identificación biométrica, todas las actividades se recopilarán en esta plataforma.

Estas leyes crean una medida desproporcionada que normaliza la vigilancia masiva. Tal y como establece la ley, obligará a todas las empresas que presten servicios o den acceso a bienes a desarrollar sistemas para registrar todas las transacciones, conservar esos datos y compartirlos con diversas autoridades en el formato que estas requieran (de acuerdo con la Ley de Inteligencia, como se explica en el siguiente apartado). Aunque estas leyes se defendieron como parte de una estrategia para localizar a personas desaparecidas, las facultades conferidas rebasan este propósito.

Ley del Sistema Nacional de Investigación e Inteligencia, Ley del Sistema Nacional de Inteligencia y la Plataforma Central de Inteligencia

Estas leyes establecen el acceso, la interconexión y la transferencia de todas las bases de datos públicas y privadas de cualquier entidad pública o privada a autoridades policiales y de inteligencia.

La Ley de Inteligencia crea la Plataforma Central de Inteligencia; una base de datos centralizada que interconectará todas las bases de datos públicas y privadas[73] para que puedan ser consultadas en tiempo real por todas las autoridades facultadas por la ley.[74] También estará conectada al Sistema Nacional de Información[75] y a la Plataforma Única de Identidad creada por la Ley de Personas Desaparecidas[76], obteniendo así todos los datos resultantes del uso obligatorio de la identificación biométrica.

Toda la información relacionada con este sistema de inteligencia será confidencial y reservada, y se podrán imponer sanciones incluso a quienes la compartan,[77] superando principios constitucionales como el interés público, la transparencia, la rendición de cuentas y la publicidad.

La ley también establece que cualquier empresa que cuente con bases de datos personales debe brindar acceso a los datos o facilitar información a las autoridades sobre diversos registros, como datos sobre vehículos, matrículas, datos biométricos, datos telefónicos, registros de la propiedad, registros fiscales, registros de armas, servicios financieros, servicios bancarios, datos sobre transporte, datos sobre salud, datos so-

72. Ley General en Materia de Desaparición Forzada de Personas, Desaparición Cometida por Particulares y del Sistema Nacional de Búsqueda de Personas [L.G.M.D.F.P.], Reformada, Diario Oficial de la Federación [D.O.F.], 16 de julio de 2025, (México). art. 12.

73. Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública [L.S.N.I.I.M.S.P.], Diario Oficial de la Federación [D.O.F.], 16 de julio de 2025, (México). art. 24 y 30.

74. *Ibidem*, arts. 36-38.

75. *Ibidem*, art. 27.

76. *Ibidem*, art. 28.

77. *Ibidem*, arts. 1 y 51.

bre telecomunicaciones, datos comerciales, datos corporativos y cualquier otro que se considere necesario para la elaboración de "productos de inteligencia".[78]

Para cumplir con estas obligaciones, las empresas deben proporcionar los datos, ya sea mediante acuerdos de colaboración con las autoridades para interconectar sus bases de datos o respondiendo a solicitudes obligatorias.[79]

Estas obligaciones de solicitud de datos incluirán a las empresas internacionales y, en algunos casos, a las empresas locales, que estarán obligadas a proporcionar información a organismos o gobiernos extranjeros, pues la Ley de Inteligencia tiene alcance internacional en los casos de cooperación entre las autoridades mexicanas y otros gobiernos, organismos o empresas.[80]

Además, la información podría ser solicitada y proporcionada por el Ejército mexicano. El paquete legislativo también reformó la Ley General de la Administración Pública Federal para otorgar a la Secretaría de la Defensa Nacional la amplia facultad de realizar actividades de inteligencia con fines de seguridad nacional.[81]

