Privacidad en la era digital.

Desafíos jurídicos y éticos de la protección de datos personales.

Privacidad en la era digital.

Desafíos jurídicos y éticos de la protección de datos personales.

Diciembre 2025

INSTITUTO CHIHUAHUENSE PARA
LA TRANSPARENCIA Y ACCESO
A LA INFORMACIÓN PÚBLICA

Privacidad en la era digital.
Desafíos jurídicos y éticos de la protección de datos personales.

Dr. Sergio Rafael Facio Guzmán
Comisionado Presidente del ICHITAIP

Lic. Karla Gabriela Fuentes Moreno
Comisionada del ICHITAIP

Mtra. María Selene Prieto Domínguez
Comisionada del ICHITAIP

Primera edición, 2025
216 p.; 160 x 215 mm.
ISBN: 978-970-96916-7-2

Coordinador del libro: Saúl Ulises García Meza
Revisión editorial: Joel Amaya Gardea
Diseño editorial: Pamela Sarahí Flores Guillén

Índice

Agradecimiento

Promover la cultura y difusión de la protección de datos personales ha sido uno de los trabajos más trascendentales que ha encabezado el Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública (Ichitaip), y este libro es solo uno de los tantos resultados que quedarán de manifiesto.

Para llevar a cabo la presente obra se extiende el agradecimiento al comisionado y comisionadas del Ichitaip Sergio Rafael Facio Guzmán, Karla Gabriela Fuentes Moreno y María Selene Prieto Domínguez, por el empeño y trabajo para hacer posible este texto, así como a los autores, que al igual que ellos, participaron con la redacción de los capítulos que lo integran, por el tiempo dedicado a la investigación y análisis del derecho a la protección de datos personales.

Es además la segunda obra que el Instituto publica a lo largo del presente año, con la invitación y colaboración de especialistas en acceso a la información pública y protección de datos personales, académicos y periodistas, mismos que se añaden al trabajo editorial y de divulgación que se ha realizado desde la creación de este organismo constitucional autónomo.

Este año salieron a la luz los títulos *Reflexiones finales, ¿qué sigue con el acceso a la información pública? La encrucijada del derecho a saber* y *Privacidad en la era digital*. Desafíos jurídicos y éticos de la protección de datos personales en un esfuerzo editorial con el propósito de llegar a más población y presentar no solo los avances en la materia, sino también las amenazas que aún persisten en contra del derecho al acceso a la información pública y a la protección de datos personales.

Uno de los principales objetivos en los trabajos de análisis e investigación es poner mayores elementos de textos de consulta, tanto para estudiantes, académicos, especialistas y de toda la ciudadanía en general. En esta última, en caso concreto, se busca sembrar y desarrollar el interés de este derecho, el de la protección de sus datos personales.

La privacidad es tan colectiva como personal. Esta afirmación es tan breve como definitiva, y a veces la falta de privacidad puede parecer inevitable, pero no siempre lo es.

Lic. Saúl Ulises García Meza

1. Protección de datos personales e inteligencia artificial

Dr. Sergio Rafael Facio Guzmán

Introducción

En recientes años, para ser más exactos al principio del 2020, vivimos una situación mundial inusitada, ya que cuando menos habían pasado cien años desde una emergencia similar de salubridad en todo el planeta a causa de un virus que trajo, entre muchas cosas negativas, un aspecto distinto. Ya nos tocará decidir desde la perspectiva personal si fue positivo o negativo.

Todo lo anterior sucedió respecto a las posibilidades de interconexión remota de manera inmediata y desde nuestro ordenador o inclusive nuestro dispositivo móvil, ya sea para cumplir con nuestros trabajos, clases, obligaciones y hasta por simple convivencia a la distancia. Debido a lo anterior, muchos especialistas consideran que se dio un salto tecnológico de al menos 10 años sin estar preparados para hacer frente a los riesgos informáticos que ello conllevaría. Me refiero a la protección de nuestros datos personales, lo que inmediatamente abordó también una situación interesante sobre un tipo de inteligencia que si bien desde 1956 ya se usaba ese término, aumentó su aplicación a la par de ese salto tecnológico en materia de informática, de aplicaciones y de nuevos tipos de programas para el uso de la inteligencia artificial.

Este tema de la inteligencia artificial por sí solo es muy amplio, pero ante los tiempos que estamos viviendo en México, donde parece que no hay interés en avanzar antes de que sea demasiado

tarde y suframos afectaciones en nuestro entorno personal, es que debemos abordarlo desde una perspectiva académica con énfasis en la interacción que tiene el uso de nuestros datos personales ante ambientes de inteligencia artificial, por lo que debemos refrendar la importancia de la protección de datos personales. Allí radica el que hoy abordemos tan importante tema.

En sí la inteligencia artificial (IA) representa una de las tecnologías más innovadoras y transformadoras de este siglo, influyendo en prácticamente todos los sectores económicos, industrias y aspectos cotidianos de la sociedad. Este informe tiene como objetivo ofrecer una explicación detallada, estructurada y actualizada de la IA, abarcando desde sus definiciones técnicas, evolución histórica y principales ramas hasta sus aplicaciones más innovadoras, los desafíos ético-sociales y el impacto en nuestra vida diaria y laboral.

Y ya que nos encontramos ante el panorama de un campo de la ciencia relacionado con la creación de computadoras y máquinas que pueden razonar, aprender y actuar, la pregunta es: ¿ante quién tenemos que hacer valer la protección de nuestros datos personales?

Inteligencia artificial

La inteligencia artificial es un campo interdisciplinario que integra ciencias exactas, sociales y aplicadas, abarcando desde el diseño de algoritmos, *software* y *hardware* en la informática e ingeniería, hasta el desarrollo de la lingüística, la neurociencia e incluso la filosofía, la psicología y la ética.

Además de esto, debemos abordar la inteligencia artificial desde la articulación con áreas específicas que han dado forma a su

desarrollo contemporáneo, siendo estas según Russell & Norvig (2021):

Procesamiento del Lenguaje Natural (PLN): Permite que las máquinas comprendan y generen lenguaje humano, aplicándose en traducción automática, *chatbots* y análisis semántico.

Visión por computadora: Se centra en que los sistemas reconozcan e interpreten imágenes y videos, con aplicaciones en seguridad, medicina y vehículos autónomos.

Robótica: Integra *hardware* y *software* para crear sistemas capaces de interactuar físicamente con el entorno, desde robots industriales hasta humanoides.

Aprendizaje automático *(machine learning)*: Núcleo de la IA moderna, donde algoritmos aprenden patrones a partir de datos para realizar predicciones o clasificaciones.

Redes neuronales artificiales: Inspiradas en la neurociencia, permiten modelar procesos de aprendizaje y reconocimiento complejo, como el reconocimiento de voz o imágenes.

> La inteligencia artificial es un campo de la ciencia relacionado con la creación de computadoras y máquinas que pueden razonar, aprender y actuar de una manera que normalmente requeriría inteligencia humana o que involucra datos cuya escala excede lo que los humanos pueden analizar. (Google Cloud, s. f.)

Para comprender mejor la inteligencia artificial y lo que representa, es necesario regresarnos a las primeras manifestaciones sobre su significado o referencia próxima, y esto nos remonta al

verano de 1956, cuando el matemático estadounidense John McCarthy, reconocido como el creador del término inteligencia artificial, reunió en la universidad privada Dartmouth College a los principales investigadores del campo de la informática y la psicología cognitiva para poner en común los potenciales avances y aplicaciones de este nuevo ámbito de investigación. De aquella cita quedaría en el recuerdo de todos los asistentes un ambicioso y aventurado pronóstico del investigador del Carnegie Mellon University Herbert Simon (1960): "En 20 años las máquinas serán capaces de llevar a cabo cualquier tipo de trabajo que un hombre pueda hacer".

Pasaron más de cinco décadas, pero ya hoy nadie puede negar que la inteligencia artificial es un componente esencial y originador de la nueva era digital en la que la capacidad técnica y desarrollo de algoritmos de las máquinas sobrepasa por mucho a la de los humanos.

En este momento nos encontramos entre dos modelos: el analógico y el nuevo paradigma digital. El primero se entiende como ya obsoleto o en camino a serlo antes de finalizar esta década, y el segundo que es encabezado por tecnologías como la inteligencia artificial, el análisis de datos o el 6G, que cada día plantean nuevos desafíos que debemos abordar desde una óptica con mayor ética y preguntas basadas en una filosofía de lo esencialmente humano que debe considerarse en este mundo tan cambiado por los avances tecnológicos y de comunicación.

Estos desafíos nos enfrentan como sociedad ante el reto de valorar, decidir y regular en consecuencia sobre qué límites queremos poner a esa inteligencia de las máquinas con el fin de garantizar que las personas, sus derechos, libertades, ideas y necesidades sigan siendo el eje principal de todo Estado.

Los gobiernos de todo el mundo tienen ya una labor urgente, con base en los derechos humanos y los objetivos que plantea el desarrollo sostenible: esta es que las nuevas tecnologías digitales iniciaron una transformación y desarrollo estos últimos 25 años a una mayor velocidad que el cambio visto en los 2 000 años anteriores. Esto conlleva un gran riesgo también: el depender tanto de la tecnología, que si esta llegase a fallar, estaríamos completamente vulnerables, por lo que siempre es importante que todo cambio real se acompañe de un cambio legal e institucional.

La inteligencia artificial en Europa

Europa lidera a nivel internacional el desarrollo ético de la inteligencia artificial, estableciendo un marco de actuación orientado a la generación de una conciencia global, basada en una visión humanista de la tecnología y que además esta sea compatible con los derechos humanos, que trabaje y esté enfocada en buscar y consolidar espacios de consenso para la regulación de este nuevo escenario digital acorde con los valores y principios fundamentales de la Unión Europea (European Commission, 2021).

España tiene la aspiración de jugar un papel fundamental en esta vocación europea, apostando firmemente por el desarrollo de esta perspectiva ética y humanista de las tecnologías de inteligencia artificial (Gobierno de España, 2020).

En el año 2021 el presidente del Gobierno presentó una Carta de Derechos Digitales, redactada a partir del minucioso trabajo de un grupo de expertos y expertas, además de acompañarse con las aportaciones de la ciudadanía a través de un proceso abierto de participación. El documento establece un primer marco sobre el cual comenzar a trabajar para abordar una regulación que

genere certidumbre, seguridad y garantías legales en el devenir de tecnologías que ya están siendo esenciales para el desarrollo de la sociedad digital, como la inteligencia artificial (Gobierno de España, 2021).

Esta carta se organiza en seis secciones y 27 categorías, que abarcan desde la protección de datos personales hasta la neutralidad de la red y la educación digital. Entre sus principios fundamentales destacan:

» Derecho a la identidad y reputación digital, garantizando que cada persona pueda controlar su presencia en línea.
» Derecho a la privacidad y protección de datos, asegurando un uso responsable de la información personal.
» Derecho a la seguridad digital, que incluye la protección frente a ciberataques y fraudes.
» Derecho a la neutralidad de la red, evitando discriminaciones en el acceso a contenidos y servicios.
» Derecho a la educación digital, fomentando competencias tecnológicas para la ciudadanía.
» Derecho a la desconexión digital, especialmente en el ámbito laboral, para equilibrar vida personal y profesional.
» Derecho a la participación democrática en entornos digitales, garantizando transparencia y acceso a la información pública (Gobierno de España, 2021).

Esta carta resalta la importancia de tener un enfoque ético y humanista en el desarrollo de distintas tecnologías, siendo en este caso la inteligencia artificial, alineándose con la estrategia europea de gobernanza digital. Aunque no tiene fuerza de ley, representa un compromiso político y social que orienta la creación de normativas futuras y políticas públicas. También ha sido recomendada ampliamente como modelo para que los países

vayan estableciendo en documentos algunos de estos preceptos y principios que permitan crear un marco general respecto al entorno actual del mundo digital en el que vivimos.

Esto confirmó a España como referencia de la Unión Europea en materia de regulación y avance ético sobre esta tecnología de alto impacto, y fue el antecedente inmediato respecto a la inteligencia artificial, teniendo como eje principal poner a disposición del resto de los países comunitarios los resultados, para que al aplicar este reglamento en cada región, sea orientado a regular determinados usos de riesgo de la inteligencia artificial en dichos países.

Inteligencia artificial en Latinoamérica

La inteligencia artificial está emergiendo como una de las tecnologías más influyentes en el desarrollo de América Latina. En los últimos años, la región ha acelerado su adopción de sistemas inteligentes en sectores como la educación, la salud, la industria y la gestión pública. Según el Índice Latinoamericano de Inteligencia Artificial 2025, elaborado por la Comisión Económica para América Latina y el Caribe (Cepal, 2025), 19 países de la región muestran avances en innovación y digitalización, aunque con marcadas diferencias en capacidades y recursos.

Brasil, Chile y Uruguay lideran la implementación de IA, destacando por sus políticas públicas, inversión en infraestructura digital y programas de formación de talento. Estos países han logrado integrar la inteligencia artificial en procesos productivos, servicios financieros y plataformas de gobierno digital. En contraste, otras naciones enfrentan limitaciones derivadas de la falta de financiamiento, escasez de especialistas y marcos regulatorios insuficientes.

La IA también está transformando el mercado laboral. Un estudio reciente revela que más del 57 por ciento de los profesionales en Latinoamérica ya emplean herramientas digitales basadas en inteligencia artificial, especialmente en procesos de selección y gestión de talento (Cepal, 2025). Esto plantea la necesidad de construir principios éticos que garanticen transparencia y equidad, evitando sesgos en la toma de decisiones automatizadas.

En el ámbito empresarial, la adopción de ERP (Planificación de Recursos Empresariales) en la nube con IA está redefiniendo la gestión corporativa. Más de la mitad de las empresas latinoamericanas han migrado parte de sus procesos a la nube, lo que ha permitido mayor agilidad y reducción de costos. El verdadero salto ocurre cuando los sistemas no solo almacenan datos, sino que "piensan" con ellos, anticipando escenarios y optimizando decisiones estratégicas (Debate, 2025).

Como vimos anteriormente, aunque la región ha ido avanzando también es cierto que se enfrentan retos críticos, tales como un déficit de talento especializado que limita la capacidad de innovación, inversión insuficiente en desarrollo de inteligencia artificial si la comparamos con otras regiones como Europa o Asia, la desigualdad digital, que genera enormes brechas entre países y dentro de las sociedades, y gobernanza y regulación insuficientes, aún en proceso de conformación, siendo estas tan necesarias para garantizar un uso ético y humanista de la IA.

En Latinoamérica la inteligencia artificial avanza más rápido de lo esperado, sin embargo, sigue siendo lenta en comparación, como ya vimos, con otras regiones. Se requieren estrategias regionales coordinadas que fortalezcan la formación de talento, impulsen la inversión y aseguren un marco ético común. Solo así podrá convertirse en un verdadero motor de desarrollo sostenible y

equitativo para la región con todo y los riesgos que esto conlleve en el manejo de nuestros datos personales.

Inteligencia artificial en México

En México, antes de la abrupta extinción del Instituto Nacional de Acceso a la Información y Protección de Datos (INAI) y del Sistema Nacional de Transparencia ordenada desde la Presidencia en el año 2024 y obedecida ciegamente por el Poder Legislativo, consumada en el 2025 sin analizar cuestiones importantes y técnicas como este nuevo entorno digital donde se exige establecer mínimos legales ante el uso desbordado de la tecnología digital, dentro de la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia, se empezaba a trabajar en un acuerdo sobre un modelo de carta similar a la europea, pero adecuada a nuestra realidad.

Mientras en México el régimen destruía las instituciones que habían contribuido a garantizar la protección de datos personales, en España desde el año 2022 se presentó, junto con la Comisión Europea, el primer piloto del Reglamento de Inteligencia Artificial. En vez de haber fortalecido instituciones como el INAI, el Gobierno mexicano prefirió extinguirlo sin tomar en cuenta la necesidad de contar con un organismo autónomo respecto a la protección de datos personales y agregar a sus funciones lo referente a la inteligencia artificial.

La IA ha dejado de ser un concepto futurista para convertirse en una realidad palpable en México en 2025. El país se encuentra en un proceso acelerado de adopción tecnológica, impulsado por la digitalización global y distintos fenómenos económicos como el *nearshoring* y la próxima renegociación del Tratado de Libre Comercio entre México, Estados Unidos y Canadá.

En México nos debe quedar claro que la inteligencia artificial ya no es una opción, sino un imperativo estratégico para la competitividad nacional dentro del ámbito internacional.

En el ámbito económico y empresarial la IA se aplica en sectores tan diversos como el comercio minorista y mayorista. Distintas empresas han comenzado a utilizar algoritmos de inteligencia artificial para analizar patrones de consumo y mejorar la atención a clientes, desde pequeños negocios hasta grandes cadenas. Asimismo, más del 67 por ciento de los trabajadores mexicanos emplean asistentes de inteligencia artificial personales para facilitar sus tareas, fenómeno conocido como Shadow AI, "cuando se utilizan herramientas de IA no autorizadas por una compañía para abordar tareas laborales" (BBVA, s. f.), lo que refleja tanto la penetración de estas herramientas como los riesgos de seguridad asociados a su utilización, y de manera relevante sobre lo que nos ocupa: nuestros datos personales.

La protección de datos personales

Los datos personales son toda información que identifica o hace identificable a una persona física. En México, la ley los reconoce como información que describe aspectos de nuestra vida privada, identidad y características, y cuya protección es un derecho fundamental.

La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2025) establece en el inciso V del artículo 2 que los datos personales son cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información, y en el inciso VI del mismo artículo se establecen que los datos personales

sensibles son aquellos datos personales que afecten a la esfera más íntima de la persona titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para esta. De manera enunciativa mas 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.

Estos conceptos son en su mayoría aceptados dentro de diversos organismos internacionales y por países que los han establecido en sus ordenamientos jurídicos, tan es así que fueron llevados a nuestras leyes.

Categorías de datos personales

» De identificación (nombre, domicilio, teléfono, correo electrónico, firma, RFC, CURP, fecha de nacimiento, edad, nacionalidad, estado civil, etc.); laborales (puesto, domicilio, correo electrónico y teléfono del trabajo); patrimoniales (información fiscal, historial crediticio, cuentas bancarias, ingresos y egresos, etc.); académicos (trayectoria educativa, título, número de cédula, certificados, etc.); ideológicos (creencias religiosas, afiliación política y/o sindical, pertenencia a organizaciones de la sociedad civil y/o asociaciones religiosas).
» De salud (estado de salud, historial clínico, enfermedades, información relacionada con cuestiones de carácter psicológico y/o psiquiátrico, etc.).
» Características personales (tipo de sangre, ADN, huella digital, etc.).
» Características físicas (color de piel, iris y cabellos, señales particulares, etc.)
» Vida y hábitos sexuales, origen (étnico y racial), entre otros.

Principios rectores de los datos personales

Calidad de los datos personales

En términos de argumentación jurídica, una idea de racionalidad y proporcionalidad en el uso y manejo de esos datos. Es una medida prudencial y de pertenencia de quien recoge los datos y el uso que les va a dar, con base en las finalidades que motivaron su uso o recolección

Consentimiento e información

Consiste en que cualquier recolección, uso, manejo y transmisión de datos personales debe hacerse del consentimiento del titular, y este debe manifestar de modo indubitable y expreso la voluntad o el asentamiento de proporcionarlos. Por lo tanto, se torna en obligación para quienes recogen los datos requerir el consentimiento de los titulares, e informarles el uso y finalidad de la recolección. Por lo general, se utilizan leyendas o formatos en que parece una advertencia para los titulares del uso que se dará a sus datos, así como un espacio en que mediante firma o selección de una afirmativa expresen el consentimiento, todo esto para que en su momento el titular pueda ejercer los derechos para solicitar el acceso, rectificación, cancelación u oposición sobre el tratamiento de sus datos, ante el sujeto obligado que esté en posesión de los mismos. Estos derechos son conocidos como derechos ARCO y según sea el caso, lo anterior servirá para constatar que no se defraudó el principio de información.

Excepciones. Casos en los que no se requiere el consentimiento del titular de los datos personales: Por razón de atención médica urgente o sanidad pública; por razones estadísticas, siempre que se disocien los datos y se impida con ello la identificación

o identificabilidad de los titulares; por mandamiento judicial; por razones contractuales con terceros, siempre que se garantice la confidencialidad de los datos mediante penas convencionales, responsabilidades legales y garantías económicas como fianzas; por razones de fuentes de acceso público, como registros civiles o de la propiedad y comercio; por razones de legalidad de las atribuciones de las instituciones públicas.

Seguridad de los datos personales

Le atañe esencialmente al poseedor de la base de datos con un conjunto variado de medidas protectoras de estos. Tales medidas van desde disposiciones, garantías y sanciones jurídicas hasta de naturaleza técnica como respaldos, claves y contraseñas, uso de equipo de cómputo *ad hoc*, y reglas internas de designación de responsables y usuarios de bases de datos, horarios de uso, entre otras.

Confidencialidad estricta

Se traduce en una restricción o inhibición a cualquier tercero distinto al titular, que impide conocer los datos personales de este. Asimismo, la confidencialidad es una forma de clasificar información; es prácticamente permanente, solo superable cuando existe el consentimiento expreso del titular.

Comunicación o transmisión de datos personales

Consiste en la sesión de estos a un tercero, pero es indispensable que tal transmisión tenga un fin lícito entre las partes de la transmisión, y tenga que ver con las atribuciones y competencias del transmisor y del receptor.

Por todo esto, es que el avance la IA va de la mano con la necesidad de legislar sobre la inteligencia artificial bajo la perspectiva de la protección de nuestros datos personales.

Legislar sobre inteligencia artificial y que el eje principal sea la protección de datos personales

El marco regulatorio de la IA en México está en proceso de construcción. Aunque existen normas sobre protección de datos personales, derechos de autor y no discriminación, el país carece de una ley integral y de una estrategia nacional específica para la inteligencia artificial. En 2025 se presentaron iniciativas legislativas que buscan establecer principios éticos, sistemas de evaluación de riesgos y mecanismos de auditoría algorítmica, inspirados en modelos internacionales como el de la Unión Europea.

Entre los retos para la correcta regulación destacan:

Transparencia y desarrollo explicativo: Garantizar que los sistemas de IA sean auditables y comprensibles para usuarios y autoridades.

Protección de datos personales: Este régimen destructor, en vez de aumentar la capacidad del INAI y establecer mecanismos claros para la gestión y protección de la información sensible, decidió extinguirlo y como decimos en párrafos anteriores, no le importó el ya tener un organismo autónomo que solo habría que perfeccionar y dotar de competencia de manera amplia respecto a la inteligencia artificial en su aplicación cuando hay de por medio datos personales.

Ética y no discriminación: Prevenir sesgos algorítmicos, discriminación y usos indebidos de la IA en sectores sensibles como salud, justicia y seguridad pública.

Responsabilidad y reparación: Definir esquemas de responsabilidad civil y penal para daños causados por sistemas de IA, así como mecanismos de reparación para personas afectadas.

La falta de coordinación federal y la ausencia de una ruta clara contrastan con experiencias internacionales, como las estrategias de la Unión Europea y Reino Unido, que ya operan ante los riesgos y realizan inversión pública y gobernanza transversal.

Las buenas intenciones no dotan de la efectividad requerida para controlar a las compañías tecnológicas. Es necesario imponer sanciones por su incumplimiento, aprobando leyes concretas, puntualizando los deberes y obligaciones para los creadores y proveedores de los algoritmos, todo basado en el respeto a los derechos humanos, es decir, garantías precisas frente al riesgo de los nuevos productos, a través de una tipificación de conductas perjudiciales y abusos de los responsables de la creación y funcionamiento de las aplicaciones que utilicen inteligencia artificial.

Tuvimos un organismo que ahora mismo sería muy útil ante este tema. Por desgracia, habrá que volver a reconstruir, en vez de mejorar lo que existió, y en estos tiempos deberá ser más rápido de lo pensado por el vertiginoso avance de la inteligencia artificial, ya que la velocidad del desarrollo tecnológico exige una actualización constante y una interpretación dinámica por parte de las instituciones.

La construcción de un ecosistema digital confiable no depende únicamente de la regulación, sino también de la cultura ciudadana en torno al uso responsable de la información. México se encuentra en un punto decisivo: aprovechar las oportunidades de la inteligencia artificial para el desarrollo económico y social, sin

sacrificar la dignidad y privacidad de las personas. El futuro de la innovación será sostenible solo si se coloca al ser humano en el centro de la ecuación tecnológica.

Referencias

Comisión Económica para América Latina y el Caribe. (2025). *Índice Latinoamericano de Inteligencia Artificial*. https://www.cepal.org/es/publicaciones/82514-indice-latinoamericano-inteligencia-artificial-ilia-2025

Debate. (2025, noviembre). *ERP en la nube con IA: el futuro de la gestión empresarial en Latinoamérica*. https://www.debate.com.mx/economia/erp-en-la-nube-con-ia-el-futuro-de-la-gestion-empresarial-en-latinoamerica-20251111-0134.html

European Commission. (2021). *Proposal for a Regulation laying down harmonised rules on artificial intelligence*. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence

Gobierno de España. (2020). *Estrategia Nacional de Inteligencia Artificial (ENIA)*. Ministerio de Asuntos Económicos y Transformación Digital. https://espanadigital.gob.es

Gobierno de España. (2021). *Carta de derechos digitales*. Plan de Recuperación, Transformación y Resiliencia. https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

Google Cloud. (s. f.). *Inteligencia Artificial (IA): una guía fácil de entender*. Recuperado el 11 de octubre de 2025 de https://cloud.google.com/learn/what-is-artificial-intelligence?hl=es-419

Instituto de Acceso a la Información Pública y Protección de Datos Personales del D. F. (2011). *Retos de la protección de datos personales en el sector público 2011*. INFODF.

Ley Federal de Protección de Datos Personales en Posesión de Particulares. 20 de marzo de 2025. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A modern approach* (4.a ed.). Pearson.

Simon, H. A. (1960). *The shape of automation for men and management.* Harper & Row.

2. Aviso de privacidad y el "acepto" a un clic en las redes sociales

Lic. Karla Gabriela Fuentes Moreno

Primero quiero empezar por definir qué es un **aviso de privacidad**, siendo este el documento a disposición de la persona titular de la información de forma física, electrónica o en cualquier otro formato generado por el responsable, a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos, de acuerdo con el artículo 2, fracción I de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2025).

Ahora definamos **"acepto"**, que con más facilidad entregamos en servicio de las aplicaciones. ¿Qué es **"aceptar"**?: f. Acción y efecto de aceptar (Real Academia Española, s. f.).

Este artículo busca hacer *conciencia* sobre el **aviso de privacidad** de las redes sociales a las que tenemos acceso, lo cual es de suma importancia para los niños, niñas y adolescentes, nuestra juventud, ya que no le dan la atención que amerita y pueden ir aceptando indiscriminadamente en tantas aplicaciones o páginas a las que tengan acceso, aunque no vuelvan a darles uso.

Esto, sin advertir que tiene muchas implicaciones en cuanto al acceso que le dan a sus datos personales. Aun cuando en el aviso nos informan el uso y tratamiento de los datos, no existe la educación o costumbre de leerlo, y no sabemos a quién se transfieren, cómo se usan o qué medidas de seguridad tienen cada

una de las aplicaciones, pero que sí está la información a la que rápidamente le damos el ¡sí! a la autorización de manejar nuestros datos en redes sociales como Instagram, Facebook, WhatsApp, X, YouTube, TikTok y Pinterest.

Hablando de autoridad vs conciencia social

Ante la importancia de garantizar dos derechos fundamentales, como lo son el **acceso a la información** y la **protección de datos personales**, por ahora más a detalle hablando de este último, nos referimos al aviso de privacidad en las redes sociales, en las que para poder acceder a cada una de ellas hay que dar clic en el aviso de privacidad, que siendo sinceros, ¿cuántas personas conocemos o nos incluimos en decir que lo leemos?, y más ante la prisa de tener acceso a la página o a la aplicación que lo esté solicitando.

En el estado de Chihuahua se regula en el artículo 11, fracción II de Ley de Protección de Datos Personales del Estado de Chihuahua (2017), que indica que el aviso de privacidad es un documento físico, electrónico o en cualquier otro formato, emitido por el responsable, mediante el cual se informa a su titular del tratamiento que se le dará a sus datos personales.

¿Cuáles son los datos personales que son tratados en las redes sociales? Enlistaré algunos:

- Nombre de usuario
- Reconocimiento facial o huella dactilar
- Contraseña
- Correo electrónico
- Número de teléfono, celular
- Foto de perfil
- Lugar de residencia

- Fecha de nacimiento
- Lugar de nacimiento
- Edad
- Idiomas
- Estudios
- Estado civil
- Educación

El listado anterior por señalar los más recabados, los cuales refieren a detalle cómo se vuelve identificable una persona, y más aun incluyendo datos sensibles como lo son el reconocimiento facial y la huella dactilar, por mencionar algunos.

Sin embargo, esta visión no solo es desde el punto de vista legal, sino por la realidad social que observo día a día como servidora pública y como madre. Con jóvenes en mi entorno, advierto una situación crítica: la **generación de plataformas digitales y redes sociales** en las que están firmando un **contrato invisible** que compromete su seguridad presente y futura a cambio de la inmediatez de la conexión actual como aceptación social o de algún grupo en particular.

El problema radica en el clic inconsciente, que solo puede ser un cuadro al que debemos darle "aceptar" para seguir con el llenado de la aplicación o página para hacer uso de la misma, y de no aceptar, no podemos tener acceso. Para la juventud, como para la mayoría, el extenso **aviso de privacidad** es un muro de texto irrelevante, un mero obstáculo que se supera con el clic en **"acepto"**, sin cuestionarse a qué cedí.

Este acto, que en la práctica es un consentimiento legalmente vinculante, se realiza sin meditar la cesión de la identidad que implica. Como garante de los derechos, considero urgente que

se comprenda qué es lo que realmente se está entregando, bajo el marco de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

El **aviso de privacidad** es un requisito legal que informa al titular sobre las **finalidades** y el **tratamiento** de sus datos. No obstante, su extensión y complejidad lo convierten en una herramienta de desinformación efectiva. Los jóvenes otorgan su consentimiento para que sus **datos personales** (nombre, fotos, comentarios, ubicación) y, lo más crítico, sus **datos sensibles**, sean recopilados.

Los **datos sensibles**[1] —la **voz**, las **facciones faciales** (biometría) e incluso datos de salud— son únicos e inalterables. Observo cómo aplicaciones de entretenimiento aparentemente inofensivas capturan estas **plantillas biométricas.**

Una vez cedidos, estos datos no pueden ser reemplazados como una contraseña, convirtiéndose en activos permanentes y vulnerables que, tras una **transferencia de datos,** pueden ser usados por un sinfín de terceros, los cuales a su vez transfieren y no tenemos conocimiento qué medidas de seguridad llevan a cabo y su finalidad.

El riesgo es mayor cuando los **niños, niñas y adolescentes (NNA) falsean su edad** para eludir los controles de restricción y dan "acepto" a avisos de privacidad, exponiéndose a contenidos y contactos inapropiados, además de carecer de la protección legal prevista para su edad, dando acceso a sus contactos, incluidos, como ellos, otros menores de edad.

[1] Artículo 2, fracción VI de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

El peligro de la entrega inconsciente de datos se multiplica a través de mecanismos inherentes al diseño de las plataformas.

Lo que no sabe la mayoría de los usuarios de redes sociales es que los avisos de privacidad incluyen una cláusula de **transferencia de datos**, que permite a la red social o aplicación original compartir su información con otras empresas (publicidad, análisis de riesgo, socios comerciales). La ley lo permite siempre que se cuente con el consentimiento, y el joven lo otorga con el clic inicial.

Este riesgo es exponencial: cada aplicación descargada indiscriminadamente se convierte en una vía de escape para los datos. El joven no solo expone su propia información, sino que autoriza la transferencia de datos de amigos y familiares contenidos en sus contactos y publicaciones, entre otros accesos que los vuelven vulnerables. Este rastro de datos personales viaja a través de una cadena de terceros sobre la que el usuario pierde todo control.

La amenaza física: geolocalización y ciberseguridad

La geolocalización es una función que, al ser activada para un juego o una publicación, convierte el entorno físico del joven en un dato digital explotable. Las coordenadas de su hogar, escuela o lugares de reunión se incrustan en los metadatos de sus publicaciones.

Desde una perspectiva de ciberseguridad y combate a la delincuencia, esta información es un mapa de vulnerabilidad. El hackeo de una base de datos expone información masiva; la geolocalización ofrece el contexto físico: permite a la delincuencia organizada perfilar, rastrear e incrementar el riesgo de secuestro, extorsión, *grooming*, *sexting*, *ciberbullying*, suplantación de identidad y *fake news* (Instituto Nacional de Transparencia, Acceso

a la Información y Protección de Datos Personales, 2018). La falta de pericia de los NNA para advertir este riesgo físico-digital es lo que nos obliga, como Estado y como garantes de derechos, a actuar con urgencia.

La pasividad en el entorno digital es un lujo que no podemos permitirnos. Observo cómo, al cesar el uso de una aplicación, la juventud simplemente borra el ícono, pero la información permanece activa en el servidor, vulnerable al hackeo y al uso por los terceros a quienes fue transferida, sin utilizar los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición), para lo cual es fundamental informar cómo ejercerlos, sensibilizar sobre cómo cuidarlos y protegerlos. Debemos empoderar a la juventud para que entienda que la ley les da el derecho de retomar el control.

- **Acceso (A):** Es el derecho a acceder a los datos personales y el tratamiento de los datos que tienen de uno mismo y que otorgamos.
- **Rectificación (R):** El derecho a corregir los datos personales por no estar actualizados, inexactos o incorrectos.
- **Cancelación (C):** Es el derecho a exigir la supresión total de sus datos de la base de la aplicación que ya no usan.
- **Oposición (O):** Es el derecho a oponerse al tratamiento de sus datos para fines específicos, como la transferencia a terceros o la publicidad dirigida.

Este derecho no se ejerce por sí solo: requiere el conocimiento que solo la educación proactiva y el mandato de los organismos garantes pueden proporcionar.

Reflexión sobre aplicar medidas de protección

Mi mensaje profesional y social se centra en la autorregulación consciente. La primera línea de defensa no es técnica, sino reflexiva, tomando personalmente las medidas mínimas, tanto para los adultos y con mayor atención y supervisión en los menores, debiendo poner suma atención y seguimiento de las aplicaciones que siguen y usan, además de las personas con las que creen que interactúan, apoyándose de los beneficios de otras aplicaciones como control parental y el uso de restricciones que cada red social o página ofrece, sin que estas sustituyan la supervisión de padres o tutores, adultos a cargo de la seguridad de los menores.

Por lo que invito a los jóvenes a:

1. **Meditar. ¿De verdad la necesito o me es útil?:** Antes de descargar indiscriminadamente, detente y piensa: **¿es realmente necesaria esta aplicación?** Si la respuesta es negativa, el riesgo de entregar tus datos supera el beneficio superficial.

2. **Elegir cuidadosamente:** Evita bajar *apps* por impulso o tendencia. Analiza la reputación de la aplicación y las peticiones de acceso que realiza.

3. **Ejercer el derecho de Cancelación:** Si la aplicación dejó de usarse o ya no deseas recibir correos de *marketing*, debes formalizar la solicitud de cancelación u oposición ante el responsable.

Aplicar medidas de seguridad indispensables:

1. **Configuración de privacidad:** Utiliza siempre el **perfil privado** en redes sociales. **Elige correctamente a quién diriges tus**

publicaciones y a quién autorizas como seguidor. Toma en cuenta personas de confianza, de tu entorno y conocidos.

2. **Contraseñas infranqueables:** Establece **contraseñas seguras** (combinación de caracteres, larga) y **modifícalas regularmente.** La peor vulnerabilidad es compartirla o reutilizarla. Por favor, muy importante: no compartirla.

Para finalizar, dejo esta conclusión y reflexión: La protección de datos personales es un derecho humano y una práctica de seguridad, por lo que la intención de este artículo, principalmente dirigido a los jóvenes, es dejar la conciencia de cuidar su identidad, así como tener presente que además están los datos que llevan a identificar a tu círculo más cercano, sean amigos o familiares, de los cuales no tienes autoridad para compartir su información y ellos mismos desconocen por dónde transita su información y los riesgos que enfrentan. Es un llamado a tener conciencia y llevar a cabo la **ciberresponsabilidad.**

A nuestra juventud, menores, mayores, cuídense, reserven sus ubicaciones en tiempo real, los datos de su escuela, los lugares que visitan. No saben quién esté viendo y siguiendo esa información que comparten y no con las mejores intenciones; eviten ponerse en peligro. Tengan presente que la información personal y sensible queda como una huella digital: lo que construyen hoy es el perfil de riesgo que los seguirá mañana, que no se puede eliminar, datos que ya no volverán a ser privados.

Observen a su alrededor, valoren los riesgos y ejerzan el control de su información. Aun cuando consideramos que es privada, o compartida con un mejor amigo, este la puede difundir. Tengan en cuenta que su privacidad no debe ser usada como intercambio de aceptación o integración de un grupo.

Cuestionen la información que ustedes mismos siguen, a las personas que siguen, observen en qué riesgos han caído, qué situaciones peligrosas o incómodas han vivido, que los lleve a cuestionarse su **clic al cuadro de "aceptar"** para que no sea un acto de sumisión, de prisa, sino una decisión informada para un futuro seguro de su persona, de sus familiares y amigos.

Bibliografía

Instituto Nacional de Ciberseguridad. (s. f.) *Informes sobre riesgos de geolocalización, contraseñas y suplantación de identidad en adolescentes (referencia conceptual sobre riesgos).* https://www.incibe.es/menores/tematicas

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2018). *Guía para el tratamiento de datos biométricos.*

Ley de Protección de Datos Personales del Estado de Chihuahua. 6 de septiembre de 2017. Periódico Oficial del Estado. https://www.congresochihuahua2.gob.mx/biblioteca/leyes/archivosLeyes/1342.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. 20 de marzo de 2025. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Naciones Unidas. (1989). *Convención sobre los Derechos del Niño*. https://www.ohchr.org/es/instruments-mechanisms/instruments/convention-rights-child

Real Academia Española. (s. f.). Aceptar. En *Diccionario de la Lengua Española*. https://dle.rae.es/aceptar

Sistema Nacional de Protección de Niñas, Niños y Adolescentes (2018, 8 de febrero). *Algunos riesgos en las redes sociales para niñas, niños y adolescentes.* https://www.gob.mx/sipinna/articulos/algunos-riesgos-en-las-redes-sociales-para-ninas-ninos-y-adolescentes?idiom=es

3. El ejercicio de los derechos ARCO como pilar de la protección de los datos personales

Mtra. María Selene Prieto Domínguez

En la sociedad actual, los datos personales se han convertido en una extensión de la identidad humana. Cada interacción digital, cada registro público o privado, deja una huella que puede ser utilizada, compartida o manipulada. En este escenario, el reconocimiento y ejercicio de los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) constituyen una de las conquistas más relevantes en la evolución de los derechos humanos en México.

Estos derechos no solo representan herramientas jurídicas, sino que encarnan una nueva forma de entender la libertad individual en el contexto de la sociedad de la información. En un entorno donde la vigilancia algorítmica, el perfilamiento automatizado y la comercialización de datos son prácticas comunes, los derechos ARCO permiten a las personas recuperar el control sobre su información personal, reafirmando su autonomía y dignidad.

Los derechos ARCO tienen su origen en el marco europeo de protección de datos. Alemania fue pionera en la década de los setenta con el concepto de "autodeterminación informativa", introducido por el Tribunal Constitucional Federal en 1983, como respuesta a los riesgos que implicaba el censo nacional. Este principio reconoce que cada individuo debe tener la capacidad de decidir sobre la recopilación, uso y difusión de su información personal.

España, en los años ochenta, consolidó este enfoque mediante la promulgación de leyes específicas que protegían los datos personales, sentando las bases para una legislación más robusta en el ámbito europeo. La Directiva 95/46/CE del Parlamento Europeo y del Consejo institucionalizó en 1995 el modelo de derechos ARCO, estableciendo un marco común para la protección de datos en los Estados miembros. Posteriormente, el Reglamento General de Protección de Datos (GDPR, 2016) reforzó estos derechos, ampliando su alcance y estableciendo estándares más estrictos para el tratamiento de datos personales, con influencia global.

La influencia del Reglamento General de Protección de Datos de la Unión Europea fue decisiva para consolidar y fortalecer el marco normativo mexicano en materia de protección de datos personales. En 2009, México incorporó formalmente los derechos ARCO mediante la reforma al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, el cual establece que "toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley" (Constitución Política de los Estados Unidos Mexicanos, 2009).

A raíz de la entrada en vigor del GDPR, México adoptó diversas medidas orientadas a cumplir con los estándares internacionales, asumiendo una postura de responsabilidad proactiva. Esto implicó el fortalecimiento de principios fundamentales en el tratamiento de datos personales, así como la implementación de mecanismos más rigurosos para proteger las transferencias internacionales de información.

Este reconocimiento constitucional representó un avance trascendental, al elevar la protección de los datos personales al

mismo rango que otros derechos fundamentales como la libertad de expresión, el acceso a la información y el derecho a la identidad. Con ello, se reafirma que el control sobre la información personal no constituye un privilegio, sino una garantía esencial que debe ser respetada y protegida con el mismo rigor que los pilares de toda sociedad democrática.

A partir de este reconocimiento se desarrollaron dos leyes que operativizaron los derechos ARCO en el país:

1. La Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP, 2010), dirigida al sector privado, misma que establece las obligaciones de empresas y organizaciones en el tratamiento de datos personales, incluyendo la obtención del consentimiento, la seguridad de la información y los mecanismos para ejercer los derechos ARCO.

2. La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO, 2017), aplicable a las instituciones públicas, la cual busca garantizar que el Estado también respete y proteja los datos personales de los ciudadanos, estableciendo principios como la licitud, finalidad, proporcionalidad y responsabilidad.

Ambas leyes establecieron procedimientos, principios y responsabilidades para garantizar el ejercicio de los derechos ARCO, así como mecanismos de impugnación ante autoridades competentes, como el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y los organismos constitucionales autónomos de las entidades federativas.

De la misma manera, las leyes mencionadas con anterioridad

describen los derechos ARCO, por lo que es necesario precisar su conceptualización:

Derecho de Acceso

El derecho de Acceso faculta al titular de los datos personales a conocer si una entidad —pública o privada— posee información sobre él, así como a obtener detalles sobre el origen, uso, finalidad y destinatarios de dicha información. Este derecho no solo implica la posibilidad de saber qué datos se tienen, sino también cómo y para qué se están utilizando.

Desde una perspectiva legal, el artículo 23 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares establece que el responsable del tratamiento debe proporcionar al titular toda la información relacionada con sus datos personales, incluyendo copias de los registros que los contengan.

Este derecho es esencial porque sin conocimiento no hay control. Permite al titular verificar la licitud del tratamiento, detectar posibles usos indebidos y tomar decisiones informadas sobre su información. En un entorno digital donde los datos se recopilan de manera constante —a menudo sin plena conciencia del usuario—, el derecho de Acceso se convierte en un mecanismo de transparencia y empoderamiento ciudadano.

Derecho de Rectificación

El derecho de Rectificación garantiza que los datos personales sean exactos, completos, pertinentes y actualizados. Su ejercicio permite al titular corregir errores, omisiones o desactualizaciones que puedan generar consecuencias negativas en su vida personal, profesional o social.

Este derecho protege la veracidad de la información, lo cual es crucial en contextos donde los datos se utilizan para tomar decisiones que afectan directamente a las personas. Por ejemplo, un error en un historial médico, un expediente académico o un reporte crediticio puede derivar en diagnósticos incorrectos, exclusión de oportunidades educativas o negativas de crédito.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, en su artículo 47, establece que el titular debe aportar los documentos que acrediten la corrección solicitada, lo que refuerza el carácter probatorio y objetivo del procedimiento. Más allá de lo técnico, este derecho refleja el principio de justicia informacional, al permitir que las personas no sean juzgadas ni tratadas con base en datos erróneos.

Derecho de Cancelación

El derecho de Cancelación otorga al titular la facultad de solicitar la eliminación de sus datos personales cuando estos hayan dejado de ser necesarios para la finalidad que motivó su recolección, o cuando el tratamiento resulte ilegítimo o excesivo.

Este derecho se basa en el principio de proporcionalidad, que exige que la conservación de los datos esté justificada por fines legítimos y no se prolongue indefinidamente. En otras palabras, los datos personales no deben permanecer en poder de las instituciones más allá del tiempo necesario.

Sin embargo, este derecho no es absoluto. En el ámbito público, existen restricciones derivadas de razones legales o de interés público. Por ejemplo, los datos contenidos en expedientes judiciales, archivos históricos o registros fiscales pueden estar sujetos a conservación obligatoria. En estos casos, se puede

aplicar el bloqueo, que impide el uso de los datos sin eliminarlos por completo.

La cancelación es, por tanto, una expresión del derecho al olvido, que cobra especial relevancia en la era digital, donde la permanencia de la información en línea puede afectar la reputación, la intimidad y la reinserción social de las personas.

Derecho de Oposición

El derecho de Oposición permite al titular negarse al tratamiento de sus datos personales por motivos legítimos, especialmente cuando dicho tratamiento pueda afectar sus derechos fundamentales o cuando se realice con fines no deseados, como publicidad, estudios de mercado o elaboración de perfiles.

Este derecho actúa como una cláusula de defensa frente a la intrusión informacional y la pérdida de control sobre la identidad digital. En el sector público, puede ejercerse cuando el tratamiento de datos comprometa la dignidad, la seguridad o la libertad del titular, salvo que exista una disposición legal que lo autorice.

En términos prácticos, este derecho permite al individuo decidir sobre el uso de su información, evitando que sea utilizada en contextos que no ha consentido o que considera inapropiados. Es una manifestación concreta del principio de libertad personal, que protege al individuo frente a la automatización de decisiones y la mercantilización de su identidad.

Por consiguiente, el concepto que articula a los derechos ARCO es el de autodeterminación informativa, entendido como la capacidad de decidir libremente sobre el uso y destino de los datos personales. En este sentido, los derechos ARCO son

manifestaciones concretas del principio de libertad personal en la era digital y constituyen el núcleo operativo de la protección de los datos personales, por la doble naturaleza jurídica que desempeñan. Por una parte, son derechos sustantivos, en tanto protegen un bien jurídico consistente en la información personal; por la otra, son derechos instrumentales, porque operan como herramientas para hacer efectiva la privacidad.

Además, México inició el proceso de adhesión al *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal* (Convenio 108) a través del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y la Secretaría de Relaciones Exteriores, cuya adhesión fue aprobada por la Cámara de Senadores el 26 de abril de 2018 y el Poder Ejecutivo publicó el decreto en el Diario Oficial de la Federación el 12 de junio de 2018, para entrar en vigor el 1 de octubre del mismo año. Este convenio fue el primer instrumento internacional jurídicamente vinculante en materia de protección de datos personales y estableció principios fundamentales como respeto a la vida privada, calidad y seguridad de los datos, derechos de las personas frente al tratamiento automatizado y supervisión por autoridades independientes.

Es así que el Convenio 108 fortaleció el marco legal nacional en materia de protección de datos personales, facilitó el intercambio seguro de información con otros países miembros, impulsó la competitividad y confianza en las relaciones comerciales internacionales y permitió a los ciudadanos mexicanos ejercer sus derechos en otros países parte del convenio, otorgando la confianza a nivel internacional de que en México había una evolución y garantía de la protección de datos personales al ser tutelados por un organismo garante e independiente de los tres

poderes del Estado.

A pesar de los avances normativos, el ejercicio efectivo de los derechos ARCO ha enfrentado diversos desafíos. La falta de cultura de protección de datos, la complejidad de los procedimientos, la opacidad de algunas plataformas digitales y la asimetría de poder entre usuarios y empresas tecnológicas dificultan el avance de la implementación.

Además, el desarrollo de tecnologías emergentes como la inteligencia artificial, el *big data* y el Internet plantea nuevos dilemas éticos y jurídicos sobre el uso de datos personales, de cómo se produce, analiza y utiliza la información. Cada clic, cada búsqueda, cada compra o desplazamiento genera información que puede ser utilizada para perfilar, clasificar o vigilar a las personas. En este contexto, la privacidad se convierte en un bien estratégico y político, cuya protección exige no solo normas, sino instituciones sólidas, cultura ciudadana y responsabilidad ética de quienes tratan los datos.

En este contexto, es fundamental fortalecer la educación digital, promover la transparencia en el tratamiento de datos y garantizar que los mecanismos de protección sean accesibles, eficaces y adaptados a las nuevas realidades tecnológicas.

Hablando del tratamiento de los derechos ARCO en el sector público mexicano, se ha experimentado una evolución significativa, impulsada por la necesidad de encontrar un equilibrio entre tres principios fundamentales: la transparencia gubernamental, la rendición de cuentas y la protección de la privacidad de los ciudadanos. Esta transformación ha sido guiada por el marco normativo establecido en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, la cual impone

obligaciones claras y específicas a las autoridades, entidades, órganos y organismos de los tres poderes de la Unión, así como a partidos políticos, sindicatos y cualquier otro sujeto que maneje información personal en el ámbito público.

La implementación de esta ley marcó un punto de inflexión en la cultura institucional del país. Históricamente, muchas dependencias públicas operaban bajo esquemas de opacidad y reserva, donde la información personal era tratada sin controles adecuados y con escasa supervisión. Con la entrada en vigor de la legislación en materia de protección de datos, se estableció un nuevo paradigma: el manejo de datos personales dejó de ser una práctica discrecional para convertirse en una responsabilidad legal y ética, que exige cuidado, diligencia y respeto por los derechos de los titulares.

Este cambio implicó la adopción de políticas internas, la capacitación de servidores públicos, la creación de unidades de transparencia y la implementación de mecanismos para atender solicitudes de acceso, rectificación, cancelación y oposición. Además, se fortaleció el papel del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales como órgano garante y los organismos autónomos garantes en las entidades federativas, encargados de supervisar el cumplimiento de estas obligaciones y de promover una cultura de protección de datos en el sector público.

En este contexto, la protección de los datos personales dejó de ser un obstáculo para la transparencia y se convirtió en un complemento indispensable. La rendición de cuentas ya no se concibe como una exposición indiscriminada de información, sino como un ejercicio responsable que respeta la privacidad de los individuos. Así, el Estado mexicano avanzó hacia un modelo

de gobernanza más abierto, pero también más consciente de los derechos fundamentales que deben ser preservados en todo momento.

A pesar de eso, en México actualmente se atraviesa una etapa de profunda transformación institucional tras la reciente reforma que contempla la desaparición de los organismos constitucionales autónomos garantes de la transparencia y la protección de datos personales. Este cambio marca un giro en el modelo de gobernanza que, por más de dos décadas, apostó por la creación de entidades independientes para asegurar el acceso a la información pública y la defensa de la privacidad ciudadana. La transición hacia un esquema en el que estas funciones son absorbidas por dependencias del Poder Ejecutivo plantea interrogantes sobre la imparcialidad, la eficacia y la continuidad de los mecanismos que garantizan derechos fundamentales.

En este encuadre de reconfiguración institucional se abre un nuevo capítulo en la relación entre el Estado y la ciudadanía en la que se pone a prueba la solidez de los avances alcanzados en materia de transparencia y protección de datos personales. La desaparición de los organismos constitucionales autónomos, que durante años fungieron como garantes imparciales de derechos fundamentales, plantea el riesgo de debilitar los mecanismos que han permitido a los ciudadanos ejercer sus derechos ARCO con certeza jurídica y confianza institucional. Estos derechos no solo requieren voluntad política, sino también estructuras operativas que aseguren procedimientos claros, accesibles y confiables, libres de interferencias o intereses gubernamentales.

La autonomía ha sido un elemento clave en la consolidación de estos derechos, ya que permite que las decisiones sobre el tratamiento de datos personales se tomen con independencia

de los poderes públicos, garantizando así la imparcialidad en la resolución de controversias y la protección efectiva de la privacidad. Sin esta autonomía, el riesgo de que el ejercicio de los derechos ARCO se vea condicionado por criterios políticos o administrativos se incrementa, lo que podría generar desconfianza ciudadana y una regresión en la cultura de transparencia que tanto ha costado construir.

En ese sentido, el procedimiento para el ejercicio de los derechos ARCO estaba garantizado: los titulares presentaban solicitudes ante las instituciones responsables del tratamiento de sus datos, estas instituciones u organismos debían dar respuesta fundada y motivada en los plazos y requisitos establecidos y, en caso de inconformidad, podían acudir a una autoridad garante especializada, cuya característica era ser imparcial, por tratarse de organismos autónomos e independientes de los tres poderes del Estado.

Hoy, tras la desaparición de esos órganos, la responsabilidad de garantizar estos derechos ha sido absorbida por dependencias del Poder Ejecutivo federal y de los gobiernos estatales, lo cual deja una incertidumbre institucional que pone a prueba la madurez democrática del país, que implica desafíos que van más allá de los ya existentes, especialmente en los casos de inconformidad, donde el ciudadano se ve obligado a recurrir a la misma estructura gubernamental que originalmente trató sus datos, lo que implica una situación de estar en presencia de ser "juez y parte".

Sin embargo, también abre una oportunidad histórica: la de construir un nuevo modelo de protección de datos basado en la responsabilidad compartida y en el fortalecimiento de la cultura de la privacidad, puesto que la vigencia de las leyes de protección de datos personales es un aspecto fundamental en el contexto

actual, marcado por el uso intensivo de tecnologías digitales y el intercambio constante de información. Es por ese motivo que a pesar de los cambios estructurales que se establecieron con la reforma constitucional, las normativas que regulan el tratamiento de la información personal continúan siendo aplicables y las instituciones, tanto públicas como privadas, están legalmente obligadas a atender las solicitudes que los ciudadanos presenten en ejercicio de los derechos ARCO, ya que siguen siendo pilares esenciales para la protección de la privacidad.

En este contexto, es fundamental que las nuevas estructuras institucionales encargadas de garantizar estos derechos actúen con rigor técnico y compromiso ético. La desaparición o debilitamiento de organismos autónomos especializados no debe traducirse en una pérdida de garantías. Por el contrario, cualquier nueva instancia debe demostrar que puede cumplir con los estándares que caracterizaban a sus antecesores: autonomía frente al poder político, capacidad técnica para resolver casos complejos y una vocación genuina de servicio público.

Esto implica no solo responder de manera oportuna y adecuada, sino también contar con mecanismos claros y accesibles para facilitar dicho ejercicio, que se sustenta en un conjunto de principios jurídicos que orientan el tratamiento responsable de los datos personales. Estos principios —como la licitud, la finalidad, la proporcionalidad, la calidad, la seguridad y la responsabilidad— no solo delimitan la actuación de las instituciones, sino que también establecen un marco ético y legal que asegura que las decisiones relacionadas con los datos personales sean coherentes y proporcionales. Es decir, que respondan a fines legítimos, que no excedan lo necesario y que respeten la dignidad de las personas.
Es así que la protección de datos personales no es solo una cuestión técnica o administrativa, sino un compromiso jurídico

y ético que exige a las instituciones actuar con transparencia, responsabilidad y respeto por los derechos fundamentales. En una época donde los gobiernos y las empresas pueden saberlo casi todo sobre nosotros, el ejercicio de los derechos ARCO se convierte en una forma de resistencia, un acto cotidiano de soberanía sobre la propia identidad.

Por eso, para que el ejercicio de los derechos ARCO se mantenga vigente y efectivo, existen grandes retos. Para lograrlo es indispensable que la ciudadanía asuma un papel activo y consciente, esto implica no solo estar informada, sino también mantenerse alerta ante posibles retrocesos, interesarse por los mecanismos de defensa de sus derechos y prepararse para ejercerlos de manera crítica y responsable. La participación ciudadana es el motor que impulsa la consolidación de una cultura de respeto a la privacidad y la transparencia.

Preservar los avances logrados en materia de derechos no se limita a conservar el marco legal existente, también implica fortalecer la vigilancia social como mecanismo de protección activa. En el contexto de los derechos de Acceso, Rectificación, Cancelación y Oposición, esta vigilancia adquiere un papel crucial. La sociedad civil, los medios de comunicación, las organizaciones no gubernamentales y los propios ciudadanos deben supervisar el cumplimiento de las obligaciones legales por parte de instituciones públicas y privadas que manejan datos personales. Esta supervisión ayuda a prevenir abusos, omisiones o decisiones arbitrarias que puedan vulnerar la privacidad, obstaculizar el acceso a la información o impedir el ejercicio de los derechos ARCO.

Además, una ciudadanía informada y participativa puede exigir transparencia en el tratamiento de sus datos, denunciar

irregularidades y promover buenas prácticas en el manejo de información personal. La vigilancia social, en este sentido, no solo protege los derechos individuales, sino que también fortalece el tejido democrático, al garantizar que el control sobre los datos personales permanezca en manos de sus titulares y no se convierta en una herramienta de poder desproporcionado.

Además, la educación en el derecho de la protección de datos personales se vuelve una herramienta estratégica y fortalece el ejercicio de los derechos ARCO, al brindar a las personas el conocimiento necesario para identificar cuándo y cómo sus datos personales están siendo utilizados. Al comprender qué son los datos personales y cómo deben ser tratados, los individuos pueden ejercer su derecho de acceso para saber qué información se tiene sobre ellos, solicitar la rectificación de datos incorrectos, cancelar aquellos que ya no son pertinentes, y oponerse a tratamientos que afecten su privacidad. Esta alfabetización digital no solo empodera, sino que convierte a cada ciudadano en un agente activo en la defensa de sus libertades, promoviendo una cultura de responsabilidad y transparencia en el entorno digital.

En conclusión, en una sociedad verdaderamente democrática, el acceso a la información pública y la protección de los datos personales deben estar firmemente resguardados frente a los vaivenes políticos y los intereses partidistas. Estos derechos no pueden estar sujetos a la voluntad del gobierno en turno ni a decisiones coyunturales que comprometan su ejercicio, por el contrario, deben estar garantizados por instituciones sólidas y transparentes, cuyo compromiso principal sea con el interés público y la defensa de los derechos fundamentales.

En ese sentido, las áreas que manejen el ejercicio de estos derechos deben operar con rigurosidad técnica y ética profesional,

por eso es indispensable que la ciudadanía tenga la certeza de que sus datos personales están protegidos por entidades que no solo cumplen con la ley, sino que también aplican estándares elevados de seguridad, confidencialidad y responsabilidad.

Por lo anterior, los derechos ARCO adquieren aquí una nueva dimensión: no son solo herramientas legales, sino actos de resistencia informacional. Ejercerlos implica reclamar el control sobre la propia identidad digital frente a los poderes públicos y privados que buscan apropiarse de ella.

Más allá del ámbito jurídico, los derechos ARCO expresan una cultura de ciudadanía digital. Deben ser el resultado de un cambio de paradigma: del ciudadano pasivo que entrega información sin cuestionar, al ciudadano consciente que exige saber, corregir y decidir sobre sus datos, porque en una sociedad democrática la privacidad no puede entenderse como aislamiento, sino como un espacio de libertad y autonomía frente al poder. Cuando los datos personales son utilizados sin consentimiento o transparencia, se vulnera no solo la intimidad, sino también la capacidad de autodeterminación del individuo.

Por consiguiente, la garantía de los derechos ARCO debe ser efectiva y confiable. Las personas deben poder ejercerlos con plena seguridad de que sus solicitudes serán atendidas de manera justa, oportuna y sin obstáculos innecesarios. Esto implica que las instituciones encargadas del tratamiento de datos personales cuenten con protocolos claros, personal capacitado y sistemas tecnológicos robustos que aseguren el resguardo adecuado de la información.

Solo bajo estas condiciones es posible construir una cultura de respeto a la privacidad y de transparencia institucional. Una

cultura en la que cada persona sea tratada con dignidad, en la que sus datos no sean vulnerados ni utilizados sin consentimiento, y en la que la información pública esté disponible para fortalecer la participación ciudadana, la rendición de cuentas y el ejercicio pleno de los derechos digitales.

Referencias

Cámara de Diputados. (2024, 20 de diciembre). *DOF publica decreto de reforma constitucional en materia de simplificación orgánica*. https://comunicacionsocial.diputados.gob.mx/index.php/notilegis/dof-publica-decreto-de-reforma-constitucional-en-materia-de-simplificacion-organica

Carbonell, M. (2020). *Derechos humanos y Constitución*. Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México.

Consejo de Europa. (1981, 28 de enero). *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio n.º 108)*. https://rm.coe.int/16806c1abd

Constitución Política de los Estados Unidos Mexicanos [Const.]. Artículo 16, párrafo 2. 1 de junio de 2009 (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. 5 de julio de 2010. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. 26 de enero de 2017. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Pérez Luño, A., Losano, M. G., & Guerrero Mateus, M. F. (1989). *La nueva libertad informática: datos personales y democracia*. Centro de Estudios Políticos y Constitucionales.

Reglamento (UE) 2016/679. 27 de abril de 2016. Parlamento Europeo y del Consejo. https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

Ruelas, J. (2024). *Privacidad, poder y resistencia digital en América Latina*. Universidad Autónoma Metropolitana.

4. El derecho al olvido en la era de la indexación permanente: génesis europea, criterios de aplicación y desafíos para México

Mtro. Ernesto Alejandro de la Rocha Montiel

Resumen

El llamado "derecho al olvido" —reconocido en la Unión Europea (UE) como derecho de supresión (Reglamento General de Protección de Datos de la Unión Europea [RGPD], 2016)— busca limitar la persistencia y accesibilidad de información personal cuando deviene inadecuada, impertinente o excesiva, respecto a información en Internet sobre alguna persona y que se encuentra indexada en motores de búsqueda, tensionando por un lado la libertad de expresión y el interés público por acceder a hechos veraces, así como la privacidad, reputación y honor de una persona por el otro. En este apartado se pretende explicar su origen jurisprudencial, su regulación o positivización en el RGPD, los criterios de ponderación elaborados por el Tribunal de Justicia de la Unión Europea (TJUE) y por autoridades de protección de datos, así como analizar brevemente la situación mexicana a la luz de dos hitos: el caso Ulrich Richter vs. Google y el expediente Sánchez de la Peña vs. Google México ante el INAI y tribunales. Se analiza la posición reciente de la Suprema Corte de Justicia de la Nación (SCJN), que ha considerado incompatible con la Constitución la incorporación del "falso" derecho al olvido en los

términos europeos, y se formulan propuestas normativas para una eventual regulación mexicana que concilie protección de datos, honra y libertad de expresión, así como críticas y alertas desde la doctrina.

Palabras clave: Derecho al olvido; derecho de supresión; protección de datos; libertad de expresión; desindexar, buscadores; RGPD; SCJN.

1. ¿Qué se entiende por derecho al olvido?

Según los criterios de las autoridades y disposiciones europeas, el "derecho al olvido" es la manifestación específica del derecho de supresión aplicado, entre otros, a motores de búsqueda en Internet, que faculta a la persona para solicitar la eliminación o desindexación de resultados que, aunque veraces, se han vuelto impertinentes, inadecuados o excesivos en relación con los fines del tratamiento y el tiempo transcurrido, o bien, cuando concurre alguna de las causas del artículo 17 del Reglamento General de Protección de Datos (RGPD, 2016) porque ya no sean necesarios, que se retire el consentimiento o que el tratamiento sea ilícito.

En este sentido, resulta conveniente subrayar dos rasgos: primero, que no equivale a borrar información de la web en su origen periodístico o documental —por lo que medios de noticias digitales, eremíticas, etc., no están obligados a eliminarla por este simple hecho—, sino a impedir o bloquear su hallazgo y acceso sistemático vía motores de búsqueda para ciertas consultas nominativas, y segundo, no es absoluto: se pondera con el derecho a la libertad de expresión y de información y con el interés público en conocer datos sobre personas (especialmente, figuras públicas) y asuntos de relevancia social (ponderación de derechos).

2. Origen: del caso Costeja vs. Google a su consolidación normativa

Dicha denominación cobró fuerza a partir de la sentencia del TJUE (2014) en el asunto C-131/12 (Google Spain y Google Inc. c. AEPD y Mario Costeja González, 13 de mayo de 2014). El señor Costeja demandó que tanto el periódico *La Vanguardia* como Google vulneraban su honor, prestigio y privacidad al publicar y conservar una nota periodística antigua que expresaba un estado inapropiado de su condición al señalársele ciertas condiciones ya no vigentes, como eran su estado civil y su condición económica como deudor. Por su parte, los tribunales español y europeo determinaron que los motores de búsqueda son responsables del tratamiento cuando indexan y ordenan información personal publicada por terceros y que —tras una ponderación caso por caso— puede ordenarse la desindexación de enlaces que afecten de modo significativo los derechos del interesado y carezcan ya de pertinencia. Además, reconocieron que estos motores sí realizan tratamiento de datos personales, echando al traste una de las principales argumentaciones de Google, que aseguraba no llevar a cabo este tipo de actividades. También se determinó que *La Vanguardia* no estaba obligado a eliminar dicha información de su archivo digital, por tratarse de una nota periodística bajo el derecho de libertad de prensa.

España, a través de la Agencia Española de Protección de Datos Personales, tuvo un papel trascendente en el tema, al resolver centenares de reclamaciones por desindexación tutelando datos personales frente a la exposición de información que produce un buscador, incluso si la información original permanecía lícita en origen. La Audiencia Nacional, y finalmente el TJUE, perfilaron en equilibrio entre privacidad y libre información, que hoy conocemos como “derecho al olvido”.

Tras Costeja, otras decisiones del Tribunal Europeo delinearon su alcance material y territorial: (a) C-136/17, GC y otros c. CNIL (TJUE, 2019a), que precisó que la prohibición de tratar categorías especiales de datos sensibles también vincula a los buscadores y que, ante solicitudes de cancelación u oposición, debe realizarse una ponderación robusta de derechos fundamentales; y (b) C-507/17, Google LLC c. CNIL (TJUE, 2019b), determinó que la obligación de desindexación no tiene alcance global, sino que se circunscribe al territorio de la Unión Europea, sin perjuicio de que en situaciones concretas puedan adoptarse medidas eficaces para evitar el acceso desde la Unión.

3. Su inclusión en el Reglamento Europeo (RGDP)

Luego de la entrada en vigor del Reglamento General de Protección de Datos en 2018, es en el artículo 17 donde se regula el derecho al olvido, señalando en seis causas la obligación del responsable a borrar o suprimir datos "sin dilación indebida": (a) los datos ya no son necesarios para los fines por los que fueron tratados; (b) retiro del consentimiento; (c) oposición al tratamiento y ausencia de interés legítimo prevaleciente; (d) tratamiento ilícito; (e) obligación legal de suprimir; y (f) datos recabados en el marco de servicios de la sociedad de la información respecto de menores.

De tal manera que los motores de búsqueda en los países de la Unión Europea donde operen tendrán que tener un apartado y procedimiento a través del cual los titulares puedan solicitar de manera sencilla y rápida que la información contenida en sus resultados de búsqueda pueda ser desindexada (eliminada de los resultados de búsqueda) por no ser veraz, pertinente o apropiada.

Cabe señalar que este derecho no es absoluto, habiendo excepciones como en el ejercicio del derecho a la libertad de

expresión e información, el cumplimiento de obligaciones legales, fines de archivo de interés público, investigación científica/ histórica o estadística y defensa de reclamaciones, que imponen la ya mencionada ponderación.

Las directrices 5/2019 del Comité Europeo de Protección de Datos (EDPB, 2019), posteriores a los fallos de 2019, sistematizan nuevos criterios prácticos como análisis del tipo de consulta, naturaleza de la información (sensibilidad, veracidad, exactitud), papel del interesado en la vida pública, tiempo transcurrido, interés del público y la adecuación/pertinencia frente a los fines del tratamiento.