En suma, la Ley de la Guardia Nacional consolida la colocación de la Guardia Nacional bajo el mando del ejército mexicano y le otorga acceso a la Plataforma Central de Inteligencia.[82] La Ley de la Guardia Nacional también fue modificada de manera ambigua para eliminar los requisitos impuestos a la Guardia Nacional para obtener autorización judicial para acceder a los metadatos y la geolocalización de los dispositivos móviles.[83]

Este paquete constituye un sistema de vigilancia masiva, donde autoridades civiles y militares podrán acceder a datos sensibles, como los lugares en los que se encuentran las personas, con quién se reúnen o hablan, y todas sus actividades diarias. Estas medidas representan herramientas para ejercer presión sobre las personas, crean un entorno hostil que inhibe la expresión de críticas políticas y la disidencia y propician el control.

78. *Ibidem*, art. 24.

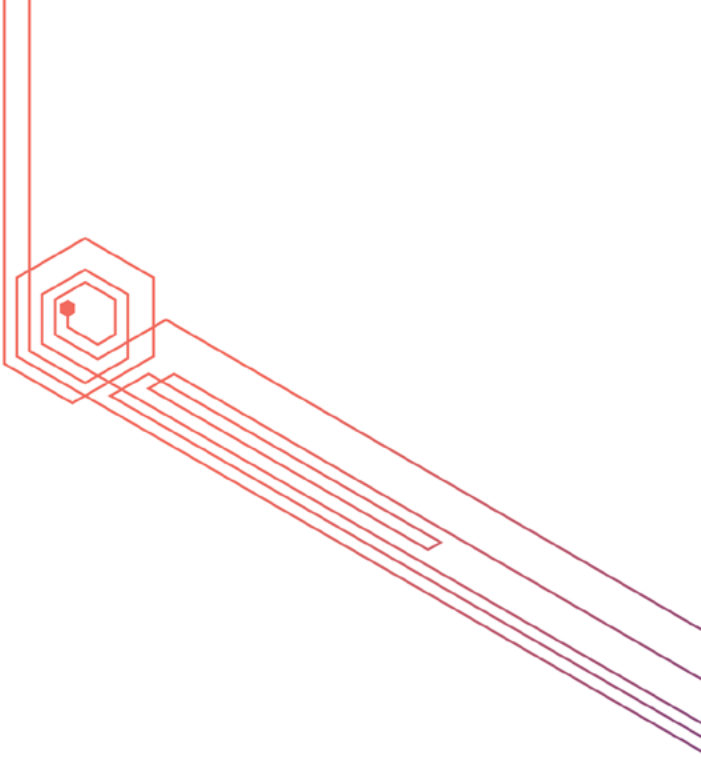
79. *Ibidem*, art. 30.

80. *Ibidem*, art. 39, C, iii.

81. Ley Orgánica de la Administración Pública Federal [L.O.A.P.F.], Reformada, Diario Oficial de la Federación [D.O.F.], 16 de julio de 2025, (México). art. 29.

82. Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública [L.S.N.I.I.M.S.P.], Diario Oficial de la Federación [D.O.F.], 16 de julio de 2025, (México). art. 44.

83. Ley de la Guardia Nacional [L.G.N.], Diario Oficial de la Federación [D.O.F.], 16 de julio de 2025, (México). art. 9, párrafo XXVI.



Diagnóstico y principios

Este informe ha proporcionado las bases para comprender el derecho a la privacidad y el derecho a la protección de datos personales en México y a nivel interamericano. Igualmente, ha desempacado las leyes vigentes en México en este ámbito, tanto las que están vinculadas directamente a datos personales, como las que guardan relación con este tema por las medidas que implican.

Las resoluciones judiciales analizadas en este documento brindan un parámetro para la dirección que debemos tomar en materia de protección de datos personales. Al mismo tiempo, las reformas recientes nos muestran un panorama nuevo, en el que establecer principios mínimos resulta retador, pero también necesario.