De esta manera se elaboraron criterios de ponderación para disminuir la discrecionalidad y estandarizar la forma en que se determine la procedencia o no del derecho:

1. Interés público actual de la información. Esto se explica con la siguiente pregunta: ¿Se trata de hechos de relevancia pública (p. ej., corrupción, salud pública, seguridad) o de interés meramente curioso? A mayor interés público, menor procedencia de retirar enlaces.
2. Rol del solicitante. No es lo mismo una figura pública o con proyección pública (cargo, liderazgo empresarial, influencia) que un particular; respecto de los primeros, el escrutinio es más intenso y la desindexación exige justificar que la intromisión excede lo tolerable.
3. Naturaleza y sensibilidad del dato. Los datos sensibles (salud, orientación sexual, creencias, etc.) merecen mayor protección; sin embargo, incluso ahí procede ponderar veracidad, interés público y finalidad informativa.
4. Exactitud, veracidad y contexto. La inexactitud o desactualización sustancial favorece la supresión/

desindexación; si la información es veraz, exacta y contextualizada, y responde a fines informativos legítimos, se refuerza el interés público.

5. Tiempo transcurrido y finalidad del tratamiento. El paso del tiempo puede volver desproporcionada la exposición agregada de datos, pero no es, por sí solo, decisivo; hay que valorar la vigencia del interés público.
6. Medida solicitada y proporcionalidad. No se solicita borrar en origen (fuente), sino desindexar en búsquedas asociadas al nombre de la persona, manteniendo la noticia accesible mediante consultas temáticas o hemerográficas, siendo una solución intermedia que limita el daño reputacional sin invisibilizar el archivo.
7. Ámbito territorial de la medida. Tras el caso C-507/17 en Francia, la desindexación obligatoria rige dentro de la UE; pueden adoptarse mecanismos de geobloqueo u otras medidas eficaces para evitar el acceso desde territorio europeo, sin imponer un "derecho al olvido" global. Esto representó uno de los grandes triunfos de los motores de búsqueda frente al alcance del derecho al olvido.

4. Situación del derecho al olvido en México: casos Sánchez y Richter

4.1. Antecedentes

Si bien México cuenta con su propio marco normativo de protección de datos personales recientemente reformado (Constitución Política de los Estados Unidos Mexicanos, artículos 6 y 16; leyes General y Federal de Protección de Datos Personales y su reglamento), con derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO), principios y deberes, la figura europea del "derecho al olvido" no está

formulada en el ordenamiento mexicano y en la práctica algunas solicitudes han intentado encauzarse por cancelación u oposición frente a resultados en motores de búsqueda y publicaciones en Internet. A continuación se exponen algunos de los casos más representativos.

4.2. El caso Sánchez de la Peña (2014-2017): INAI, libertad de expresión y revisión judicial

En 2014, el empresario Carlos Sánchez de la Peña solicitó a Google México la remoción de enlaces que lo asociaban con una nota periodística de 2007. Ante la negativa, interpuso como recurso un procedimiento de protección de derechos ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) (exp. PPD.0094/14), que en enero de 2015 resolvió ordenar a Google México remover los enlaces, aludiendo —controvertidamente— al "derecho al olvido" (INAI, 2015). La revista *Fortuna*, afectada por la resolución, impugnó con apoyo de organizaciones de libertad de expresión y en agosto de 2016 un tribunal colegiado concedió el amparo y anuló la resolución del INAI, ordenando reponer el procedimiento para garantizar la audiencia de la revista y salvaguardar la libertad de expresión.

Este caso expuso dos puntos trascendentes: 1) la duda sobre si los buscadores pueden ser tratados como responsables sujetos a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) por sus funciones de indexación; y 2) la necesidad de un test de ponderación robusto que evite convertir la desindexación en una censura indirecta de contenidos periodísticos.

4.3. El caso Ulrich Richter vs. Google: daño moral y plataformas

En una vía distinta —responsabilidad civil por daño moral— se ubica Ulrich Richter Morales vs. Google. El litigio se origina por las constantes publicaciones de un blog difamatorio en su contra. En 2022, la Octava Sala Civil de la Ciudad de México condenó a Google al pago de 5 000 millones de pesos por daño moral, decisión que la empresa impugnó; en 2023 se dictaron medidas de suspensión mientras el asunto pasaba a la Suprema Corte de Justicia de la Nación (SCJN). Aunque no es un litigio de "derecho al olvido", la discusión pública lo asoció con la capacidad de exigir a plataformas que atiendan contenidos ilícitos o difamatorios alojados en sus servicios. El asunto fue turnado al actual presidente de la Corte sin fecha para su resolución.

4.4. Criterio reciente de la SCJN: incompatibilidad del "falso derecho al olvido"

En febrero de 2023 la SCJN (Primera Sala) publicó una tesis en la que sostiene que el "derecho al olvido", tal como ha sido entendido y formulado en la Unión Europea, resulta incompatible con las normas constitucionales mexicanas sobre libertad de expresión y libre acceso a la información (artículos 6 y 7), subrayando que en México no existe definición legal clara de esa figura, que su redacción importa ambigüedad y que el simple transcurso del tiempo no despoja a la información pública de su interés (SCJN, 2023). Este posicionamiento evita recepciones acrílicas de la solución europea y exige un diseño normativo propio, si se quisiera avanzar hacia una regulación.

La tesis también aclara que los motores de búsqueda que actúan como "medios o vehículos neutros a los contenidos creados por terceros" no pueden ser considerados responsables por dichos

contenidos. Esto significa que el buscador no es un responsable primario del contenido en sí, sino un canal de información.

Mientras que la normativa europea permite a las personas exigir la eliminación de información personal en Internet bajo ciertas condiciones, la SCJN consideró que una aplicación similar en México entraría en conflicto con los derechos fundamentales consagrados en su Constitución.

5. La conveniencia de reconocer y regular esta figura

Aun aceptando las consideraciones vertidas por la Primera Sala de la SCJN, puede argumentarse que regular un mecanismo específico de supresión o desindexación sería pertinente por las siguientes razones:

1. Respeto de la autodeterminación informativa. La acumulación y fácil localización por nombre propio crea un efecto ampliador del daño que no estaba presente en el tráfico de la información analógica; un remedio focalizado (desindexación nominativa) podría mitigar impactos reputacionales injustificados sin suprimir archivos periodísticos.
2. Claridad procedimental y seguridad jurídica. La experiencia del desaparecido INAI en la protección de datos personales en el caso de Sánchez mostró carencias de procedimiento (audiencia a medios de comunicación). Una regulación podría establecer legitimación, estándares probatorios, notificación a fuentes periodísticas, plazos y un test de ponderación con variables explícitas y vista a terceros interesados (rol público, veracidad, actualidad, fuente, finalidad, tiempo, alcance).
3. Coherencia con estándares internacionales de datos personales. Sin importar el nombre que se le atribuya, ya sea "olvido" o "supresión/desindexación", un marco claro alineado

con principios de minimización, limitación de finalidad y responsabilidad proactiva ayudaría a interoperar mejor el ejercicio y límites de este derecho, junto con la actualización de principios en materia de protección de datos personales, como se ha hecho en Europa (transferencias y cumplimiento para actores mexicanos con operación en Europa, privacidad por defecto y diseño, etc.).

4. Mejoras graduales y proporcionales. Frente a la disyuntiva "todo/nada", la desindexación nominativa, la deslistación temporal o la inserción de avisos/contexto pueden ser remedios menos lesivos que eliminar contenidos en origen y más eficaces que litigios largos por daño moral.
5. Transparencia y rendición de cuentas de intermediarios. Exigir registros de solicitudes, informes de cumplimiento y mecanismos de apelación fortalece la confianza y evita decisiones opacas o arbitrarias de plataformas, así como dictámenes de viabilidad en las plataformas, aplicaciones y sistemas que traten datos personales, por parte de las autoridades garantes para poder operar y sus respectivas certificaciones.
6. Criterios de ponderación. Como se mencionó en líneas anteriores, la legislación europea y los organismos reguladores establecieron una serie de criterios que ayudan a disminuir la discrecionalidad y a ponderar los casos en que es totalmente procedente la desindexación de datos en motores de búsqueda, impidiendo además que este derecho se vuelva absoluto y automático.

6. Críticas y riesgos señalados por la doctrina y especialistas

Además de los aspectos señalados por la Corte, tanto a nivel doctrinal como de organizaciones internacionales de libertad de expresión, se han planteado objeciones relevantes:

1. Riesgo de censura indirecta. La desindexación puede transformarse en una "borradora reputacional" y no en depuradora de hechos veraces y de interés público, afectando la memoria social y la labor periodística. De ahí que varios estándares insistan en ponderaciones estrictas y en la no automaticidad del tiempo transcurrido. La propia SCJN recalcó que el paso del tiempo no despoja por sí mismo el interés público.
2. Efecto global indeseado. Intentos de remover vínculos a escala mundial podrían generar una "carrera a la baja" (*race to the bottom*) de estándares de expresión; el TJUE en C-507/17 impidió generalizar esa pretensión.
3. Uso sin medida y control basado en el poder de ciertos sectores. En la práctica, quienes más recursos tienen podrían conseguir "limpiezas de reputación" frente a resultados desfavorables pero relevantes para el escrutinio público. Las directrices del EDPB sugieren, por ello, mayor escrutinio cuando se trate de figuras públicas.
4. Conflicto con el derecho a saber y el archivo. La labor hemerográfica y de archivo de medios, bibliotecas y repositorios se vería afectada si se confunde desindexación con eliminación; la respuesta regulatoria debe preservar el acceso temático o por otros criterios no nominativos.
5. Fragmentación regulatoria y cargas de cumplimiento. Sin claridad normativa, las plataformas aplican políticas propias (a veces más amplias o más estrechas que los estándares legales), lo que puede producir inconsistencias, opacidad y decisiones asimétricas. Posibilidad de actuación discrecional por las mismas plataformas y sistemas de búsqueda.

7. Conclusiones para México

De todo lo anterior se puede concluir una serie de recomendaciones

en el caso de que se desee implementar una figura como el derecho al olvido en México, las cuales se pueden resumir en las siguientes propuestas puntuales:

1. No "trasplantar" el modelo europeo tal cual. Queda claro que no se puede reconocer un derecho al olvido que trate el tiempo como factor determinante *per se* ni que erosione la presunción de publicidad de la información. Cualquier reforma debe ser un trabajo fino, no una copia.

2. Establecer un remedio de "desindexación nominativa" cuidadosamente acotado, distinto de borrar en origen, con:
   a. Causales inspiradas en el artículo 17 del RGPD (necesidad, licitud, consentimiento, etc.), pero incorporando excepciones fuertes para libertad de expresión, información y archivo.
   b. Test de ponderación explícito (rol público, veracidad, interés actual, sensibilidad del dato, contexto, tiempo transcurrido, finalidad del tratamiento, proporcionalidad de la medida).
   c. Garantías procesales: audiencia efectiva a medios/autores, notificación a terceros afectados, posibilidad de oponerse y de apelar. La lección del caso Sánchez es inequívoca.
   d. Ámbito territorial: limitar efectos a México, con herramientas técnicas proporcionales (geolocalización, etc.), siguiendo el criterio C-507/17.
   e. Colaboración de las empresas y corporaciones que manejen motores de búsqueda y similares para que sean parte del proceso y no queden solamente contraparte.

3. Armonizar la vía de datos personales con la civil (daño moral/difamación). El caso Richter demuestra que, en ausencia de una vía de desindexación normada, los conflictos migran a la responsabilidad civil, con reparaciones potencialmente

desmesuradas y debates complejos sobre la responsabilidad de intermediarios. Un cauce de datos personales, con remedios proporcionales y auditables, puede despresurizar los litigios sin desalentar la libre expresión.

4. Transparencia y debida rendición de cuentas respecto a:
   a. Publicación periódica (anónima y agregada) de estadísticas de solicitudes de cancelación y/u oposición, tasas de aceptación/rechazo y principales motivos.
   b. Informes de impacto en libertad de expresión.
   c. Procedimientos expeditos para corregir inexactitudes sin suprimir noticias veraces y limitarse al plazo de 20 días que marcan nuestras leyes.

5. Educación digital y corregulación.
   a. Estándares de etiquetado contextual (p. ej., sentencias posteriores de absolución enlazadas a notas antiguas).
   b. Rectificaciones visibles sin borrar hemeroteca, como fue en el caso Costeja.
   c. Fomento de buenas prácticas editoriales y de indexación responsable.

8. Epílogo: memoria, reputación y acceso a la verdad

El “derecho al olvido” no es una llave para ocultar el pasado, sino un diálogo sobre cómo preservamos la memoria colectiva sin convertir la indexación algorítmica en una pena perpetua para la identidad digital de las personas. La experiencia europea muestra que sí es posible atender las asimetrías creadas por buscadores sin anular el archivo periodístico: la desindexación nominativa es una herramienta especial sujeta a una ponderación de derechos estricta y a excepciones concretas y específicas. México, con su tradición constitucional de máxima publicidad, puede

desarrollar un instrumento propio, más nítido y compatible con su jurisprudencia y normativa, que proteja a la vez la dignidad de las personas, su autodeterminación informática y el derecho a saber.

Referencias

Agencia Española de Protección de Datos. (2023, 10 de noviembre). *Derecho de supresión ("al olvido"): buscadores de Internet*. https://www.aepd.es/areas-de-actuacion/internet-y-redes-sociales/derecho-al-olvido

Álvarez, M. (2015). *Derecho al olvido en Internet: El nuevo paradigma de la privacidad en la era digital*. Editorial Reus.

Artículo 19 México. (2016-2023). *Informes sobre libertad de expresión y memoria digital en Internet*. Artículo 19 México.

Ausloos, J. (2011). The 'right to be forgotten' - Worth remembering? *Computer Law & Security Review*, *28*(2), 143-152. https://ssrn.com/abstract=1970392

Calcaneo Monts, M. A. (2019). Big data, big data analytics y datos personales en los tiempos del Internet: de la autorregulación estadounidense al Reglamento General de Protección de Datos de la Unión Europea. *Estudios en Derecho a la Información*, *1*(8), 21-44. https://doi.org/10.22201/iij.25940082e.2019.8.13882

Comité Europeo de Protección de Datos. (2019). *Directrices 5/2019 sobre los criterios del derecho al olvido en los casos de motores de búsqueda en virtud del RGPD*. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_es.pdf

Cubillos Vélez, A. (2017). La explotación de los datos personales por los gigantes de Internet. *Estudios en Derecho a la Información*, *1*(3), 27-55. https://doi.org/10.22201/iij.25940082e.2017.3.10823

De Terwangne, C. (2012). Le droit à l'oubli: un droit de l'ère numérique. *Revue du droit des technologies de l'information*, 47, 245-275.

González Fuster, G. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Springer.

Guerrero Santillán, E. C. (2018). *El derecho al olvido digital en México*. Universidad de Guadalajara.

Guzmán Camacho, J. J. (2023). El ejercicio del derecho al olvido en México. *Estudios en Derecho a la Información*, *1*(16), 35-49. https://doi.org/10.22201/iij.25940082e.2023.16.18070

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2015). *Resolución PPD.0094/14* (Sánchez de la Peña vs. Google México). https://inicio.inai.org.mx/AcuerdosDelPleno/ACT-PUB-20-05-2015.09%20ACG.pdf

Koops, B. J. (2011). Forgetting footprints, shunning shadows: A critical analysis of the 'right to be forgotten'. *SCRIPTed*, *8*(3), 229-256. http://dx.doi.org/10.2139/ssrn.1986719

R3D: Red en Defensa de los Derechos Digitales. (2016-2023). *Informes y análisis sobre desindexación, libertad de expresión y responsabilidad de intermediarios*. R3D: Red en Defensa de los Derechos Digitales.

Rallo Lombarte, A. (Ed.). (2014). *El derecho al olvido en Internet. Google versus España*. Centro de Estudios Políticos y Constitucionales.

Reglamento General de Protección de Datos. 27 de abril de 2016. Parlamento Europeo y del Consejo. https://www.boe.es/doue/2016/119/L00001-00088.pdf

Pérez, H. E. (2019). *Datos personales y libertad de expresión en México: tensiones y puntos de equilibrio*. Revista Mexicana de Derecho Constitucional.

Suprema Corte de Justicia de la Nación. (2023, 24 de febrero). *Tesis de la Primera Sala sobre la incompatibilidad del "derecho al olvido" europeo con la Constitución mexicana*. Gaceta del Semanario Judicial de la Federación. https://www.scjn.gob.mx/sites/default/files/comunicacion_digital/2023-03/Precedentes_y_tesis_1aSala_24_feb_al_17_mar_2023.pdf

Tribunal de Justicia de la Unión Europea. (2014, 13 de mayo). *Asunto C-131/12, Google Spain y Google Inc. c. AEPD y Mario Costeja González*. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62012CJ0131

Tribunal de Justicia de la Unión Europea. (2019a, 24 de septiembre). *Asunto C-136/17, GC y otros c. CNIL*. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62017CA0136&from=ES

Tribunal de Justicia de la Unión Europea. (2019b, 24 de septiembre). *Asunto C-507/17, Google LLC c. CNIL*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62017CJ0507

Tribunal Electoral del Poder Judicial de la Federación. (2023). *Los claroscuros del derecho al olvido en la era digital*. Sentencia 1 BvR 16/13. Sentencia STC 58/2018. Editorial TEPJF.

Valderrama, M. (2016, 23 de agosto). *Derecho al olvido en el contexto iberoamericano* [Presentación]. Foro Derecho al olvido, tutela integral de la privacidad. Visión Iberoamericana, Ciudad de México, México.

5. Derecho a la protección de datos personales, una fundamentación ontológica

Dr. Jesús Manuel Guerrero Rodríguez
Dr. David Reynaldo Díaz Rascón
Dr. Rodrigo Ramírez Tarango

Resumen

Este estudio analiza y demuestra desde la filosofía y diversas ciencias que la persona humana es el fundamento ontológico del derecho a la protección de datos personales. Se analiza cómo este derecho tiene sustento en la naturaleza del ser humano; ello significa que no encuentra su justificación solo en motivos de carácter individual, ni en un acto legislativo o decreto gubernamental, sino que la autoridad política se limita a declarar la existencia de este derecho ya presente en el ser humano.

Palabras clave: Persona; derecho; causa; orden natural; datos personales.

Introducción

Conocer y responder cuál es el fundamento ontológico del derecho a la protección de datos personales implica estudiar y comprender su naturaleza, justificación y existencia, es decir, "saber de un modo radical lo que es, plantear el problema de su auténtica y rigurosa existencia y de su sentido" (Tagle, 1950). Esto implica conocer y determinar sus causas y principios.

En este estudio se expone, a través de la razón, de forma rigurosa desde la filosofía clásica y contemporánea, el método filosófico y descriptivo con la revisión de autores clásicos y contemporáneos, mediante un método crítico multidisciplinar (Halpern, 2014; Paul & Elder, 2002) desde la metafísica, antropología, gnoseología, psicología, biología y ética, el fundamento ontológico del derecho a la protección de datos personales, con lo cual se demostrará que la persona o ser humano (Organización de los Estados Americanos, 1969), considerando su orden natural y la participación de este en los primeros principios de la razón, es el fundamento esencial del derecho referido, analizando el marco legal de referencia, la ontología de la persona, de cuya condición se sigue la dignidad humana, fundamentos ineludibles para el conocimiento y cimentación del derecho que nos ocupa.

De tal forma que, si la persona en cuanto ente es el fundamento ontológico del derecho a la protección de datos personales, significa que no encuentra su justificación solo en motivos de carácter individual, ni en un acto legislativo o decreto gubernamental, sino que por ese acto la autoridad política, a través del poder o poderes competentes, se limita a reconocer, en el sentido de aceptación de la existencia de este derecho que posee el ser humano intrínsecamente por el hecho de ser persona. De tal modo que, contrario a lo que algunos estudiosos del derecho afirman, la esencia y existencia objetiva de tal derecho no proviene necesariamente de motivos sociales o bien de la existencia o reconocimiento de la ley positiva del legislador ordinario, pues lo más que puede determinar esta sería su reconocimiento como algo anterior a ella y frente a otros hombres, pero nunca su creación.

Marco jurídico de referencia del derecho a la protección de datos personales

La Convención Americana sobre Derechos Humanos (1969) no cuenta con un artículo que mencione expresamente "derecho a la protección de datos personales", tampoco con una definición expresa de este derecho; no refiere término concreto sobre qué es o cuál es su fundamento. Sin embargo, se advierten en esta, redacciones que permiten inferir ese derecho. Por ejemplo, en los artículos 11, 12 y 13 establece el respeto de la honra y al reconocimiento de la dignidad, la privacidad, libertad de conciencia, libertad de pensamiento y expresión; lo anterior implica aspectos como creencias religiosas, filosóficas y morales, y opiniones políticas, de tal modo que se refiere a los fenómenos, operaciones o manifestaciones que produce o expresa el ser humano.

La Convención sobre los Derechos del Niño (1989), en el artículo 16, numerales 1 y 2, protege la vida privada o intimidad de los niños, en el sentido de que no serán objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y a su reputación, así como el derecho que el niño tiene a la protección de la ley contra esas injerencias o ataques.

La Constitución Política de los Estados Unidos Mexicanos (2024) le otorga el carácter de derecho autónomo al reconocerlo en el artículo 6, apartado A, fracción II, en el sentido de que "la información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes". Luego, en el artículo 16 determina que "toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar

su oposición, en los términos que fije la ley" (Constitución Política de los Estados Unidos Mexicanos, 2024). Sin embargo, en la redacción de ambos preceptos no se especifica que la persona sea el fundamento de dichos datos, sino solo titular de aquellos, y pareciera le otorga el derecho a las personas de decidir libremente sobre el uso de su información personal, lo que es erróneo.

Sobre el concepto datos personales, la Suprema Corte de Justicia de la Nación (SCJN, 2024) hizo patente que la expresión datos personales es un concepto de orden constitucional, hecho que se desprende los artículos 6 apartado A, fracción II y 16 de la Carta Magna. Esto significa que goza de una jerarquía superior por ser un bien jurídicamente protegido por la Constitución federal.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017), en el artículo 3, fracción IX, establece que los datos personales son "cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información". Por datos personales sensibles establece que son:

> aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para ésta. De manera enunciativa mas 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. (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017, artículo 3, fracción X)

En la redacción del artículo 6 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados pareciera encontrarse la fundamentación ontológica del derecho en cuestión, sin embargo, encontramos la palabra "concerniente", término que de ningún modo es empleado por el legislador en el sentido de que sea la persona el fundamento del derecho objeto de estudio, sino que, de acuerdo con el Diccionario de la Lengua Española (2023), significa que "atañe, afecta o interesa", es decir, que incumbe a la persona.

Fundamentación y noción del derecho a la protección de datos personales por los tribunales

La Suprema Corte de Justicia de la Nación afirma que la protección de datos personales es un derecho fundamental, como tal:

> encuentra su justificación en motivos de carácter individual y social, los primeros porque permiten a las personas el desarrollo de su autonomía personal y la elección de la manera en que una persona se identifica y elige conducirse; por otro lado, los motivos de carácter social radican en su importancia actual para el correcto desarrollo de las relaciones de consumo, así como en la distribución justa y equitativa de todo tipo de bienes y servicios. (Suprema Corte de Justicia de la Nación [SCJN], 2023, párrafo 3)

El máximo tribunal del país no precisa cuáles sean esos motivos que permiten el desarrollo de la autonomía personal, ni que permiten "la elección de la manera en que una persona se identifica y elige conducirse" (SCJN, 2023). Observamos que el pronunciamiento con el cual la SCJN justifica el derecho a la protección de datos personales no va más allá del nivel de la integración de los datos sensibles en relación con las cosas exteriores, del propio cuerpo

y de las propias sensaciones, no así de lo que es la persona tanto en esencia como en naturaleza. Por ello estimamos que esta justificación proviene de un equívoco de lo que la persona es y cuál sea su fin, resultado de confundir la esencia del ser humano con lo sensible, sus propiedades, funciones, facultades y operaciones, lo que hace imposible un discernimiento fructuoso, de donde se observa que el derecho a la protección de datos personales tiene como fundamento una identidad construida desde el exterior, de una agrupación o "complejo" de representaciones o de "identificaciones" de lo que creemos que somos, incluso en motivos de carácter social ligados al consumo. Nada más alejado de la realidad, pues una cosa es lo que pensamos ser y, otra muy diferente, lo que real y verdaderamente somos.

La persona o ser humano

En la filosofía clásica el hombre fue definido por Aristóteles (1994) como "por naturaleza un animal social", un *"politikón zôion"* (πολιτικὸν ζῷον). El sustantivo *zôion* quiere decir "ser viviente", "animal", y el adjetivo que le acompaña lo califica como perteneciente a una *polis*, que es a la vez la sociedad y la comunidad política. Más allá de su instinto gregario, el hombre es un ser social, porque es el único animal en la naturaleza que habla y, por tanto, comunica, comparte y confronta sus ideas a otros seres del mismo género; en virtud de esto, de manera natural crea instituciones como la familia y el Estado, así como diversas formas de organización social.

El ser humano ontológicamente es persona, no es un dato o fenómeno más entre otros, ni organismo exclusivamente biológico, ni solo un sistema, sino que de acuerdo con Ceferino Boecio, citado por Martí (2017), es una "sustancia individual de naturaleza racional" (p. 113). Etimológicamente viene del latín *substantia*, que

significa “lo que está debajo o lo permanente bajo los fenómenos, es lo que tiene su ser, no en otro, sino en sí” (Brugger, 1962, p. 450); es decir, tiene subsistencia propia, lleva en sí el ser, lo que equivale a existir en sí mismo, de tal manera que existe de modo independiente.

En este sentido, la persona es una realidad que existe con vida psíquica, es decir, con percepción, pensamiento, memoria y pasiones (emociones), sobre todo entiende y comprende lo que conoce, tiene conciencia de sí y de que está teniendo conciencia, etcétera, lo que constituye su actividad “mental” y orgánica propias, una y múltiple, contiene y desarrolla propiedades, funciones, facultades y operaciones. Lo anterior compone lo que conocemos como esencia y naturaleza de la persona humana, que hace imposible que el derecho positivo, ley positiva o ciencia jurídica puedan existir sin un trabajo preliminar de abstracción para conocer en toda su estructura entitativa lo que es la persona y, en consecuencia, responder: ¿por qué es el fundamento del derecho a la protección de datos personales y derecho positivo en general?

Por ser persona, dice Martín Echavarría (2022):

> el ser humano tiene una perfección que no poseen los otros entes materiales: es capaz de entender la esencia de las cosas, es capaz de volver sobre sí mismo (reflexión) y está dotado de libre arbitrio, de tal manera que es dueño de sus actos, de modo que no es ‘actuado’, sino que actúa él por sí mismo, haciendo de la persona lo más individual y activo. (p. 205)

Esta afirmación es acorde con el pensamiento de Tomás de Aquino, quien expresa que “de un modo más especial y perfecto se da lo particular y el individuo en las sustancias racionales, que tienen

dominio de sus actos, y no son solo actuados, como las demás cosas, sino que actúan por sí mismos" (S. T., I, q. 29, a. 1).

Esta concepción de Echavarría (2022), con fundamento en el Aquinate, es trascedente por su consecuencia en la fundamentación ontológica del derecho a la protección de datos personales, porque precisamente la persona es dueña de sus actos por los cuales produce datos personales y sensibles, tiene poder moral o dominio sobre estos, los realiza o no, los obra o no, los hace o no los hace; en este sentido es el hecho de actuar, de acuerdo con Echavarría (2022), y no de ser actuado. Esto tiene como consecuencia, por justicia, la protección del Estado, por el respeto que se exige a la interioridad del ser humano que obra, que desencadena por sí mismo los actos singulares que se caracterizan por ser datos precisamente del orden personal, tales como el honor, la reputación, la vida privada y, consecuentemente, la dignidad humana, entre otros.

Además de los datos mencionados, la persona capta en sí lo intelectual y lo sensible de un objeto o hecho, por ejemplo, de una situación familiar, económica, política, religiosa o de una enfermedad. Esto impacta en su organismo mediante la producción de emociones, siente tristeza o alegría, puede enfermar; también impacta el intelecto o inteligencia, de ello produce conceptos, ideas, formula juicios que puede o no expresar, de tal modo que genera información en su intimidad y que solo a ella le pertenecen. Por las mismas facultades intelectivas, entendimiento, voluntad y la libertad como cualidad de la segunda, así como las facultades orgánicas que manifiesta la persona, posee un conocimiento más profundo de sí misma. En esta experiencia de intimidad personal no requiere el concurso de persona alguna o del derecho para desencadenar la producción de unas determinadas categorías de información personal o sensible, por ejemplo información

emocional, sentimientos, estados psicológicos de ánimo como la alegría, el miedo, la tristeza, la culpa, el amor o la frustración, información de la cual es titular, y que en determinado momento puede ser objeto de un expediente clínico de carácter médico, psicológico o psiquiátrico, laboral o académico.

De igual modo, en esa comunicación íntima o intrapersonal, la persona produce pensamientos, creencias, ideas sobre sí misma, convicciones religiosas o ideológicas que guían su conducta. Aspiraciones personales, metas, motivaciones profundas que no comparte públicamente, sobre las que tiene un poder moral porque le pertenecen, son propias, es en última instancia la causa eficiente de que sean o existan. Por tal razón puede disponer de todos estos datos o información puesto que es generada por ella e inmediatamente para sí. Tal es el "principio del derecho a la propiedad" que respecto de la información en cuestión se entiende como el control exclusivo que tiene sobre dichos datos y usarlos y disfrutarlos y, en su caso, de compartirlos.

Esta concepción de información personal tiene implicaciones importantes dado que, como datos personales, irreductiblemente están vinculados a los actos humanos, siendo aquellos en los que participa el intelecto, la voluntad y la libertad, considerados parte de la identidad y la dignidad de la persona. De ahí que, su recopilación, almacenamiento y uso deben ser realizados con el consentimiento informado de la persona cuya titularidad le es atribuida, garantizando su autonomía y libertad como cualidad de la voluntad que, con conocimiento, otorga el consentimiento para el tratamiento de sus datos personales.

La persona humana es un sujeto individual y racional (indica todas las capacidades del hombre), y esta es quien realiza los actos humanos, en los que participa el entendimiento, la voluntad y la

libertad. Estos actos humanos —al igual que los actos sobre los cuales la persona es materialmente dueña pero no tiene dominio sobre estos ni responsabilidad, como el soñar, o una enfermedad como el cáncer, que no son producto de la inteligencia o voluntad— producen datos personales y estos son los que el Estado tiene la obligación de garantizar y proteger respecto de todo individuo al modo de no ser interferido o molestado por terceros o por una autoridad en ningún aspecto de su persona y vida privada, en especial aquellos que corresponden a los extremos más personales de la vida y del entorno familiar (intimidad), o que permiten el desarrollo integral de su persona y personalidad, incluida la dignidad humana.

Persona fundamento de datos personales

Regis Jolivet (1959) señala que toda la vida psíquica tiene como sujeto al ser humano, quien se nos da primero empíricamente, como un "yo" físico y moral que perdura a través de todas las transformaciones psicológicas, y condicionan el sentimiento de nuestra identidad personal. El "yo" "es, pues, objetivamente, el conjunto de todos los fenómenos orgánicos, fisiológicos y psicológicos que constituyen a un sujeto determinado" (Jolivet, 1959). Esos fenómenos se nos revelan mediante datos sensibles, expresiones de tristeza, alegría, dolor o intangibles, ideas que no pueden ser percibidas por el tacto.

Más tarde ese yo objetivo tiene en el ser humano el poder de conocerse a sí mismo. Esta conciencia subjetiva es además preparada y condicionada por el confuso y sordo sufrimiento de existir como sujeto, pero también por la clara y serena alegría o felicidad de saberse vivo y consciente, con plenitud interior, sentimientos que acompañan todos los fenómenos psíquicos y que el ánima debe poseer lo mismo que el hombre. Pero el yo

propiamente dicho, que tiene no solo conciencia de subjetividad, sino noción de esa subjetividad y posesión de sí por la reflexión, es el privilegio de la persona, única de decir "yo".

Javier Hervada (1994) explica que persona es el hombre en cuanto ser dotado de inteligencia y libertad y como tal, superior por naturaleza a todas las demás creaturas (y cosas). Esta superioridad del ser humano sobre los que carecen de razón es lo que permite hablar de "dignidad de la persona humana" sujeto de derecho, debiendo este, por imperativos del derecho natural, reconocerles una esfera de libertad individual mediante el reconocimiento (declaración de existencia sería la palabra idónea) de una serie de derechos fundamentales.

Como substancia existente por derecho propio, su *juris*, que es perfectamente "incomunicable". El ser de la persona es un ser suyo, de modo que, para hablar en términos actuales, diríamos que la nota distinta de la persona es la propiedad (Ferrater Mora, 1980, p. 2552); entonces hablamos de "jus". Finnis (1992, p. 235) señala que el "significado verdadero, estricto y propio" de "jus" ha sido planteado por Francisco Suárez como "una clase de poder moral [facultas] que todo hombre tiene, ya sobre sus propios bienes ya respecto de aquello que le es debido". De tal modo que esencialmente el "jus" es algo que pertenece a la naturaleza humana y los primeros principios del conocimiento.

En este sentido, podemos afirmar que cada persona tiene "bienes", además de ser en sí un bien. Estos los encontramos en la identidad personal propia, identidad biológica propia, es incomunicable, responde a una singularidad biológica, es único o irrepetible histórica y biográficamente, es un ser absoluto desde su concepción, posee autonomía, además de contar con interioridad y apertura relacional.