En conclusión, el presente análisis arroja el siguiente diagnóstico:

I. Marco constitucional y convencional

- **Reconocimiento de Derechos:** La CPEUM reconoce el **derecho a la privacidad y la protección de datos personales**, incluyendo el derecho a la **autodeterminación informativa** (control sobre la información personal). La **intimidad** (que incluye la protección de datos sensibles) requiere garantías reforzadas.
- **Invalidez del PANAUT:** La SCJN declaró inconstitucional el Padrón Nacional de Usuarios de Telefonía Móvil (PANAUT) por generar una **afectación intensa y desproporcionada** a la privacidad y la autodeterminación informativa. En la sentencia respectiva, argumentó que el consentimiento era nulo por ser obligatorio y que existían medidas menos restrictivas.
- **Estándares en actividades de inteligencia que implican el tratamiento de información personal:** La Corte IDH establece que el derecho a la autodeterminación informativa, en el contexto de actividades de inteligencia, es un **derecho autónomo y exigible** que se materializa mediante el control que la persona ejerce sobre su información personal en manos de las autoridades públicas. Este derecho se materializa cuando la persona ejerce **control sobre su información**. Las actividades de inteligencia, al implicar una injerencia en la vida privada, deben contar con **control judicial obligatorio** y deben estar previstas en ley con controles específicos y cumplir con la **prueba de proporcionalidad** (perseguir un fin legítimo, ser idóneas, necesarias y proporcionales). La ausencia de control judicial hace estas acciones incompatibles con la CADH.
- **Desmantelamiento de Órganos Garantes (2024):** La reforma de simplificación orgánica de diciembre de 2024 eliminó el INAI a nivel constitucional. Esto se considera un retroceso por la pérdida de autonomía y especialización.
- **Debilitamiento judicial:** La **reforma judicial de 2024** eliminó las salas especializadas de la SCJN y limitó los **efectos generales de los amparos** contra normas. Esto afecta la protección de datos al reducir la posibilidad de beneficiar a terceros y puede causar rezago y falta de especialización.

II. Nuevo esquema de autoridades y leyes

- **Centralización de la Autoridad:** Las nuevas leyes de protección de datos de marzo de 2025 formalizan que la SABG herede las atribuciones del extinto INAI. Se crea la Agencia de Transformación Digital y Telecomunicaciones (ATDT) con facultades para la identidad digital y gestión de bases de datos centralizadas.
- **Amplitud en excepciones y consentimiento tácito:** Las nuevas leyes mantienen el **consentimiento tácito** como regla general (excepto para datos sensibles) y conservan **amplias excepciones** para el tratamiento y transferencia de datos sin consentimiento (por ejemplo, cuando una ley lo disponga o por orden/mandato de autoridad competente), lo que genera **vulnerabilidad** para los titulares de los datos personales.
- **Ausencia de Evaluación de Impacto obligatoria:** La ley **no establece la obligación** para los particulares de realizar Evaluaciones de Impacto en la Protección de Datos Personales (**EIPDP**). Se pierde oportunidad para regular el creciente tratamiento masivo de datos y los modelos de negocio basados en ellos.

III. Riesgos de vigilancia masiva (Paquete de leyes de julio 2025)

- **Geolocalización:** La nueva Ley de Telecomunicaciones mantiene la obligación para las empresas de conservar metadatos y facilita el **acceso a la geolocalización en tiempo real** de dispositivos móviles a diversas autoridades, sin controles judiciales efectivos que eviten abusos.
- **Identificación Biométrica Obligatoria:** La Ley General de Población y la Ley en Materia de Desaparición Forzada establecen la **identificación biométrica obligatoria (CURP biométrica)** para acceder a servicios públicos y privados. Junto con la Plataforma Única de Identidad, crea un sistema que **normaliza la vigilancia masiva** de las personas, sin controles ni justificación.
- **Plataforma Central de Inteligencia:** La nueva Ley de Inteligencia crea una Plataforma Central de Inteligencia que obligará a **interconectar bases de datos públicas y privadas** (incluyendo datos sensibles como los financieros, de salud, y biométricos) para consulta en tiempo real por autoridades policiales y de inteligencia (incluyendo el Ejército). Esto institucionaliza la vigilancia masiva con información clasificada como confidencial.