La identidad de ser persona o sustancial refleja la esencia y dignidad permanente de la persona, vinculando metafísica, psicología y derecho; a esta identidad corresponden los datos personales que remiten a la estructura ontológica y esencial de la persona, que lo hacen ser lo "que es" de manera única e irrepetible. Estos datos no cambian a lo largo de la vida, por ejemplo, el ser, concretamente la persona como individuo único, significa que a pesar de los cambios del cuerpo él permanece en sí en el tiempo, de tal modo que el "yo" quien se identifica como el mismo ser humano a los 5, 10, 20, 40 y 60 años permanece, no cambia. Lo mismo sucede con el sexo biológico cromosómico, huellas dactilares, ADN, iris y diferentes huellas biométricas invariables, entre otros; estos datos permanecen desde la concepción hasta la muerte.

También encontramos datos personales de identidad accidental, es decir, aquellos que cambian y no son permanentes. Estos refieren propiedades accidentales de la persona, requieren de esta para existir, son aspectos que pueden existir o no en la persona, así como modificarse sin alterar la esencia de aquella. De este modo encontramos el domicilio, el estado civil, la ocupación o profesión, el correo electrónico, número telefónico, estado de salud, cuentas bancarias, etcétera.

Derecho a la protección de datos personales: ¿derecho natural o subjetivo?

Estudiar desde la perspectiva de la ontología una prerrogativa fundamental establecida como tal en la Constitución exige precisar si se trata de un derecho natural, inscrito en la esencia misma de la persona, o de un derecho subjetivo que depende de la voluntad y facultad de la persona, o bien de ambos.

Ferrajoli afirma que las prerrogativas fundamentales son "todos

aquellos derechos subjetivos que corresponden universalmente a todos los seres humanos en cuanto dotados del *status* de personas, de ciudadanos o de personas con capacidad de obrar" (Aguilar Cisneros & Rincón Mayorga, 2022, p. 40). Efraín González (2003) sobre el derecho subjetivo o facultad jurídica, argumenta que "es la potestad moral del titular del Derecho sobre lo justo objetivo que le debe el obligado". De este modo podemos decir que para poseer derechos se requiere ser persona, de tal manera que sin esta aquellos no existen. Luego, podemos afirmar con Del Vecchio (1953) "que no queda más que recurrir a la naturaleza humana, es decir, buscar en la conciencia de nuestro ser el fundamento último del derecho" (p. 37).

Felipe Fierro (2017), al abordar el análisis del "derecho subjetivo", explica que "históricamente constituye una suplantación del derecho natural, en cuanto al poder de la persona sobre un bien material o inmaterial, ante el cual ejerce un dominio derivado de su propia esencia de ser hombre o bien porque esté convenido" (p. 343). En este sentido, para Grocio, precisa el Dr. Fierro (2017), "el Derecho natural es como una norma humana puesta por la autonomía y la actividad del sujeto. Libre de todo presupuesto objetivo y explicable mediante la razón, esencial instrumento de la subjetividad humana" (p. 345).

El doctor Fierro comenta también que los derechos subjetivos existen "pero no pueden fundamentarse en el hombre mismo, solo y absoluto, sin considerar el orden natural y como tal la participación de éste en los primeros principios de la razón en el ser humano" (Fierro, 2017, p. 345). Coincidimos con esta afirmación dado que hemos afirmado que el ser humano en tanto sustancia de naturaleza racional, existe con vida psíquica y orgánica propias ordenadas naturalmente entre sí, y hacia un fin. Se manifiestan ordenados a través de rasgos concretos y propios, que podemos

describir en los siguientes conceptos: funciones, propiedades, facultades y operaciones sobre los cuales tienen un poder moral, es decir, poseerlos, hacer o exigir alguna cosa respecto de ellos, los cuales a su vez constituyen sus datos personales o datos sensibles.

Cabe destacar que este poder moral viene del derecho entendido en sentido estricto que consiste, a decir de Barbedette (1984), en "el poder moral que cada quien tiene de disponer de lo suyo o de reclamar lo que le es debido" (p. 138).

Sobre el concepto "propiedad" en los seres humanos, siguiendo a Jesús Ambriz (2022, p. 104), podemos decir que es la manera de manifestarse, por ejemplo el peso específico, la talla, el magnetismo, etcétera; la "función" es la manifestación orgánica de las diferentes partes del cuerpo, por ejemplo función respiratoria, digestiva, renal, hepática, cardiaca, etcétera; la "facultad" es el poder que tiene la persona, como sustancia racional, de producir ciertos fenómenos, por ejemplo facultad intelectual, imaginativa, volitiva, etcétera; y la "operación" es el acto de una facultad, por ejemplo operación abstractiva o generación de la idea, juicios, raciocinios, actos o voluntarios, etcétera.

Las funciones, propiedades, facultades y operaciones constituyen expresiones ordenadas de la sustancia individual de naturaleza racional, es decir, de la persona concreta en cuanto ser individual, quien por los primeros principios del conocimiento se da cuenta de ello; por tanto, los datos personales son manifestaciones que constituyen expresiones de la sustancia humana concreta. De ahí que la naturaleza humana sea esencial para comprender el fundamento ontológico del derecho a la protección de datos personales.

En este orden de ideas coincidimos con el Dr. Fierro Alvídrez y estimamos que los derechos subjetivos existen, en tanto fundados en la razón natural iluminada por los primeros principios del orden moral, que juzga rectamente sobre lo que conviene hacer y lo que debe evitarse según la naturaleza humana y su fin. Dicho de otro modo, sin desviaciones provocadas por las pasiones, los instintos o algún interés personal, sino con fundamento de la razón natural.

Principio de causalidad y derecho

Aristóteles (1994) explica en *Metafísica* que lo que no ha existido siempre no puede comenzar a ser por sí solo, sino que necesita una causa que lo ponga en movimiento. Este principio es el fundamento mismo de la noción de causa, que también se puede enunciar como "todo fundamento tiene una causa", del cual depende realmente de alguna manera la existencia de un ente contingente o no necesario. Este principio es elemental para comprender cuál es el fundamento ontológico en virtud del cual el derecho existe.

Lo anterior permite establecer válidamente que el derecho es contingente, pues de acuerdo con Ferrater Mora (s. f.), "lo contingente es aquello que puede ser y puede no ser" y efectivamente, metafísicamente el ente contingente ha sido considerado como aquel que no es en sí, sino en otro. De este modo, podemos afirmar que el derecho no existe por sí mismo, por tanto, no puede entenderse como absoluto ni autónomo en su ser, debido a que tiene necesidad de una causa. Esto significa que el derecho no empezó a existir de la nada, sino que tiene un fundamento razón determinante del porqué existe y del modo en que existe.

Eduardo García Máynez, de postura positivista, en su libro

Filosofía del Derecho admite que relativamente al concepto de sujeto de derecho, la definición pertenece al campo de la filosofía "y, aun cuando interese a todas las ramas de los derechos privado y público, no puede ser resuelto por ninguna de ellas, ya que se trata de uno de los conceptos fundamentales de nuestra ciencia" (García, 2009, p. 238).

El derecho a la protección de datos personales, como cualquier conocimiento, debe partir de la realidad, de lo que existe, de lo que es, de lo contrario caeríamos en el inmanentismo, es decir, tendríamos que lo representado como contenido de la conciencia o lo que imaginamos es la única realidad para "crear o reconocer" el derecho, en oposición a lo que está fuera de ella; de este modo sería tanto como pretender construir un derecho de la inexistencia, de la nada, desde lo absurdo. En síntesis, es pretender hacer ciencia desde la conciencia de una persona, desdeñando así la existencia del ente o ser, realidad material o inmaterial que constituye el fundamento de todo conocimiento.

Barbedette (1984) sostiene, ente otras cuestiones, que "la esencia del derecho no consiste en un poder físico sino moral, es decir, conforme a la razón y las reglas de la moral". También sustenta que "el sujeto del derecho es una persona moral, dotada de inteligencia y voluntad" (Barbedette, 1984), de donde resultan los elementos necesarios para la existencia del acto humano, el cual produce efectos en el orden moral y en orden jurídico, por esto el acto es objeto inmediato del derecho, dado el poder moral que posee una persona (que se dice moral) de hacer o no hacer, o bien de exigir de otro una determinada conducta.

Como todo derecho, el de protección de datos personales produce un efecto, porque determina en otro una relación correlativa, es decir, existe otra persona obligada a respetarlo, es lo que

conocemos en el derecho actual como bilateralidad de la norma jurídica. De esto deducimos el objeto, fin o propósito inmediato del citado derecho, pues cualquier persona tiene derecho a exigir que los demás respeten sus datos personales.

De este modo, la persona humana constituye el fundamento ontológico y realidad que sustenta el derecho de protección de datos personales, como el derecho en general. La existencia y finalidad de este derecho tiene como causa próxima el ser humano. Este no se trata pues, simplemente de un concepto creado a partir de un juicio del entendimiento, sino que encuentra sustento en un ente que existe en la realidad como ser racional y libre, y cuya existencia precede al derecho en general.

Persona realidad ontológica: fundamento o causa del derecho a la protección de datos personales

Es claro que nuestro punto de partida sobre el fundamento del derecho a la protección de datos personales no es el principio genético-histórico, ni la razón pura o práctica, tampoco la utilidad social o motivos de carácter individual y social, o bien, autopercepción del ser humano por la cual se pretende construya sus derechos, sino que hemos puesto de manifiesto la constitutiva dimensión del orden natural y la participación de este en los primeros principios de la razón en el ser humano, por la cual descubre el fundamento ontológico de derecho referido.

Cuando las personas reflexionan acerca del derecho generalmente lo asocian con leyes, códigos que expide el Gobierno, no se molestan en pensar si ellas son la causa del derecho o si es un órgano del Gobierno quien lo crea. No obstante, desde la tradición filosófica clásica del derecho y, particularmente desde la filosofía del derecho, y el derecho concretamente subjetivo, este ha sido

definido como una potestad moral y jurídica que tiene una persona para exigir lo que le es debido por justicia, de tal modo que esta pretensión o facultad es atribuida a un sujeto, quien puede exigir a otro sujeto que está obligado a cumplir. Un ejemplo sería exigir al Estado cómo debe usar su información personal, y el Estado a su vez tiene en todo momento el deber de respetar la decisión de la persona, salvo las excepciones que la propia ley establece.

El derecho a la protección de datos personales no se trata solo de motivos de carácter individual y social que permiten a las personas el desarrollo de su autonomía personal y la elección de la manera en que se identifica y elige conducirse sobre estos. No, el derecho a la protección de datos personales es una cosa que existe y que se observa en la naturaleza del ser humano, por tanto, pertenece a una determinada persona, quien tiene el poder moral sobre sus datos. Materialmente este derecho son los datos personales a través de los cuales se expresa la identidad sustancial y accidental dado que están unidos a aspectos íntimos, identidad persona sustancial e identidad accidental que comprende aspectos sociales, contables, profesionales o biográficos, que representan a la persona en sí y a una o varias dimensiones de esta y, por tanto, merecen protección.

Quien es causa próxima (no remota, la cual es objeto de otro estudio), fuente que produce y desencadena la existencia del derecho en cuestión, es el ser humano o persona, es quien lo realiza a través de su esencia y racionalidad por la cual, a través de los primeros principios, conoce su intimidad, su yo, sus facultades que se expresan en operaciones, como la inteligencia que se revela por el pensamiento y los raciocinios que utiliza para deducir cosas, otras veces para adoptar una filosofía, un estilo de vida personal; otra revela sus datos personales por su naturaleza orgánica (enfermedades, rasgos físicos, lunares, cicatrices, etc.) y

sobre esa información cuenta con la posibilidad moral de control y disposición de su propia información, sobre lo cual, el orden jurídico positivo, lo que conocemos como ley no hace, sino por un acto de la razón ordenada, regular el tratamiento de datos, determinando los deberes de los responsables de tal tratamiento y dando orden al modo que el titular puede acceder, rectificar, cancelar u oponerse al tratamiento de los mismos.

De este modo, el ser humano o persona es causa eficiente próxima o principio de donde procede el derecho a la protección de datos personales, el cual podemos entender de dos modos: primero, desde lo moral y lo ontológico, en el sentido de que el ser humano o persona es la fuente del derecho por su naturaleza, y en última instancia decide cómo obrar o no. El segundo modo, desde lo jurídico, por el cual el legislador declara la existencia de ese derecho, lo formaliza positivamente y protege mediante la expedición de leyes.

Como resultado encontramos que el fin del derecho a la protección de datos es garantizar el respeto a la persona y su dignidad humana, a la intimidad, a la libertad y a la autodeterminación informativa. Su propósito es evitar que la persona sea reducida a un objeto de uso o vigilancia, protegiendo su integridad frente al poder público y privado.

El derecho a la protección de datos personales no debe entenderse solo como una figura jurídica moderna, sino como la expresión de una facultad moral y ontológica de la persona humana. A través de sus causas, podemos comprender que este derecho tiene una realidad propia, fundamentada en la justicia y en la naturaleza del ser humano. Esto nos permite afirmar que el derecho subjetivo a controlar nuestros datos personales no depende únicamente de la voluntad y razón de la persona, ni del consentimiento de la ley,

sino que brota del ser mismo de la persona y, por tanto, esta es verdaderamente el fundamento ontológico de aquel.

Conclusiones

El derecho a la protección de datos personales encuentra su fundamento próximo ontológico en la naturaleza del ser humano. Este fundamento existe, en tanto, fundado en la razón natural iluminada por los primeros principios del orden moral, que juzga rectamente sobre lo que conviene hacer y lo que debe evitarse según la naturaleza humana y su fin, dicho de otro modo, sin desviaciones provocadas por las pasiones, los instintos o algún interés personal, sino con fundamento de la razón natural.

Por tanto, el fundamento ontológico no consiste en un poder físico o acto del Estado por el cual otorga ese poder, sino de un poder moral conforme a la razón, que tienen las personas de hacer algo o de obligar a los otros a hacer algo.

Este poder moral de hacer algo respecto de sus datos personales o sensibles proviene de la naturaleza del ser humano, regulada por la ley natural, que permite todo lo que no está prohibido. En concordancia, la verdadera ley positiva solo declara, apoyada en la autoridad del Estado, lo que radica en el orden o derecho natural, que prescribe la ley natural, que otorga al hombre el poder de exigir lo que le es debido.

Por tanto, es un error buscar el fundamento ontológico del derecho a la protección de datos personales en sola razón práctica y voluntad del ser humano no fundadas en la naturaleza de su ser, en la utilidad social o motivos de carácter individual y social.

Bibliografía

Aguilar Cisneros, K. Y., & Rincón Mayorga, C. A. (2022). La definición de las indeterminaciones constitucionales relacionadas con la seguridad social. *Derecho Social y Sociedad*, (34), 95-120. https://doi.org/10.22201/iij.24487899e.2022.34.16731

Ambriz, J. (2022). *Medicina humanística.* Editorial Folia.

Aquino, T. (Obra original publicada en 1274). *Suma teológica.* 1, q. 29, a 1.

Aristóteles. (1994). *Metafísica* (T. Calvo Martínez, Trad.). Editorial Gredos.

Barbedette, D. (1984). *Ética o filosofía moral conforme al pensamiento de Aristóteles y Santo Tomás* (S. Abascal, Trad.). Editorial Tradición.

Brugger, W. (1962). *Diccionario de filosofía.* Editorial Herder.

Constitución Política de los Estados Unidos Mexicanos [Const.]. Artículo 6, apartado a, fracción II. 20 de diciembre de 2024 (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Del Vecchio, G. (1953). *Filosofía del Derecho.* Bosch.

Echavarría, M. (2022). *De Aristóteles a Freud, y vuelta.* Ediciones COR IESU.

Ferrater Mora, J. (1980). Diccionario de filosofía, III (2.a ed.). Alianza Editorial.

Ferrater Mora, J. (s. f.). Contingencia. En Diccionario de filosofía. Recuperado el 23 de octubre de 2025, de https://www.ferratermora.org/ency_concepto_ad_contingencia.html

Fierro Alvídrez, F. J. (2017). *Introducción al estudio del derecho* (1.a ed.). Cámara de Diputados, LXIII Legislatura.

Finnis, J. (1992). *Ley natural y derechos naturales* (C. Orrego, Trad., estudio preliminar). Abeledo-Perrot.

García, E. M. (2009). *Filosofía del Derecho* (17.a ed.). Editorial Porrúa.

González, E. (2003). *Temas de Filosofía del Derecho* (2.a ed.). Limusa.

Halpern, D. F. (2014). *Thought and knowledge: An introduction to critical thinking* (5th ed.). Psychology Press.

Hervada, J. (1994). *Introducción crítica al Derecho Natural.* Editorial Minos, S.A. de C.V.

Jolivet, R. (1959). *Curso de Filosofía.* Ediciones Desclée, de Brouwer.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. 26 de enero de 2017. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Martí, G. (2017). Sustancia individual de naturaleza racional: el principio personificador y la índole del alma separada. *Metafísica y Persona*, (1), 113-129. https://doi.org/10.24310/Metyper.2009.v0i1.2849

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (1989, 20 de noviembre). *Convención sobre los Derechos del Niño.* https://www.ohchr.org/es/instruments-mechanisms/instruments/convention-rights-child

Organización de los Estados Americanos. (1969). *Convención Americana sobre Derechos Humanos (Pacto de San José).* https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

Paul, R., & Elder, L. (2002). *Critical thinking: Tools for taking charge of your professional and personal life.* Pearson Education.

Real Academia Española. (2023). Concernir. En *Diccionario de la Lengua Española*. https://dle.rae.es/concernir

Suprema Corte de Justicia de la Nación. (2023). *Derecho a la protección de datos personales. Su aplicabilidad y alcances respecto de personas fallecidas en el ámbito civil* [Tesis]. Gaceta del Semanario Judicial de la Federación, Libro 23, Tomo II. https://sjf2.scjn.gob.mx/detalle/tesis/2026107

Suprema Corte de Justicia de la Nación. (2024). *Amparo directo en revisión 6061/2022*. https://www.scjn.gob.mx/sites/default/files/listas/documento_dos/2024-02/ADR%206061.pdf

Tagle, J. R. (1950). *Afinidades ontológicas entre el ser y el deber ser del derecho*. Actas del Primer Congreso Nacional de Filosofía (Mendoza 1949), tomo III. Universidad Nacional de Cuyo.

6. La protección de datos personales y los derechos humanos

Dr. Alejandro Carrasco Talavera

1. Introducción

El reconocimiento de derechos humanos y fundamentales es un proceso extenuante y lleno de obstáculos. Cuando hablamos de la protección de datos personales y el derecho a la vida privada tenemos que reconocer que su configuración no ha sido sencilla ni una graciosa concesión, sino una conquista precedida por muchas batallas sociales y legales. El derecho a la vida privada y la protección de datos personales ha sido una necesidad individual y social, sobre todo en la actualidad, donde el uso de los avances informáticos y el Internet han hecho latente que se debe concretar el derecho que tienen todas las personas al reconocimiento, control del uso y transmisión de datos personales.

Por datos personales podemos entender, de acuerdo con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2025), "cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información".

De igual forma, la citada ley distingue entre datos personales y datos personales sensibles, siendo estos últimos "aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo

grave para ésta" (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2025). De manera enunciativa mas no limitativa, la citada ley considera 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.

El antecedente más conocido del derecho a la vida privada y, por ende, a la protección de datos personales, lo encontramos en un artículo publicado el 15 de diciembre de 1890 en la *Harvard Law Review* elaborado por los abogados Samuel D. Warren y Louis D. Brandeis,[1] titulado "The right to privacy",[2] sobre todo inspirados por la obra del juez Thomas M. Cooley *A treatise on the law of torts or the wrongs which arise independent of contract*,[3] de donde tomaron las siguientes ideas:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone", Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops". For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of the invasion of privacy by the newspapers, long keenly felt, has been but recently discussed

[1] Se puede consultar en https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf
[2] Trad. El derecho a la privacidad.
[3] Trad. Tratado sobre el derecho de los agravios o los males que surgen independientemente del contrato.

by an able writer.[4] (Cooley, 1879)

El artículo, de acuerdo con William L. Prosser (1969), se ubica en un contexto peculiar: en el año 1890 la señora Warren, una mujer de Boston, llevaba a cabo en su hogar eventos sociales de manera continua, era la hija del senador Bayard de Delaware, y su esposo era un joven productor de papel con una posición económica desahogada, quien hacía solo un año antes había dejado de practicar el derecho para dedicarse a la empresa familiar heredada. Socialmente hablando, la señora Warren era parte de la élite, por lo que los periódicos de Boston y especialmente el *Saturday Evening Gazette*, que se especializaba en temas de la "alta sociedad", cubrió sus fiestas con tanto detalle desagradable que se consideró que el medio de comunicación estaba rayando en el amarillismo. En esa época Boston era una ciudad muy conservadora y se consideraban de mal gusto publicaciones de ese tipo, por lo que el colmo fue cuando diversos periódicos publicaron habladurías sobre la boda de la hija del señor Warren, por lo que acudió con su socio legal Louis D. Brandeis y como resultado publicaron el artículo titulado "The right to privacy", que sería un parteaguas en la implementación de este derecho.

La finalidad de dicha obra es poner de manifiesto la necesidad de reconocer el derecho a la privacidad. Tres años después de su publicación, un tribunal hacía uso del concepto de privacidad,

[4] Trad. Las más recientes invenciones y métodos de negocio llaman la atención sobre el siguiente paso que debe darse para la protección de la persona y para garantizarle lo que el juez Cooley llama el derecho a "ser dejado en paz". Las fotografías instantáneas y la industria periodística han invadido los recintos sagrados de la vida privada y doméstica; y numerosos dispositivos mecánicos amenazan con hacer realidad la predicción de que "lo que se susurra en el armario se anunciará desde los tejados". Durante años ha existido la sensación de que la ley debe ofrecer algún recurso ante la circulación no autorizada de imágenes de particulares; y el mal hecho por los periódicos al invadir la privacidad, profundamente sentido desde hace mucho tiempo, ha sido analizado recientemente por un escritor competente.

como argumento para emitir una sentencia, específicamente en el caso Marks & Joffra, donde un estudiante de Derecho en Nueva York demandó a un periódico debido a que publicó su retrato en una nota sobre un concurso de popularidad al que el demandante se oponía. La resolución estableció el caso a favor del impetrante basándose en el respeto debido a la propia imagen, a la falta de consentimiento del interesado y a que todas las personas tenemos el derecho a ser "dejadas en paz", dejando el antecedente de que ningún medio de comunicación o institución tiene el derecho a usar el nombre o la fotografía de alguien sin su consentimiento.

Queda claro con lo anterior que el derecho a la vida privada o a la intimidad personal es, en principio, uno de los límites clásicos del derecho de acceso a la información pública, salvo, como lo establece Villanueva (2006), cuando existan intereses preponderantes de orden colectivo que justifiquen de manera legítima una intrusión en este derecho personalísimo.

2. Reconocimiento como derecho en el ámbito internacional

Dentro de los diversos instrumentos internacionales que le dan el carácter de derecho humano sobresale la Declaración Americana de Derechos y Deberes del Hombre de 1948, la cual en su artículo 5.o establece que: "Toda persona tiene derecho a la protección de la ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar" (Naciones Unidas, 1948), siendo la primera declaración de derechos internacional que protege la vida privada con fundamento en la dignidad del ser humano. Poco después nació la Declaración Universal de Derechos del Hombre de 1948, indicando en su artículo 12 que: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación. Toda persona tiene el derecho a la protección de la ley contra tales

ataques o injerencias" (Organización de los Estados Americanos, 1948).

Por su parte, en el Convenio Europeo de Derechos Humanos existe una referencia a la vida privada en el artículo 6.°, que trata sobre la prohibición del acceso a la sala de juicio, de la prensa o el público, cuando: "los intereses de los menores o la protección de la vida privada de las partes en el proceso así lo exijan o en la medida en que sea considerado estrictamente necesario por el tribunal, cuando en circunstancias especiales la publicidad pudiera ser perjudicial para los intereses de la justicia" (Consejo de Europa, 1950), mientras que en su numeral 8.° establece que: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia" (Consejo de Europa, 1950).

El Pacto Internacional de Derechos Civiles y Políticos de 1966 es similar en cuanto a lo que establece la Declaración Americana de Derechos y Deberes del Hombre, mientras que la Convención Americana sobre Derechos Humanos (Pacto de San José) de 1970, en su artículo 11 habla sobre la protección del derecho a la honra y la dignidad.

En Europa, en 1981 se crea el *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su protocolo adicional relativo a las autoridades de control y a los flujos transfronterizos de datos*, teniendo como fin "garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto a sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona" (Consejo de Europa, 1950). Cabe mencionar que México se adhirió

a este convenio en el año 2018, quedando claro que en todos los países democráticos y de derecho el respeto a la privacidad es uno de los valores supremos en la convivencia social (González, 2005).

3. La regulación de la protección de datos personales en México

El 20 de julio de 2007 se publicó en el Diario Oficial de la Federación una importante reforma constitucional, misma que consistió en la introducción de un segundo párrafo en el artículo sexto[5] de dicha norma fundamental, marcando un antes y un después en materia de acceso a la información pública. Antes de esta reforma, la carta magna se limitaba a establecer —a partir de una modificación en 1977— que "el derecho a la información será garantizado", lo cual, como es fácil imaginar, dejaba un sentimiento de incertidumbre en quien leyera el numeral 6 de la Constitución, pues su redacción

[5] Artículo 6o. (...)
Para el ejercicio del derecho de acceso a la información, la Federación, los Estados y el Distrito Federal, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad.
II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes.
III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.
IV. Se establecerán mecanismos de acceso a la información y procedimientos de revisión expeditos. Estos procedimientos se sustanciarán ante órganos u organismos especializados e imparciales, y con autonomía operativa, de gestión y de decisión.
V. Los sujetos obligados deberán preservar sus documentos en archivos administrativos actualizados y publicarán a través de los medios electrónicos disponibles, la información completa y actualizada sobre sus indicadores de gestión y el ejercicio de los recursos públicos.
VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.
VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.

críptica dejaba mucho que desear en cuanto a la claridad que el legislador debe siempre buscar.[6]

De igual forma, con la creación de leyes de transparencia en las diversas entidades federativas comenzó a transformarse la manera en la que las personas que habitan el país se relacionan con las autoridades o entes que reciben y ejercen recursos públicos o realizan actos de autoridad en el ámbito federal, estatal y municipal. Sin duda, la inclusión de la transparencia en el día a día de las y los mexicanos creó una cultura de involucramiento con el quehacer político e institucional, mismo que por décadas operó desde la oscuridad y llevando como estandarte la opacidad. Es así que a través de los últimos años la ciudadanía asimiló la idea de que es posible solicitar información a las autoridades y estas, a su vez, tuvieron que cambiar de paradigma, pues lo que antes era privado se convirtió en público y accesible en páginas de Internet y redes sociales.

Actualmente la redacción del artículo 6.° constitucional, luego de diversas modificaciones, ha quedado como sigue en su apartado A (Constitución Política de los Estados Unidos Mexicanos, 2014):

> A. Para el ejercicio del derecho de acceso a la información, la Federación y las entidades federativas, en el ámbito de sus respectivas competencias, se regirán por los siguientes principios y bases:

[6] Como antecedente interesante, tenemos que el 10 de noviembre de 2006 los gobernadores de Aguascalientes, Chihuahua, Veracruz y Zacatecas, junto con el entonces jefe de Gobierno del Distrito Federal, presentaron una iniciativa para adicionar el artículo 6.° constitucional. A este proyecto se le conoció como "Iniciativa Chihuahua", donde se proponía la protección de la vida privada y un procedimiento expedito para el acceso y rectificación de datos personales. Dicho proyecto establecía lo siguiente: "La información que se refiera a la vida privada y los datos personales se considerará como confidencial y será de acceso restringido en los términos que fije la ley".

I. Toda la información en posesión de cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal, es pública y sólo podrá ser reservada temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes. En la interpretación de este derecho deberá prevalecer el principio de máxima publicidad. Los sujetos obligados deberán documentar todo acto que derive del ejercicio de sus facultades, competencias o funciones, la ley determinará los supuestos específicos bajo los cuales procederá la declaración de inexistencia de la información.
II. La información que se refiere a la vida privada y los datos personales será protegida en los términos y con las excepciones que fijen las leyes. Para tal efecto, los sujetos obligados contarán con las facultades suficientes para su atención. Por lo que hace a la información relacionada con los datos personales en posesión de particulares, la ley a la que se refiere el artículo 90 de esta Constitución determinará la competencia para conocer de los procedimientos relativos a su protección, verificación e imposición de sanciones.
III. Toda persona, sin necesidad de acreditar interés alguno o justificar su utilización, tendrá acceso gratuito a la información pública, a sus datos personales o a la rectificación de éstos.
IV. Se establecerán mecanismos de acceso a la información pública y procedimientos de revisión expeditos que se sustanciarán ante las instancias competentes en los términos que fija esta Constitución y las leyes.
V. Los sujetos obligados deberán preservar sus documentos en

archivos administrativos actualizados y publicarán, a través de los medios electrónicos disponibles, la información completa y actualizada sobre el ejercicio de los recursos públicos y los indicadores que permitan rendir cuenta del cumplimiento de sus objetivos y de los resultados obtenidos.

VI. Las leyes determinarán la manera en que los sujetos obligados deberán hacer pública la información relativa a los recursos públicos que entreguen a personas físicas o morales.

VII. La inobservancia a las disposiciones en materia de acceso a la información pública será sancionada en los términos que dispongan las leyes.

VIII. Los sujetos obligados deberán promover, respetar, proteger y garantizar los derechos de acceso a la información pública y a la protección de datos personales. 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.

Los sujetos obligados se regirán por la ley general en materia de transparencia y acceso a la información pública y protección de datos personales, en los términos que ésta se emita por el Congreso de la Unión para establecer las bases, principios generales y procedimientos del ejercicio de este derecho.

El ejercicio de este derecho se regirá por los principios de certeza, legalidad, independencia, imparcialidad, eficacia, objetividad, profesionalismo, transparencia y máxima publicidad.

> La ley establecerá aquella información que se considere reservada o confidencial.

Parte esencial de este apartado A del artículo 6.º constitucional es que por primera vez la carta magna otorga de manera expresa e inequívoca el derecho de acceso a la información, como especie del derecho a la información, convirtiéndose en derecho fundamental y no solo humano. Cabe mencionar que lo establecido en dicho numeral es un mínimo que deben manejar las instancias de gobierno en el tema de transparencia.

Ahora, en cuanto al derecho a la protección de datos personales, tenemos que es un derecho que permite a las personas conocer y controlar su información cuando la otorgan a las instituciones públicas y/o privadas, así como asegurarse de que se utilice de forma adecuada. Este se encuentra previsto en el segundo párrafo del artículo 16 constitucional, que confiere a las personas el control sobre su información personal y las faculta para decidir quién, cómo, cuándo y hasta qué punto utilizará su información personal. Además, les garantiza el acceso, rectificación, cancelación y oposición al tratamiento de sus datos personales (derechos ARCO):

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. (Constitución Política de los Estados Unidos Mexicanos, 2014, art. 16)

Los derechos ARCO tienen como implicación que la autoridad deberá respetar lo siguiente: el Acceso: lo cual significa acceder a los datos personales, así como conocer la información relacionada con las condiciones y generalidades de su tratamiento; la Rectificación: es decir, rectificar los datos personales cuando los datos resulten inexactos, incompletos o no estén actualizados; la Cancelación: que significa la facultad de cancelar los datos personales de los archivos, registros, expedientes y sistemas del responsable, a fin de que los mismos ya no se encuentren en su posesión y dejen de ser tratados, y la Oposición: la cual lleva aparejada la posibilidad de oponerse al tratamiento o exigir el cese del mismo, cuando cause perjuicio o daño a la persona titular o produzca efectos jurídicos no deseados.

4. Análisis actual de la protección de datos personales en México

Como es bien sabido, el 20 de diciembre de 2024 se publicó en el Diario Oficial de la Federación el *Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos*, en materia de simplificación orgánica, con la finalidad de extinguir diversos organismos autónomos constitucionales, entre ellos el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Con posterioridad, el 20 de febrero de 2025 la titular del Ejecutivo a nivel federal presentó ante el Senado una iniciativa con proyecto de decreto por la que se propuso expedir las siguientes leyes: a) Ley General de Transparencia y Acceso a la Información Pública; b) Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y c) Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

Finalmente, el 20 de marzo de 2025 se publicó la nueva Ley

General de Protección de Datos Personales en Posesión de Sujetos Obligados, los cuales son en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Concordamos con Alejandro Ortega (2010) cuando afirma que, en la comunidad internacional, la protección de los datos personales, de la vida privada y de la intimidad, de la injerencia de autoridades y de otras personas gobernadas, goza de un nivel que el sistema jurídico mexicano está muy lejos de alcanzar. La desaparición del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, junto con los institutos locales, es una clara violación al principio de progresividad de los derechos humanos, establecido en el artículo 1.° constitucional.

El principio de progresividad, tratándose de derechos humanos, implica el gradual progreso para lograr su pleno cumplimiento, es decir, que para el cumplimiento de ciertos derechos se requiera la toma de medidas a corto, mediano y largo plazo, pero procediendo lo más expedita y eficazmente posible. Este principio se ha relacionado particularmente con los derechos económicos, sociales y culturales, pero aplica también para los civiles y políticos, procurando por todos los medios posibles su satisfacción en cada momento. La progresividad se relaciona de forma estrecha con la prohibición de retrocesos o marchas atrás injustificadas a los niveles de cumplimiento alcanzados, la “no regresividad” en la protección y garantía de derechos humanos.

La Suprema Corte de Justicia de la Nación (SCJN) ha establecido que el principio de progresividad impone una prohibición de regresividad: el legislador tiene prohibido, en principio, emitir actos legislativos que limiten, restrinjan, eliminen o desconozcan

el alcance y la tutela que en determinado momento ya se reconocía a los derechos humanos, y el aplicador tiene prohibido interpretar las normas sobre derechos humanos de manera regresiva, esto es, atribuyéndoles un sentido que implique desconocer la extensión de los derechos humanos y su nivel de tutela admitido previamente. En congruencia con este principio, el alcance y nivel de protección reconocidos a los derechos humanos tanto por la Constitución como por los tratados internacionales deben ser concebidos como un mínimo que el Estado mexicano tiene la obligación inmediata de respetar (no regresividad) y, a la vez, el punto de partida para su desarrollo gradual (deber positivo de progresar) (SCJN, 2017).

Todo lo anterior implica que es necesario que no se vuelvan a dar condiciones de opacidad por parte de las instituciones y que la nueva normatividad no provoque que las instituciones lleven a cabo una mera simulación en cuanto al reconocimiento, control del uso y transmisión de datos personales. No basta que exista un recurso, este tiene que ser efectivo en orden a la protección de los derechos humanos. En el Caso del Tribunal Constitucional, la Corte Interamericana de Derechos Humanos (1987) establece que:

> la inexistencia de un recurso efectivo contra las violaciones a los derechos reconocidos por la Convención constituye una transgresión de la misma por el Estado Parte en el cual semejante situación tenga lugar. En ese sentido debe subrayarse que, para que tal recurso exista, no basta con que esté previsto por la Constitución o la ley o con que sea formalmente admisible, sino que se requiere que sea realmente idóneo para establecer si se ha incurrido en una violación a los derechos humanos y proveer lo necesario para remediarla. No pueden considerarse efectivos aquellos recursos que, por las condiciones generales

> del país o incluso por las circunstancias particulares de un caso dado, resulten ilusorios. (p. 7)

En ese mismo sentido, el Tribunal regional plantea que:

> Los recursos son ilusorios cuando se demuestra su inutilidad en la práctica, el Poder Judicial carece de la independencia necesaria para decidir con imparcialidad o faltan los medios para ejecutar las decisiones que se dictan en ellos. A esto puede agregarse la denegación de justicia, el retardo injustificado en la decisión y el impedimento del acceso del presunto lesionado al recurso judicial. (Corte Interamericana de Derechos Humanos, 1987, p. 7)

Los órganos garantes que regulen el acceso a la información y la protección de datos personales deben ser imparciales, independientes y especializados para evitar caer en las simulaciones de las que habla la Corte Interamericana, es decir, es vital que sus funciones no guarden relación de subordinación jerárquica con ningún órgano administrativo. Quienes se encargan de la transparencia tienen que ser transparentes, solo así se contará con instituciones sólidas y con una protección real de nuestros derechos humanos.

Referencias

Consejo de Europa. (1950). *Convenio Europeo para la protección de los derechos humanos y de las libertades fundamentales*. https://www.echr.coe.int/documents/d/echr/convention_spa

Consejo de Europa. (1981). *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*. https://rm.coe.int/16806c1abd

Constitución Política de los Estados Unidos Mexicanos [Const.]. 7 de enero de 2014 (México). https://www.diputados.gob.mx/LeyesBiblio/ref/cpeum.htm

Cooley, T. (1879). *A treatise on the law of torts or the wrongs which arise independent of contract*. Callaghan and Company. https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1010&context=books

Corte Interamericana de Derechos Humanos. (1987). *Garantías judiciales en estados de emergencia (arts. 27.2, 25 y 8 Convención Americana sobre Derechos Humanos).*

González, J. L. (2005). Transparencia y acceso a la información judicial. En J. A. Caballero Juárez, Carlos G. Gregorio, M. Popkin, & E. Villanueva, *El acceso a la información judicial en México: una visión comparada* (pp. 161-177). Universidad Nacional Autónoma de México. http://ru.juridicas.unam.mx:80/xmlui/handle/123456789/10562

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. 20 de marzo de 2025. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. 20 de marzo de 2025. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Ley General de Transparencia y Acceso a la Información Pública. 20 de marzo de 2025. Diario Oficial de la Federación. https://www.dof.gob.mx/nota_detalle.php?codigo=5752569&fecha=20/03/2025#gsc.tab=0

Naciones Unidas. (1948). *Declaración Universal de Derechos Humanos*. https://www.un.org/es/about-us/universal-declaration-of-human-rights

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

Organización de los Estados Americanos. (1948). *Declaración Americana de Derechos y Deberes del Hombre*. https://www.cndh.org.mx/sites/default/files/doc/Programas/TrataPersonas/MarcoNormativoTrata/InsInternacionales/Regionales/Declaracion_ADDH.pdf

Organización de los Estados Americanos. (1969). *Convención Americana sobre Derechos Humanos (Pacto de San José).* https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

Ortega, A. (2010). *La tutela de la vida privada, y de los datos personales en México en Derechos Humanos: temas y problemas.* Comisión Nacional de los Derechos Humanos.

Prosser, W. (1960). *Privacy. California Law Review*, *48*(3), 383-423. https://lawcat.berkeley.edu/record/1109651?v=pdf

Suprema Corte de Justicia de la Nación. (2017). *Principio de progresividad de los derechos humanos. Su concepto y exigencias positivas y negativas* [Tesis]. Gaceta del Semanario Judicial de la Federación. https://sjf2.scjn.gob.mx/detalle/tesis/2015305

Villanueva, E. (2006). *Derecho de la información.* Miguel Ángel Porrúa.

Warren, S., & Brandeis, L. (1890). *The right to privacy. Harvard Law Review*, *4*(5), 193-220. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

7. La protección de datos personales sensibles en el derecho internacional y su reflejo en el orden jurídico mexicano

Dr. Socorro Márquez Regalado

Resumen

El estudio se refiere a la protección de datos sensibles a la luz del sistema jurídico internacional y del nacional en México. Partiendo de lo establecido en la Convención Americana sobre Derechos Humanos o Pacto de San José, el cual prescribe la protección a la vida familiar, al domicilio, a la vida privada, a las comunicaciones telefónicas y a los datos derivados del uso del Internet, se valoran las resoluciones de la Corte Interamericana de Derechos Humanos que interpretan y amplían las dimensiones de ese derecho y se dimensiona cómo esas interpretaciones son incorporadas en el derecho mexicano, tanto de carácter constitucional como legal. El estudio contempla también el análisis de tratados internacionales signados en el marco de la ONU, así como un estudio de esta organización relativo al derecho a la privacidad en la era digital. Se concluye que el Estado mexicano ha incorporado las figuras derivadas del derecho internacional y de la jurisprudencia de la Corte Interamericana de Derechos Humanos para la protección de los datos personales en los tipos antes mencionados. Se hace énfasis en los principios que rigen el tratamiento de datos personales derivados de los órdenes jurídicos internacional y nacional: el consentimiento informado, la licitud, la proporcionalidad, la necesidad y la responsabilidad. Se advierte la necesidad de promover la educación y la sensibilización

para evitar que los datos personales sensibles sean usados sin autorización del ciudadano.

Palabras clave: Datos personales; sistema jurídico internacional; domicilio; vida privada y familiar; comunicaciones; Internet.

1. Introducción

La Convención Americana sobre Derechos Humanos (en adelante, Pacto de San José) establece en su artículo 11.2 que: "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" (Organización de los Estados Americanos [OEA], 1969). Este párrafo del Pacto de San José tiene un gran significado, por lo que regula y por el reflejo normativo que tiene para México.

En cuanto a su contenido, porque prohíbe la arbitrariedad, no solo de los actos de Estado, sino de los particulares, para proteger contra el abuso de poder o la injerencia en la vida privada, que *lato sensu* considerada es *per se* amplísima. Pero, además desglosa en elementos esa privacidad, en cuanto al seno familiar, al domicilio, a la correspondencia, a la honra y a la reputación.

En cuanto al impacto que tiene para México, la relevancia se encuentra en la sentencia 293/2011 emitida por la Suprema Corte de Justicia de la Nación, en virtud de que hace obligatorias las sentencias de la Corte Interamericana de Derechos Humanos (en adelante, Corte IDH), en los siguientes términos:

> Por último, en cuanto al segundo tema relativo al valor de la jurisprudencia emitida por la Corte IDH, el Tribunal Pleno determinó por mayoría de 6 votos, que la jurisprudencia

> emitida por la Corte Interamericana de Derechos Humanos es vinculante para los todos los órganos jurisdiccionales, siempre que dicho precedente favorezca en mayor medida a las personas. (Suprema Corte de Justicia de la Nación [SCJN], 2011, párrafo 14)

Al respecto, es importante acotar que dicha jurisprudencia es obligatoria para México aun y cuando nuestro país no haya sido parte en el litigio, por lo que todas las sentencias que se mencionarán aplican para cumplimiento de los jueces mexicanos. De hecho, las sentencias referidas son un parámetro de control de la regularidad constitucional y provocaron en México una serie de reformas en materia de derechos humanos en diversas legislaciones.

En virtud de esos elementos que evidencian la relevancia de las sentencias de la Corte IDH, el objeto del presente análisis es describir cómo las convenciones internacionales y la interpretación que de ellas hace la Corte Interamericana de Derechos Humanos abordan la protección de datos personales, en los términos y alcance del artículo 11.2 del Pacto de San José.

Los datos personales también son un bien jurídicamente protegido en la Constitución Política de los Estados Unidos Mexicanos desde 2009, en el cumplimiento del criterio de convencionalidad y de las sentencias de la Corte Interamericana de Derechos Humanos. La máxima norma jurídica de México plantea en el artículo 16, párrafo 2, que:

> Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a

> los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros. (Constitución Política de los Estados Unidos Mexicanos, 2009)

Otro elemento importante para contextualizar el presente estudio son las definiciones de "datos personales" y "datos personales sensibles", que son aspectos necesarios para determinar por qué se analizan el domicilio, las comunicaciones, la vida privada, la vida familiar y los datos derivados del uso del Internet. Esos conceptos están expresados en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados expedida en 2017.

Datos personales son "cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información" (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017, artículo 3, fracc. IX). Mientras que datos personales sensibles son:

> Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa mas 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. (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2017, artículo 3, fracc. X)

Como se puede observar, los datos personales, ordinariamente considerados, son información de los ciudadanos, mientras que los datos personales sensibles son de diferente naturaleza y su enunciación en la ley no es limitativa, refiriéndose a aspectos íntimos, no solo datos, sino aquellas circunstancias que puedan poner en riesgo a la persona y que deben ser resguardadas. Es así como, en esta interpretación, los objetos materiales de estudio son claramente pertinentes en la clasificación de datos personales sensibles.

2. Desarrollo

2.1. La protección del domicilio y la vida privada

En el caso de las Masacres de Ituango vs. Colombia hay una expresión que implica la relación entre el domicilio y la vida privada, en virtud de que esta última depende de aquella:

> La Corte considera que el ámbito de la privacidad se caracteriza por quedar exento e inmune a las invasiones o agresiones abusivas o arbitrarias por parte de terceros o de la autoridad pública. En este sentido, el domicilio y la vida privada se encuentran intrínsecamente ligados, ya que el domicilio se convierte en un espacio en el cual se puede desarrollar libremente la vida privada. (Corte Interamericana de Derechos Humanos, 2006, p. 83)

Lo sucedido en Antioquia, Colombia, entre 1996 y 1997, implica una serie de ataques perpetrados por paramilitares con la aquiescencia de agentes del orden del Estado contra la población civil. Se relatan homicidios, desplazamiento forzado, tortura, violencia sexual, desapariciones y violación al domicilio. La Corte IDH condenó al Estado colombiano por su responsabilidad

obligándolo a aplicar medidas de reparación integral, investigación, sanción a los responsables, restitución de tierras e indemnización a las víctimas, así como la implementación de medidas de no repetición.

Aquí se ha de apuntar que la Suprema Corte de Justicia de la Nación ha seguido la pauta de lo pronunciado por la Corte IDH en diversas sentencias, destacando que la vida privada es, en sentido negativo, lo que no constituye vida pública; el ámbito reservado frente a la acción y el conocimiento de los demás. Es aquello que el sujeto no quiere compartir con todos, solo está reservado para aquellos que el sujeto elige; habla de actividades en la esfera particular que tiene que ver con el hogar y la familia.

Hay otras dos sentencias de la Corte IDH que se refieren a la protección de injerencias extrañas en la vida privada y el domicilio: caso Escué Zapata vs. Colombia, sentencia del 4 de julio de 2007, Fondo, Reparaciones y Costas. Serie C No. 165; y el caso Fernández Ortega y otros vs. México, sentencia del 30 de agosto de 2010, excepciones Preliminares, Fondo, Reparaciones y Costas. Serie C No. 215. Estas sentencias fortalecen el marco normativo internacional en la materia, pero se omite su análisis concreto en virtud de que el fondo de su contenido se encuentra en línea, con un sentido muy similar a la emitida contra Colombia.

2.2. La protección de las comunicaciones personales

La protección de comunicaciones personales fue analizada por la Corte IDH en el caso Tristán Donoso vs. Panamá en 2009. Los hechos son relativos a la intervención ilegal de comunicaciones del periodista y abogado Santander Tristán Donoso en un caso penal en el cual no era imputado. El contenido de esas comunicaciones telefónicas de Donoso fue divulgado en medios de comunicación

de manera ilegal. La Corte determinó que se violaba el derecho a su vida privada y a la libertad de expresión y que no se cumplió con los estándares de necesidad y proporcionalidad establecidos en la Convención Americana sobre Derechos Humanos. Al respecto, se refiere que las restricciones de los derechos establecidos en el artículo 30 del Pacto de San José deben ser exclusivamente en los siguientes términos:

> Las restricciones permitidas, de acuerdo con esta Convención, al goce y ejercicio de los derechos y libertades reconocidas en la misma, no pueden ser aplicadas sino conforme a leyes que se dictaren por razones de interés general y con el propósito para el cual han sido establecidas. (Organización de los Estados Americanos, 1969)

La Corte IDH concluyó que los hechos tuvieron un efecto amedrentador, por lo que condenó al Estado panameño a reconocer su responsabilidad en un acto público, a reformar su marco normativo para prohibir la interceptación de conversaciones telefónicas, a pagar indemnización por daño material e inmaterial y a reembolsar a la víctima los gastos del proceso legal.

Las comunicaciones personales guardan un espacio cualitativamente importante en la Constitución Política de los Estados Unidos Mexicanos, calificándolas como inviolables, y establece que se debe sancionar, por la legislación penal, los actos que atenten contra la libertad de dichas comunicaciones, así como su privacía. La Carta Magna también especifica que en los juicios donde las comunicaciones personales sean aportadas voluntariamente, el alcance de estas será valorado siempre y cuando esté relacionado con la comisión de un delito, pero “en ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley (Constitución Política de los

Estados Unidos Mexicanos, 1996, artículo 16, párrafo 9).

De hecho, la Suprema Corte de Justicia de México en diversas sentencias ha interpretado la norma constitucional agregando aspectos no considerados literalmente. Se refiere a los datos obtenidos mediante llamadas telefónicas que son interceptados y usados para ubicar georreferencialmente al ciudadano. En el amparo directo en revisión 2880/2020, sentenciado en 2023, se refiere a ello en los siguientes términos:

> el alcance del derecho a la privacidad y el correspondiente a la inviolabilidad de las comunicaciones privadas, para constatar que, si bien los datos conservados no constituyen una comunicación en sentido estricto, sí están protegidos por las prerrogativas correspondientes a las comunicaciones privadas y no solo por las genéricas del derecho a la privacidad, pues esos datos revelan un cúmulo de información acerca de los hábitos, contactos, afinidades y lugares frecuentados por las personas; además de que, en su conjunto, sirven para localizar el lugar de donde se realizaron las llamadas registradas y, con ello, sitúan al usuario de la línea telefónica en condiciones similares a la geolocalización. (SCJN, 2023)

Estas aportaciones son particularmente importantes en tanto que la tecnología en la actualidad permite esas intervenciones telefónicas y los datos obtenidos pueden ser usados para abusar del poder, ubicando a las personas y espiándolas para fines que están fuera de sus facultades expresamente establecidas en la ley.

2.3. La protección de la vida familiar

Como se vio, la protección normativa del artículo 11 del Pacto

de San José se refiere explícitamente a la protección de la vida privada, del domicilio, de las comunicaciones y de la vida familiar. Al respecto de la vida familiar, la sentencia de la Corte IDH en el caso Escué Zapata vs. Colombia del 4 de julio de 2007 condena al Estado colombiano por la violación de varios derechos en perjuicio del líder indígena Germán Escué Zapata y sus familiares. Los hechos se refieren a su detención ilegal, tortura y ejecución extrajudicial por agentes del Estado en 1988.

En este caso, el Estado colombiano asumió su responsabilidad por un conjunto de violaciones a distintas libertades y derechos: en principio el derecho a la vida, a la libertad e integridad de las personas, y el referido a la garantía de atención judicial, no solo de la víctima, Germán Escué Zapata, sino también de sus familiares.

Al efecto, la Corte IDH ordenó que Colombia pagara indemnización por haber causado daños materiales e inmateriales. Además, sentenció que se realizaran investigaciones exhaustivas para juzgar, identificar y sancionar a quienes hubieren causado los mencionados daños. Asimismo, ordenó realizar actos públicos en los cuales reconociera su responsabilidad por los hechos ocurridos y aportar recursos económicos para cubrir una beca de estudios a la hija del indígena fallecido. En los mismos términos, para que pagara tratamiento psicológico y médico a los familiares.

La ejecución extrajudicial de Escué fue causa de que la Corte IDH obligara al Estado a tomar medidas para prevenir violaciones futuras de derechos humanos en su territorio. En el caso particular, se analiza el derecho a la protección de su vida familiar que se menciona en el artículo 11.2 del Pacto de San José, pues el ingreso ilegal de personal contratado por el Estado a la vivienda de la familia indígena implicaba además la presencia de los familiares de

la víctima ejecutada. La Corte IDH hace una interpretación amplia al considerar dentro del concepto de "honra y de la dignidad" la protección a la vida familiar que se tiene en un domicilio, además del derecho a la correspondencia.

2.4. La protección de los datos derivados del uso del Internet

Una resolución de la Asamblea General de la Organización de las Naciones Unidas pronunciada el 18 de diciembre de 2013 se refiere al derecho de toda persona a la privacidad de los datos derivados del uso del Internet en la era digital. La resolución se basa en los siguientes tratados internacionales:

a. La Declaración Universal de los Derechos Humanos se refiere a esta garantía en los siguientes términos: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (Organización de las Naciones Unidas [ONU], 1948, artículo 12).
b. Asimismo, el Pacto Internacional de Derechos Civiles y Políticos en los siguientes términos: "1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques" (ONU, 1966, artículo 17).

De ambos tratados internacionales se deriva la obligación de los Estados Parte de evitar injerencias arbitrarias a la vida privada de las personas, a la vida en familia, al domicilio y a la correspondencia. En dicha resolución, de número 68/167, se reconoce que, derivado del desarrollo tecnológico de hoy día,

los gobiernos e incluso instituciones y empresas privadas tienen capacidad de interceptación y vigilancia del ciberespacio, así como de recopilar datos de los internautas. Llama a ambas instancias a evitar que, con ello, se violen derechos humanos, concretamente el relacionado con el derecho a la privacidad (ONU, 2014).

Se exhorta a adoptar medidas concretas para evitar dicho fenómeno, e incluso prevenirlo, cumpliendo de esa manera con el derecho internacional en los siguientes términos:

> Exhorta a todos los Estados a que respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales, y adopten medidas para poner fin a las violaciones de esos derechos y creen las condiciones necesarias para impedirlas, como cerciorarse de que la legislación nacional pertinente se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos. (ONU, 2014)

En la resolución se amplía la obligación de los Estados y las instancias privadas para que se desarrollen mecanismos de supervisión a cargo de entes independientes, mismos que deben ser, además, capaces de asegurar la transparencia en el uso de las herramientas digitales.

El motivo de la resolución de la ONU en comento está fundamentado en que existen ciertos procesos digitales que permiten el procesamiento y uso de datos con autorización de los usuarios, por medio de un "aviso de privacidad". Este tipo de práctica tiene una explicación en diversos documentos, particularmente se enuncia en este estudio lo referenciado por la Comisión Interamericana de Derechos Humanos de 2017 denominado "Derecho a la privacidad y protección de datos personales".

En ese documento se hace una relatoría de lo que ha surgido en Internet como herramientas nuevas diseñadas para extraer información personal del usuario:

> De las numerosas herramientas que se han creado para rastrear a los usuarios de internet, dos ejemplos conocidos son las cookies y los web bugs. Las cookies son pequeños fragmentos de texto que los navegadores de internet almacenan en la computadora de un usuario. La cookie se "registra" con el navegador de internet cada vez que el usuario accede a ese navegador y puede usarse para supervisar el historial de sesión del usuario, almacenar cualquier preferencia, etc. Por lo habitual, los web bugs (también llamados beacons o baliza web) son invisibles para el usuario, ya que su tamaño apenas alcanza 1x1 píxeles, y se incluyen en las páginas web y los correos electrónicos. (Comisión Interamericana de Derechos Humanos, 2017, p. 80)

Esto indica la importancia de la protección de datos personales porque cuando se accede a una página web o el correo electrónico que contiene el *web bug*, este envía la información al servidor (incluida la dirección IP del usuario, la hora y la fecha en que fue vista la página o correo electrónico y el navegador en que se vio), lo que puede infringir el derecho a la privacidad que se encuentra previsto en los tratados internacionales referidos.

3. Conclusiones

Primera: Existen normas internacionales que regulan el derecho a la protección de datos personales sensibles que tiene su reflejo en el orden jurídico mexicano. Particularmente, en la jurisprudencia de la Corte Interamericana de Derechos Humanos se desagregan aspectos que complementan el derecho a la vida privada, al

domicilio, a las comunicaciones y a los datos derivados del uso del Internet. Esa jurisprudencia internacional también es recogida por precedentes de la Suprema Corte de Justicia en México.

Segunda: Para llegar a tal estadio fue necesario que los jueces mexicanos de la Corte Suprema emitieran un criterio de vinculabilidad de la jurisprudencia de la Corte Interamericana de Derechos Humanos, lo cual permitió a los legisladores mexicanos reformar los marcos constitucional y legal que regulan este derecho humano.

Tercera: Los Estados están obligados a cumplir con esas normas nacionales e internacionales, pero la dinámica del avance tecnológico de los medios de comunicación digitales requiere del diseño de formas de supervisión —independientes y efectivas— y una verificación puntual para asegurarse de que las normas se estén cumpliendo. Particularmente en una rama que evoluciona de manera vertiginosa, literalmente en tiempo real, se requieren también herramientas tecnológicas de vanguardia para resguardar los datos personales.

Cuarta: Otro aspecto importante es capacitar y sensibilizar a los integrantes de los poderes del Estado y de las organizaciones privadas, para que tengan claridad de lo que la normatividad establece y eviten los abusos de poder, apropiándose de los datos personales o cometiendo arbitrariedades que invadan la esfera familiar, el domicilio, la vida privada o las comunicaciones tanto en medios análogos como digitales.

Quinta: Los principios que rigen el tratamiento de datos personales sensibles son el consentimiento informado, la licitud, la proporcionalidad, la necesidad y la responsabilidad. Esto implica

también hacer interpretaciones, no solo jurídicas, sino éticas para el tratamiento de los datos personales.

Referencias

Comisión Interamericana de Derechos Humanos. (2017). *Derecho a la privacidad y protección de datos personales [Capítulo IV]. Estándares para una Internet libre, abierta e incluyente*. Colección Comisión Interamericana de Derechos Humanos. https://biblio.juridicas.unam.mx/bjv/detalle-libro/7241-estandares-para-una-internet-libre-abierta-e-incluyente-coleccion-comision-interamericana-de-derechos-humanos

Constitución Política de los Estados Unidos Mexicanos [Const.]. Artículo 16, párrafo 2. 1 de junio de 2009 (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Constitución Política de los Estados Unidos Mexicanos [Const.]. Artículo 16, párrafo 9. 3 de julio de 1996 (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

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

Corte Interamericana de Derechos Humanos. (2007). *Caso Escué Zapata vs. Colombia Sentencia de 4 de julio de 2007. Fondo, Reparaciones y Costas. Serie C No. 165*. https://www.corteidh.or.cr/docs/casos/articulos/seriec_165_esp.pdf

Corte Interamericana de Derechos Humanos. (2009). *Caso Tristán Donoso vs. Panamá, Sentencia de 27 de enero de 2009. Excepciones Preliminares, Fondo, Reparaciones y Costas. Serie C No. 139*. https://www.corteidh.or.cr/docs/casos/articulos/seriec_193_esp.pdf

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. 26 de enero de 2017. Diario Oficial de la Federación. https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017#gsc.tab=0

Organización de las Naciones Unidas. (1948). *La Declaración Universal de los Derechos Humanos*. https://www.un.org/es/about-us/universal-declaration-of-human-rights

Organización de las Naciones Unidas. (1966). *Pacto Internacional de Derechos Civiles y Políticos*. https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

Organización de las Naciones Unidas. (2014, 21 de enero). *El derecho a la privacidad en la era digital (A/RES/68/167)*. https://docs.un.org/es/A/RES/68/167

Organización de los Estados Americanos. (1969). *Convención Americana sobre Derechos Humanos (Pacto de San José)*. https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf

Suprema Corte de Justicia de la Nación. (2011). *Sentencia 293/2011*. https://www2.scjn.gob.mx/asuntosrelevantes/pagina/seguimientoasuntosrelevantespub.aspx?id=129659&seguimientoid=556

Suprema Corte de Justicia de la Nación. (2023). *Amparo directo en revisión 2880/2020*. https://www.scjn.gob.mx/sites/default/files/listas/documento_dos/2023-11/231122-ADR-2880-2020.pdf

8. Marco jurídico y principios de protección de datos en el ámbito educativo. México vs Unión Europea/Estados Unidos

Dr. Diego U. Sandoval Aguirre

Introducción

La gestión educativa cada día se convierte en algo más complejo ya que genera y concentra cantidades enormes de información personal del alumnado: datos de identificación (nombre, edad, dirección), datos académicos (calificaciones, evaluaciones), datos de salud (enfermedades, problemas médicos, alergias) y datos de interacción con las propias plataformas educativas (entradas, salidas, tareas), por mencionar algunos, que representan una gran cantidad de metadatos que requieren ser resguardados. La protección de esos datos exige medidas no solo técnicas y administrativas, sino también jurídicas, es decir, comprender y conocer el marco jurídico hacia el interior de las instituciones educativas es una necesidad imperante ya que ello conlleva derechos, pero también obligaciones y responsabilidades. En México, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) rige las instituciones educativas privadas; para el caso de instituciones educativas públicas es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO). La Unión Europea se rige por el Reglamento General de Protección de Datos (GDPR), y la Ley de Derechos Educativos y Privacidad Familiar (FERPA) en Estados Unidos. Estas servirán para un análisis comparado en el que se explicarán los principios legales, clasificación de los tipos

de datos relevantes para el sector educativo e identificación de roles y responsabilidades institucionales.

Principios generales de la protección de datos en el ámbito educativo

Algunos de los principios que sirven de guía en el marco jurídico analizado son:

- **Licitud, lealtad y transparencia:** El tratamiento de los datos debe realizarse conforme a la ley.
  - » México: Los datos personales deben recabarse y tratarse de manera lícita, sin medios engañosos o fraudulentos (Ley Federal de Protección de Datos Personales en Posesión de los Particulares [LFPDPPP], 2025, artículo 6).
  - » Unión Europea: La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental (Reglamento General de Protección de Datos [GDPR], 2016, artículo 1).
  - » Estados Unidos: El propósito de esta parte es establecer requisitos para la protección de la privacidad de los padres y estudiantes conforme a la Ley de Educación General (FERPA, 2024).

- **Limitación de la finalidad:** Los datos deben recogerse para fines explícitos, legítimos y determinados, y no usarse de forma incompatible con esos fines.
  - » México: El tratamiento debe limitarse al cumplimiento de las finalidades establecidas en el aviso de privacidad (LFPDPPP, 2025, artículo 11).
  - » Unión Europea: El tratamiento de datos personales con fines distintos (…) solo debe permitirse cuando sea compatible (GDPR, 2016, artículo 50).

  - » Estados Unidos: Una agencia o institución educativa puede divulgar registros educativos (…) a funcionarios que tengan intereses educativos (FERPA, 2024).

- **Minimización de datos:** recoger solo lo estrictamente necesario para la finalidad educativa o administrativa.
  - » México: El tratamiento debe ser necesario, adecuado y relevante (…) el responsable debe esforzarse razonablemente para limitar el período de tratamiento al mínimo indispensable (LFPDPPP, 2025, artículo 12).
  - » Unión Europea: Los datos personales deben ser adecuados, pertinentes y limitados a lo necesario (GDPR, 2016, artículo 39).
  - » Estados Unidos: No se establece explícitamente este principio.

- **Exactitud y conservación limitada:** Mantener los datos actualizados y no conservarlos más tiempo del necesario.
  - » México: Una vez que los datos dejen de ser necesarios (…) deben ser suprimidos previo 'bloqueo' (LFPDPPP, 2025, artículo 10).
  - » Unión Europea: Los datos personales solo deben tratarse si la finalidad (…) no pudiera lograrse razonablemente por otros medios (…) se limite a un mínimo estricto su plazo de conservación (GDPR, 2016, artículo 39).
  - » Estados Unidos: No se establece explícitamente este principio.

- **Seguridad e integridad:** Aplicar medidas técnicas y administrativas para proteger confidencialidad, integridad y disponibilidad.
  - » México: El responsable debe establecer y mantener medidas de seguridad administrativas, técnicas y físicas (…) informar

al titular de forma inmediata (LFPDPPP, 2025, artículo 19).
  - » Unión Europea: Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas (GDPR, 2016, artículo 39).
  - » Estados Unidos: La ley (…) establece requisitos para la protección de la privacidad de padres y estudiantes (FERPA, 2024).

- **Responsabilidad proactiva (*accountability*):** Documentar decisiones, registros de tratamiento y demostrar cumplimiento.
  - » México: El responsable velará por el cumplimiento de los principios de protección de datos y deberá adoptar las medidas necesarias (LFPDPPP, 2025, artículo 13).
  - » Unión Europea: El responsable debe aplicar medidas técnicas y organizativas apropiadas para garantizar y demostrar que el tratamiento es conforme con el reglamento (GDPR, 2016, artículo 71).
  - » Estados Unidos: No se establece explícitamente este principio.

- **Transparencia e información:** Las personas deben ser informadas de forma clara y accesible sobre el tratamiento de sus datos personales.
  - » México: El responsable debe informar al titular, a través de un 'Aviso de Privacidad', sobre la existencia y características principales del tratamiento (LFPDPPP, 2025, artículo 14).
  - » Unión Europea: El principio de transparencia exige que toda información y comunicación relativa al tratamiento (…) sea fácilmente accesible (GDPR, 2016, artículo 39).
  - » Estados Unidos: Cada agencia o institución educativa notificará anualmente a los padres de los estudiantes (…) de sus derechos conforme a la ley (FERPA, 2024).

- **Consentimiento:** El tratamiento de datos personales está sujeto al consentimiento del titular, salvo excepciones específicas.
  - » México: El consentimiento puede ser expreso (…) o tácito (…). Sin embargo, para datos financieros, patrimoniales o sensibles, debe ser expreso y por escrito (LFPDPPP, 2025, artículo 7).
  - » Unión Europea: El consentimiento debe darse mediante un acto afirmativo claro (…) no deben constituir consentimiento el silencio, las casillas ya marcadas o la inacción (GDPR, 2016, artículo 32).
  - » Estados Unidos: El padre o estudiante debe proporcionar un consentimiento escrito firmado y fechado antes de que una institución educativa divulgue información identificable (FERPA, 2024).

- **Derechos del interesado:** Las personas físicas tienen derechos fundamentales sobre sus datos personales.
  - » México: La ley otorga los derechos ARCO (Acceso, Rectificación, Cancelación y Oposición) (LFPDPPP, 2025, artículo 2, fracción VII).
  - » Unión Europea: Los interesados deben tener derecho a acceder a los datos personales recogidos (…) rectificación o supresión (GDPR, 2016, artículo 63).
  - » Estados Unidos: Un padre o estudiante debe tener la oportunidad de inspeccionar y revisar los registros educativos del estudiante (FERPA, 2024)

Estos principios evidencian la fuerte necesidad del resguardo de la información en la misión pedagógica de las instituciones. Si bien los marcos legislativos de México, la Unión Europea y Estados Unidos comparten similitudes en la protección y privacidad de datos, existen algunas diferencias en alcance y especificad de los principios. Las coincidencias en los principios de licitud,

finalidad, seguridad y consentimiento demuestran un consenso internacional en torno a la dignidad y derechos de los estudiantes. Sin embargo, la ausencia en algunos principios en la normatividad de los Estados Unidos refleja vacíos que limitan la integralidad de la protección. Estos principios deben constituir una guía ética y jurídica que oriente a las instituciones educativas hacia prácticas responsables y transparentes en el manejo de datos personales.

Contexto normativo internacional en protección de datos: México, Unión Europea y Estados Unidos

México: La regulación en cuanto a la protección de datos en las instituciones de educación depende de si son entidades públicas o privadas. Para las públicas existe la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada el 20 de marzo de 2025. Como sujetos obligados se entiende a cualquier autoridad, entidad, órgano y organismos de los poderes Ejecutivo, Legislativo y Judicial, así como órganos autónomos, fideicomisos y fondos públicos a nivel federal, estatal y municipal.

La regulación para las instituciones de educación privadas se enmarca en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, también publicada el 20 de marzo de 2025. Para ambas leyes su regulación y supervisión recae en la Secretaría Anticorrupción y Buen Gobierno, que entre sus funciones se encuentra el conocer y resolver los procedimientos de protección de derechos y de verificación e imponer sanciones.

Unión Europea: Los requisitos operativos del Reglamento General de Protección de Datos en algunos casos son más estrictos que los de México. Por citar alguno, en la evaluación de impacto de privacidad para actividades de alto riesgo existe la obligación de designar un delegado de protección de datos en casos concretos,

además de sanciones económicas proporcionales. En el caso de instituciones educativas que operan en la Unión Europea, el GDPR exige un mayor nivel de garantías técnicas, documentación y transparencia.