Con base en este diagnóstico, la legislación aplicable a la protección de datos puede ser reformada para combatir las áreas de oportunidad y brindar las garantías efectivas en un mundo digitalizado de la siguiente manera:

I. Fortalecimiento Institucional

- **Restaurar la autonomía de los Órganos Garantes:** Se recomienda **restaurar o fortalecer un órgano garante autónomo y especializado (como el INAI)**, evitando la centralización en un órgano del Poder Ejecutivo para protegerlo de posibles presiones políticas.

- **Garantizar la colegialidad de órgano encargado de protección de datos:** Es crucial **asegurar la toma de decisiones colegiada y plural** en el órgano encargado de la protección de datos. Esto impulsaría debates profundos y contrapesos internos.
- **Establecer requisitos para jueces:** Es necesario **establecer requisitos mínimos de elegibilidad y especialización** para los jueces encargados de resolver controversias en materia de datos personales, a fin de garantizar la calidad de las resoluciones.

II. Oportunidades para reforzar la protección de datos personales

- **Aplicabilidad extraterritorial:** Establecer la **aplicabilidad extraterritorial de las leyes de protección de datos personales** mexicanas. Esto implica que la legislación debe aplicarse a cualquier entidad o persona que trate datos de personas en México, sin importar su domicilio legal ni la ubicación física desde la cual se realice el tratamiento, a fin de brindar protección incluso cuando sus datos sean procesados por responsables establecidos en el extranjero.
- **Garantizar la autodeterminación informativa:** El Estado debe reconocer el principio de la autodeterminación informativa como parte del derecho a la protección de datos personales, como lo ha interpretado la SCJN y la Corte IDH. La autodeterminación informativa debe garantizarse a través de lo siguiente:
    1) Medidas de supervisión robustas, por parte de autoridades independientes que reconozcan el derecho de acción legal directa por parte de las personas titulares de datos personales.
    2) Derechos ARCO obligatorios, sin posibilidad de excepciones y sin cargas innecesarias para la persona titular.
    3) Aviso de privacidad simple con opciones de opt out.
    4) Reducir el alcance de las excepciones para obtener consentimiento en el tratamiento de datos personales.
    5) Principio de minimización de datos obligatorios.
- **Abordar el consentimiento obligatorio:** Se recomienda **incluir disposiciones que eviten el aprovechamiento de las excepciones al consentimiento.** Además, es necesario erradicar cualquier práctica en la que la entrega de datos no esenciales sea una condición obligatoria para acceder a un servicio.
- **Revertir el modelo de consentimiento tácito:** Se debe revertir este modelo para evitar abusos en el tratamiento de datos personales. Para ello, es necesario establecer obligaciones que establezcan la forma en que se procesarán sus datos, en formatos susceptibles de comprensión, así como los mecanismos para ejercer los derechos ARCO. Tal como han reconocido la SCJN y la CIDH, el consentimiento no configura un elemento relevante cuando se obliga a otorgar el mismo para acceder a un servicio. Para que exista un consentimiento real deben cumplirse 3 requisitos:
    1) Acceso a la política de privacidad del servicio de una manera simplificada y entendible para la persona usuaria.

2) Que exista una acción activa de consentimiento por parte de la persona usuaria; es decir, que su silencio no se entienda como un consentimiento tácito que autorice el tratamiento de datos.
3) Brinde la opción de negarse a tratar datos personales no esenciales para la prestación del servicio.