Estados Unidos: La Ley de Derechos Educativos y Privacidad Familiar protege los registros educativos en aquellas instituciones que reciben fondos federales, se centra en los derechos de los padres o del estudiante elegible en los casos de inspección, acceso y corrección de expedientes académicos, además de que regula la divulgación sin consentimiento en aquellas ocasiones específicas, por ejemplo emergencias de salud u órdenes judiciales. Su enfoque es más funcional y al sector educativo más que genérico.

Mientras la LFPDPPP, la LGPDPPSO y el GDPR exigen una fuerte base jurídica y documentación clara, la FERPA estructura los derechos desde la óptica de acceso a expedientes concretos. La normativa mexicana podría beneficiarse del rigor documental del GDPR y de la claridad de procedimientos en FERPA en cuanto al acceso e inspección.

Los distintos tipos de datos y su tratamiento diferencial en el entorno educativo

En el ámbito educativo existen varias categorías que implican niveles de protección y obligaciones.

1. **Datos personales:** La información que identifica a un estudiante, docente o trabajador. Su tratamiento debe limitarse a fines académicos o administrativos y se debe contar con consentimiento informado (LFPDPPP, 2025; LGPDPPSO, 2025).
2. **Datos personales sensibles:** Se incluye la información sobre

salud, origen étnico, creencias religiosas, orientación sexual e ideología. Se requiere consentimiento expreso y por escrito para su tratamiento y solo se justifica por razones médicas o inclusión educativa (LFPDPPP, 2025; LGPDPPSO, 2025).

3. **Datos académicos y conductuales:** Se consideran los expedientes educativos y su uso o divulgación con fines de mercadotecnia requiere consentimiento de los padres o del estudiante con mayoría de edad (FERPA, 2024).
4. **Datos anonimizados o disociados:** Si se utilizan en investigaciones o estadísticas educativas, se pueden tratar sin consentimiento, siempre y cuando no se identifique al titular, protegiendo de esta manera la confidencialidad (LFPDPPP, 2025; GDPR, 2016).
5. **Datos de menores:** Cuentan con protección reforzada; el consentimiento obligatorio lo debe otorgar el padre, madre o tutor, priorizando siempre el bienestar del menor (LGPDPPSO, 2025; GDPR, 2016).

El tratamiento diferencial en el entorno educativo en todas las legislaciones va en el sentido de la sensibilidad y finalidad del uso de los datos. Los datos comunes pueden procesarse con fines académicos, mientras que los de menores o sensibles exigen un nivel de consentimiento expreso, justificación legal y medidas reforzadas de seguridad.

Roles y responsabilidades institucionales

- **Responsable del tratamiento:** Es el sujeto obligado, persona física o moral, de carácter público o privado, obligado a guardar los principios de lealtad, licitud, finalidad, consentimiento, calidad, proporcionalidad, información y responsabilidad en su manejo (LFPDPPP, 2025; LGPDPPSO, 2025). Es responsable de aplicar medidas técnicas y organizativas para demostrar y

garantizar que el tratamiento cumple con el reglamento (GDPR, 2016). Recae en las agencias educativas locales, las cuales desarrollan políticas de privacidad; asegura el consentimiento para encuestas que involucren datos sensibles (FERPA, 2024).

- **Encargado:** Es la persona física o jurídica, autoridad pública, servicio u otro organismo que trata los datos personales por cuenta del responsable, sola o conjuntamente con otras, siguiendo las instrucciones de este último y garantizando confidencialidad (LGPDPPSO, 2025; LFPDPPP, 2025; GDPR, 2016). En Estados Unidos el concepto de encargado no se utiliza como tal formalmente, sin embargo, esa actividad recae en las agencias educativas locales.

- **Delegado de protección de datos:** Es una figura obligatoria para las autoridades y organismos públicos, así como para entidades privadas cuya actividad principal implique tratamiento a gran escala o manejo de datos sensibles. Asesora, supervisa el cumplimiento normativo, coopera con la autoridad de control y actúa como punto de contacto para los titulares y el regulador (GDPR, 2016). En México y Estados Unidos no existe una figura como tal; en México en las instituciones privadas se obliga a designar una persona o departamento para el tratamiento de datos personales y cumplimiento de las políticas de privacidad. En los organismos públicos la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados prevé tres figuras:

  - » Unidad de Transparencia, que tramita solicitudes ARCO y funge como enlace con los titulares.
  - » Comité de Transparencia, que supervisa el cumplimiento de la política de protección de datos.
  - » Responsable designado por la institución, que implementa

medidas, coordina programas de seguridad y notifica vulneraciones a la autoridad y al titular.

En Estados Unidos esa figura recae en las agencias educativas locales y en el Departamento de Educación, que son responsables de implementar las políticas de privacidad.

- **Docentes y personal administrativo:** Los docentes y el personal administrativo de instituciones educativas públicas o privadas son considerados personas que intervienen en el tratamiento de datos personales, por lo que deben guardar confidencialidad, aplicar las medidas de seguridad dictadas por el responsable y observar los principios de licitud, finalidad, calidad, proporcionalidad e información (LFPDPPP, 2025; LGPDPPSO, 2025). Actúan bajo la autoridad del Reglamento General de Protección de Datos y solo pueden tratar datos siguiendo sus instrucciones. Cualquier incumplimiento puede constituir una infracción grave del principio de confidencialidad y seguridad (GDPR, 2016). En la Ley de Derechos Educativos y Privacidad Familiar las escuelas oficiales cuentan con acceso legítimo a los expedientes educativos, pero solo en la medida en que sea necesario para cumplir sus funciones profesionales. No pueden divulgar información personal de estudiantes sin el consentimiento previo de los padres o del estudiante mayor de edad (FERPA, 2024).

La protección de datos en el ámbito educativo representa una gran coordinación entre los responsables, encargados, delegados y personal. Cada uno de estos actores debe garantizar la licitud, confidencialidad y seguridad en el tratamiento de los datos. Cada una de las legislaturas vistas asegura su cumplimiento y respeto a la privacidad, promueve la transparencia y fortalece la confianza institucional.

Recomendaciones operativas finales para una hoja de ruta institucional para la protección de datos

1. Diseñar institucionalmente una política integral de privacidad. Difundir y desarrollar políticas de protección de datos personales que integren los principios de lealtad, licitud, consentimiento, calidad, proporcionalidad e información (LFPDPPP, 2025; LGPDPPSO, 2025).
2. Crear un comité de protección de datos. Establecer un comité responsable de supervisar el cumplimiento normativo, que será el encargado de coordinar auditorías, gestionar solicitudes ARCO y reportar vulneraciones, de acuerdo con el principio de responsabilidad proactiva (GDPR, 2016).
3. Implementar mecanismos de consentimiento y avisos de privacidad accesibles. Garantizar la recolección de datos acompañada de un aviso de privacidad claro, en formato físico o electrónico, especificando finalidades, derechos ARCO y transparencia de datos (LFPDPPP, 2025; LGPDPPSO, 2025).
4. Fortalecer la seguridad administrativa, técnica y física. Aplicar un sistema de gestión de seguridad que incluya análisis de riesgos, inventario de datos, controles de acceso, cifrado y protocolo de respuesta ante vulneraciones (LGPDPPSO, 2025; GDPR, 2016).
5. Promover la cultura de la privacidad en la comunidad educativa. Incluir formación continua para docentes, administrativos y estudiantes sobre derechos de privacidad, uso responsable de tecnologías y manejo de información sensible (FERPA, 2024).
6. Establecer procedimientos de atención a derechos ARCO y evaluación de impacto. Definir canales accesibles para solicitudes de acceso, rectificación, cancelación y oposición, así como realizar evaluaciones de impacto (LGPDPPSO, 2025; GDPR, 2016).

7. Garantizar transparencia y rendición de cuentas. Implementar auditorías periódicas y reportes de cumplimiento dirigidas a las autoridades correspondientes, asegurando la trazabilidad y mejora continua en los procesos de tratamientos de datos.

Conclusión

Se realiza un análisis del marco jurídico que rige la protección de datos personales en el ámbito educativo, articulando los principios que garantizan la privacidad, la transparencia y el uso responsable de la información en instituciones educativas. Presenta una revisión de las normativas mexicana, de la Unión Europea y de Estados Unidos, que coinciden en reconocer el derecho de toda persona a decidir el tratamiento de sus datos. Asimismo, se resalta la obligación de las instituciones educativas de implementar medidas técnicas, administrativas y organizativas que aseguren la confidencialidad, integridad y disponibilidad de la información, consolidando un ambiente de respeto y responsabilidad institucional, en donde cada estudiante, docente y administrativo se sienta seguro de que su información se encontrará resguardada conforme a la ley.

Bibliografía

Ley de Derechos Educativos y Privacidad Familiar. Actualizada en 2024. U.S. Government Publishing Office. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Ferpa-for-parents-spanish.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. 20 de marzo de 2025. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. 20 de marzo de 2025. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Reglamento General de Protección de Datos. 27 de abril de 2016. Parlamento Europeo y del Consejo. https://www.boe.es/doue/2016/119/L00001-00088.pdf

9. 25 años de la evolución del control estatal de los datos: leyes de seguridad pública nacional, telecomunicaciones y radiodifusión

M. C. Guillermo Ávila Olivas.
M. P. Mario Alberto Valdez Borunda.

1. Introducción

En los últimos 25 años México ha experimentado una transformación profunda en la relación entre Estado y ciudadanía a partir del manejo estratégico de la información. Este proceso es consecuencia de una evolución paulatina en la que el Estado ha pasado de proclamarse garante de derechos a consolidarse como administrador central del flujo de datos personales. Desde una perspectiva de análisis político-jurídico inspirada en la teoría del Estado contemporáneo, este tránsito ha abierto una discusión ineludible: ¿hasta qué punto la protección de la privacidad puede coexistir con la expansión permanente del control estatal?

A partir del año 2000 la alternancia política generó expectativas de apertura institucional y fortalecimiento de la democracia, sin embargo, la adopción de tecnologías digitales modificó la estructura orgánica del poder público. La creciente digitalización en diferentes ámbitos sociales permitió al Estado acceder a volúmenes de información antes impensables. La gestión pública comenzó a apoyarse en bases de datos integradas y sistemas de identificación, lo que incrementó su capacidad de seguimiento

poblacional y su margen de intervención en nombre de la eficiencia gubernamental. Esta transformación no solo obedeció a necesidades técnicas de administración pública, sino que expone un nuevo modo de ejercicio del poder sustentado en la gestión de información.

A la par, el discurso de seguridad fue adquiriendo un peso decisivo. Frente al avance del crimen organizado, el aumento de la violencia y la percepción de riesgo colectivo, se justificó la "securitización" ampliando las facultades estatales. El discurso político introdujo una narrativa de excepcionalidad que normalizó la vigilancia bajo el argumento de salvaguardar el orden social. Desde entonces, la recolección y centralización de datos se ha consolidado como herramienta prioritaria para la gestión estatal del orden y el control social.

En coherencia con esta problemática, el presente análisis adopta una perspectiva diacrónica y comparativa, lo que permite examinar la continuidad de los cambios institucionales más allá de las diferencias partidistas. Bajo este enfoque metodológico, un repaso transexenal revela que esta tendencia no pertenece a un solo gobierno o ideología: fue compartida por administraciones de distintas orientaciones políticas. Más allá de las variaciones discursivas, todas impulsaron reformas estructurales que ampliaron el acceso estatal a la información ciudadana y fortalecieron el aparato administrativo de observación pública.

La evolución normativa vinculada al control de información revela un patrón estructural: el aparato jurídico mexicano ha transitado de un sistema garantista a un diseño institucional que prioriza la eficacia operativa del Estado por encima de las salvaguardas de privacidad. Analizar esta transición es imprescindible para comprender la configuración actual del poder público y su impacto

en los derechos ciudadanos. En suma, este capítulo examina la reorganización del poder estatal en torno al control de datos como un hecho político y jurídico propio de la era digital, lo que implica una redefinición de la relación entre información, autoridad y ciudadanía.

2. La constante gubernamental

El análisis histórico comparado muestra que, en México, el control estatal de la información no ha sido un suceso excepcional. Por el contrario, constituye una estrategia sostenida de poder que ha sido reforzada de forma continua por los sucesivos gobiernos federales. Aunque cada administración ha justificado sus decisiones bajo argumentos distintos —seguridad pública, combate al crimen organizado, eficiencia administrativa o modernización tecnológica—, todas ellas han coincidido en un punto central: la expansión progresiva del acceso del Estado a los datos personales de la población.

Como advierte Cabrera Pimentel (2012), desde inicios del siglo XXI comenzó a consolidarse una arquitectura de la información de seguridad, basada en plataformas interconectadas capaces de integrar datos civiles, judiciales y administrativos. Esta integración informática, que inició bajo el objetivo formal de "profesionalizar" la seguridad pública, sentó las bases para un modelo de gestión estatal apoyado en el control sistemático de la información ciudadana.

Esta tendencia se confirma en análisis recientes. México Unido contra la Delincuencia (2025) señala que las iniciativas de reforma en materia de seguridad pública promovidas en los últimos años incrementaron las facultades de las instituciones encargadas de la investigación e inteligencia, bajo la narrativa de enfrentar riesgos

internos y amenazas criminales. A esta lógica se suma el proceso de transformación normativa del sector de telecomunicaciones, que amplió las facultades estatales para requerir información a concesionarios de servicios y operadores de redes. El tránsito de la antigua normativa a la Ley en Materia de Telecomunicaciones y Radiodifusión (2025) ilustra cómo la infraestructura legal se adaptó para permitir un acceso gubernamental más amplio a los datos generados en entornos digitales.

En perspectiva analítica, estos cambios no pueden interpretarse únicamente como reformas legales solitarias o respuestas circunstanciales a crisis de seguridad. En realidad, se trata de una transformación estructural del Estado, que ha desplazado al modelo original para consolidar un esquema de vigilancia normalizada. El resultado ha sido claro: los datos personales se han convertido en un componente del poder estatal y en una herramienta estratégica para la administración política de la sociedad.

3. Implicaciones teóricas y metodológicas

El punto de partida de esta investigación es la idea de que el control estatal de los datos personales es una expresión contemporánea de la forma en que el Estado ejerce y sostiene su poder. Desde una perspectiva clásica sobre la teoría del Estado, puede afirmarse que toda estructura gubernamental tiende a ampliar sus capacidades de intervención conforme dispone de nuevos mecanismos administrativos (Weber, 1993). En esta lógica, la gestión de datos se ha convertido en uno de los instrumentos más eficaces del poder estatal moderno, lo que explica su creciente centralidad dentro de las políticas públicas en México.

Este estudio asume, además, que el fenómeno no puede ser analizado desde una mirada normativista limitada al contenido de las leyes, sino a partir de su función política. Como advierte Bobbio (1997), el orden jurídico no solo regula el ejercicio del poder: también lo legitima y lo reorganiza. Bajo este enfoque, la progresiva expansión del acceso estatal a la información personal se interpreta como parte de una transformación estructural del Estado mexicano, vinculada a la consolidación de infraestructuras de manejo y supervisión de datos institucionalizada.

Metodológicamente, se adopta un enfoque comparativo diacrónico para examinar cambios normativos y operacionales entre 2000 y 2025, identificando tanto continuidades como rupturas a lo largo de los distintos sexenios. El análisis se apoya en fuentes legislativas primarias, como la Ley General del Sistema Nacional de Seguridad Pública (2009) y la Ley en Materia de Telecomunicaciones y Radiodifusión (2025), así como en estudios de referencia sobre plataformas de gestión informacional de seguridad (Cabrera Pimentel, 2012) y análisis independientes sobre reformas en materia de vigilancia estatal (México Unido contra la Delincuencia, 2025).

Este enfoque metodológico permite evitar sesgos partidistas y ubicar el estudio dentro de dinámicas estructurales del poder. Más que describir leyes, el objetivo es comprender cómo se construye la capacidad del Estado para obtener, centralizar y utilizar información ciudadana como un recurso estratégico. El análisis documental se complementa con una revisión crítica de exposiciones de motivos legislativas y discursos oficiales, lo que permite examinar la manera en que la narrativa de seguridad ha funcionado como justificación para normalizar el control del gobierno en la era digital.

4. Periodización y marco temporal justificado

El periodo comprendido entre 2000 y 2025 representa un punto de inflexión en la configuración del Estado mexicano y marca la transición hacia un patrón de poder basado en el control sistemático de la información. No se trata únicamente de un ciclo político, es un periodo estructural en el que convergen transformaciones tecnológicas, institucionales y discursivas que rediseñaron la relación entre ciudadanía y Estado, especialmente a través de la gestión de datos personales y la expansión de capacidades de manejo gubernamental.

El primer eje que justifica esta periodización es la digitalización acelerada del aparato estatal, impulsada a partir del año 2000. Este proceso derivó en la creación de plataformas interoperables de información, registro poblacional y gestión administrativa. Según el Instituto Federal de Telecomunicaciones (IFT, 2022), entre 2000 y 2022 se aprobaron tres grandes reformas en telecomunicaciones que modificaron de manera profunda la infraestructura tecnológica nacional y fortalecieron la capacidad del Estado para operar con datos masivos. La transformación digital no fue únicamente técnica: amplió la intermediación estatal sobre la vida social, adquirida ahora a través de mecanismos basados en datos.

El segundo eje corresponde a la securitización del Estado mexicano, consolidada a partir de 2006 con el impulso de políticas de excepcionalidad justificadas en el combate a la delincuencia organizada. Diversos análisis legislativos han documentado que esta estrategia habilitó la intervención militar en tareas de seguridad pública y sirvió como justificación para ampliar las facultades del Estado en vigilancia y monitoreo social (Centro de Estudios Sociales y de Opinión Pública, 2010). En este

contexto, el discurso de la seguridad se convirtió en herramienta de legitimación política para normalizar la expansión del poder estatal sobre la información ciudadana.

El tercer eje es la centralización de la información, intensificada entre 2018 y 2025. Durante este periodo se consolidó un sistema nacional de inteligencia digital capaz de articular información biométrica, financiera, de movilidad e identificación civil bajo control federal.

Como dispone la Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública (2025), la Plataforma Central de Inteligencia institucionaliza la interconexión con bases de datos públicas y prevé el acceso a fuentes privadas mediante convenio o requerimiento oficial, reforzando la colaboración obligatoria entre autoridades (arts. 24, 27, 28 y 30); diversos análisis señalan que el diseño habilita criterios amplios que pueden tensionar la protección de datos.

En conjunto, estos procesos permiten sostener que entre 2000 y 2025 México dejó atrás un modelo de burocracia administrativa tradicional para avanzar hacia un Estado gestor de información, donde el poder ya no se ejerce solo mediante la coerción física o jurídica, sino también a través de la gestión centralizada de datos como recurso estratégico de gobierno.

5. Comparativa por sexenio

5.1. Vicente Fox (2000-2006)

Durante el sexenio de Vicente Fox, la seguridad pública en México experimentó un cambio normativo iniciando con la promulgación de la Ley de Seguridad Nacional en 2005, mismo año en que

México atravesó una crisis penitenciaria centrada en el penal federal de La Palma, que derivó en operativos extraordinarios, alertas oficiales y reacomodos internos. La Procuraduría General de la República (PGR) abrió diligencias y arraigos, mientras la Secretaría de Seguridad Pública (SSP) escaló medidas de seguridad mediante una serie de boletines y despliegues federales. La coyuntura estuvo acompañada por hechos de violencia asociados y una amplia cobertura mediática a lo largo del año. En paralelo, hacia junio de 2005 el Ejército reportó acciones relevantes contra el narcotráfico en el sureste del país (Secretaría de Seguridad Pública Federal, 2005, 14 de enero, 16 de enero, 20 de enero, 21 de enero, 15 de febrero, 15 de junio; Procuraduría General de la República, 2005; Secretaría de la Defensa Nacional, 2005). Esta ley establecía principalmente las bases para la coordinación interinstitucional y el intercambio de información entre las diferentes entidades federales, estatales y municipales; de esta manera ampliaba la cooperación y facilitó el flujo de datos críticos en pro de la seguridad del país. Simultáneamente a esto, se establecieron identidades poblacionales a través de sistemas como la Clave Única de Registro de Población (CURP) y el Registro Nacional de Población (Renapo), sentando así las bases para una mayor capacidad de registro y control estatal.

En el ámbito de telecomunicaciones, en 2006 fueron aprobadas las reformas a la Ley Federal de Radio y Televisión y a la Ley Federal de Telecomunicaciones, conocidas como “Ley Televisa”, señalada como una ley monopólica para las televisoras dominantes Televisa y TV Azteca; sin embargo, un año más tarde la Suprema Corte de Justicia de la Nación declaró inconstitucional el refrendo automático y a perpetuidad de las concesiones de radio y televisión, sin el pago de una contraprestación al Estado (Becerril & Aranda, 2007).

La ley tenía como propósito reordenar el sector ante la convergencia tecnológica y el surgimiento de los servicios digitales (Ley Federal de Radio y Televisión, 2006; Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley Federal de Telecomunicaciones y de la Ley Federal de Radio y Televisión, 2006).

El avance legislativo priorizó el acopio y la circulación de información sin articular salvaguardas proporcionales para la convergencia tecnológica, interoperabilidad, trazabilidad pública, ni para los usos secundarios de la información. La gobernanza de datos permaneció fragmentada, bajo administraciones sectoriales sin coordinación transversal (Ley de Seguridad Nacional, 2005, arts. 1 y 27; Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley Federal de Telecomunicaciones y de la Ley Federal de Radio y Televisión, 2006; Acuerdo por el cual se dan a conocer el Procedimiento Técnico de Captura de Información y el Procedimiento Técnico de Intercambio de Información, 2006).

El sexenio de Fox fijó cimientos modernos, como la estandarización de catálogos administrativos y el impulso a la formalización de registros únicos, lo que abrió el camino para futuras integraciones y mejoras en la calidad del dato (Gómez & Sosa, 2007; Ley de Seguridad Nacional, 2005).

5.2. Felipe Calderón (2006-2012)

Este sexenio se destacó por la securitización, la estrategia de seguridad se militarizó y priorizó operativos contra cárteles; la literatura crítica señala que esto elevó los homicidios, fragmentó a las organizaciones criminales, formando nuevas, y generó abusos a derechos humanos, sin resolver corrupción ni impunidad.

Además, la cooperación con EE. UU. vía Iniciativa Mérida reforzó capacidades coercitivas más que el fortalecimiento institucional y la prevención, mientras surgían autodefensas en territorios desprotegidos (Rosen & Zepeda Martínez, 2015). La Ley General del Sistema Nacional de Seguridad Pública (2009) y el despliegue de Plataforma México y el Sistema Único de Información Criminal (SUIC) homologaron catálogos e integraron flujos informativos entre autoridades de seguridad y justicia. Estos desarrollos fortalecieron la colaboración técnica interinstitucional y sentaron las bases para sistemas avanzados de conectividad. En el sector de telecomunicaciones se afianzaron los esquemas de coordinación entre operadores y el Estado, prefigurando los lineamientos de la futura Ley Federal de Telecomunicaciones y Radiodifusión de 2014.

Las críticas contemporáneas apuntan a que la securitización amplió la recolección y cruce de datos sin desarrollar paralelamente auditorías independientes, métricas de proporcionalidad o transparencia de uso. Persistió un entorno normativo disperso en términos de control ciudadano. No obstante, este periodo profesionalizó la gestión informacional del Estado y consolidó por primera vez un tablero nacional de datos operativos para la prevención y análisis delictivo, lo que mejoró la coordinación federal y estatal (Cáceres Parra, 2017).

5.3. Enrique Peña Nieto (2012-2018)

El mandato de Peña Nieto modernizó el marco legal en materia de comunicaciones con la promulgación de la Ley Federal de Telecomunicaciones y Radiodifusión en 2014, cuyo artículo 190 —y el agregado 190 bis— instauró la conservación obligatoria de datos y su colaboración con autoridades bajo control judicial (Ley Federal de Telecomunicaciones y Radiodifusión, 2014). En paralelo,

la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017) reforzó los derechos ARCO (conjunto de derechos que permiten a las personas acceder, rectificar, cancelar y oponerse al tratamiento de sus datos personales) y la protección de la información tratada por organismos públicos, aunque habilitó excepciones justificadas por razones de seguridad nacional.

El intento de la Ley de Seguridad Interior en 2017, declarada inconstitucional por la Suprema Corte en noviembre de 2018, puso de relieve la tensión entre el fortalecimiento operativo y el respeto a los límites constitucionales (Suprema Corte de Justicia de la Nación [SCJN], 2018).

En el sexenio de Enrique Peña Nieto la política de seguridad mantuvo continuidades sustantivas respecto al periodo previo: aunque su primer año registró un ligero descenso frente al último de Calderón, el contexto de alta violencia, el incremento de delitos como secuestro y extorsión, y la disputa entre múltiples cárteles persistieron. El énfasis oficial en reformar y coordinar policías no impidió el uso de tropas en focos críticos (Rosen & Zepeda Martínez, 2015). La combinación de facultades de retención y excepciones amplió la capacidad estatal de vigilancia sin suficientes contrapesos. Sin embargo, se consolidaron principios y procedimientos claros para la exigibilidad de derechos y para la revisión judicial de las medidas extraordinarias en materia de datos personales.

5.4. Andrés Manuel López Obrador (2018-2024)

La creación de la Guardia Nacional en 2019 representó una reestructuración sustantiva de la arquitectura federal de seguridad pública que reconfigura los flujos de información operativa e inteligencia del Estado.

En materia de telecomunicaciones, la reforma que instauró el Padrón Nacional de Usuarios de Telefonía Móvil fue declarada inconstitucional por la SCJN el 25 de abril de 2022, al advertirse la desproporción e invasión de la privacidad derivada de la exigencia de datos biométricos (SCJN, 2022b).

Durante el periodo analizado se observa una concentración del poder regulatorio y presiones sobre instituciones autónomas (Krauze, 2020), inicialmente con la intención de fusionar reguladores, sin embargo, esa fusión no ocurrió. En su lugar, en julio de 2025 se extinguieron la Comisión Federal de Competencia Económica y el Instituto Federal de Telecomunicaciones y sus funciones se reorganizaron: se creó la Comisión Nacional Antimonopolio para competencia económica y una nueva autoridad sectorial en telecomunicaciones, la Comisión Reguladora de Telecomunicaciones (CRT), bajo la Ley en Materia de Telecomunicaciones y Radiodifusión; por su parte, la Comisión Reguladora de Energía no se fusionó, sino que se integró a la Secretaría de Energía como órgano desconcentrado con autonomía técnica (reforma de diciembre de 2024 y desarrollos subsecuentes). Persistió una agenda de transparencia ambivalente, con señalamientos de opacidad y asignación discrecional de contratos, que tensionó el discurso anticorrupción con la rendición de cuentas efectiva (Krauze, 2020; Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública, 2025).

Las tensiones entre la centralización del dato en materia de seguridad y el papel del órgano garante (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales) generaron conflictos sobre la autonomía y eficacia de la protección de datos personales. Según el fallo de la Corte, las medidas de registro masivo carecían de proporcionalidad

y finalidad legítima, lo que invalidó el esquema (SCJN, 2022b). Aun con estos conflictos, el sexenio logró ciertos avances en la coordinación de bases de datos y la consolidación de criterios técnicos de operatividad. La revisión judicial de propuestas como el Padrón Nacional de Usuarios de Telefonía Móvil fortaleció una cultura de estricta proporcionalidad y reafirmó la funcionalidad de los controles constitucionales como límites efectivos al poder de vigilancia estatal (SCJN, 2022a; SCJN, 2022b).

5.5. Claudia Sheinbaum (2024-2025)

La nueva Ley General del Sistema Nacional de Seguridad Pública (2025) establece la homologación de registros, la actualización cotidiana y una rectoría técnica con capacidad de enlace con servicios de inteligencia y centros de mando. Paralelamente, la Ley en Materia de Telecomunicaciones y Radiodifusión (2025) reordena las competencias regulatorias, abroga la Ley Federal de Telecomunicaciones y Radiodifusión de 2014 y prevé la sustitución del Instituto Federal de Telecomunicaciones por un órgano dependiente del Ejecutivo federal.

Las observaciones críticas apuntan a que la arquitectura de alta interoperabilidad incrementa la capacidad de injerencia del Estado sin contrapesos externos equivalentes, lo que activa debates sobre autonomía y transparencia (R3D, 2025; Centro Latinoamericano de Administración para el Desarrollo & Secretaría General Iberoamericana, 2025). No obstante, la homologación normativa y la disciplina en la actualización de registros corrigen rezagos históricos, mejoran la calidad y oportunidad del dato, y facilitan la coordinación interinstitucional, mostrando un intento por lograr coherencia estructural en el nuevo sistema de control y transmisión de información pública.

6. Conclusión

En el capítulo se pone en manifiesto que la transición legal de México en los ámbitos de la seguridad pública, las telecomunicaciones y el tratamiento de datos personales entre 2000 y 2025 no puede considerarse como un fenómeno aislado ni como el resultado de decisiones coyunturales dependientes de un solo gobierno. Por el contrario, compone un proceso estructural transexenal que ha consolidado un tipo de Estado basado en la centralización de la información como mecanismo para la toma de decisiones y el ejercicio del poder público (Ley General del Sistema Nacional de Seguridad Pública, 2025).

El tránsito de la normativa de la Ley de Seguridad Nacional (2005) y la Ley General del Sistema Nacional de Seguridad Pública (2009) hasta la versión reformada de 2025 evidencia una reconfiguración progresiva del diseño institucional mexicano. Mientras el sistema original estaba sustentado en principios como el federalismo cooperativo, la intervención judicial y los derechos ARCO, las recientes reformas han dado prioridad a la interoperabilidad digital, el acceso expedito a información estratégica y la integración de bases de datos con fines preventivos y de seguridad (Ley en Materia de Telecomunicaciones y Radiodifusión, 2025).

Este proceso ha sido acompañado por una evolución normativa paralela en el sector de telecomunicaciones. El paso de la Ley Federal de Telecomunicaciones y Radiodifusión (2014) a la actual Ley en Materia de Telecomunicaciones y Radiodifusión (2025) muestra el cambio de un enfoque que consideraba la infraestructura digital como medio para garantizar derechos comunicativos, para dar paso a su reconducción como instrumento de seguridad nacional. Esta transición implicó un reforzamiento de funciones regulatorias a cargo del Poder Ejecutivo, como un recordatorio

a la figura de la concesión de funciones originales del Estado, modificando la organización institucional y reduciendo márgenes de supervisión ciudadana (Ley en Materia de Telecomunicaciones y Radiodifusión, 2025).

México ha ingresado plenamente a una etapa de Estado basado en la información preventiva, que se caracteriza por la vigilancia constante y el registro sistemático de la población con argumentos de eficiencia operativa y combate a la criminalidad (Instituto Federal de Telecomunicaciones, 2022).

El desafío que enfrenta, tras 25 años de reformas en seguridad, telecomunicaciones y tratamiento de datos, no trata solo en medir cuánta información puede y debe administrar el Estado, sino en establecer límites, controles verificables y garantías efectivas para su gestión. La democracia parte de un gesto inicial de confianza política: la ciudadanía transfiere el ejercicio del poder a sus representantes mediante elecciones libres. Esa confianza, sin embargo, es condicional; la teoría del Estado recuerda que todo poder delegado exige control para permanecer legítimo (Bobbio, 1997; Weber, 1993).

Referencias

Acuerdo por el cual se dan a conocer el Procedimiento Técnico de Captura de Información y el Procedimiento Técnico de Intercambio de Información. 21 de septiembre de 2006. Diario Oficial de la Federación. https://dof.gob.mx/nota_detalle_popup.php?codigo=5121057

Becerril, A., & Aranda, J. (2007, 1 de junio). *Golpe a la ley Televisa; declara la Corte inconstitucional el refrendo automático*. La Jornada. https://www.jornada.com.mx/2007/06/01/index.php?section=politica&article=003n1pol

Bobbio, N. (1997). *Estado, gobierno y sociedad.* Fondo de Cultura Económica.

Cabrera Pimentel, P. (2012). *Construcción de plataformas de seguridad*. Universidad Nacional Autónoma de México.

Cáceres Parra, O. R. (2017). El sistema de información e inteligencia Plataforma México. *Revista Latinoamericana de Estudios de Seguridad*, (21), 175-190. http://dx.doi.org/10.17141/urvio.21.2017.2916

Centro de Estudios Constitucionales. (2022). *La finalidad legítima en el test de proporcionalidad y en la Suprema Corte de Justicia de la Nación*. Suprema Corte de Justicia de la Nación.

Centro de Estudios Sociales y de Opinión Pública. (2010). *Seguridad pública y participación de las fuerzas armadas en México*. Cámara de Diputados.

Centro Latinoamericano de Administración para el Desarrollo & Secretaría General Iberoamericana. (2025). *Estudio sobre experiencias de interoperabilidad en Iberoamérica*.

Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley Federal de Telecomunicaciones y de la Ley Federal de Radio y Televisión. 11 de abril de 2006. Diario Oficial de la Federación. https://www.ordenjuridico.gob.mx/Federal/PE/APF/APC/SCT/Decretos/2006/11042006(1).pdf

Gómez, R., & Sosa, P. (2007). Reforma de la legislación en radio, televisión y telecomunicaciones en México. *Quaderns del CAC*, (25), 65-82.

Instituto Federal de Telecomunicaciones. (2022). *Diagnóstico del sector de telecomunicaciones 2000-2022*. IFT México.

Krauze, E. (2020, julio). Un gobierno destructor. *Letras Libres*, *259*. 8-15. https://letraslibres.com/revista/un-gobierno-destructor/

Ley de Seguridad Nacional. 31 de enero de 2005. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf

Ley del Sistema Nacional de Investigación e Inteligencia en Materia de Seguridad Pública. 16 de julio de 2025. Diario Oficial de la Federación. https://www.dof.gob.mx/nota_detalle.php?codigo=5763160&fecha=16/07/2025#gsc.tab=0

Ley en Materia de Telecomunicaciones y Radiodifusión. 16 de julio de 2025. Diario Oficial de la Federación. https://www.dof.gob.mx/nota_detalle.php?codigo=5763167&fecha=16/07/2025#gsc.tab=0

Ley Federal de Radio y Televisión. 11 de abril de 2006. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFRT_110406.pdf

Ley Federal de Telecomunicaciones y Radiodifusión. 14 de julio de 2014. Diario Oficial de la Federación. https://www.sct.gob.mx/fileadmin/Comunicaciones/LFTR.pdf

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. 26 de enero de 2017. Diario Oficial de la Federación. https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017#gsc.tab=0

Ley General del Sistema Nacional de Seguridad Pública. 2 de enero de 2009. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP.pdf

Ley General del Sistema Nacional de Seguridad Pública. 16 de julio de 2025. Diario Oficial de la Federación. https://www.dof.gob.mx/nota_detalle.php?codigo=5763159&fecha=16/07/2025#gsc.tab=0

México Unido contra la Delincuencia. (2025). *Análisis sobre iniciativas de leyes en materia de seguridad pública.*

Procuraduría General de la República. (2005, 19 de enero). *Boletín 043/05* [Comunicado de prensa].

R3D: Red en Defensa de los Derechos Digitales. (2025, 6 de agosto). *El gobierno mexicano refuerza sus capacidades de vigilancia con el nuevo paquete de leyes.* https://r3d.mx/2025/08/06/el-gobierno-mexicano-refuerza-sus-capacidades-de-vigilancia-con-el-nuevo-paquete-de-leyes/

Rosen, J. D., & Zepeda Martínez, R. (2015). La guerra contra el narcotráfico en México: una guerra perdida. *Reflexiones*, *94*(1), 153-168. https://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S1659-28592015000100153

Secretaría de la Defensa Nacional. (2005, junio). *Reporte de localización y destrucción de 44 plantíos de marihuana* [Comunicado/parte informativo].

Secretaría de Seguridad Pública Federal. (2005, 14 de enero). *Boletín de prensa 018/05* [Comunicado de prensa].

Secretaría de Seguridad Pública Federal. (2005, 16 de enero). *Boletín de prensa 023/05* [Comunicado de prensa].

Secretaría de Seguridad Pública Federal. (2005, 20 de enero). *Boletín de prensa 027/05* [Comunicado de prensa].

Secretaría de Seguridad Pública Federal. (2005, 21 de enero). *Boletín de prensa 029/05* [Comunicado de prensa].

Secretaría de Seguridad Pública Federal. (2005, 15 de febrero). *Boletín de prensa 057/05* [Comunicado de prensa].

Secretaría de Seguridad Pública Federal. (2005, 15 de junio). *Boletín de prensa 152/05* [Comunicado de prensa].

Suprema Corte de Justicia de la Nación. (2018, octubre). *Acción de Inconstitucionalidad 6/2018, Ley de Seguridad Interior.*

Suprema Corte de Justicia de la Nación. (2022a). P*leno de la SCJN declara inconstitucional el sistema normativo que crea el Padrón Nacional de Usuarios de Telefonía Móvil* [Comunicado No. 137/2022].

Suprema Corte de Justicia de la Nación. (2022b). *Sentencia dictada por el Tribunal Pleno de la Suprema Corte de Justicia de la Nación en la Acción de Inconstitucionalidad 82/2021 y su acumulada 86/2021.*

Weber, M. (1993). *Economía y sociedad*. Fondo de Cultura Económica.

10. De las notas periodísticas y la protección de datos personales: la encrucijada entre informar y proteger.

Lic. Saúl Ulises García Meza

Resumen

El presente texto busca analizar, entre otras cuestiones, la importancia de la libertad de expresión y la protección de datos personales en notas periodísticas, sin dejar de lado el acceso a la información pública, derechos fundamentales que posee cualquier ciudadano a la luz de lo establecido en la Constitución general, con énfasis particular en el análisis de estos derechos en cada nota periodística.

Se observa la legislación mexicana vigente en materia de libertad de expresión, acceso a la información y protección de datos personales, con un preámbulo de los géneros informativos y opinativos en el periodismo. Se analiza la correspondencia entre los medios de comunicación y la protección de datos personales.

También se recuerda la importancia entre el trabajo de las instituciones de transparencia y protección de datos personales con el gremio de periodistas y medios de comunicación, el cual inició hace casi dos décadas y que, a raíz de las reformas a las leyes en transparencia, ha quedado en una especie de pausa, la cual debería ser solo eso, una pausa, para luego dar continuidad a esta colaboración, buscar el ganar-ganar, siempre en el respeto a la persona como ser humano y en la libertad de expresión que tiene todo periodista y medio de comunicación.

Se describen los retos para el periodista y el medio de comunicación de velar por la protección de los datos personales, más aún cuando la exclusividad de la información recabada por el medio de comunicación incluya datos personales o inclusive datos personales sensibles. Es ganar la nota completa, con sus detalles, y/o buscar la protección de los datos personales.

Palabras clave: Notas periodísticas; protección de datos personales; libertad de expresión; acceso a la información; privacidad.

1. La nota informativa, artículo de opinión y columna política

Existen dos géneros periodísticos: el informativo y el opinativo. En el primer género, el **informativo**, se encuentran las notas periodísticas, el reportaje, la entrevista y la crónica (aunque para esta última hay autores que señalan que comparte algo del género opinativo).

Mientras que en el género **opinativo** podemos encontrar el artículo de opinión, la columna política y la editorial. En el artículo de opinión, quien lo redacta es responsable en su totalidad de su contenido. En la columna política y en la editorial, es el medio de comunicación el responsable de lo que ahí se publica.

La **nota periodística** es por excelencia la principal herramienta de los periodistas y medios de comunicación. Son miles de notas publicadas diariamente a lo largo del país. Y van desde la redacción de una nota que hable sobre una persona atropellada en una calle poco transitada, una rueda de prensa convocada por un funcionario, de un informe de gobierno, de algún atentado o desastres naturales, hasta las más complejas, que sin llegar a ser reportaje, incluyen datos relevantes.

Para la redacción de notas periodísticas o informativas, así como los artículos de opinión y las columnas políticas, sobre todo en estos tres, es donde se encuentran más datos personales publicados, ya sea por desconocimiento de la regulación normativa, por costumbre o por el simple hecho de informar en su mayor dimensión de los detalles que envuelven al hecho noticioso.

Los medios de comunicación tienen herramientas que son utilizadas para defender la libertad de expresión, sobre todo de ataques o censura del Gobierno e inclusive de amenazas del crimen organizado. La **editorial** ha sido usada precisamente para ello, para defender al medio de comunicación de amenazas que están ocurriendo o que están por ocurrir. Hay mucha información que incomoda a los gobiernos y a los grupos criminales.

Lo anterior, sin dejar de mencionar que la editorial es el texto perfecto para dejar en claro cuál es la línea editorial del medio de comunicación. Los medios impresos, sobre todo, han dejado testimonio de grandes editoriales, muchas de ellas han aparecido en momentos históricos y críticos para la vida de un país o entidad federativa. En los principales rotativos es común leer editoriales que van desde el cambio de gobierno, en crisis económicas, en alguna guerra o hasta el hecho de advertir la caída de una democracia.

También hay muchos autores de artículos de opinión que, sin ser periodistas, han utilizado el **artículo de opinión** como un espacio de defensa de los medios de comunicación o inclusive de otro periodista o medio para difundir sus ideas, para hablar de alguna iniciativa, para criticar al gobierno o para difundir en exclusiva temas relevantes para la vida pública del país.

En tanto que la **columna política** (que no todos los medios de

comunicación tienen) es el espacio por excelencia donde se publican los *tips* políticos, los trascendidos y aquella información que surge de manera exclusiva en los lugares de la toma de decisiones tanto para el sector público como para la iniciativa privada.

La columna política es el espacio utilizado para la publicación de trascendidos sin la necesidad de publicar de manera textual la fuente informativa; el periodista y/o medio de comunicación conocen a la fuente, tienen en su poder el documento o testimonio del que en muchas ocasiones hacen referencia. Es otro espacio que los periodistas y medios de comunicación tienen para defender su trabajo, la libertad de expresión y desde luego su propia línea editorial.

Sin dejar de lado a la entrevista, la crónica y el reportaje, en los que también en muchas ocasiones se publican datos personales, encontramos entonces en la nota periodística, en la editorial y en el artículo de opinión los espacios informativos donde más se publican datos personales.

2. La protección de datos personales en la legislación mexicana

Como seguramente se anotará en el presente libro, vale la pena recordar qué son los datos personales, concepto que se ha socializado a raíz del tratado que se le da a estos a través de los diferentes niveles de gobierno y que ha quedado plasmado en la legislación vigente en México desde el artículo sexto de la Constitución general, en su apartado A, numeral II, que protege la vida privada y los datos personales.

Y se vuelve a manifestar en el artículo 16 constitucional, al señalar que toda persona tiene derecho a la protección de sus datos

personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas, o para proteger los derechos de terceros.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en su artículo tercero a la letra refiere que los **datos personales** son cualquier información concerniente a una persona identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información como el nombre, domicilio, número telefónico, clave de elector o Clave Única de Registro de Población.

En tanto que los **datos personales sensibles** son aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para esta. El artículo tercero, fracción X señala que "de manera enunciativa mas 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" (Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 2025).

Especial atención merecen los datos personales sensibles, es decir, aquellos cuya indebida divulgación —ya sea por el Estado o por particulares— afectaría la esfera más íntima del ser humano o le provocaría un riesgo grave, como por ejemplo el origen racial o étnico, el estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical y

opiniones políticas, entre otros (Vizcarra, 2017).

Luego entonces tenemos también la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en la que sin duda vale la pena mencionar lo que señala el artículo 9: "El responsable no estará obligado a recabar el consentimiento de la persona titular para el tratamiento de los datos personales cuando: (…) II. Los datos personales figuren en fuentes de acceso público" (Ley Federal de Protección de Datos Personales en Posesión de los Particulares, 2025).

La **privacidad**, la intimidad y la protección de los datos personales son derechos fundamentales y deben ser respetados por el Estado.

Como es sabido, los medios de comunicación y periodistas hacen de las fuentes de acceso público una de sus principales materias primas para la elaboración de notas informativas, tanto de la que ya se encuentra publicada en diferentes sitios públicos como de aquella que emana directamente del funcionario público.

No puedo cerrar este apartado sin hacer énfasis en la **privacidad**; son muchas las formas en que se nos está arrebatando esta. A veces la falta de privacidad puede parecer inevitable, pero no siempre lo es. Aunque hay prácticas de recogida de datos que son casi imposibles de evitar, a menudo disponemos de más opciones de las que resultan más obvias. Y siempre que tengamos una alternativa es importante elegir la más favorable a la privacidad, no solo para la protección de nuestros datos personales, sino también para hacer saber a gobiernos y empresas que la privacidad nos importa (Véliz, 2021).

3. El acceso a la información y la libertad de expresión como derechos fundamentales

La encrucijada, tal como lo refiere el título del presente capítulo, inicia con la ponderación de derechos, en este caso en particular el de la libertad de expresión y el de la protección de datos personales.

Y es que algunos derechos consagrados en la carta magna mexicana entran en colisión cuando se ejercen sin la consideración del otro, dicho de otra forma, sin ser empáticos. Como diría un maestro del derecho a la información: "algo fácil de explicar, pero complejo de ejercer".

Tenemos entonces el derecho a la *libre expresión* de las ideas por cualquier medio, frente a los *derechos a la intimidad, a la vida privada y a la protección de datos personales.*

En ese orden de ideas, entendemos que a través de los medios masivos se pueden satisfacer los derechos a la **libre expresión de las ideas y a la información**, el primero principalmente por periodistas y comunicadores, mientras que el segundo por las personas que accedemos a sus contenidos para saber lo que pasó, lo que se dijo, lo que se planea, lo que se propone (Ramírez-Tarango, 2019).

Es importante plasmar lo que nos señala la Constitución general en su artículo sexto constitucional, que establece que "la manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en

los términos dispuestos por la ley" (Constitución Política de los Estados Unidos Mexicanos, 2009). El **derecho a la información** será garantizado por el Estado.

Mientras que el artículo séptimo constitucional refiere que:

> Es inviolable la libertad de difundir opiniones, información e ideas, a través de cualquier medio. No se puede restringir este derecho por vías o medios indirectos, tales como el abuso de controles oficiales o particulares, de papel para periódicos, de frecuencias radioeléctricas o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios y tecnologías de la información y comunicación encaminados a impedir la transmisión y circulación de ideas y opiniones. (Constitución Política de los Estados Unidos Mexicanos, 2009)

Continua este mismo artículo señalando que "ninguna ley ni autoridad puede establecer la previa censura, ni coartar la libertad de difusión, que no tiene más límites que los previstos en el primer párrafo del artículo 6.° de esta Constitución. En ningún caso podrán secuestrarse los bienes utilizados para la difusión de información, opiniones e ideas, como instrumento del delito" (Constitución Política de los Estados Unidos Mexicanos, 2009).

El mal entendimiento en la relación de sinergia entre estos derechos puede dar origen a una apreciación equivocada, por quien informa y por quien recibe la información, y genera consecuencias, particularmente por la influencia que los medios de información desempeñan en nuestra sociedad.

El acceso a la información es un **derecho humano** reconocido internacionalmente, cuyo ejercicio efectivo permite a la ciudadanía supervisar la gestión pública, prevenir actos de corrupción y

participar de manera informada en los asuntos de interés colectivo. De igual manera, la protección de datos personales cobra especial relevancia en un contexto global donde la información se ha convertido en un activo estratégico. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) como garante de ambos derechos, se enfrentó a la tarea de equilibrar estas dos dimensiones, asegurando que la transparencia no comprometiera la **privacidad** de los individuos (Rodríguez Castillo, 2025).

Ambos derechos, el de acceso a la información y el de la libertad de expresión, consagrados en la Constitución, son utilizados por los medios de comunicación, principalmente para la publicación de información privilegiada y exclusiva, que en muchas de las ocasiones dan cuenta de la corrupción, delitos y vínculos criminales.

Frente a la corrupción, uno de los antídotos más poderosos es el derecho de acceso a la información pública. Reconocido constitucionalmente como derecho humano, permite conocer cómo se toman decisiones, cómo se ejercen recursos y qué fundamentos respaldan los actos de gobierno. En esencia, el acceso a la información redistribuye poder: debilita la discrecionalidad y fortalece la vigilancia social (Abbud Yepiz, 2025).

Ante las recientes modificaciones a las leyes generales en materia de transparencia y protección de datos personales, se deben crear modelos que otorguen más accesibilidad y buen desempeño, no se deben extinguir las facultades de los órganos autónomos, sino especializar y capacitar a las personas que puedan responder de manera efectiva a las necesidades. Asimismo, es necesario crear mecanismos que faciliten el acceso a la ciudadanía para **garantizar** que estos dos derechos (el de acceso a la información pública y el

de la protección de datos personales) lleguen a toda la población (Domínguez, 2024).

4. Retos para el periodista y la protección de datos personales en los géneros informativos y opinativos

Los periodistas y los medios de comunicación asumen un reto sumamente interesante: de inicio, conocer la legislación vigente en materia de protección de datos personales. Es importante adentrarse a este derecho fundamental, lo cual no debería limitar el trabajo —dada la libertad de expresión—, sino que este ayudará a una profesionalización más exhaustiva para el periodista y su medio de comunicación.

Se debe ser sumamente cuidadoso: cada nota, editorial o artículo deberán ser analizados por los periodistas a la luz del caso concreto. No son fórmulas mágicas que se puedan utilizar de manera genérica. No es una tarea fácil.

Y muy importante, distinguir la información personal que pertenece en sí a los funcionarios y servidores públicos, ya que al estar al **servicio público** (recibir un salario emanado del erario) el escrutinio de la ciudadanía y de los periodistas podrá ser mayor; inclusive la propia Suprema Corte de Justicia de la Nación así lo ha resuelto, y será mayor a la de cualquier otro particular que no sea servidor público.

Como lo citamos al inicio de este texto, la ponderación de la libertad de expresión, el acceso a la información y la protección de los datos personales son un reto para todo profesional de la información. Cada nota periodística narra un acontecimiento distinto, o bien, es la continuidad de otro previamente publicado;

es algo novedoso, por ello, la insistencia de analizar cada una de ellas.

De nueva cuenta, como refiere uno de los maestros del derecho a la información, antes de publicar datos personales en medios masivos de información las personas responsables de la elaboración de esos contenidos deben considerar el derecho a la privacidad, el que tiene todo individuo a separar aspectos de su vida del escrutinio público. Se trata de cuestiones relacionadas con la familia, estado civil, datos financieros y salud, es decir, al mismo cuerpo lo separamos del escrutinio público, una marca, un tatuaje, una enfermedad.

El derecho a la privacidad confiere a las personas control sobre su información personal. Esto implica a la noción de autodeterminación: autonomía o independencia para decidir a quién la entrega; decidir a quién, cómo, cuándo y hasta qué punto utilizará esa información personal. Eso le da poder a los ciudadanos, según Ramírez-Tarango (2019), "porque las personas poseen los primeros y deciden entregarlos, una vez entregados pueden solicitarlos a quien se los entregaron, pueden pedir que se rectifiquen, que se cancelen, oponerse a cómo los están tratando. Esos son los elementos mínimos para entender la protección de los datos personales y los posibles conflictos con el ejercicio de la libertad de expresión a través de los medios masivos" (pp. 15-16). El trabajo colaborativo entre el gremio de periodistas y el Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública, en cuanto a la capacitación, cursos, diplomados y talleres, sembró las bases para una mayor sensibilización, sumado a la profesionalización del gremio, en cuanto al acceso a la información y protección de datos personales se refiere.

Se debe buscar un equilibrio entre el derecho de acceso a la

información y el derecho a la protección de datos personales, es decir, balancear el derecho de las personas a controlar la forma en que se recopilan, almacenan y utilizan sus datos personales, y el derecho que tienen las personas y organizaciones al uso razonable de los datos personales con fines comerciales legítimos y de una manera segura y protegida (Vizcarra, 2017).

Ante las reformas en materia de acceso a la información y protección de datos personales en México y en las entidades federativas, el gremio de periodistas y las dependencias que ahora asuman los trabajos de transparencia deberán seguir con la misma sinergia, sobre todo en cuanto a la protección de datos personales. La capacitación constante brindada por especialistas en la materia, tendrá —además de colaboración— la continuidad del entendimiento de estos derechos fundamentales expuestos a lo largo del presente texto, para el beneficio de quien informa y de quien recibe dicha información.

Son entonces bastantes los retos para los periodistas y los medios de comunicación, quienes a la luz de la libertad de expresión y del acceso a la información pública llevan a la ciudadanía la información que todos los días se genera en cada rincón del país. El reto se centrará en el manejo y en la protección de los datos personales.

Referencias

Abbud Yepiz, J. A. (2025). El derecho a saber como herramienta estructural contra la corrupción. En S. U. García (Coord.), *Reflexiones finales, ¿qué sigue con el acceso a la información pública? La encrucijada del derecho a saber* (pp. 13-22). Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública.

Constitución Política de los Estados Unidos Mexicanos [Const.]. 1 de junio de 2009 (México). https://www.diputados.gob.mx/LeyesBiblio/ref/cpeum.htm

Domínguez, S. P. (2024). Retos que atraviesa el acceso a la información pública y la protección de datos personales ante la reforma constitucional. *Acceso*, 08-09.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. 20 de marzo de 2025. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. 20 de marzo de 2025. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Ramírez-Tarango, R. (2019). Libertad de expresión frente a la protección de datos personales. *Acceso*, 15-16.

Rodríguez Castillo, M. V. (2025). Avances del Sistema Nacional Anticorrupción gracias al derecho de acceso a la información pública y la transparencia en México, y perspectivas a la luz de la nueva Ley General de Transparencia. En S. U. García (Coord.), *Reflexiones finales, ¿qué sigue con el acceso a la información pública? La encrucijada del derecho a saber* (pp. 111-121). Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública.

Véliz, C. (2021). Privacidad es poder. *Datos, vigilancia y libertad en la era digital*. Penguin Random House.

Vizcarra, A. E. (2017). *La privacidad y la protección de datos personales*. Biblioteca Jurídica Virtual del Instituto de Investigaciones Jurídicas de la UNAM. https://archivos.juridicas.unam.mx/www/bjv/libros/12/5718/10.pdf

11. La protección de datos personales en México: oportunidades y desafíos en la era de la identidad digital

Mtro. Juan Carlos Fuentecilla Chávez

Resumen

Actualmente, la protección de datos personales en México atraviesa un proceso de transformación, que surge de la necesidad del Gobierno de modernizar la gestión pública y que derivó en cambios legislativos recientes que modificaron el diseño institucional con el que se contaba y, en gran medida, estaba ya consolidado.

Este texto analiza brevemente el estado actual de la protección de datos personales en México, especialmente en el contexto de la desaparición del anterior órgano garante y la implementación de nuevos mecanismos de identidad digital, como la versión digital avanzada de la Clave Única de Registro de Población (CURP) o CURP biométrica, frente al nuevo marco normativo.

La centralización y fragmentación institucional plantean retos importantes sobre la implementación de los nuevos marcos normativos, la autonomía en la tutela de este derecho y la capacidad para generar lineamientos claros frente a fenómenos emergentes como el uso de datos biométricos, la inteligencia artificial y las redes sociales.

Este panorama sugiere que el Gobierno se encuentra en un momento clave donde puede encaminarse hacia un sistema robusto, que combine innovación tecnológica, con estándares internacionales de protección de datos o, por el contrario, retroceder en la salvaguarda de un derecho considerado esencial en toda democracia contemporánea.

Palabras clave: Protección de datos personales; identidad digital; datos biométricos; reforma; CURP biométrica.

1. Introducción

La protección de datos personales en México atraviesa un momento de transformación significativa que presenta oportunidades y desafíos únicos para fortalecer este derecho fundamental. Con la implementación de nuevos esquemas de identidad digital y la reorganización de los entes públicos garantes de este derecho, el Estado se enfrenta al desafío de poder construir un modelo que permita equilibrar las necesidades de modernización y eficiencia del Gobierno con la protección efectiva de los datos personales.

En este sentido, se pretende realizar una breve descripción de la situación anterior y actual de este derecho, desde una perspectiva crítica y constructiva, reconociendo los avances logrados y, a su vez, identificando áreas de oportunidad que permitan una mejora en la aplicación de este derecho.

Para lograr lo anterior se presentan los antecedentes normativos que han configurado el sistema mexicano de protección de datos, se analizan los cambios recientes y sus principales características y, finalmente, se examina la implementación de la identidad digital y los registros gubernamentales de datos.

2. El surgimiento del derecho a la protección de datos en México

Si bien el derecho a la protección de datos personales en México es de reciente reconocimiento, es importante mencionar que principalmente durante los últimos 23 años se ha establecido una base normativa sólida a su alrededor.

El desarrollo de este derecho está ligado a su vez a la transparencia y al acceso a la información, que surgió de manera formal con la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG), publicada en 2002.

El Grupo Oaxaca —que propició esta ley— fue resultado, de acuerdo con Escobedo (2022):

> de un fenómeno inédito de movilización de opinión pública que tuvo su punto de inflexión con la realización del Seminario Nacional "Derecho a la Información y Reforma Democrática" convocado por la Universidad Iberoamericana, la Fundación Información y Democracia, la Fundación Konrad Adenauer, El Universal, la Asociación de Editores de los Estados, la Asociación Mexicana de Editores y la Fraternidad de Reporteros de México, el 23 y 24 de mayo de 2001 en Oaxaca, Oaxaca. Una vez que el Grupo empezó a incidir en la opinión pública para gestionar el tema del derecho a la información en su vertiente de derecho de acceso a la información pública, surgió el imperativo de las denominaciones. Como respuesta a ello, fue la periodista Ginger Thompson, corresponsal del New York Times, quien por primera vez denominó la movilización emergente como "Grupo Oaxaca" a partir del lugar en que se realizó el encuentro académico. (p. 71)

Este movimiento de la sociedad civil —que a decir de varios especialistas en ningún momento tuvo, ni pública ni privadamente, el propósito de articular una expresión deliberativa tan importante— derivó en varias iniciativas para crear una ley de transparencia, misma que terminó de formalizarse en junio de 2002 a consecuencia de una iniciativa presentada por el presidente de la república en turno, Vicente Fox, la cual fue presentada en noviembre de 2001 y aprobada en abril del siguiente año.

Sin embargo, esta ley solo contempló la protección de datos personales en posesión de sujetos obligados (entes de gobierno), dejando a la deriva la protección de datos personales en posesión de particulares.

Posteriormente, ya en el marco de la propuesta de Agenda Digital Nacional en el año 2009, México tuvo a bien elevar a rango constitucional el derecho a la protección de datos personales mediante la reforma al artículo 16 constitucional, estableciendo que "toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros" (Constitución Política de los Estados Unidos Mexicanos, 2009), constituyéndose así la base del actual sistema con la inclusión de los derechos ARCOP (Acceso, Rectificación, Cancelación, Oposición y Portabilidad), demostrando el compromiso de México con los estándares internacionales más avanzados de la época.

Con la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) en el año 2010, México

se posicionó como pionero en América Latina en la defensa de este derecho. Los ocho principios establecidos en esta ley (licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad) continúan siendo la base del sistema actual y constituyen un activo importante que se debe proteger y robustecer.

La creación del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) como órgano constitucional autónomo en 2014, y la posterior Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) de 2017, completaron un marco normativo fuerte y robusto que ha servido como modelo para otros países de la región.

Sin duda, este desarrollo institucional logró generar capacidades técnicas importantes, formar especialistas calificados y sentar precedentes valiosos que representan un patrimonio de conocimiento del cual el nuevo sistema puede y debe nutrirse. Sin embargo, también se debe reconocer que contar con un marco normativo sólido no garantizó al cien por ciento que este derecho se aplicara correctamente o que se defendiera de manera efectiva. En México, la defensa de este derecho aún no ha recibido la atención y prioridad que merece.

3. El nuevo marco institucional: características y potencialidades

Derivado de la reforma impulsada en 2024 por el Ejecutivo federal, que básicamente planteó la simplificación orgánica de la administración pública federal mediante la extinción de diversos organismos autónomos, entre ellos el INAI, se dio paso a una redistribución de facultades, concentrando funciones regulatorias en el Poder Ejecutivo, lo que llevó a una nueva legislación en

materia de protección de datos personales, la cual fue aprobada el 20 de marzo de 2025.

Esta reforma transformó el diseño institucional en materia de protección de datos personales en México, ya que eliminó los organismos autónomos especializados y a su vez estableció un sistema fragmentado de autoridades responsables de la tutela de este derecho. Previo a la reforma, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales fungía como la autoridad nacional autónoma, acompañado por 32 organismos homólogos en las entidades federativas, todos caracterizados por su autonomía reconocida en la ley.

Como se ha podido advertir por varios especialistas en la materia (Peña Llanes, 2025), la desaparición del órgano garante autónomo genera dudas sobre la capacidad de México de cumplir con mecanismos internacionales de protección de datos personales como el Convenio 108 Plus, el cual exige autoridades independientes y con capacidad técnica para supervisar, sancionar y cooperar internacionalmente.

Actualmente, a nivel federal la Secretaría Anticorrupción y Buen Gobierno es la nueva autoridad encargada de la protección de datos personales tanto para el sector público como para el privado, asumiendo las funciones regulatorias, de supervisión y sanción que anteriormente ejercía el INAI.

En el ámbito local, respecto a los datos personales en posesión de sujetos obligados, las competencias se fragmentan en los órganos encargados de la Contraloría Interna u homólogos de los poderes Ejecutivo, Legislativo y Judicial, así como en los órganos constitucionales autónomos y algunas otras autoridades de las

entidades federativas, eliminando los 32 organismos autónomos estatales garantes de este derecho y generando hoy en día cierta incertidumbre respecto a la reasignación de facultades.
En este sentido, este nuevo modelo plantea retos importantes que requieren de:

1. **Coordinación interinstitucional:** Se requiere establecer mecanismos eficientes de coordinación entre las diferentes autoridades garantes.
2. **Estándares mínimos unificados:** Aunque la aplicación sea sectorial, los principios y estándares mínimos deben ser uniformes. Esto requiere lineamientos generales claros que todas las autoridades deban observar.
3. **Sistema de información integrado:** La implementación de una plataforma tecnológica compartida permite a los ciudadanos conocer qué autoridad es competente para sus solicitudes y dar seguimiento unificado a sus trámites.

4. La CURP biométrica a la par de este nuevo modelo

La reciente implementación de la CURP biométrica en México —aprobada mediante decreto publicado en el Diario Oficial de la Federación el 16 de julio de 2025, en la que se reforma el artículo 91 bis de la Ley General de Población—, que consiste en incorporar datos biométricos (como huellas dactilares, reconocimiento facial o iris) a la CURP, representa un momento clave en la evolución del marco normativo de protección de datos personales, ya que de cara a un momento de incertidumbre frente a las nuevas reformas en materia de protección de datos personales, se plantea este esfuerzo por unificar los registros poblacionales que contienen datos personales sensibles y que a su vez pueden llegar a comprometer permanentemente la privacidad de las personas.

Esta incorporación de datos biométricos plantea riesgos significativos a largo plazo, ya que, a diferencia de la recolección de otros datos personales, los datos biométricos comprometidos no pueden ser reemplazados fácilmente. Es decir, mientras la evolución normativa de este derecho en los últimos años ha tendido a fortalecer la protección de datos personales, reconociendo este derecho fundamental y desarrollando principios puntuales con el fin de limitar y controlar el tratamiento de los datos personales, la propuesta de la CURP biométrica representa un reto importante, ya que en lugar de restringir el uso de la información personal plantea ampliar por parte del Gobierno la recolección de los mismos, pudiendo llegar a generar tensiones con el marco histórico orientado a la garantía y protección de la privacidad de los datos personales.

4.1. La naturaleza especial de los datos biométricos

De acuerdo con el Reglamento General de Protección de Datos de la Unión Europea, los datos biométricos son "datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos" (Reglamento General de Protección de Datos, 2016), y estos a su vez representan una categoría especial de datos personales que requieren protección reforzada, ya que por regla general en la mayoría de las normativas este tipo de datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas.

Instancias como la Agencia Española de Protección de Datos (AEPD, 2023) consideran el tratamiento de datos biométricos, tanto para identificación como para autenticación, como un

tratamiento de alto riesgo que incluye categorías especiales de datos, ya que implican el manejo de información personal sensible que, en caso de verse comprometida, podría provocar daños irreparables a la privacidad y seguridad de las personas.

4.2. Experiencias internacionales

4.2.1. India

Uno de los casos de mayor referencia respecto a la implementación de un sistema biométrico nacional es el de la India, que desde su implementación hasta la fecha cuenta con cerca de 1 043 millones de datos personales y que surgió con la idea de simplificar la vida cotidiana y blindar la entrega de beneficios públicos (Kotnana, 2025).

En 15 años, Aadhaar se consolidó como la mayor infraestructura de identidad biométrica del mundo y pieza clave de la India digital. Este sistema, a decir de algunas fuentes, ha logrado reducir costos y tiempo de verificación en diversos ámbitos. A su vez, ha permitido la depuración masiva de padrones del Gobierno, evitando así duplicidades en la entrega de apoyos y generando mecanismos de entrega más eficientes, lo que ha llevado a generar ahorros importantes.

Por otra parte, este sistema no ha estado exento de problemas: se han señalado riesgos para la privacidad y fallos en la autenticación biométrica que han derivado en la exclusión de grupos vulnerables. Asimismo, ha sido objeto de críticas por el potencial de habilitar vigilancia, exclusión y discriminación cuando no existen salvaguardas robustas, transparencia y evaluaciones independientes.

Este sistema logró sus metas de identificación masiva, eficiencia y ahorro, y es hoy en día un pilar de la India digital, pero su implementación ha producido exclusiones y riesgos de privacidad que aún requieren correcciones, salvaguardas y vías alternativas de identificación.

4.2.2. Estonia

Estonia ofrece un modelo diferente de identidad digital que también gestiona datos biométricos y que ha logrado equilibrar modernización con protección de derechos. Este sistema ha representado ahorros para el Gobierno del equivalente al 2 por ciento del PIB anualmente, y ha permitido que el 99 por ciento de los servicios gubernamentales estén disponibles en línea (El Hakim, 2025). Este sistema surgió con el objetivo de construir una sociedad digital eficiente sin comprometer la privacidad de sus ciudadanos.

El "éxito" del modelo radica en su diseño descentralizado. X-Road, su plataforma de intercambio seguro, interconecta las bases de datos gubernamentales y privadas permitiendo que cada institución mantenga sus propios datos, pero a su vez comparta información de manera segura cuando es necesario, en lugar de crear una base de datos central masiva como en India (e-Estonia, s. f.).

La diferencia fundamental con otros sistemas es que Estonia construyó su sistema de privacidad desde el diseño inicial. Los ciudadanos tienen acceso a conocer sobre quién accede a sus datos personales y cuándo; cada consulta queda registrada y puede ser verificada. Este sistema funciona bajo estrictas medidas de protección de datos, con consentimiento explícito requerido para acceder a información y cumplimiento amplio de

las regulaciones europeas de privacidad —que hasta la fecha son de las más robustas—. Incluso, este sistema cuenta con respaldos de su base de datos fuera del territorio nacional con la finalidad de garantizar continuidad en situaciones de crisis.

5. Oportunidades y desafíos para México

El sistema mexicano plantea una concentración institucional que genera oportunidades para una implementación más coordinada, pero también proyecta interrogantes sobre la autonomía de los controles democráticos.

Como lo documenta Rangel (2025), actualmente con las reformas aprobadas persisten vacíos reglamentarios y se han eliminado referencias clave de salvaguardas. Sin atender estos pendientes, el país corre el riesgo de profundizar la asimetría entre expansión de capacidades de allegarse datos personales y controles efectivos de los mismos.