- **Clasificar datos biométricos como datos sensibles:** Es crucial **catalogar expresamente los datos biométricos para fines de identificación como datos sensibles** en ambas leyes, para otorgarles una protección reforzada.
- **Limitar la Vaguedad de las Excepciones:** Se debe **limitar o acotar la redacción de excepciones vagas** para el tratamiento sin consentimiento (por ejemplo, cuando "una disposición jurídica así lo disponga" o "salvaguarda de un interés público") para evitar justificaciones arbitrarias.

III. Oportunidades de Mecanismos Preventivos y Judiciales

- **Obligar a EIPDP para particulares:** Se debe **establecer la obligación de realizar Evaluaciones de Impacto en la Protección de Datos Personales (EIPDP)** para el sector privado en la LFPDPPP ante el tratamiento masivo de datos.
- **Mejorar disposiciones existentes para la EIPDP de sujetos obligados:** Las disposiciones existentes sobre la EIPDP deberían **revisarse, evaluarse, auditarse, actualizarse y mejorarse periódicamente.** Estas evaluaciones deben **justificar la proporcionalidad de la medida sujeta a evaluación** a través de las escalas de finalidad legítima, idoneidad, necesidad, proporcionalidad de la medida. En suma, es necesario establecer medidas que sancionen efectivamente las vulneraciones de datos personales.
- **Establecer plazos de conservación claros:** Es necesario establecer **plazos de conservación proporcionales** para los datos en el sector privado, a fin de limitar la discrecionalidad.
- **Revertir la posibilidad de otorgar amparos con efectos generales:** Es necesario **revertir la posibilidad de otorgar efectos generales a las suspensiones y amparos contra normas**, especialmente en un contexto de digitalización de trámites, de facultades de autoridades públicas en el tratamiento de datos y de modelos de negocio basados en ello.
- **Incluir la Portabilidad en Derechos ARCO:** Se recomienda **integrar formalmente el derecho a la Portabilidad** entre los derechos ARCO para reforzar el control del titular sobre sus datos personales.

IV. Oportunidades para contener la vigilancia masiva

- **Revocar disposiciones que facilitan la vigilancia masiva:** Se debe **derogar o someter a un estricto control judicial las disposiciones** del paquete de leyes de julio de 2025 respecto a la conservación de metadatos y el acceso a la geolocalización en tiempo real (Ley de Telecomunicaciones), accesos irrestrictos de la Plataforma Central de Inteligencia e interconexiones obligatorias (Ley de Inteligencia), rastreos en tiempo real sin controles y condicionamiento de CURP biométrica para acceso a servicios (reformas

en materia de desaparición), facultades amplias en materia de inteligencia para actividades de inteligencia con fines de seguridad nacional (Ley Orgánica), así como robustecer requisitos para el control judicial.

- **Abordar el tratamiento automatizado de datos: Establecer controles y salvaguardas claros y específicos** para el uso de algoritmos en decisiones que afecten a las personas.
- **Prohibir la interconexión obligatoria de datos personales sin controles:** Es necesario **prohibir la interconexión obligatoria** de bases de datos públicas y privadas (fiscales, de salud, financieras) en plataformas de inteligencia.
- **Establecer control judicial obligatorio para actividades de inteligencia que impliquen acceso a datos personales:** La Ley de Inteligencia debe **exigir control y autorización judicial** para el acceso a datos en la Plataforma Central de Inteligencia y la Plataforma Única de Identidad.
- **Fijar controles de temporalidad y destrucción: Fijar controles y límites estrictos de temporalidad** para la conservación de datos en manos de autoridades y particulares para evitar archivos permanentes y el abuso de la información personal.



De la Ley al Principio

Desempaque normativo y principios para la protección de datos en México

R3D: Red en Defensa de los Derechos Digitales
Escrito por: Francia Pietrasanta
Editado por: José Flores
Portada e interiores: Gibrán Aquino

Diciembre de 2025

R3D
Red en Defensa
de los Derechos Digitales

Brot
für die Welt



R3D
Red en Defensa
de los Derechos Digitales

Brot
für die Welt