En la actualidad México procesa anualmente millones de trámites que se beneficiarían de la automatización biométrica, por ejemplo la renovación de documentos oficiales, servicios de salud, programas educativos, programas de apoyo social y verificaciones bancarias.

La eliminación de duplicidades en bases de datos gubernamentales, como se ha visto en países como India —donde la autentificación biométrica se ha usado, entre otras cosas, para proteger los subsidios gubernamentales reduciendo el fraude—, podría generar ahorros operativos significativos que si se aplican de manera correcta pueden llegar a mejorar la calidad de los servicios públicos, generando mayor eficiencia y eficacia gubernamental, pero con un alto costo en perjuicio de la privacidad de las personas.

En otras palabras, esta integración pretende generar eficiencia administrativa reduciendo trámites burocráticos, eliminando documentación múltiple y facilitando el acceso a servicios públicos, a la vez que intenta transformar las capacidades de investigación y procuración de justicia en materia de desaparición y búsqueda de personas mediante la integración de datos forenses y registros civiles, ya que se desea vincular con el Sistema Nacional de Personas Desaparecidas, lo cual puede llegar a acelerar las investigaciones y mejorar las tasas de identificación de víctimas. Sin embargo, estos beneficios podrían representar un alto costo si no se garantizan medidas de protección de datos personales con controles estrictos, transparencia y supervisión independiente, donde el riesgo de uso indebido de los mismos y las posibles filtraciones anularían por completo los potenciales avances.

A la par de esta situación, es importante que México mantenga y fortalezca su participación en el ecosistema internacional de protección de datos, sobre todo en el contexto actual donde el país ratificó el Convenio 108[1] del Consejo de Europa, comprometiéndose a estándares internacionales de protección de datos personales, pero sin haber suscrito la versión moderna de este, mejor conocido como Convenio 108 Plus (CETS n.º 223).

La desaparición del INAI y la concentración de funciones en la Secretaría Anticorrupción y Buen Gobierno plantean interrogantes sobre la capacidad real de México para cumplir con los requisitos del Convenio 108 Plus, que exige autoridades independientes con capacidad técnica para supervisar, sancionar y cooperar

[1] El Convenio 108 es el primer tratado internacional jurídicamente vinculante en materia de protección de datos personales, aplicable a todo el procesamiento de datos realizado por los sectores público y privado, incluyendo autoridades judiciales y de seguridad nacional, y promueve flujos transfronterizos de datos con garantías adecuadas.

internacionalmente. La ausencia de disposiciones obligatorias sobre notificación de incidentes de seguridad y evaluaciones de impacto refleja lagunas normativas relevantes frente a estándares internacionales avanzados, aumentando la vulnerabilidad del sistema ante posibles brechas de seguridad (Peña Llanes, 2025).

Para que la CURP biométrica constituya un avance real en la modernización del Estado mexicano sin sacrificar derechos fundamentales, el Gobierno debe procurar:

- **Limitación estricta de la recolección y uso de datos biométricos** a lo estrictamente necesario, estableciendo fines específicos y legítimos.
- **Evaluaciones de impacto** en la protección de datos para identificar y mitigar riesgos potenciales, siguiendo los estándares internacionales.
- **Protección de datos desde el diseño** (Privacy by Design), con mecanismos de supervisión desde el diseño de los sistemas.
- **Transparencia** que establezca el consentimiento informado y explícito, así como avisos claros sobre la recolección y uso de los datos por parte de las instituciones.
- **Mecanismos efectivos, sencillos y accesibles** para que cualquier persona pueda ejercer de manera correcta sus derechos ARCOP.
- **Mecanismos de seguridad** de datos biométricos, incluyendo cifrado de extremo a extremo, almacenamiento seguro y auditorías regulares.
- **Adecuación con estándares internacionales** como el Convenio 108 Plus y el Reglamento General de Protección de Datos de la Unión Europea.

6. Conclusiones

México atraviesa un momento decisivo donde debe demostrar que es posible modernizar el Estado mediante tecnologías avanzadas sin sacrificar los principios democráticos y constitucionales que costó décadas construir.

La protección de datos personales en México se encuentra en un momento de transformación que, adecuadamente gestionado, puede resultar en un sistema más fuerte y eficiente. El nuevo marco institucional, aunque diferente al modelo tradicional, presenta retos que si no se atienden pueden significar un retroceso frente a la protección de este derecho fundamental, pero a su vez plantea oportunidades para la innovación y la mejora continua, que bien aprovechadas traerían grandes beneficios.

La implementación de la CURP biométrica puede convertirse en un catalizador para establecer mejores prácticas de protección de datos, siempre y cuando se implementen las medidas pertinentes y suficientes para mantener el equilibrio entre eficiencia gubernamental y privacidad ciudadana.

Así pues, resulta indispensable que el Gobierno pueda contar con recursos tecnológicos que logren hacer más eficiente la administración pública, siempre y cuando a la par se construya un sistema suficientemente fuerte de protección de datos. Sin embargo, el éxito no depende únicamente de la tecnología o el marco normativo. Se requiere un compromiso verdadero de todos los actores involucrados: Gobierno, sector privado, academia y sociedad civil.

El futuro de la protección de datos personales no está predeterminado, sino en constante construcción, y todos los

sectores de la sociedad tienen un papel que desempeñar en darle una adecuada forma. México requiere lograr una protección efectiva de este derecho fundamental cuidando los datos personales de la ciudadanía mientras aprovecha las oportunidades de la era digital.

En este sentido, el país tiene la oportunidad de demostrar que es posible modernizar el Estado y aprovechar las ventajas de la transformación digital sin sacrificar la privacidad y los derechos fundamentales de los ciudadanos. El camino no está exento de desafíos ni de errores, pero con voluntad política, cooperación entre sectores y aprovechamiento inteligente de la tecnología, es posible construir un sistema de protección de datos que combine eficiencia, transparencia y respeto por los derechos fundamentales y que, a su vez, sea ejemplo para la región y el mundo.

Referencias

Agencia Española de Protección de Datos. (2023). *Guía sobre tratamientos de control de presencia mediante sistemas biométricos*. https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf

Consejo de Europa. (s. f.). *Lista completa: Firmas por tratado (CETS n.º 223)*. Oficina de Tratados. Recuperado el 16 de octubre de 2025 de https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=223

Constitución Política de los Estados Unidos Mexicanos [Const.]. Artículo 16, párrafo 2. 1 de junio de 2009 (México). https://www.diputados.gob.mx/LeyesBiblio/ref/cpeum.htm

e-Estonia. (s. f.). *X-Road: Interoperability services*. Recuperado el 16 de octubre de 2025 de https://e-estonia.com/solutions/interoperability-services/x-road/

El Hakim, Y. (2025, 14 de enero). *What are Estonia's verifiable credentials? A 2025*

expert guide. VerifyEd. https://www.verifyed.io/blog/estonia-verifiable-credentials

Escobedo, J. (2002, julio). *Movilización de opinión pública en México: el caso del Grupo Oaxaca y de la Ley Federal de Acceso a la Información Pública* [Ponencia]. I Congreso Latinoamericano de Ciencia Política, Salamanca, España.

GBG. (2021). *Digital identity in practice - Estonia and the e-state*. https://www.gbg.com/en/blog/digital-identity-in-practice-estonia/

GDPR Advisor. (2023, 25 de junio). *GDPR and biometric data: Privacy implications and regulatory compliance*. https://www.gdpr-advisor.com/gdpr-and-biometric-data-privacy-implications-and-regulatory-compliance/

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (s. f.). *El Convenio 108 y el Comité Consultivo*. https://inicio.inai.org.mx/nuevo/convenio108.pdf

Jyothish, R. (2018, 22 de enero). *Sistema de identificación biométrica de India está filtrando información personal — y las agencias estatales no lo solucionan*. Global Voices. https://es.globalvoices.org/2018/01/22/sistema-de-identificacion-biometrica-de-india-esta-filtrando-informacion-personal-y-las-agencias-estatales-no-lo-solucionan/

Kotnana, N. (2025, 28 de septiembre). *15 years of Aadhaar: Achievements and challenges for the world's largest biometric ID system*. ETV Bharat. https://www.etvbharat.com/en/!opinion/15-years-of-aadhaar-achievements-and-challenges-for-the-world-largest-biometric-id-system-enn25092701704

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. 20 de marzo de 2025. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf

Peña Llanes, J. J. (2025, 20 de marzo). *Datos personales en evolución: implicaciones internacionales de los cambios legislativos de México*. PDP Talks Webinar.

Rangel, L. (2025, 9 de julio). *Protección de datos personales: ¿a qué institución le corresponde tras la desaparición del INAI?* Animal Político. https://animalpolitico.com/verificacion-de-hechos/te-explico/proteccion-datos-personales-inai

12. Cultura y conciencia ciudadana sobre la protección de datos personales en Chihuahua

Mtra. Lucía Patricia Jiménez Carrillo
Lic. Ricardo Espinoza Rodríguez

1. Introducción

En la era digital, la información personal se ha convertido en un recurso estratégico de alto valor, cuyo manejo responsable representa un desafío prioritario para las instituciones públicas y privadas. La protección de los datos personales es hoy un derecho humano fundamental, consagrado en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (2017), que garantiza la privacidad, la autodeterminación informativa y el control sobre los datos de cada individuo.

México ha desarrollado un sólido marco normativo en torno a este derecho, encabezado por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO, 2017) y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP, 2010). A nivel estatal, el Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública (Ichitaip) funge como autoridad garante, encargada de promover, vigilar y garantizar el cumplimiento del derecho a la protección de datos personales.

Sin embargo, más allá del marco legal, la consolidación de una cultura ciudadana de la privacidad depende de la conciencia social y del conocimiento que la población tenga sobre el tema. En este

contexto, la Encuesta sobre Protección de Datos Personales en el Estado de Chihuahua 2025 (Ichitaip, 2025) permite analizar el nivel de sensibilización, ejercicio de derechos y conocimiento institucional entre los habitantes de distintas regiones.

2. Metodología del estudio

La Encuesta sobre Protección de Datos Personales en el Estado de Chihuahua 2025 fue realizada entre el 1 de octubre y el 1 de noviembre de 2025, con el propósito de medir el grado de conocimiento, percepción y ejercicio de los llamados derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

El diseño estadístico consideró un nivel de confianza del 95 por ciento y un error muestral del 5 por ciento, con una muestra total de 1 650 entrevistas aplicadas a personas mayores de edad distribuidas en ocho municipios del estado.

Tabla 1. Distribución de la muestra por localidad
La muestra fue equitativa en cuanto a género (50 % mujeres y

Localidad	Población (Inegi, 2020)	Tamaño de muestra
Chihuahua	937 674 habitantes	380 encuestas
Ciudad Juárez	1 512 450 habitantes	380 encuestas
Parral	116 662 habitantes	200 encuestas
Ojinaga	24 534 habitantes	120 encuestas
Nuevo Casas Grandes	65 753 habitantes	150 encuestas
Bocoyna	23 351 habitantes	120 encuestas
Camargo	49 499 habitantes	150 encuestas
Guachochi	50 180 habitantes	150 encuestas

Fuente: Ichitaip, 2025.

50 % hombres) y representativa en términos socioeconómicos: 55 por ciento medio y medio-bajo, 9 por ciento alto y medio-alto, y 37 por ciento medio. Esta distribución permite observar el fenómeno con amplitud territorial y social.

3. Resultados principales

3.1. Nivel de conocimiento general

El 83 por ciento de los encuestados manifestó haber escuchado hablar sobre la protección de datos personales. Municipios como Ojinaga (90 %), Nuevo Casas Grandes (88 %) y Juárez (86 %) muestran los niveles más altos de conocimiento, mientras que Bocoyna (75 %) y Guachochi (70 %) reportan los más bajos.

Estas diferencias reflejan que el acceso a la información y las condiciones tecnológicas influyen directamente en la comprensión de los derechos digitales, lo que plantea el desafío de fortalecer las estrategias de comunicación en comunidades rurales e indígenas.

3.2. Factores sociodemográficos

El conocimiento varía según el nivel socioeconómico y la edad. En los estratos AB/C+, el 96 por ciento conoce el tema, frente al 68 por ciento del grupo D/C-. Por grupos de edad, el mayor conocimiento se observa entre los 26 y 40 años (99 %), seguido por las personas de 41 a 55 años (96 %), mientras que entre los mayores de 56 años el porcentaje desciende a 62 por ciento.

Estos resultados evidencian que la alfabetización digital y el acceso educativo son factores determinantes en la comprensión de los derechos de privacidad.

3.3. Ejercicio de los derechos ARCO

A pesar del alto nivel de conocimiento, solo el 5 por ciento de las personas encuestadas ha realizado alguna solicitud relacionada con la protección de sus datos personales. Las instituciones más señaladas son las compañías telefónicas, los bancos y la Fiscalía del Estado. Los municipios con mayor nivel de ejercicio son Chihuahua y Nuevo Casas Grandes, ambos con 12 por ciento.

Esto demuestra una brecha entre el conocimiento y la acción: la población sabe que posee derechos, pero no siempre conoce cómo ejercerlos o confía en la efectividad de los mecanismos.

3.4. Reconocimiento institucional

El 73 por ciento de los encuestados reconoce que es propietario de sus datos personales y que las instituciones deben proporcionarles la información que soliciten; sin embargo, solo 18 por ciento identificó correctamente al Ichitaip como la autoridad estatal encargada de garantizar este derecho. El mayor reconocimiento se da en Nuevo Casas Grandes (41 %) y Chihuahua capital (30 %), y el más bajo en Ojinaga (8 %) y Guachochi (10 %).

4. Casos prácticos y criterios relevantes del Ichitaip

El papel del Ichitaip no se limita a la promoción del derecho a la privacidad, sino que también emite criterios interpretativos que orientan a los sujetos obligados sobre la correcta aplicación de la ley. Entre los más significativos se encuentran los siguientes:

4.1. Criterio Relevante 005/2023. Expediente clínico de persona fallecida

El Instituto resolvió que el cónyuge supérstite tiene derecho de acceso a los expedientes médicos y administrativos del fallecido *(de cujus)*, al considerar que este derecho se relaciona con el acceso a la verdad y con las garantías familiares reconocidas en la Constitución y en la Convención Americana sobre Derechos Humanos.

El organismo precisó que negar dicha información constituye un obstáculo arbitrario al conocimiento de la verdad y un entorpecimiento a las garantías jurídicas del cónyuge sobreviviente, quien puede requerir información para proteger los intereses de su familia (Ichitaip, 2023a).

4.2. Criterio Relevante 010/2023: Causa de muerte y derechos ARCO

En otro caso, el Instituto determinó que la modificación de la causa de muerte en un certificado de defunción no corresponde al ejercicio del derecho de rectificación previsto en el artículo 34 de la Ley de Protección de Datos Personales del Estado de Chihuahua.

El documento aclaró que este tipo de información constituye un diagnóstico médico, cuya revisión o modificación corresponde exclusivamente a autoridades o personal de salud competente. El organismo garante solo puede garantizar el ejercicio de los derechos ARCO, pero no sustituir la función técnica o médica de certificar causas de defunción (Ichitaip, 2023b).

Estos criterios demuestran la complejidad y madurez institucional con la que el Ichitaip interpreta la legislación vigente, delimitando con precisión los alcances del derecho a la protección de datos personales frente a otros ámbitos jurídicos, como la salud o la procuración de justicia.

5. Conclusiones

El fortalecimiento de una cultura de protección de datos personales en Chihuahua no depende únicamente de la existencia de leyes o instituciones garantes, sino de la participación activa y consciente de las personas en la defensa de su derecho a controlar su información personal. En un entorno cada vez más digitalizado, donde la circulación de datos es constante, la corresponsabilidad entre ciudadanía, gobierno y sector privado se convierte en un elemento esencial para preservar la confianza social y el respeto a los derechos humanos.

Los resultados de la Encuesta sobre Protección de Datos Personales en el Estado de Chihuahua 2025 muestran que las empresas privadas, especialmente las compañías telefónicas y los bancos, son las más señaladas por la ciudadanía en materia de vulneraciones o mal manejo de información. Este hallazgo coincide con los datos nacionales reportados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI, 2023), que durante 2023 impuso multas por un total de 46 849 777 pesos a personas físicas y morales que infringieron la Ley Federal de Protección de Datos Personales en Posesión de los Particulares.

De acuerdo con el INAI, los sectores más sancionados fueron los servicios financieros y de seguros (21.4 millones de pesos),

información en medios masivos (6.7 millones de pesos) y comercio al por menor (5.4 millones de pesos). Las infracciones más frecuentes incluyeron el tratamiento indebido de datos personales, el incumplimiento del deber de confidencialidad y la omisión de elementos obligatorios en el aviso de privacidad. En el mismo periodo, se iniciaron 293 procedimientos de protección de derechos ARCO, la mayoría vinculados con el derecho de acceso (155 casos), cancelación (122) y oposición (79), destacando que los sectores con mayores inconformidades fueron medios masivos (25.8 %), servicios financieros (20.6 %) y salud y asistencia social (16.5 %).

Estos datos evidencian la necesidad de reforzar la responsabilidad corporativa y la ética empresarial en el tratamiento de datos personales. Las empresas deben incorporar políticas claras de privacidad, capacitar a su personal y garantizar que sus sistemas de seguridad cumplan con los principios de licitud, consentimiento, finalidad, proporcionalidad y responsabilidad establecidos en la ley.

Exigir que las instituciones públicas y privadas traten los datos conforme a estos principios no es solo una obligación legal, sino una práctica ciudadana que fortalece el tejido democrático. El ejercicio de los derechos ARCO representa la herramienta más efectiva para que las personas ejerzan control sobre su información, corrigiendo desequilibrios entre quienes la gestionan y quienes son titulares de ella.

La consolidación de una sociedad digital justa y segura requiere de instituciones fuertes, ciudadanos informados y una cultura de corresponsabilidad. Solo a través de la participación activa y la educación en derechos digitales será posible mantener el

equilibrio entre la innovación tecnológica y la protección efectiva de la privacidad, asegurando que el progreso esté siempre al servicio de las personas y no a costa de su libertad o integridad.

Referencias normativas y bibliográficas

Constitución Política de los Estados Unidos Mexicanos [Const.]. Artículo 16. 15 de septiembre de 2017 (México). https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf

Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública. (2023a). *Criterio Relevante 005/2023. Expediente clínico de persona fallecida.* https://www.ichitaip.org/2023/06/20/criterio-relevante-05-2023-expediente-clinico-de-persona-fallecida/

Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública. (2023b). *Criterio Relevante 010/2023*. Causa de muerte determinada en el certificado de defunción no corresponde al ejercicio de los derechos ARCO. https://www.ichitaip.org/2023/12/08/criterio-relevante-10-2023-causa-de-muerte-determinada-en-el-certificado-de-defuncion-no-corresponde-al-ejercicio-de-los-derechos-arco/

Instituto Chihuahuense para la Transparencia y Acceso a la Información Pública. (2025). *Encuesta sobre Protección de Datos Personales en el Estado de Chihuahua 2025*.

Instituto Nacional de Estadística y Geografía. (2020). *Censo de Población y Vivienda 2020*. https://www.inegi.org.mx/programas/ccpv/2020/

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (2023, 7 de enero). *Multas impuestas en 2023 por infringir Ley Federal de Protección de Datos Personales suman más de 46 mdp: INAI* [Comunicado de prensa]. https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-007-24.pdf

Ley de Protección de Datos Personales del Estado de Chihuahua. 6 de septiembre de 2017. Periódico Oficial del Estado. https://www.congresochihuahua2.gob.mx/biblioteca/leyes/archivosLeyes/1342.pdf

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. 5 de julio de 2010. Diario Oficial de la Federación. https://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010#gsc.tab=0

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. 26 de enero de 2017. Diario Oficial de la Federación. https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017#gsc.tab=0

13. La delgada línea entre el derecho a la información y la autodeterminación informativa

Mtro. Nicolás Juárez Caraveo

El ejercicio de la protección de datos personales, la digitalización y el flujo masivo de datos han elevado dos derechos fundamentales al debate: el derecho a la autodeterminación informativa y el derecho a la información pública.

La tensión entre el periodismo y la protección de datos personales prevalece entre la dificultad de equilibrar el derecho a la privacidad con la libertad de expresión e información pública.

Si bien pudieran considerarse dos derechos contrapuestos, en el ejercicio de los mismos se ha demostrado que pueden convivir, y mejor aún, unirse en el objetivo de proteger al individuo en su potestad de decidir sobre el uso de su información, y el principio de control social donde el ciudadano tiene la facultad de fiscalizar al poder público.

La autodeterminación informativa y el derecho a la información son derechos fundamentales que coexisten en un Estado de derecho. Su relación es en gran medida de complementariedad, ya que el acceso a la información pública es un medio indispensable para que el individuo ejerza control sobre sus datos personales.

Con esta idea, la autodeterminación informativa empodera al individuo para controlar su información personal, mientras que

el derecho a la información promueve la transparencia y la libre circulación de datos de interés público, un insumo fundamental para el desarrollo de un periodismo libre e informado.

En este entorno, se manifiestan como derechos fundamentales de innegable relevancia. Mientras que el derecho a la información busca democratizar el acceso al conocimiento y fortalecer la transparencia gubernamental, la autodeterminación informativa defiende la esfera de control individual, por lo que estos dos derechos se enfrentan en una dialéctica en constante evolución, y en muchas ocasiones enfrentados.

Un derecho irrenunciable: la autodeterminación informativa

De acuerdo con Guilio Adinolfi (2007), el derecho a la autodeterminación informativa:

> es un típico corolario de la sociedad moderna, en la cual las informaciones pueden dañar de la misma manera que la violencia física; sin embargo, el elemento caracterizador de este derecho es la autonomía del consentimiento, la posibilidad de autorizar, bloquear, oponerse, ratificar, de quedarse indiferente respecto a las circulaciones de voces, rectius informaciones, acerca de la persona misma. (p. 7)

El derecho a la autodeterminación informativa, también conocido como derecho a la protección de datos personales, es personalísimo e inherente al individuo. Según Murillo de la Cueva y Piñar Mañas (2009):

> deriva de la dignidad y la libertad, entendida como la facultad de la persona de decidir cuándo y en qué medida se revela información sobre su propia vida. La jurisprudencia y la

> doctrina lo definen como el derecho a controlar la información que terceros tienen sobre uno mismo, así como la capacidad de conocer, acceder, rectificar y cancelar los datos personales. (p. 89)

La efectividad de la autodeterminación informativa se asienta sobre los principios fundamentales del consentimiento informado, donde el tratamiento de los datos personales es legítimo solo si el titular ha prestado su consentimiento de manera libre, expresa e inequívoca, conociendo de antemano la existencia de la base de datos, su propósito y el uso que se le dará a la información.

Además, debe fijarse una finalidad limitada, donde los datos deben ser recogidos para un propósito específico y no pueden ser utilizados para fines distintos sin una nueva autorización del titular. Por último, es importante contemplar la calidad de los mismos datos, que deben ser veraces, actuales, exactos y pertinentes para el fin con el que fueron recolectados.

En relación con el periodismo, se vulneran los datos personales al momento de revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales; afiliación sindical, opiniones políticas o preferencia sexual.

Para Bonilla Gutiérrez (2024), "la erosión de la autodeterminación informativa se manifiesta también en el hecho de que las personas, en la mayoría de los casos, desconocemos por completo qué datos se recopilan, con qué propósito y cómo se utilizarán" (p. 125).

Su esencia: democratizar el conocimiento

El derecho a la información es un derecho fundamental reconocido

a nivel internacional y consagrado en diversas constituciones y ordenamientos jurídicos. Se define como una facultad que abarca la prerrogativa de toda persona para buscar, investigar, recibir y difundir informaciones de toda índole.

De acuerdo con López-Ayllón (2000), "el derecho a la información (o la libertad de expresión o la libertad de información) comprende así tres facultades interrelacionadas: las de buscar, recibir o difundir informaciones, opiniones o ideas, de manera oral o escrita, en forma impresa, artística o por cualquier otro procedimiento" (p. 163).

Este derecho no solo se ejerce en relación con la información que emana del Estado, sino también con aquella que es de relevancia pública, independientemente de la fuente.

En este sentido, se considera tanto un derecho autónomo como un instrumento esencial para el ejercicio de otros derechos, especialmente los de participación política y de control de los asuntos públicos.

La finalidad principal del derecho a la información es fortalecer el sistema democrático, ya que una ciudadanía informada es una condición necesaria para la participación activa, la transparencia en las actuaciones estatales y la rendición de cuentas por parte de los poderes públicos.

Por ello, se ha conceptualizado como un "derecho-deber" que sostiene las demás garantías constitucionales y se considera un patrimonio colectivo, bajo los principios de veracidad y máxima publicidad.

El principio de veracidad permite la protección constitucional

únicamente a la información veraz, responsable y ecuánime, ya que la información que es falsa o injuriosa no goza de amparo, y su corrección o supresión no se considera una limitación al derecho a la información, sino una garantía del respeto a los derechos de terceros.

Por otra parte, el principio de máxima publicidad se aplica a la información que se encuentra en posesión del Estado o de cualquier entidad pública que es, por regla general, de acceso público. Las excepciones a este principio deben ser claras, estrictamente necesarias en una sociedad democrática y estar definidas por ley, como es el caso de la información reservada por razones de interés público o seguridad nacional.

La coexistencia armónica

La relación entre la autodeterminación informativa y el derecho a la información no es inherentemente conflictiva, sino que en muchos casos se refuerzan mutuamente: el derecho a la información se convierte en un medio para que el individuo ejerza su autodeterminación informativa.

Al permitir el acceso a archivos y documentos en poder de entidades públicas, el derecho a la información faculta a los ciudadanos para conocer qué datos personales se han recopilado sobre ellos, y sin duda este es uno de los aportes más relevantes. Este conocimiento es un prerrequisito indispensable para poder solicitar la rectificación, actualización o supresión de dichos datos. Para los individuos, el acceso a la información pública no es un fin en sí mismo, sino un medio instrumental para la protección de la privacidad.

Por otra parte, la transparencia en la gestión pública de datos

fortalece la autodeterminación, ya que una ciudadanía informada puede supervisar y controlar la actuación de las autoridades. El correcto ejercicio de la autodeterminación es una condición elemental para el funcionamiento de una comunidad democrática, ya que un individuo que no puede controlar la información sobre sí mismo pierde su capacidad de libre autodeterminación y de participación efectiva en la vida pública.

La coexistencia de estos dos derechos fundamentales crea un sistema de pesos y contrapesos esencial para una sociedad libre. El derecho público a la información faculta a los ciudadanos para vigilar y fiscalizar el poder del Estado, previniendo abusos y la opacidad.

Por lo tanto, el derecho a la información contrarresta el poder del Estado sobre la sociedad, mientras que la autodeterminación informativa contrarresta el poder de las corporaciones y los sistemas centralizados sobre el individuo. Esta estructura legal evita que la información, como patrimonio colectivo, se convierta en una herramienta de dominación.

Puntos de conflicto

A pesar de su complementariedad, el enfrentamiento entre el interés público en la información y la protección de los datos personales es un desafío recurrente.

Esto surge cuando la información que es de interés público o se encuentra en registros públicos contiene datos personales del titular. La tensión se genera entre el interés de la sociedad en acceder a datos veraces y la facultad de un individuo para controlar la difusión de su propia información.

Es importante ponderar caso por caso para determinar qué información puede divulgarse, considerando que no toda información de interés público debe ser necesariamente publicada si vulnera derechos de terceros.

Será entonces de suma importancia la autorregulación periodística para evitar la intervención judicial frente a posibles daños, promoviendo que las decisiones sobre el interés público prevalezcan sobre el interés particular en ciertos aspectos.

La proliferación digital y las nuevas tecnologías transforman las dinámicas sociales y afectan los derechos humanos, incluyendo la privacidad y el honor.

La tendencia legislativa en países como Argentina, Brasil, Colombia y México incorpora el "derecho al olvido" ligado al honor, aunque existen debates respecto a su compatibilidad con los sistemas de derechos humanos interamericanos que protegen la libertad de expresión.

Por otra parte, con los avances tecnológicos y la digitalización de la información nos enfrentamos al paradigma de esta contraposición de derechos, donde el derecho al olvido no busca eliminar la información de Internet, sino impedir su "difusión universal e indiscriminada" a través de los buscadores cuando dicha información ha perdido su relevancia o es obsoleta.

Un caso relevante que ha definido este derecho a nivel global es el de Google Spain S. L. v. Agencia Española de Protección de Datos. Los hechos se basan en la queja de Mario Costeja González, quien solicitó la eliminación de los enlaces de Google que dirigían a una noticia sobre una subasta de inmuebles relacionada con un

embargo de 1998, ya resuelto. La Agencia Española de Protección de Datos desestimó la queja contra el periódico *La Vanguardia*, ya que la publicación original era legal, pero la aceptó contra Google, ordenándole que retirara los enlaces.

Otro caso sucedió en Perú, donde un expresidente del Poder Judicial solicitó que se borraran en Internet noticias relacionadas con su patrimonio personal, argumentando protección de datos personales. La autoridad sancionó a la plataforma de búsqueda Google Perú por no poder eliminar esas noticias. Este caso evidencia cómo la Ley de Protección de Datos puede ser utilizada para limitar la difusión de información periodística de interés público, generando una tensión que requiere ponderación.

En Chihuahua de la misma manera existen procedimientos en contra de medios de comunicación, solo que por su naturaleza permanecen reservados.

Otros escenarios de conflicto incluyen el uso de datos personales en el periodismo y el acceso a registros públicos frente al derecho a la reinserción social de un individuo con un pasado judicial o penal. La jurisprudencia ha sostenido que el derecho a la información debe detenerse ante los derechos fundamentales al honor, la intimidad y la propia imagen.

Según Ramírez (2020), "el periodismo es un bien público. La tentación del poder siempre será limitar aquella prensa que sea incómoda —y toda prensa real lo es— a través de marcos normativos que hagan el trabajo periodístico más difícil o bien mediante una presión política y económica en contra de las casas editoriales que termina siendo censura previa o censura" (p. 45).

¿Cómo conciliar ambos derechos?

La naturaleza relativa de los derechos fundamentales es el punto de partida para su armonización, ya que ningún derecho humano es absoluto en su contenido, y su ejercicio encuentra un límite en los derechos de los demás.

Para resolver estos conflictos es necesario identificar los principios de idoneidad, necesidad y proporcionalidad en sentido estricto, donde el beneficio de la medida debe ser mayor que el sacrificio o el costo que impone al derecho afectado.

Por otra parte, la masificación de la información a través de *big data* y el desarrollo de la inteligencia artificial están reconfigurando fundamentalmente el panorama de la protección de los datos personales y la dinámica de poder en el entorno digital.

Los medios de comunicación deben cambiar la forma en la que recaban los datos personales de los involucrados en sus publicaciones, y sobre todo cuidar el tratamiento de dicha información, a fin de garantizar el correcto uso de la información recopilada y de sus datos sensibles.

Sin duda, lo mejor para evitar un enfrentamiento etimológico y legal en ambos derechos es reconocer la naturaleza y límites de cada uno.

Como ya se dijo, los principios de la autodeterminación informativa se basan en que el individuo tiene la potestad de decidir sobre el uso de su información. Los datos se recogen para un propósito específico y no pueden ser desviados; el tratamiento de datos requiere el consentimiento libre e informado del titular, y se debe proteger la autonomía individual y la privacidad.

Mientras, los principios del derecho a la información pública parten de que el ciudadano tiene la facultad de fiscalizar el poder público. La información es, por regla general, pública con excepciones limitadas; el acceso a la información no requiere justificación o motivación, y este derecho garantiza la transparencia y la participación ciudadana.

Referencias

Adinolfi, G. (2007). Autodeterminación informativa, consideraciones acerca de un principio general y un derecho fundamental. *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*, *1*(17), 3-29. https://doi.org/10.22201/iij.24484881e.2007.17.5807

Bonilla Gutiérrez, J. C. (2024). IA y privacidad: Protegiendo la autodeterminación informativa en la era digital. *Revista de la Facultad de Derecho de México*, *74*(290), 125-148. https://doi.org/10.22201/fder.24488933e.2024.290.89719

López-Ayllón, S. (2000). El derecho a la información como derecho fundamental. En J. Carpizo, & M. Carbonell, *Derecho a la información y derechos humanos* (pp. 157-181). Instituto de Investigaciones Jurídicas, UNAM. https://infocdmx.org.mx/pdfs/literatura/Derecho%20a%20la%20informaci%C3%B3n%20como%20derecho%20fundamental.pdf

Murillo de la Cueva, P. L., & Piñar Mañas, J. L. (2009). *El derecho a la autodeterminación informativa.* Fundación Coloquio Jurídico Europeo.

Ramírez, D. (2020). La inherente tensión entre los datos personales y el periodismo. En R. Bucio, L. Curzio, A. Morgan, D. Ramírez, J. Soto, G. Torres, & J. Torres, *Periodismo y la protección de datos personales* (pp. 43-62). Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

“Privacidad en la era digital. Desafíos jurídicos y éticos de la protección de datos personales” es una obra que reúne voces de especialistas de la materia, juristas, académicos y comunicadores que analizan el derecho a la protección de datos personales a la luz de la legislación nacional e internacional, casos prácticos, fundamentos y retos en la era digital. El presente texto se convertirá en una obra de consulta, mismo que se suma a la divulgación del derecho de la protección de datos personales, bajo la tutela del órgano garante constitucional.

Sergio Rafael Facio Guzmán
María Selene Prieto Domínguez
Karla Gabriela Fuentes Moreno
Ernesto Alejandro de la Rocha Montiel
Jesús Manuel Guerrero Rodríguez
David Reynaldo Díaz Rascón
Rodrigo Ramírez Tarango
Alejandro Carrasco Talavera
Socorro Márquez Regalado
Diego U. Sandoval Aguirre
Guillermo Ávila Olivas
Mario Alberto Valdez Borunda
Saúl Ulises García Meza
Juan Carlos Fuentecillas Chávez
Lucía Patricia Jiménez Carrillo
Ricardo Espinoza Rodríguez
Nicolás Juárez Caraveo